TOWARDS A TRANSDISCIPLINARY CYBER FORENSICS GEO-CONTEXTUALIZATION FRAMEWORK

by

Mohammad Meraj Mirza

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Polytechnic Institute

West Lafayette, Indiana

August 2023

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Umit Karabiyik, Chair

Department of Computer and Information Technology

Dr. Marcus K. Rogers

Department of Computer and Information Technology

Dr. Baijian Yang

Department of Computer and Information Technology

Dr. Tathagata Mukherjee

Department of Computer Science, University of Alabama, USA

Approved by:

Dr. Kathryne A. Newton

I dedicate my work to my parents, my wife, my sisters, my family, my loved ones, my educators & mentors, myself, and all who believe in me...

ACKNOWLEDGMENTS

I want to begin by expressing my sincere gratitude and appreciation to Allah, the Almighty, for granting me the strength, wisdom, and perseverance to complete this dissertation and navigate life. All praise is for Allah, the Lord of all worlds...

I owe an outstanding debt of gratitude to my family, especially my Parents, who have always been my pillars of support and inspiration throughout my life and academic journey. Your unwavering *love* and encouragement have helped me overcome the challenges and obstacles that I encountered along the way. In addition, my Wife, whose unwavering *love*, patience, companionship, and understanding have been my constant sources of motivation, encouragement, and support throughout this journey and, In Shaa Allah, the life journey to come. Alhamdulillah, I am forever grateful for your presence in my life, without which I could not have completed this dissertation. Your warmth has kept me going...

To my educators and mentors, thank you for believing in me when I doubted myself, seeing the potential I could not see in myself, and pushing me beyond my limits. You have generously shared your knowledge and experience, imparting valuable life lessons that cannot be found in any textbook. In the continuation of my "Life Walks," I will carry with me the invaluable lessons and guidance bestowed upon me, offer support and encouragement whenever possible, and endeavor to inspire others to discover their potential and chase their dreams...

A special thanks goes to my advisor and the rest of the committee members, who gave me invaluable guidance, insight, and feedback throughout this research project. Their expertise and knowledge have helped refine my research, and their encouragement and support have motivated me to continue.

I also would like to thank the government of the Kingdom of Saudi Arabia, Taif University, the Saudi Arabian Cultural Mission (SACM), the Department of Computer and Information Technology at Purdue University, and the Lab of Investigative Technologies and Ubiquitous and Mobile Investigative Techniques and Technologies (UMIT^2) at Purdue University for providing me with the necessary resources and funding to pursue my academic goals. Without their support, this dissertation would not have been possible.

Finally, I would like to thank my friends who have been by my side and provided me with their support, encouragement, and companionship throughout this journey. Your belief in me has been a great source of strength and inspiration.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

3D	Three-Dimensional
ACPO	Association of Chief Police Officers
APOLLO	Apple Pattern of Life Lazy Output'er
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifier
CTF	Capture the Flag
CTTF	Computer Forensic Tool Testing
Covid-19	Coronavirus Disease 2019
CIA	Confidentiality, Integrity, and Availability
CSV	Comma-Separated Values
DBMS	Database Management System
DF	Digital Forensics
DFINT	digital forensic intelligence
DMS	Decimal Degrees, Degrees-Minutes-Seconds
DoJ	Department of Justice
ET	Eastern Time
ESDFIM	Enhanced Systematic Digital Forensic Investigation Model
EXIF	Exchangeable Image File Format
FAA	Federal Aviation Administration
GDFM	General Digital Forensics Model
GIS	Geographic Information System
GMS	Global System for Mobile Communication
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
KML	Keyhole Markup Language
LI	Location Intelligence
MAC	Media Access Control
MD5	Message Digest

NFC	Near Field Communication
RAM	Random-Access Memory
Regex	Regular Expressions
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
OSINT	Open Source Intelligence
OS	Operating System
PIN	Personal Identification Number
NIJ	National Institute of Justice
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
iLEAPP	iOS Logs, Events, And Plists Parser
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
RAM	Random Access Memory
plist	Property List Format
SHA1	Secure Hash Algorithm, version 1
SHM	Shared Memory
SIM	Subscriber Identity Module
SSID	Service Set Identification
SWGDE	Scientific Working Group on Digital Evidence
UAVs	Unmanned Aerial Vehicles
UTC	Coordinated Universal Time
UTM	Universal Transverse Mercator
URL	Uniform Resource Locator
VM	virtual Machine

WAL	Write-Ahead Log
Wi-Fi	Wireless Fidelity
WSL	Windows Subsystem for Linux

ABSTRACT

Technological advances have a profound impact on people and the world in which they live. People use a wide range of smart devices, such as the Internet of Things (IoT), smartphones, and wearable devices, on a regular basis, all of which store and use location data. With this explosion of technology, these devices have been playing an essential role in digital forensics and crime investigations. Digital forensic professionals have become more able to acquire and assess various types of data and locations; therefore, location data has become essential for responders, practitioners, and digital investigators dealing with digital forensic cases that rely heavily on digital devices that collect data about their users. It is very beneficial and critical when performing any digital/cyber forensic investigation to consider answering the six Ws questions (i.e., who, what, when, where, why, and how) by using location data recovered from digital devices, such as where the suspect was at the time of the crime or the deviant act. Therefore, they could convict a suspect or help prove their innocence. However, many digital forensic standards, guidelines, tools, and even the National Institute of Standards and Technology (NIST) Cyber Security Personnel Framework (NICE) lack full coverage of what location data can be, how to use such data effectively, and how to perform spatial analysis. Although current digital forensic frameworks recognize the importance of location data, only a limited number of data sources (e.g., GPS) are considered sources of location in these digital forensic frameworks. Moreover, most digital forensic frameworks and tools have yet to introduce geo-contextualization techniques and spatial analysis into the digital forensic process, which may aid digital forensic investigations and provide more information for decision-making. As a result, significant gaps in the digital forensics community are still influenced by a lack of understanding of how to properly curate geodata. Therefore, this research was conducted to develop a transdisciplinary framework to deal with the limitations of previous work and explore opportunities to deal with geodata recovered from digital evidence by improving the way of maintaining geodata and getting the best value from them using an iPhone case study. The findings of this study demonstrated the potential value of geodata in digital disciplinary investigations when using the created transdisciplinary framework. Moreover, the findings discuss the implications for digital spa-

tial analytical techniques and multi-intelligence domains, including location intelligence and open-source intelligence, that aid investigators and generate an exceptional understanding of device users' spatial, temporal, and spatial-temporal patterns.

1. INTRODUCTION

This chapter aims to offer an overview of the research study. First, the chapter provides background information on the topics and then highlights current problems, scope, research question, and hypotheses.

1.1 Background

Humans are drastically influenced by the rapid advancement of technologies that change their daily environment. These technological developments have enhanced user experiences, expedited various domains, and greatly expanded the capabilities of smartphones and the Internet of Things (IoT). Humans interact with various smart devices (e.g., smartphones, wearable devices, drones, autonomous vehicles, and robotics) daily that require many types of data to enhance the experience and assist in providing more capabilities. For example, today, everyone relies on their smartphones to stay up-to-date with the digital world and to stay in touch with other sophisticated and smart objects, such as IoT devices. As the variety of technologies that enable digital or physical connection between individuals continues to grow, the importance of personally identifiable information (PII) and other types of geographical, personal digital identification will only continue to increase [1], [2].

According to [3], the number of smartphone mobile network subscriptions will reach 7 billion worldwide in 2024. A recent study predicted and projected that the number of mobile users in the United States by 2024 will reach more than 300 million users [4], [5] (see Figure 1.1 for the exact numbers projected by year). Furthermore, another forecast estimated that the number of IoT devices will reach around 24 billion by 2030 due to rapid technological increase [6]. Apple has managed to ship around 225 million smartphones globally in 2022, with an average of 220 million devices over the past decade, taking the second position after Samsung [7]. On the other hand, shipments did not increase dramatically in 2020 due to COVID-19; however, Apple was able to increase its market share to 40% of the total market share of smartwatches and maintain its dominance against many other competitors [8]. Furthermore, in 2020, Apple managed to ship around 30.9 million Apple Watches [8]. Therefore, with the increase of devices connected to our lives (e.g., smart watches), the

primary device (e.g., smartphone) that connects to all of these IoT devices is collecting and storing an enormous amount of data. Furthermore, drone technology has advanced significantly and is expected to reach USD 60 billion by 2025 [9], and according to [9], consumer drones generated more than USD 1.25 billion in sales in the United States in 2020. Furthermore, consumer drone shipment is expected to reach 2.4 million units worldwide in 2023 [9], and many of these customer-grade drones can now be controlled by smartphones.

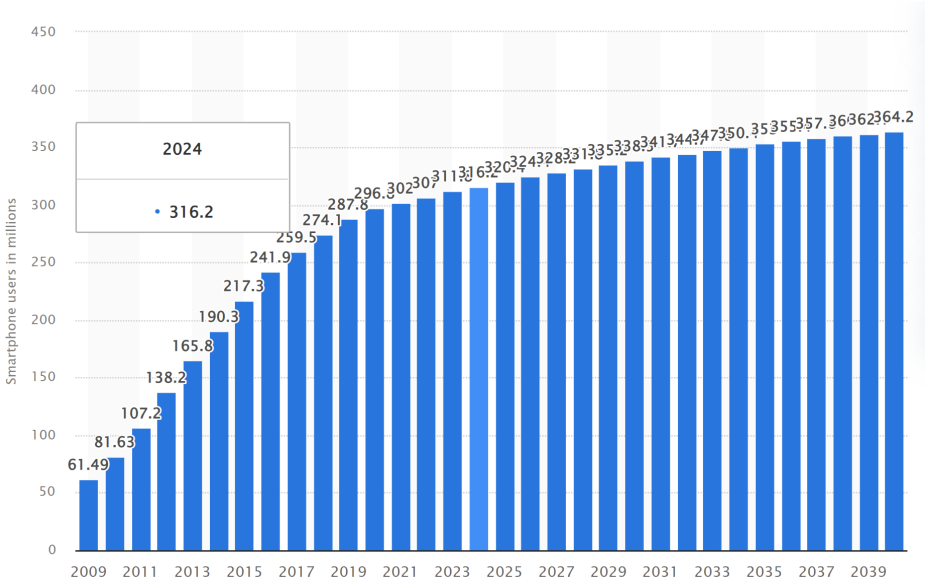


Figure 1.1. Estimated number of smartphone users in the United States from 2018 to 2040 [5]

According to the National Institute of Justice (NIJ), digital devices are valuable for the identification and conviction of some types of crime because they are everywhere and hold a large amount of user data [10]. Furthermore, due to the increasing usage of these smart devices more than ever, they are part of many types of crimes [11]. Therefore, the storage and preservation of digital evidence can help solve these crimes when digital devices are available to investigators. Location data from smartphones and other IoT and digital devices (e.g., wearable devices) are becoming increasingly commonplace in criminal investigations. They can be used to locate a suspect at the crime site and generate movement and past locations using the Global Positioning System (GPS), Bluetooth, or Wi-Fi data records that can indict them as in the *Kohberger's* case [12]. However, defense attorneys may utilize smartphone ev-

idence to support their client's alibi, contextualize damning acts, or show that they were far from the crime scene. Contemporary criminal defense is heavily based on the admissibility of this evidence and its limits. Personal user data that have a geographic dimension (e.g., geodata) recovered from digital devices are becoming more critical in investigating and prosecuting a wide range of offenses. Various geodata may be obtained utilizing digital devices in an investigation environment, which are essential considerations for several investigative contexts. In addition, the growing usage of smart devices has also made them appear in many investigations and be a crucial component in solving a wide variety of cases.

1.2 Problem Statement and Significance

Many years have passed since the increasing importance of digital forensics was brought to public attention [13], [14]. Currently, digital forensic tools are trying to cope with advancements in technology, aid their capabilities with the latest and most outstanding digital technology that has been used in other fields, and try to adapt it to the cyber forensic system. As a result, many advanced digital forensic tools have begun to emerge to aid cyber forensic investigations of digital devices, including the open source (e.g., Autopsy [15]) and proprietary (e.g., GrayKey [16], Cellebrite [17] and Magnet AXIOM [18]). Although the technical aspects of cyber forensics have generally been divided into various types depending on the technology used (e.g., computer forensics and mobile/IoT device forensics), there are many challenges to deal with because most of these technologies are rapidly advancing. For example, mobile forensics is challenging due to the increased functionality and development of these devices, which have become pocket-sized computers with plenty of storage.

Moreover, to combat the growing demand for guidelines and standards for digital forensics, many have been developed and put to work by large agencies in the US. The National Institute of Standards and Technology (NIST) provides the digital forensics community with well-defined digital forensic processes for different devices. For example, in [19], NIST provided guidelines for mobile devices consisting of four main phases. The process starts with the preservation phase, which covers many subphases, such as search, identification, and evidence collection. In all parts of the preservation phase, the evidence must be retained in

its original state, as failure to do so can result in destroying a part of the whole evidence. In addition, many instructions are provided in the acquisition, examination, and documentation phases to facilitate the process.

In addition, the digital forensics community continues attempting to adapt to the frequent changes in the data obtained, examined, and analyzed from these devices. This is evident from the increased efforts of many researchers in this field. Furthermore, in an ongoing effort of one of the seven technical divisions of the Information Technology Laboratory at the NIJ, the Software Quality Group has been testing and ensuring computer forensic software functions and identifying defects [20]. For digital forensics investigators and practitioners, confidence and understanding of the tool's ability to perform its function appropriately are critical. Therefore, the NIST Computer Forensic Tool Testing Program (CFTT) develops these test criteria, techniques, and reports to help tool makers, users of these tools, and interested parties understand any anomalies discovered in the tested digital forensic tools [20], [21]. In addition, these data are then used to improve products and alert users and other relevant parties. According to the group website [20], the group uses tools, methods, and models to improve the quality of the development and maintenance of digital forensic software.

Geodata is one of the many types of data digital forensic investigators come across in any investigation. This is because geodata has become an important asset that developed applications are using and collecting to optimize and help improve their applications, restrictions, and services provided to meet the user's expectations. Many technologies, including, but not limited to, smartphones, cars, tracking devices, watches, computers, laptops, cameras, drones, robots, and others, preserve and utilize geodata. Therefore, location data are considered of tremendous value and have become essential in the cyber forensics domain. In addition, it may provide forensic analysts with valuable leads that can help in forensic investigation and design. Current research efforts have focused on providing clear general guidelines and standards. Recently, NIST highlighted the challenges related to the identification phase of cyber cloud forensics, where geodata has been considered an essential component that can help find evidence [22].

Although many studies and research efforts offer investigators comprehensive instruction and guidelines, they fall behind in highlighting all types of geodata and how to deal with them. Different types of geodata are not always identified directly with the latest digital forensic tools. These tools depend heavily on using GPS coordinates preserved in EXIF tags, artifacts, or different file types that can contain and present embedded geodata (e.g., audio, video, documents, spreadsheets, databases, etc.). However, straightforward GPS data still pose challenges for digital forensic tools that deal with many GPS records, such as GPS tracks found on unmanned aerial vehicles (UAVs) flight paths. According to [23], [24], digital forensic tools (e.g., Autopsy, Cellebrite, Magnet AXIOM) did not represent comprehensive and accurate geodata for encrypted flight logs.

According to [25], the use of geodata in a variety of sectors is increasing. In digital forensics, despite the fact that these data can be used to aid in investigations, prosecute and convict offenders and victims, indict suspects, and give evidence in court cases, there has been little use of spatial analysis methods in the digital forensics community and industry. Therefore, there is a growing need for effective analytical solutions due to the rapid availability of vast amounts of data from many sources, such as sensors, logs, and structured data forms. According to [26], the widespread use of positioning technology may have helped facilitate human activities in the physical world while allowing various location spoofing techniques.

Wade et al. [27] discuss how there is no need for false evidence to enter the courtroom to thwart justice. According to their findings, when prospective witnesses are shown false or misrepresented evidence, they may be forced to testify about events they never participated in [27]. This is alarming, as courts of justice worldwide increasingly value digital evidence in the same way as they do eyewitness testimony. Furthermore, due to the large amount of information accessible and the potential provided by digital evidence to investigate and prove a crime, digital forensics has become a crucial component of practically every criminal investigation [28]. Although these digital devices can provide valuable evidence, they are generally treated with mistrust and confusion in criminal justice procedures, which can be reasonable in some cases [28]. Therefore, there could be changes in whether recovered data

from digital devices are manipulated or fabricated, which puts a considerable burden on investigators and the admissibility of the evidence.

Freitas and Curry in [29] discuss the basic principles of data analysis and indicate that the quality of an analysis is directly related to the quality of the data being studied. When making critical decisions, concerns about data integrity may significantly impact operations. Although existing digital forensic tools can keep up with technological changes, they cannot handle increasingly complex geodata curation techniques. Moreover, mobile device acquisition tool testing done by [20], [21] still lacks complete tests for geodata other than GPS points due to the reliance on test set-up requirements documents such as the "Quick Start Guide for Populating Mobile Test Devices" [30].

Furthermore, it is evident that not all data formats representing geospatial/geolocation information are considered when populating mobile devices. The [30] guideline is considered one of the essential documents for populating Mobile Devices developed by NIST. Section 8 of the NIST document talks about only a few types of geolocation data [30]. It concentrated only on GPS-related applications, routes, check-ins, and geotagged information. There are more than just these to consider when populating geolocation data. In geography, location is generally referred to as an exact place on Earth, often defined in terms of latitude and longitude. However, there is more to add when incorporating the latest technological advancements. Other types can represent and hold geographic information when investigated (e.g., Internet Protocol (IP) addresses, WiFi, SSID, BSSID, text, images, and even a simple sequence of 3 words [31]). However, they need a particular way to relocate them to a physical location. These types pose many challenges to investigators because they are represented in different data formats/schemes that are not necessarily considered explicit geodata formats. Although these digital forensic tools are trying to add functionality to deal with these types of geodata, they lack comprehensive spatial analysis and visualization for these critical artifacts that can add probative geo value while helping to consolidate recovered evidence.

According to [25], many fields are adopting methods to capture, process, edit, analyze, and present geodata. Although these data can help in investigations, penalizing and convicting criminals, indicting victims, initiating suspects, and providing evidence in court cases, adaptation rates have been limited in digital forensics, especially in incorporating spatial

analysis techniques. On the other hand, with a large volume of data in some instances, investigators are conducting investigations to determine what is needed and relevant within the full extent of the data [32]. If more than one of these cases coincides with big data, it is difficult for investigators to juggle them simultaneously [11]. Therefore, providing context-based content is essential for digital forensic investigators. However, there are no ways to enhance digital forensic investigations by providing geographic contextualization for each step. Moreover, a lack of frameworks dealing with geographic contextualization needs to be filled in.

Although the NIST National Initiative for Cybersecurity Education (NICE) framework provides comprehensive guidance for digital forensic investigators, it does not explicitly emphasize the importance of geospatial or Geographic Information Systems (GIS) skills in the field. Therefore, this study highlights the necessity of incorporating geospatial expertise into cyber forensics investigations, mainly when dealing with geodata. Geodata, whose many forms include location information, spatial patterns, and relationships, are increasingly prevalent in digital devices and play a significant role in cyber forensic investigations. One of the many goals of this study is to bridge the gap between the NIST NICE framework and the field's evolving needs by demonstrating the practical significance of geospatial skills in digital forensics investigations.

Therefore, it is critical to undermine every possible technique that can be used to deal with geodata to provide relevant information that can later be used to help the investigator by adding a geo-contextualization dimension. One of the many techniques to unlock the full potential of geodata is using Open-Source Intelligence (OSINT) as a tool to geolocate different types of data that have the possibility of having a geographical extent. Many fields have benefited from many intelligence domains, such as location intelligence and open-source intelligence. Because of the focus on the forensic soundness of the recovered evidence, these techniques have not been studied with thought. However, they can add to existing guidelines by providing investigators with valuable insights using geodata recovered from cases, from crime sequences to helping in building insightful reports.

Additionally, other investigative analysis techniques, such as pattern-of-life (PoL) analysis, which is used to help identify user behaviors and unusual activities, have been lim-

ited to recovered evidence. Recovering geodata is essential, but using it to help build a geographically-focused user's day-to-day behavior (e.g., geo-PoL analysis) can lead to a story that conveys well-explained events to a geographical extent. Although investigators need to recover, geolocate, and visualize geodata, connecting dots and patterns to derive meaning and stories is at the top of what investigators are required to do. Furthermore, geodata and related information can be helpful when complemented with PoL analysis techniques. As a result, these analytical techniques would benefit from geodata to correlate behaviors and patterns with locations.

1.3 Research Question and Scope

Although each geodata's implementation, acceptability, significance, and procedural legitimacy differ depending on the amount of data stored and collected for each case, investigators need to understand the forms in which geodata can be stored. In addition, it is equally essential to know various temporal and geospatial analytical techniques to provide geo-contextual reasoning that improves cyber forensics investigations and evidence representation for intelligence and forensics investigations. Although the acceptability and importance of geodata vary depending on the situation and environment of each incident, there are many ways to preserve spatial and temporal information from smart devices and the advantages that come with doing so that can break down barriers for practical cyber forensics analysis. The approach aims to help transform information and the available data into knowledge to aid investigations. In addition, the comprehensive analysis helps to build a complete narrative of the digital evidence and supports identifying critical actions or behaviors that may be essential to the investigation.

This proposed study aims to answer the following research questions and hypotheses:

1. Can a comprehensive mobile forensics investigation infuse with an interdisciplinary approach that integrates technological, geographical, intelligence domains, and cyber forensics perspectives be used to build a cyber forensics transdisciplinary geo-contextualization framework?

- H_1: A cyber forensics transdisciplinary geo-contextualization framework can be created.

2. Can the cyber forensics transdisciplinary geo-contextualization framework complement, enrich, and assist mobile forensics investigations in cases of geodata?

    - H_2: The transdisciplinary approach fosters techniques to complement and validate recovered geodata.
    - H_3: The transdisciplinary approach enriches and geo-contextualizes different data, leading to a notable impact on cyber forensic analysis and more effective geo-contextualization than traditional investigative methods.
    - H_4: The transdisciplinary approach assists in uncovering and identifying spatiotemporal information that can improve PoL analysis and add geo-added value to investigations.

1.4 Assumptions

The assumptions for this research include the following:

- Geography, spatial thinking, and GIS are major concepts and methods in digital forensic investigations.
- Geolocation services are enabled on the investigated devices.
- Geolocations are present on the investigated device.
- Different geodata types are present in the investigated devices.
- Digital forensic images of advanced logical/full file system extraction are available to the investigator.
- Relevent case digital forensic images are available.
- The recovered geodata may have longitude, latitude, and altitude data (i.e., x, y, and z).

- Current digital forensics guidelines and frameworks are not optimized to deal with geodata.
- Studying and examining different types of evidence can reveal their geo-added value.
- OSINT approach can help locate and geocode digital evidence.
- Well-known digital forensic tools cannot visualize most types of geodata.
- Geo-located evidence can significantly aid in building a geo-PoL analysis.
- Intelligence domains (e.g., location intelligence and open-source intelligence) can add to existing guidelines by providing investigators with valuable insights for geodata.
- Plotting data onto a map puts it into a geo-context and may reveal new insight and understanding of the user's activities.
- The transdisciplinary approach links domains with common factors.

1.5 Limitations

The limitations of this study include the following:

- Research only investigated iOS versions 13.3.1, 13.4.1, 14.1, 14.2, 14.3, 15.0.2, and 16.1.1.
- Only devices that can be jailbroken were used.
- Logical/full file system extractions were the main source of forensic data.
- The Department of Computer and Information Technology and Ubiquitous and Mobile Investigative Techniques and Technologies (UMIT^2) Lab at Purdue University offers licenses for specific commercial tools, which means that commercial investigation, acquisition, examination, and analysis tools are restricted to these.
- Only a few commercial digital forensic tools were used.
- The study did not cover continuous health data for an extended period.

1.6 Delimitations

The delimitations of this study include the following:

- The study focused only on technical aspects of the cyber forensics process.
- This study was designed for iOS and may not apply to other digital devices and OSes (e.g., Android OS)
- The research did not cover the acquisition and analysis of live iOS sysdiagnose logs.
- The study dealt with images of jailbroken devices.
- This research did not cover recovering and examining data stored in the cloud (e.g., iCloud).
- Creating a module to compact anti-forensics techniques was out of the scope of this study.
- The study did not assess the performance of the digital forensic tools used.
- The study did not cover COVID-19 contact tracing on iOS.

2. BACKGROUND

This chapter is divided into parts that focus on different aspects that work as the backbone of this research. These concepts will be used as building blocks in this research and help build the transdisciplinary approach. In addition, it will guide the research and help to form relevant findings.

2.1 The Evolution of Transdisciplinary Approaches

When researching or advancing knowledge, the frameworks can usually range from a single discipline, where researchers from the same field collaborate but with bounded methodologies, to multidisciplinary, where researchers from multiple disciplines work together; to cross-disciplinary, where researchers from related but different disciplines collaborate; to interdisciplinary, where researchers from unrelated disciplines collaborate; and to transdisciplinary, where researchers work with non-academic partners to address real-world problems [33]–[37]. Each has its advantages and disadvantages; the description of each approach is as follows.

- Discipline, intradisciplinary, or mono-disciplinary: It is a branch of knowledge limited to one body of knowledge [33]. In other words, this method limits researchers or research and analysis to being bounded by the context of a single discipline [37].
- Multidisciplinary: According to many dictionaries, multi means many and more than one [34]. Therefore, when multiple disciplines collaborate in research or try to solve a problem without integrating their concepts or methodologies, it is known as multidisciplinary research [33]. This approach involves conducting research in parallel with each discipline contributing its perspective without necessarily incorporating them.
- cross-disciplinary: In this approach, similar to the multidisciplinary approach, there is no transfer of methodologies, ideas, and techniques throughout the body of knowledge [35]. However, it involves close relationships between the same discipline of interest, distinguishing it from multidisciplinary [35].

- Interdisciplinary: This research involves collaboration among multiple disciplines, explicitly sharing and integrating concepts or methodologies. This results in a mutual enrichment of knowledge and understanding between the collaborating disciplines [33].

- Transdisciplinary: The transdisciplinary approach surpasses the limitations of previous methods by bringing together investigators or researchers from various fields, which involves integrating and moving beyond discipline-specific approaches to develop new conceptual, theoretical, methodological, and transnational innovations that can address a common problem [33], [36]. Therefore, breaking the boundaries of traditional disciplines allows this approach to have a more comprehensive and collaborative effort toward problem-solving [33]. In addition, this approach usually also integrates non-scientific fields and stakeholders and adds them to the equation. As a result, innovative solutions to complex issues can arise by embracing, infusing, and utilizing these different frameworks and perspectives.

Fortunately, advances in techniques, technologies, and disciplines allowed research to collaborate, enabling the integration of different disciplinary frameworks [38]. Adopting a comprehensive approach and seeing the connections between several academic subjects helps to solve problems and issues. Although it requires realizing relationships and tremendous efforts, it can help us solve complex social and technological problems. For digital investigators, it is essential to specialize in a particular area and be well-rounded in several domains to have a broader perspective encompassing different disciplines that can help open up new perspectives and avenues of investigation. Figure 2.1 taken from [37] shows the defined approach sequence.

2.2 Digital Forensics

The greater the technological advancement, the more these devices have become essential to many people's lives. In fact, recent research predicted and projected that the number of mobile users in the United States would reach approximately 320 million by 2025 and approximately 18 billion mobile phones worldwide in 2025 [39], [40]. In addition, many other devices can be directly or indirectly linked to many mobile devices that many people

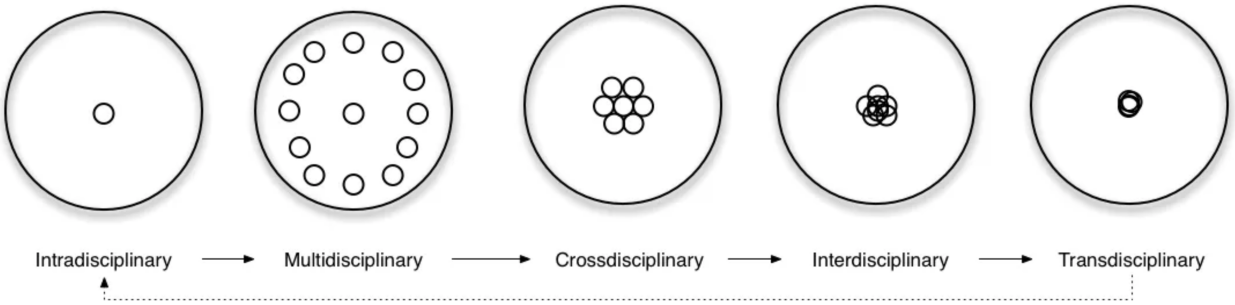


Figure 2.1. Illustration by [37] of the different approaches.

carry around, such as smartwatches, IoT devices, vehicles, etc. Therefore, according to other statistics in [6], projected that the number of IoT devices would reach around 30 billion by 2030 due to the rapid advancement of technology.

Furthermore, digital devices and sensors (e.g., IoT devices) are becoming essential daily activities, and the amount of data inside these devices is increasing dramatically. As a result, the principal device (e.g., smartphone) communicating with all of these IoT devices collects and stores massive amounts of data. In the last decade, geolocation usage has grown significantly in many applications. This growth has been directly influenced by smart devices and technology that make collecting and using this kind of information easier. Although technological improvements are beneficial to society by allowing better communication and other advantages related to data, they can also be used to initiate, maintain, and even record unlawful conduct in some circumstances. Only a few digital forensic tools have started to include the essential capabilities and features to deal with this development, even though this increase has been going on for a while.

Digital devices are becoming valuable for the identification and conviction of various crimes, as they are ubiquitous and contain a large amount of personal user data [10]. Furthermore, due to the widespread use of smart devices, they have become a significant factor in the resolution of a wide range of crimes [11], [41], [42]. The digital evidence that can reside on these devices can help solve crimes if detectives have access to digital devices that store and preserve digital evidence [10], [43].

More than ever, law enforcement is highly relying on digital evidence in criminal investigations, which is becoming a part of many investigations [10], [44], [45]. Law enforcement can use digital evidence the same way that they can use any other piece of evidence to try to pinpoint the exact moment and location of an occurrence in order to prove that a person or group of people was the catalyst for criminal activity.

The Science of Digital Forensics refers to the process of collecting, evaluating, and reporting digital evidence. Everything happens between when a piece of digital evidence is found and when it is publicly evaluated and used in judicial procedures [46], [47]. Although many believe that digital forensics is the only component of criminal investigations, it has emerged as a potential source of tools and methodologies to help preserve and analyze digital materials, particularly historical materials [48].

Digital forensics is a broad discipline that includes, but is not limited to, computer forensics, IoT forensics, network forensics, cloud, live, mobile device forensics, database forensic analysis, multimedia forensics, memory forensics, and drone forensics [49]–[54]. Due to the large diversity of digital devices and technology in digital forensics, each has its features and obstacles.

The diversity of the areas of digital forensics mirrors the variety of digital devices and technologies used in current criminal activities, showing the importance of digital forensics in civil and criminal investigations and convictions [49], [50], [55]. Digital forensics practitioners used to focus on computer data; however, with the development of mobile devices, social networks, and cloud storage, digital forensics specialists must be able to collect and evaluate several types of data and data from different locations [52], [56], [57]. Moreover, digital forensics is facing an expanding data explosion. The digital forensics community must adapt to these challenges as data grows in diversity and volume.

Furthermore, with the variety and abundance of data and the constant advancement of technology, forensic investigations are becoming increasingly complex. Still, they are also critical to the analysis and extraction of relevant information [51], [58], [59]. To deal with the growing variety and amount of data, the digital forensics community must support methods and technologies that help them create and maintain high-quality data that can lead to valuable results that can be analyzed [59], [60].

2.2.1 Mobile Forensics

Technical aspects of digital forensics have generally been divided into various types depending on the technology used (e.g., computer forensics and mobile/IOT device forensics). As a result, mobile forensics has emerged as a form with the increasing functionality and development of these devices, which have become pocket-sized computers with large storage. Although it is a challenging new domain, the digital forensics community continues to attempt to find ways to adapt to the frequent changes in the data collection, examination, and analysis of these devices.

Android and iOS are among the most widely used mobile device operating systems, which have thrived more due to Covid-19 [2], [61]. iOS follows Apple's security tradition, focusing on data encryption, secure boot, sandboxing, and code signing [62]–[64]. These features aim to protect users and their sensitive data. Furthermore, Apple prioritizes privacy and security in design [65]. The iOS has app permissions, location services settings, and a privacy dashboard that shows which applications are accessing data. Therefore, Apple advertises that iOS security and privacy work together to create a safe and private mobile experience [66]. Therefore, continuous improvements make iOS popular for consumers seeking security and privacy.

iOS Forensics

iOS forensics involves extracting, analyzing, and interpreting data from iOS devices such as iPhones and iPads [67]. iOS forensics has become significant for law enforcement, private detectives, and digital forensic practitioners as mobile devices have become ubiquitous [68]. iOS forensics gathers evidence for court cases and different types of investigations. Examples of data include, but are not limited to, call records, text messages, emails, app usage data, location data, and social media activity. Forensic practitioners employ specialized tools and procedures to access the device's file system and recover pertinent data, such as logical and physical extraction methods.

According to [69], keeping up with iOS updates is a significant difficulty in iOS forensics. New versions of iOS can affect data storage and security. In order to efficiently capture and

evaluate data from mobile devices, iOS forensic practitioners must be up-to-date on the latest techniques and tools [50]. Although iOS forensics is a complicated and ever-changing field, applying forensic methods to iOS devices' specific problems, researchers and practitioners might find helpful evidence for legal and investigative purposes.

The sort of investigation type, capabilities (e.g., tools and knowledge, and data needed to determine the ways to obtain iOS evidence. Common iOS evidence-collection methods include:

- Physical acquisition: This method involves creating a bit-by-bit copy of the device's storage using specialized hardware or software tools, such as GrayKey [70], [71]. The physical acquisition can retrieve deleted data and is useful because iOS devices flag deleted files for overwriting instead of deleting them. Physically obtaining data can damage the equipment or data; therefore, only experienced forensic practitioners with the right set of tools can perform this procedure. On the other hand, the physical acquisition does not always ensure detected data recovery, because the possibility that deleted data by the user or the system can be overwritten increases with time.

- Logical acquisition: This method has many names and types. This method generally involves accessing the device's file system via a software tool such as iTunes or a forensic tool such as Cellebrite [17], Magnet Axiom [72]. The logical acquisition can retrieve contacts, call logs, text messages, photos, application data, and other third-party data, which can be used when the physical acquisition is impossible [73], [74]. The weakness of this method is that it usually cannot recover deleted files.

- Live acquisition: This method involves accessing data from a currently used device, often through remote access or monitoring software [75]. The live acquisition can retrieve active app usage, databases, logs, chat conversations, and location data.

- Cloud Acquisition: Device or user credentials are used to access cloud data (e.g., iCloud or Google Drive) [76], [77]. Cloud acquisition retrieves photographs, contacts, app data, messages, and backups.

- Manual acquisition: The investigator presses the phone keypad/screen to access the phone's contents [78]. This is the simplest way; the investigator does not require prior experience extracting data from mobile devices to apply it.

- chip-Off acquisition: The approach includes physically removing the internal chips of a device and reading the information contained within them [78]. Usually, this approach is used as a last resort when logical or physical acquisition fails or the data is encrypted.

Each approach has drawbacks; therefore, forensic professionals must carefully assess the data sought and how each acquisition method can affect the device and data. Court admissibility and chain of custody must be followed [79].

2.3 Common Digital Forensics Practices and Frameworks

The digital forensic investigation begins with identification and ends with the presentation. There are several ways to apply this approach, depending on the kind of device and equipment the investigator is looking at, where the evidence comes from, and the type of investigation. For example, mobile devices and personal computers may provide more extensive and diverse information about the device's owner than other forms.

According to [80], practitioners and academics see what is crucial in digital forensics in a different way. As a result of dealing with urgent issues, practitioners often focus on advancing what can make it easier to conduct thorough and timely investigations [80]. However, academics are concerned with theories such as formalization and standardization [80]. Many frameworks and standards have been developed to overcome some of the challenges investigators face when they are required to investigate digital devices and advance the digital forensics community. Well-known examples of these standards for digital devices are discussed in the following subsections, depending on the type of technology.

2.3.1 Guidelines on Computer and Mobile Device Forensics

One of the most well-known complete mobile device forensics guidelines is the NIST Special Publication 800-101, which includes a well-defined digital forensics process used by

many law enforcement and researchers [81], [82]. This model consists of 4 stages: preservation of the mobile device, acquisition, examination, analysis, and reporting. Another famous model is provided by the Scientific Working Group on Digital Evidence (SWGDE), which has helped the digital forensics community by developing many best practices, such as best practices constructed for mobile phone forensics, evidence collection and acquisition of mobile devices, and the famous SWGDE Model Standard Operation Procedures for Computer Forensics [83]–[85].

Regarding visualizing all crucial components of a digital forensic investigation, Rigby and Rogers in [86] have demonstrated their general digital forensic model (GDFM) using a multidimensional "cube" graphical representation. Figure 2.2 illustrates the cubic shape and the components. The model consists of 7 main processes divided into two main stages. The first is the collection phase, which starts with preparation, is followed by identification, preservation, and ends with the collection. The second stage is the analysis phase, which starts with an examination followed by analysis and presentation. Furthermore, there are many other guidelines and standardizations, such as ISO / IEC 27037: 2012 [87], ESDFIM [88]; Computer forensics field triage process model [89]; Electronic Crime Scene Investigation: A Guide for First Responders, which was developed by the DOJ injunction with NIST [90], and Interpol [91].

The National Initiative for Cybersecurity Education (NICE), published under NIST special publication number 800-181 [92], describes the Work Roles by tasks, knowledge, and skills required. Furthermore, revision 1 [93] provides a description of how tasks, knowledge, and skills can be used to create work roles in the cybersecurity workforce in more detail. Figure 2.3 illustrates the building blocks of the work roles. Geospatial analytical tasks and skills are only listed under "exploitation analyst," whereas skills are reported under four main roles: "exploitation analyst," "security control assessor," "target network analyst," and "target developer." However, they were not listed under any of the following investigative roles: cybercrime investigator, law enforcement/counterintelligence forensics analyst, and cyber defense forensics analyst.

On the other hand, Garfinkel in [14], discussed how there is an absence of standard abstractions and data formats; moreover, many of the existing digital forensics software is

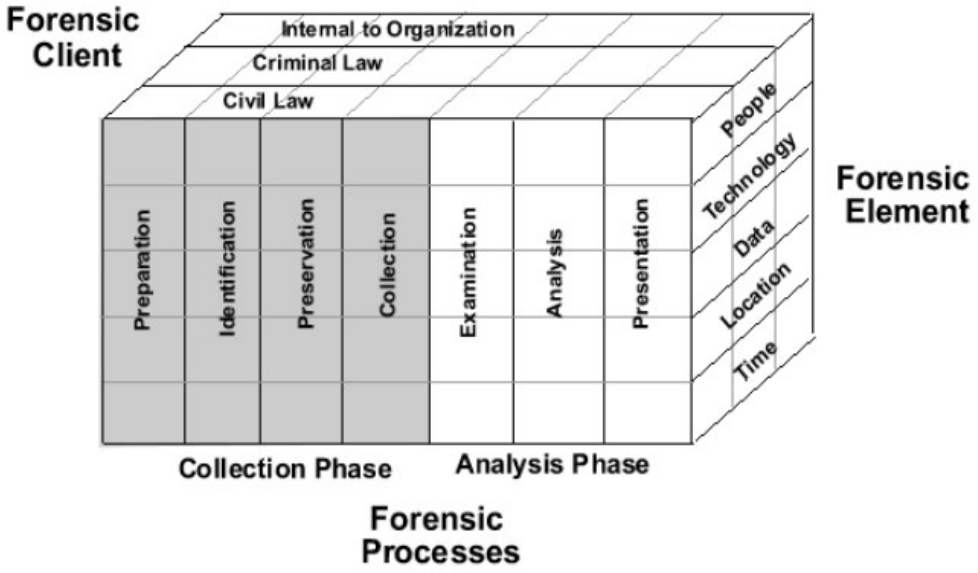


Figure 2.2. DFGM by Rigby et al. [86]

still following what he called the 'visibility, filter, and report model.' This model was built with the intention of identifying the information and then presenting it to the investigator in an elegant way.

Garfinkel also mentioned in [14], that there is a need for digital forensic tools to overcome some of the challenges related to visual analytics by integrating techniques that help investigators guide investigations better. In addition, it is a great burden for the digital forensics community, where most current digital forensics models and processes lack comprehensive techniques to deal with geodata.

The literature shows that the use of geolocation and geospatial data has increased dramatically in the last decade; these rates have been directly influenced by smart devices and technology that enable this collection and usage of data. However, only a few digital forensic tools have mimicked this increase and started to incorporate some capabilities and features to deal with this evolution. In addition, the authors of [94] emphasize the importance of developing and implementing comprehensive digital forensic readiness plans.

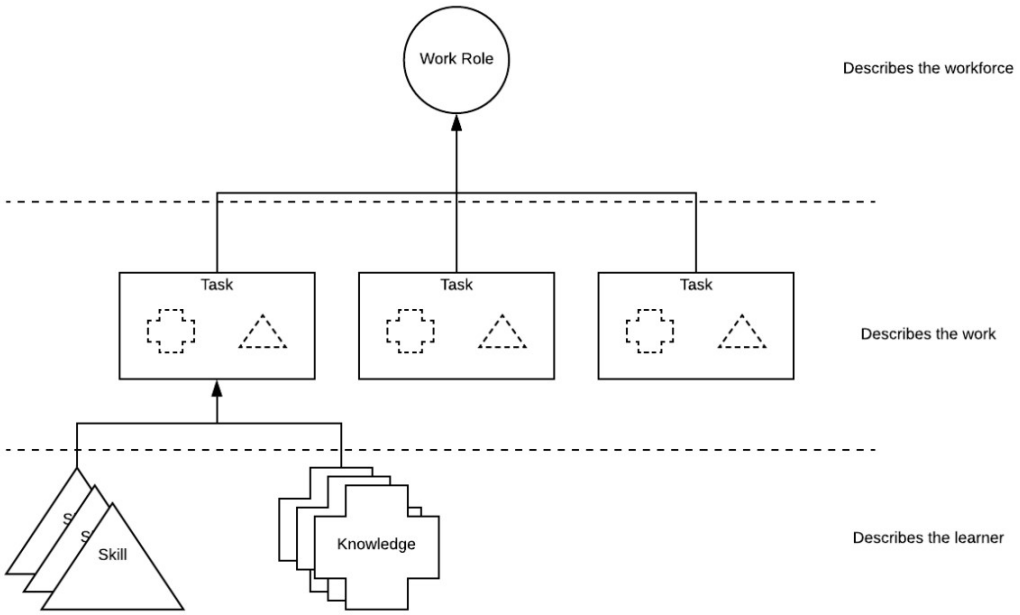


Figure 2.3. Building blocks of the work roles by [93]

2.3.2 UAV Forensics Frameworks

UAV forensics is a new branch of study that discusses drone analysis in more detail. The nature of UAV digital forensics differs from that of other devices. Although many UAV investigations are based on standards such as ACPO [95] and NIST, they lack adequate instructions and guidelines for drone forensics [96]. Furthermore, drones have a wide range of sensors that complicate digital forensic investigations by requiring the use of specialized equipment and inspection techniques [97]. Furthermore, the authors in [97] discussed that essential and critical information could remain missing if the examiners are not well qualified or prepared.

Today, many consumer drones use mobile devices to control and store data. Consequently, mobile device forensics is a critical step in drone investigations when the device is available. Drones can store data from the drone to the mobile device [98]. Mobile device forensics can also trace drone controls and data in cases of smuggling or espionage. Drone and mobile device forensics require particular knowledge, equipment, and legal and regulatory awareness.

These aspects of digital forensics may become increasingly significant as drones and mobile devices become more popular.

The researchers in [96] took the DJI Phantom 3 as a case study and proposed a process consisting of 20 steps within the three main stages of preparation, examination, and report. However, the researchers in [99] proposed a 10-step technical drone forensic investigation process compatible with a wide range of drone models, which was later suggested as a useful source by Interpol in [91]. Furthermore, the researchers in [100] have examined the underlying architecture of drone sensors, including components such as Wi-Fi and cameras, and then constructed a general drone forensic model that can be utilized to aid in digital investigations. Therefore, mobile device forensics is becoming an essential element in drone forensic frameworks.

2.4 Geodata

One of the many pieces of information that may reside on these devices is location data. They can be found in many of these devices and in cases where law enforcement and investigators are involved. In addition to being found in many cases, according to the NIJ [10], related location information can actually convict or even prove innocence; therefore, it has become an asset for digital investigators to pay attention to such data. Moreover, in [101], the NIST has highlighted in their recent document regarding the challenges of cloud forensics that knowing the geolocation of the investigated device is considered an essential element in the identification process, due to the fact that it can help in identifying and answering the "where" question, which can help in answering the other W's.

2.4.1 Background and Main Aspects of Geographic Contextualization

The term geo-contextualization refers to putting a concept in a specific setting that arises as a result of the geographical perspective. Therefore, in this research, the focus will concentrate on two of the most well-known geo-contextual elements [102] that are crucial in the geo-contextualization approach, and they are:

- Temporal: The study of time uncovers patterns that span time periods [102], [103].

- Spatial: The study of space that helps position actions in physical dimension [102], [103].
- spatial-temporal (Spatiotemporal): The study and analysis of data when it is collected across both space and time.

Furthermore, the ISO/TC 211 family of standards [104], defines geographic data, and information are defined as data and information that have an implicit or explicit relationship with a place relative to the Earth. They have many naming schemes, including "geospatial data," "geoinformation," and "geodata." Geodata represents a physical location on Earth, which makes it different from other types of data by adding an intriguing location and a spatial dimension to the data. Therefore, throughout our research, we will use the terms implicit or explicit with geodata, and the following are the definitions used.

- Explicit Geodata: It is a type of data that can be used directly to locate a place on Earth [104].
- Implicit Geodata: Data types that can be used to indirectly point to a physical location [104].

The phrase "geolocation" refers to the process of determining the geographical position of an object, person, or device through the use of technologies such as GPS, Wi-Fi, cellular network triangulation, and IP address [105], [106]. Moreover, geolocation can locate a person, device, or event such as a social media post, photo, or transaction. Geolocation data can be used in digital forensics to locate a suspect, victim, or witness at a certain time and place, which can be crucial evidence in a criminal case.

Due to the increasing use of applications that incorporate geolocation services as main functions, increasingly people now at least know what typical geodata (e.g., Global Positioning System (GPS) coordinates) look like. GPS data are well studied and often used in digital forensics, but many other types of location-based data (e.g., explicit and implicit) may be useful to an inquiry. Examples include cellular towers, Wi-Fi, Bluetooth, and social media check-in data. Although GPS is well studied and many digital forensic tools have started to incorporate parsers and maps that help investigators visualize them, these different formats

pose challenges. They are difficult to obtain or analyze without the appropriate tools. Many digital forensic investigators are unaware of the geodata that could aid their investigations or how to evaluate and interpret them.

As important as knowing all the types of data that can provide or hint at a piece of location information, it is equally important to understand the forms in which location and geodata can be preserved and to know their location on devices. Smartphones can collect and store a large amount of data daily with or without user interaction, which is essential, particularly in digital forensics.

2.4.2 Approaches to Deal with Temporal and Spatial Elements of Data

There are many approaches that can be used when investigating digital forensic cases. One of many approaches has been to recover timestamps, which play an important role in cyber forensics and may be used as a source of evidence [107], [108] because determining the exact date and time of an incident is crucial as part of any forensic investigation [109]. Timeline analysis is the practice of looking at the dates and times of various system events, such as the creation, modification, and access of files and other data artifacts [107]–[109].

Although it sounds easy to recover timestamps correctly, this is not true. In one of the recent updates, Magnet AXIOM, a well-known digital forensics tool, released an update to fix some of the issues the tool has faced in parsing the correct timestamp of the video EXIF data [110]. As a result, recovering timestamps correctly and effectively remains a challenge. As recovering timestamps is crucial in building and structuring events in a temporal dimension, space, in turn, is more difficult to recover and takes more time to be analyzed due to complicity and the need for further investigation. Furthermore, to determine where the action occurred, a deeper investigation must be conducted involving the location of a series of actions preceding and following the investigated event.

2.4.3 Spatial Thinking

Although understanding how to use forensic tools is essential, it is only one part of the job description of forensic practitioners [111]. Therefore, according to [111], core forensic

competencies such as data carving, operating system competency, the ability to design custom programs, as well as the ability to think analytically will continue to be essential for digital forensic practitioners, who must also understand the forensic process and have the necessary investigative skills.

Spatial thinking is one of many skills that can benefit investigators and help them use space to solve cases. Therefore, this process can increase the investigator's rapid throughput and support decision-making. According to the National Research Council et al., [112], spatial thinking has three aspects: concepts of space, techniques to express views in a visual form, and reasoning processes. Therefore, the idea of space is the factor that separates it from any other thinking. The space factor makes it possible to organize and arrange problems and challenges, uncover answers, and articulate possible solutions to properties of space such as proximity, continuity, and separation [112]. This allows actions and things to be perceived, remembered, and judged by the dynamics and static aspects of things through the representation of relationships in the space structure [112].

Furthermore, location information can be conveyed in various ways, the most common being physical; however, depending on the context, other ways include absolutely, relatively, or symbolically [113]. Therefore, in a physically conveyed meaning, one's precise location may be determined via a coordinate system (e.g., GPS). The absolute location is defined by a local reference frame whose resolution is proportionate to the grid size that explains it. Relative location manifests how close a person is to sites that are too well known in their immediate surroundings. In the standard language, a user's position is represented by a symbolic location, which provides abstract information about the user's geographical context.

- The absolute location is a fixed position on Earth, usually stated in latitude and longitude. GPS and mapping technology use these location data.
- Relative location describes a site's relationship to surrounding locales. A store may be "next to the gas station" or "across from the park."
- Symbolic locations are represented by symbols or icons rather than physical locations. This includes map markers and emojis.

Digital forensics investigators can better read and analyze geodata by understanding these diverse ways of expressing location information as they might be extracted from devices. It is critical to facilitate them in investigations.

2.5 Technologies used for Location Approximation

Many beneficial technological in daily applications use LBS to offer useful services such as real-time location and the ability to locate nearby locations of interest (e.g., businesses and restaurants), and these technological services use different technologies such as Bluetooth, GPS, RFID, NFC, WLAN, and recently IoT devices have combined the force to help pinpoint the user location on the large Earth surface [114]–[119]. Moreover, other types can represent and hold geographical information when investigated (e.g., Internet Protocol (IP) addresses [120], WiFi, SSID, Bluetooth, BSSID, text, images, and even a simple sequence of 3 words [31]). However, they need a special way to relocate them to a physical location. These types pose many challenges to investigators because they are represented in different data formats/schemes that are not necessarily explicitly geodata formats.

The following subsections will dive into the two widely used technologies for location approximation, covering each technology and its advantages and limitations.

2.5.1 GPS

One of the most well-known location detection systems in existence is GPS, which is part of the Global Navigation Satellite System (GNSS). GNSS also includes other satellite systems such as GLObalnaya NAvigatsionnaya Sputnikovaya Sistema in Russian (GLONASS) and Galileo, which the European Union created through the European Space Agency [121]. To determine geographical locations, GPS offers an effective set of teleological tools and frameworks [113]. In fact, according to [122], the US Department of Defense began making satellites accessible to the general public in the 1980s, allowing global satellite coverage to be consistent and widespread. Therefore, using a differential reference or the wide area augmented system (WAAS), GPS receivers may calculate their position within a few meters of the Earth's surface.

Global satellite coverage is consistent and widespread, allowing receivers to calculate their location within a few meters using a differential reference or the wide area enhancement system [122].

To report location, GPS uses a trilateration method to measure distances [123]. Therefore, GPS receivers use latitude, longitude, and altitude to determine their exact location on the planet [122]. A GPS receiver must be attached to the signal of at least three satellites to monitor movement to compute a two-dimensional location (that is, latitude and longitude); furthermore, when four or more satellites are in view of the receiver, the receiver may calculate a three-dimensional location (that is, latitude, longitude, and altitude) [113], [122]. Additionally, it is possible for some chips to receive multiple signals by integrating these signals to improve the accuracy and availability of the localization.

According to [124], accurate location information can be found on current smartphones through the use of assisted GPS (A-GPS). A-GPS uses smartphone networks (i.e., cellar and WiFi) in conjunction with a GPS antenna to speed up the process of determining one's current position [124]. A researcher argued that the A-GPS found in smartphones has less accuracy than consumer-grade GPS receivers in some cases [114]. The researcher in this study [114] examined, compared, and discussed the localization technologies of A-GPS, WiFi, and cell positioning to measure their precision on an iPhone 3G device. Therefore, according to this research, the comparison of A-GPS, WiFi, and Cellular positioning localization technologies to measure their precision on an iPhone 3G device showed that the average value of the root mean square deviation (RMSE) of the iPhone 3G was 9 meters for horizontal tests and 10.6 meters for vertical tests outdoors (see Figure 2.4 for the scatter plot), and this was less accurate compared to consumer-grade GPS receivers [114].

Furthermore, researchers in [125] examined the position accuracy of A-GPS of two phones (Motorolai580 and Sanyo SCP-7050), which according to the authors were classified as high-sensitivity GPS-enabled mobile phones against recreational grade GPS units (i.e., handheld GPS units) such as Garmin 75MAp and Trimble Juno ST. The authors have done 3 types of tests, dynamic outdoor test, static indoor test, and static outdoor test (see Figure 2.5 for the scatter plots of the outdoor test). They found that there was never an inaccuracy greater than 30 meters during static external tests and that the average horizontal inaccuracy of the

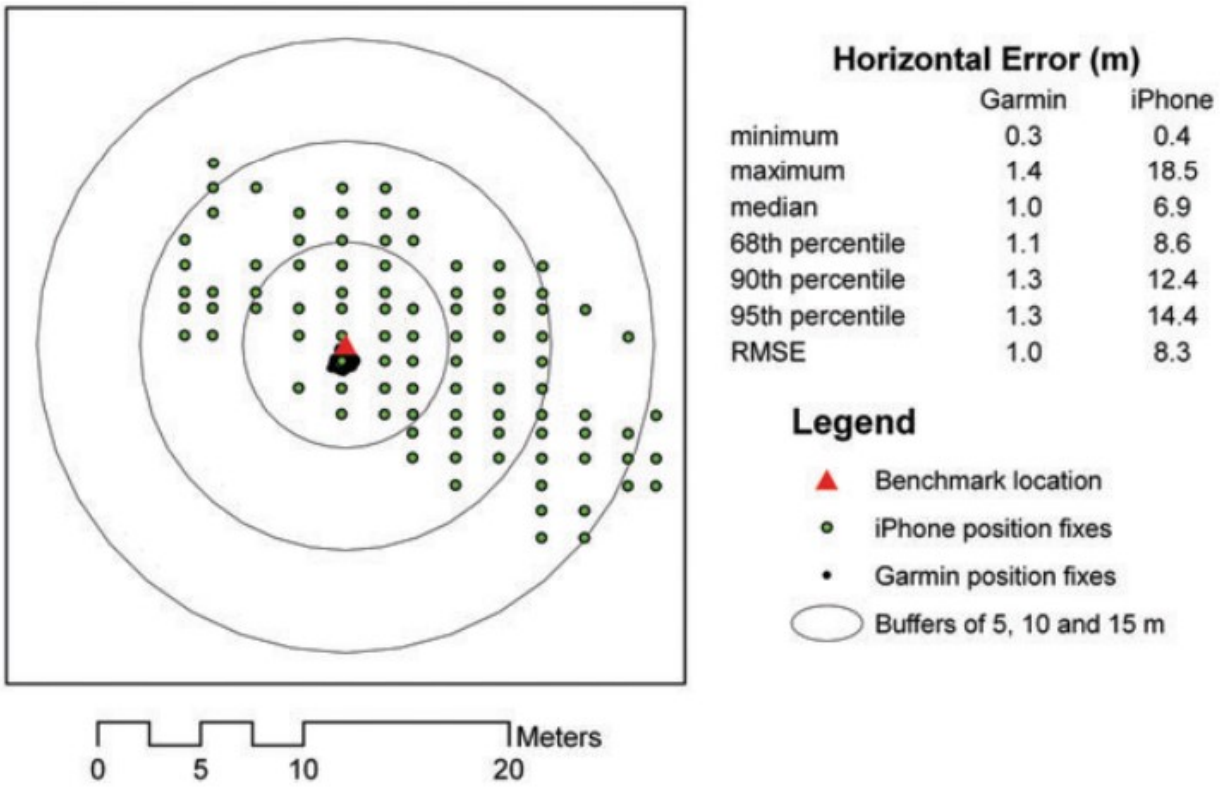


Figure 2.4. Scatter plot that demonstrates comparable horizontal accuracy of the A-GPS in the iPhone and Garmin GPS device by [114]

location of the mobile phone was found to be between 5 and 8.5 meters [125]. Furthermore, the square deviation of the root means was found to be between 6 and 12.5 meters, which the authors found to be very similar to the findings in [114]. Finally, researchers also pointed out that when interior tests were included, the maximum positional inaccuracy never exceeded 100 meters when a good GPS location fix was obtained, which is in compliance with the precision required by E911 [125].

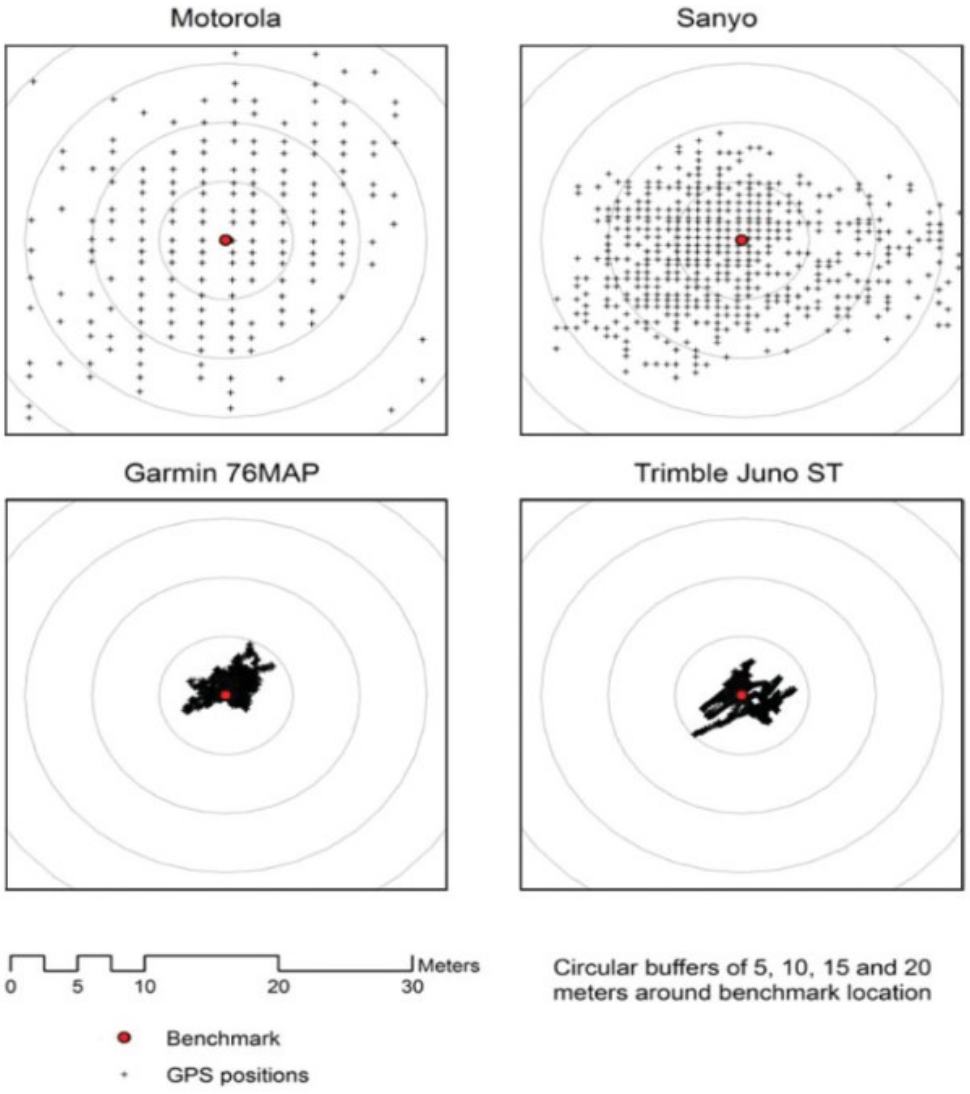


Figure 2.5. Scatter plots of the static outdoor tests by [125] that demonstrate accuracy of the tested devices.

The research in [126] is a study in which the authors have used the iPhone 6 to test its GPS accuracy in an urban environment. In other words, the researchers [126] examined, compared, and discussed the localization technologies of A-GPS, WiFi, and cell positioning to measure their precision on an iPhone 6 device. Therefore, according to this research, the average horizontal position inaccuracy of the iPhone 6 ranges between 7 and 13 meters depending on conditions (e.g., environmental and weather conditions), which is comparable to the normal accuracy levels reported by recreational grade GPS receivers in likely high multipath settings [126].

Although GPS accuracy is shown from the literature that it can be within a couple of meters, this accuracy depends on several factors such as GPS module or chip accuracy, receiver noise, the tetchiness used, surroundings, and weather [114], [126]. Therefore, a crucial aspect of GPS is in regard to indoor positions; it is often not sufficient alone. As a result, GPS-based outside positioning systems have been ruled out on many occasions as a feasible solution for indoor location applications due to their many shortcomings [127]. As a result of the limitations imposed by satellite-based external positioning systems for indoor use (e.g., GPS, GLONASS, Galileo), many researchers have proposed an extensive spectrum of indoor positioning systems that use wireless communication protocols during the last two decades [128].

2.5.2 Wireless Based Communication Protocols for Localization

The IEEE 802.11 standard for Wireless Local Area Networks (WLANs), also known as WiFi, has been in use for more than 15 years [129]. Wi-Fi positioning locates individuals using WiFi access points around the individual [114], [130]. It is found to be more accurate in locations with a high density of WiFi access points [114].

Moreover, according to [131], it is possible to accurately predict the position of a user in an indoor environment using wireless fingerprinting; however, this depends heavily on the distance between the user and the access points around. Researchers in [132] discussed that a precision of 1 meter is possible with WiFi-based location techniques without the need for special equipment. Newer types of indoor location positioning, such as ultra-wideband sys-

tems, can achieve an accuracy of up to one-centimeter [133]; however, it requires specialized hardware design.

In indoor environments, the overarching goal of localization is to obtain a level of accuracy that varies depending on the environment and the problem being investigated [134]. Furthermore, according to [135], precision can vary from room level to decimeter level when using signals that are accessible within indoor contexts depending on the type of signal used (e.g. WiFi, Bluetooth, and RFID).

Wireless networks use Wi-Fi to broadcast and utilize the Basic Service Set Identifier (BSSID) to identify other wireless interfaces and assign them accordingly. In addition, the Service Set Ientification (SSID) contains a sequence of characters that represent the name of the WLAN. Various BSSIDs and SSIDs are stored and used to provide very accurate location information through various online services [136]–[138].

wigle.net database [139] is an example of these services that hold a large amount of BSSID along with Media Access Control (MAC) addresses for many access points and are capable of locating a specific access point with a particular MAC address with high precision [137], [138], [140]. According to the wigle.net stats graph [141], the number of unique WiFi networks worldwide is more than 1 billion as of February 2023, and of this number, the United States has more than 500 million (see Figure 2.6 [141] for the number of WiFi access points that are geolocated around the world). This database also contains information on Bluetooth and cell towers that can be used to geolocate them. More than 1 billion unique Bluetooth devices have locations and around 20 million geolocated cell towers [142]. Researchers in [143] have looked at SSID from a forensic perspective and emphasized that professionals will appreciate that such things establish ties between the digital world and the physical world, which can help in digital investigations that seek to alleviate information as much as possible.

On the other hand, Bluetooth Low Energy (BLE) aims to offer basic Bluetooth capabilities while using as little energy as possible, and due to its low power consumption, BLE is now available on almost every smartphone, making it a viable choice for many applications, and has recently been put to good use during Covid-19 to monitor mobile contacts [144], [145].

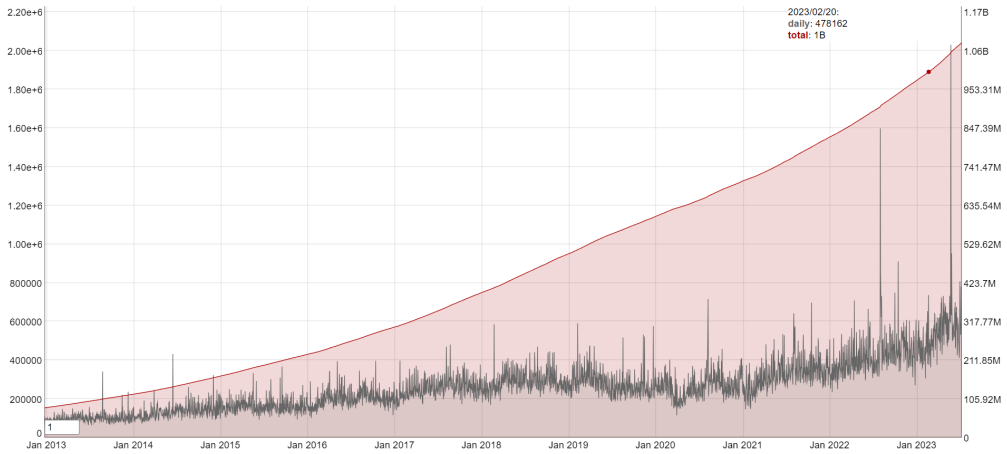


Figure 2.6. The number of geolocated Wi-Fi access points worldwide is over 1 billion as of February 2023 [141].

According to [146], IoT is becoming increasingly prevalent in a broad variety of industries, and this may have resulted in the information from wireless sensors and IoT devices becoming more crucial in the daily life of humans. IoT devices are utilized in many applications such as social media applications, smart homes, smart devices, etc. [146]. Moreover, the authors discussed that IoT/WSN data can have both time and space characteristics, allowing and enabling correlation concerning the changing location of devices over time, which they described as a "temporal-spatial correlation."

Table 2.1. Summary of the Precision among the Technologies Discussed

Technology	Accuracy
GPS	Around 10 Meters
WiFi	Can be as good as 1 cm, however, it depends on the software and hardware
IP Address	100 Present for country level, around 30 present for city level

2.5.3 Accuracy of Data-Based Measurements in Other considerable Technologies

The accuracy of IP address georeference to geographical location techniques may be determined by how well it converts an IP address to a ZIP code, city, state, or national location [147]. In [148], the researchers found that the location of the IP of the client independently was very accurate at the national level, achieving approximately 100 current precision. Furthermore, the authors found that the accuracy was significantly poorer at the regional level and that better databases only provided around half of the correct estimates.

When it comes to the city level, the precision was about 30%, with a median discrepancy of about 10 kilometers between the estimated and actual coordinates. Therefore, according to the researchers in [149], the use of IP addresses as digital evidence is critical, but problematic due to the complexity they carry. [150], [151] illustrates that mapping IP addresses to their location has been well-researched in the literature; however, with regard to digital forensic tools, there is yet to be a benefit from existing open-source databases.

Furthermore, data from the carrier network can be triangulated to estimate the location of a device, and the distance between cell IDs that the device visits can be used to estimate its speed; however, the precision of these cannot be compared with the data provided by the device's specific hardware (e.g., GPS receivers)[152], which provides more precise measurements, in general. Table 2.1 summarizes the precision of the technologies.

2.6 Geographic Information Systems (GIS): An In-Depth Look

GIS technology allows the collection, management, and analysis of large amounts of geodata [153]. The GIS may integrate data from several sources. For example, it examines where things are located geographically and utilizes that information to create maps and 3D scenarios. GIS provides the unique ability to dive deeper into the data, allowing users to make better decisions [154]. Many GIS technologies are widely used by government agencies, corporations, and nonprofits in their day-to-day operations. In terms of dealing with space and time, GIS technologies are able to efficiently process spatial components, while also offering sophisticated analytical and modeling capabilities [155]. GIS developments have come a long way since the 1980s, especially in dealing with geographical entities and focusing on human or social traits rather than just geographical limits [156].

According to the dominant academic understanding of GIS, which Goodchild shaped in [157], it is both a collection of tools to collect geographical data and a way of thinking about spatial data. However, according to [158], GIS are vastly different today, at least in terms of technology and the ways utilized to store and transport data because geospatial analysis and GIS as a whole are rapidly evolving. The authors in [158] discussed that in [159] virtual globes software, such as Google Earth [160] made GIS capabilities available to the public and have acted as a catalyst for these developments.

2.6.1 GIS Concepts and Components

Along with geodata and metadata, some common terminologies are used in GIS, and they are:

- Vector Geodata: Information and the representation of geodata on a map shown as dots (points), lines, or polygons based on mathematical formulas or explicit location (i.e., X, Y, Z) [161], [162]. There are three main types of them:
  - Point: Is the representation of a geographical feature too small to be shown as a line or area, or has distinct X and Y [162].

  - Line: A set of ordered coordinates that are used to show the geometry of narrow linear objects such as contours, highway center lines, and streams [162].
  - Polygon: This is a geographical feature defined by a collection of properties associated with the polygon and consisting of a closed line.

- Raster Geodata: Data representing geographic features as a grid of cells or pixels, each cell containing a value representing a feature or attribute [161]–[163].
- Projection: A mathematical method that can flatten the curved surface of the earth while retaining as much of its shape, distance, and area as feasible [164].
- Topology: The spatial relationships between geographical features, such as adjacency, intersection, connectivity, separation, or containment [165], [166].
- Geocoding: This converts a textual address or location description into latitude and longitude coordinates for a map [167]. Moreover, geocoding involves comparing an address or location description to a reference database of streets, cities, and landmarks and then calculating the location's geographic coordinates.
- Reverse Geocoding: This is the process of converting geographic coordinates into textual addresses, whereas address geocoding converts addresses into coordinates [168].
- Georeferencing helps GIS, remote sensing, and mapping users overlay, compare, and analyze geographical data. Georeferencing aligns maps and photographs, corrects size and perspective errors, and integrates diverse data into a geographic framework.
- Geoprocessing: This GIS framework analyzes, manipulates, and transforms geographical data [169]. Geoprocessing uses geographic analysis to generate new data sets and information and solve complicated problems using spatial analysis frameworks [169].

2.6.2 The Forensic Role of GIS and Spatial Analysis in Forensics and Digital Forensics

GIS incorporates various forms of data layers, using data structures based on geographical location. In particular, the data have a geographical dimension and are considered to be

a significant part of the geographical aspect. The GIS data set includes a base map that overlaps images, locations that can be expressed in various ways, and various data linked to tables. To this end, geospatial data and GIS technologies have a forensic role to play.

One of the first times location data were used to solve a large problem was in an epidemiological investigation, which helped figure out what was going on with cholera in London in the middle of the nineteenth century. Studies and research discussed by John Snow and Henry Whitehead in [170] have been completed. They were looking for clues and trying to build a chain between events with the help of location and mapping, which led to solving the mystery of cholera. Whitehead worked on local investigations, and Snow used scientific methods to collect data. As a result, the ghost map, which was the product of the study, is often considered one of the first known cases in which geographic knowledge and location-based data were used to understand an epidemic [170].

On the other hand, in digital forensics, many spatial information is omnipresent inside devices seized and discovered at a crime scene or devices used in committing crimes. It can provide many valuable clues when analyzed. Spatial analysis allows us to properly assess and forecast our knowledge, comprehend and understand trends in human activity and their spatial representation, assist us in decision-making, and a variety of other spatial analysis applications [171].

In addition, there are many types of geoprocessing technologies in GIS. Many of them allow buffering, overlaying, intersecting, and geographic statistics. These allow one to perform a spatial analysis of points, lines, or polygons. Therefore, geoprocessing can help analysts, investigators, and decision-makers understand spatial patterns and relationships, make informed judgments, and solve complicated spatial challenges in complex investigations.

2.6.3 GIS: As a Digital Forensic Tool

GIS technology can allow an investigator to collect, manage, and analyze large amounts of geodata. GIS can integrate data from various sources. For example, it examines where things are located geographically and utilizes that information to create maps and 3D scenarios. GIS may provide investigators with tools and the unique ability to dive deeper

into geodata, allowing users to make better decisions [154]. GIS technologies can efficiently process spatial components while offering sophisticated analytical and modeling capabilities [154], [171]. Moreover, it can deal with space and time aspects to provide spatiotemporal analysis. Therefore, many GIS technologies are widely used by government agencies, corporations, and nonprofits in their day-to-day operations. In addition, it has been helping Law enforcement Agencies all over the world fight and prevent crimes [172]. Therefore, it can be used in digital forensics as a helper tool and for proactive tasks that can help with forensic and digital forensic intelligence tasks.

GIS combines a variety of data layers, many of which are geospatial in nature. Geospatial data are considered to be a substantial component of the geographic aspect of the data. GIS data include a base map that can be added with photos, locations that can be categorized in different ways, and other pieces of information that are linked to a database. Therefore, the author will examine geographic data and GIS technologies, both of which have a digital forensic application. In comparison, digital forensics has a wealth of geographic information stored on seized devices that may provide critical information during the examination of crime scenes or devices used to conduct crimes. Using spatial analysis may improve our ability to analyze and anticipate our knowledge, grasp human activity patterns and their geographical representation, and use that information to make more informed decisions.

In addition to all of this, GIS can leverage analytical powers that provide geospatial analysis, which is still not integrated into digital forensic tools and processes. Therefore, geospatial information technologies have a crucial forensic role to play here. GIS is one of the most popular technologies. It has tools that combine many different types of data layers by using data structures based on where they are in the world. When the data have geographic dimensions, it is a handy tool.

Moreover, many techniques can be used to help investigate without compromising or missing implicit geodata. Geocoding is one of the most widely used processes, which starts by taking information and turning it into its geographical location. This process aims to take any information that can be tied to a location and turn it into the latitude and longitude of that location so that it can be easily recognized by most tools. For example, you can geo-locate an IP address to an actual location.

2.6.4 Spatial Analysis in GIS: A Forensic Perspective

GIS incorporates a wide variety of various forms of the data layer, leveraging geographic location-based data structures. Much of the data have a geographical dimension and are considered to be a significant part of the geographical aspect. GIS data contain a base map that overlays with pictures, locations that can be expressed in many ways, and various data connected to tables. To this end, geospatial data and GIS technologies have a digital forensic role to play that needs to be studied.

However, in digital forensics, much spatial information inside devices seized found at a crime scene or devices used in committing crimes is omnipresent and can provide valuable clues when analyzed. The authors [173] discussed that patterns and frequency of geodata from many sources and applications are needed. Therefore, spatial analysis enables us to adequately assess and forecast our knowledge, comprehend, and understand trends in human activity and their spatial representation, assist us in decision-making, and many other applications of spatial analysis.

2.6.5 Interpretation and Visualization

Forensic tools must combine interactive visualization with automated ways of analyzing data to show data in unique ways and allow investigators to guide the investigation interactively. Maps are useful tools for narratives [174]; therefore, to take full advantage of evidence-based story reconstruction, the geographic context must be taken into account when evaluating the data presented. Therefore, it is critical to undermine every possible technique that can be used to deal with geodata to provide relevant information that can later be used to help the investigator by adding a geo-contextualization dimension.

In their book [175], Harrington and Cross discussed how Google Earth has helped digital forensic investigators use maps and street photographs to integrate them into seizing, acquiring, examining, and reporting. Furthermore, researchers in [176] have discussed geospatial forensic tools that can be incorporated into digital forensics and GIS methods. The authors also devised a model for a forensic GIS environment that can be used as a guide. They men-

tioned that there is a substantial need for customized tools that use GIS to meet investigator requirements [176].

2.7 Intelligence

Another example of the many techniques to unlock the full potential of geodata is the use of OSINT. OSINT is also known as "open source intelligence" because it is based on publicly available and accessible data sources. Furthermore, Hassan and Hijazi in [177] talk about OSINT and identify digital forensic investigators as the primary target audience for their work. OSINT approaches are becoming more critical in enhancing existing models and frameworks. In [178], a team of researchers developed a strategy that combined DFINT with OSINT and then used Maltego as a significant tool to aid in the process. OSINT can also be a tool to geolocate different data that can have the possibility of having a geographical extent. Many fields have benefited from many intelligence domains, such as location intelligence and open-source intelligence. However, due to the focus on the forensic soundness of the recovered evidence, these techniques have not been studied with thought. However, they can add to existing guidelines by providing investigators with valuable insights using geodata recovered from cases from crime sessions to help build insightful reports.

Furthermore, OSINT may provide investigators with possible ways to approach the problem faced in an investigation because current digital forensic processes and tools are not well optimized to deal with all types of geospatial data. In civil and criminal cases, it would be very beneficial for the investigator to use publicly available data to help build relationships and discover unknowns that can lead to better connections between evidence. Furthermore, OSINT may be practical in providing a rich source of information that can help geo-contextualize the events.

2.7.1 The Role of Intelligence in Proactive Decision-Making

Explore how intelligence domains (such as location intelligence and open source intelligence) can add to existing guidelines by providing investigators with valuable information using geodata recovered from cases ranging from crime sessions to helping to build insightful

reports that show patterns of behavior for a user using smart devices. Consolidate digital evidence. Many techniques can transform data into notable and actionable intelligence. According to S. Gibson in [179], intelligence provides independent information to decision-makers that are timely, accurate, relevant, verifiable, answers a question, and allows for proactive decision-making.

2.7.2 OSINT

OSINT is intelligence gathered from publicly available and accessible data sources [180]. Furthermore, in the Hassan and Hijazi book [177], they have listed digital forensic investigators as one of the primary target audiences. Increasingly, there is a need to incorporate OSINT approaches to improve current models and frameworks. For example, researchers in [178] created a technique in which they combined DFINT and OSINT and then used Mtheltego as the primary tool to help the process [181].

2.7.3 Location Intelligence (LI)

It is critical to undermine every possible technique that can be used to present geodata to provide location intelligence, accurate and relevant information that can later be used to help the investigator in a given case, as geolocation information with all its types would be considered as enormous potential clues and provide evidence for digital forensic investigators. Arguments for good documentation and presentation come to another level when dealing with evidence containing many geodata types. Reporting and displaying these data require analytical and categorical skills to convey precise information. In cases where their geodata is present, they can guide or give the investigation an extra spatial dimension as a reference for time.

2.7.4 The Confluence of Digital Forensics, GIS, and Multi-Intelligence Domains for Geodata

Multiple geospatial analytical techniques and multi-intelligence domains, including location intelligence and open source intelligence, can aid investigators and generate an ex-

ceptional understanding of the spatial and temporal behavioral patterns of users of smart devices. These techniques may help discover, identify, and uncover hidden spatiotemporal patterns to provide geo-contextual reasoning that improves evidence investigation, collection, illustration, visualization, and reporting. Therefore, there is a need to study the confluence of digital forensics, geographic information systems, geospatial analytical techniques, and multi-intelligence domains for geodata in digital forensics and how it can improve investigations.

3. REVIEW OF LITERATURE AND STUDIES

The purpose of this chapter is to review the related literature on the problem studied in the research.

3.1 Geodata in Digital and Cyber Forensics

Geodata are one of the many types of data digital forensic investigators come across in any investigation. This is because geodata have become an important asset that developed applications have started using and collecting to optimize and help improve their applications, restrictions, and services provided to meet the user's expectations. Many technologies, including, but not limited to, smartphones, cars, tracking devices, watches, computers, laptops, cameras, drones, robots, and others, preserve and utilize geodata. Therefore, location data is considered of great value and has become essential in the digital forensics domain. Additionally, it may provide forensic analysts with valuable leads, which can aid forensic investigation and design-making. The following subsection explores research studies related to geodata in the fields of digital and cyber forensics.

3.1.1 Smartphones

In a recent study, researchers in [120] have found important information about the user's whereabouts recovered from different artifacts. The authors were able to identify the user's general location based on data exchanged in the apps, along with some applications that store IP addresses. Taking into account the importance of the IP address in the cases demonstrated and how it can generally locate the user, researchers in [120] have demonstrated a tool that can be used to geolocate IP addresses found in a case and cross-validate if any of these IP addresses are of importance to investigators. It was found in this study that there was one IP address that had hit at a city-level accuracy because it intersected geotagged images within the same case. They were even able to find the same IP address of the user but with another digital forensic image of the device that had a newer operating system. On the other hand, the researchers in [2] examined more than 28 apps for the iOS and Android

operating systems and found that there are many apps that keep geodata (e.g., GPS, IP address) stored.

In addition, the authors of [23] have found that GPS data gathered from the device can go back seven days before the image is taken. Their study used Apple and Android devices to control a DJI Mini 2 drone. The authors found that the Apple device had obliterated any information written in the iPhone database storing location data after a while. Therefore, investigators must acquire the devices as quickly as possible. Moreover, the author in [182] has made a great deal looking into iOS cashed geolocations data and have concluded that the system collected data are protected against third-party faking apps, which arguably makes them forensically valuable.

Never before has it been so easy to record, observe, and investigate the whereabouts and activities of people using GPS information from mobile phones. This allows for various exciting new uses that depend on accurate location information. The authors of [183] have looked at different mapping applications (e.g., Google Maps, MapQuest, Waze, Bing Maps, and Scout GPS) on Android and iOS OSs. They found valuable location information for the user's navigation requests. Similar findings for HEREwego and Waze applications were highlighted in [184].

Furthermore, the Life360, a popular family locator app, was examined on an iOS device, and researchers in [73] found that GPS coordinates were recoverable. Furthermore, they found that the iSharing app keeps the user's location on Android devices [73]. Moreover, in [185], the authors completed a forensic analysis of the same Life360 app, where the authors demonstrate the extent and types of forensic artifacts and sensitive data that could be acquired using commercial and open-source tools from the app on iOS and Android devices' digital forensic images. For example, the geolocations and addresses of the user and other contacts in the app were significantly recovered artifacts, along with much other sensitive information about the user. Moreover, the authors highlighted that devices' network traffic artifacts also could hold many valuable information and that devices that have not been jailbroken could still be used to retrieve some information, including those running more recent versions of iOS.

Even in mobile games, GPS information is present. For example, the PokeonGo game was analyzed and found to keep records of the user's GPS location in log files called 'Crittercism' [186]. On the other hand, the vehicle path and the location of the user were recovered from the UBER app [187], [188]; finally, in a comprehensive forensic analysis of two OSs (i.e., Android and iOS), researchers in [2] found multiple apps that keep GPS-related information on the device.

3.1.2 IoT and Wearable Devices

The prevalence of portable devices in our daily lives has expanded as there is a movement towards a healthier lifestyle, which has fueled the user's concerns about accurately measuring, improving, and maintaining their health and fitness levels. Additionally, forensic investigators increasingly view them as critical evidence due to the widespread use of smartphones and wearable devices in our daily lives. As evidenced in several recent court cases, these wearable devices came in handy, where they have been corroborated to prove and disprove the suspect's whereabouts. The information stored within and in their smartphone apps has helped create a timeline that describes the leading events in a crime.

Although smartwatch shipments did not increase dramatically in 2020 due to COVID-19, Apple could increase its market share to 40% of the total market share of smartwatches and maintain its dominance against many other competitors [8]. Furthermore, in 2020, Apple managed to ship around 30.9 million Apple Watches [8]. For a device of such a compact size, the Apple Watch is indeed very powerful. With every new model, they are getting smarter and more versatile; many things can be done with them depending on which model/series; this ranges from viewing incoming notifications, tracking activities, monitoring heart rate, and measuring blood oxygen levels to taking an ECG that is only available on the latest model.

Due to the capabilities of wearable devices, fitness trackers can be used as substantial evidence in criminal prosecutions. For example, they can be instrumental in describing a victim's behavior or physical condition in the moments leading to death. Moreover, they may

contain related information that could also be useful in determining the suspect's activities and movement in spatiotemporal dimensions.

Therefore, researchers in [189] have investigated the Fitbit Versa 2, which is a common brand of wearable trackers in the Fitbit line of products. The authors have examined the information that the mobile application generates and stores. In addition, the authors have highlighted many information stored in plain text, such as the user's credit card number, heart rate, and most importantly, GPS locations [189]. In another recent study of a forensic analysis of Fitbit Versa on a Google Pixel device running Android 10 and an iPhone 7Plus running iOS, Fitbit Versa found that when it detects activity, it starts recording the activity the location of the user [190]. Moreover, the authors found that the activity logs keep user speed [190]. They also mentioned that when GPS connectivity is unavailable through the fitness tracker, the app uses a feature to use the GPS location from the paired mobile device [190].

In an exciting work, the researchers in [191] took the populating fitness trackers (e.g., Ionic smartwatch and the Alta tracker) to an additional step, where they used Fitbit devices in three different ways to fill and collect data: on a desktop computer, on a mobile device, and on the Web. They found that the data were stored on the Fitbit device until it pushed these data and synced them to the cloud using the app's desktop, web, or mobile versions. The authors also claim that they were the first to recover evidence that the data logs were then synced in one of the three ways (i.e., desktop, web, and mobile apps), and this could have helped them understand why the GPS logs were only being populated and synced using the mobile app version. In similar research, both the Ionic and Alter trackers were used, but this time to measure accuracy [192]. The researchers found that these two trackers are in the proper settings, providing accurate GPS tracks. The authors were able to recover from both trackers and argued that these artifacts are important to look at if they were to appear in a case.

Furthermore, the Fitbit Alta HR tracker was also investigated, and researchers in [193] found that it keeps activity recorded together with GPS data within the SQLite3-formatted exercise database called *exercise_db*. Similar findings were also reported by [194] for Amazon Halo, Garmin Connect, and Mobvoi on an Android smartphone device. They even found that

the Garmin Connect application stores explicit and implicit geodata of the user. Therefore, the application could locate users with city-level accuracy without a smartphone's GPS. Forensic investigators may like these apps' location data, even if the user doesn't register workouts; this tracking may help detectives discover a suspect near an incident. Moreover, users of Connect the Warables with their application do not realize that their devices are tracking their whereabouts whenever they go to a new/different place. In addition, many other IoT devices have started to collect geodata. For example, GPS information was restored from one of the IoT lamps in the study [195]. The researcher was able to locate where this lamb was set up.

3.1.3 UAV

Researchers [97] demonstrated the use of 3D mapping for drone paths and discovered an issue in the Cellebrite forensic tool when it comes to visualizing the paths. The authors demonstrated differences in results and findings between the four tools used for UAV forensics. First, they illustrated that none of the tools is capable of displaying 3D data even when the elevation was recovered. Second, non-reproducible results may cause substantial issues with the integrity of recovered evidence. Finally, the aggregation of GPS locations may lose the accuracy and completeness of recovered evidence.

Furthermore, the researchers [23] were able to extract valuable PII that would help investigate. The authors were able to recover the location of the first time the iPhone was used to connect to the drone, which in their experiment was the setup location. They assumed that the location was obtained by phone rather than by drone since they set the drone inside a building with poor GPS signals for the first time. Furthermore, the researchers could only decrypt the flight log files containing GPS and sensor data using the https://airdata.com/ website, which is not developed for digital forensics. This is crucial because the encryption used cannot be decrypted using the digital forensic tools they used, and this could cause the investigator to have interpretation and analysis issues.

Furthermore, in terms of UAVs, researchers in [196] were able to restore GPS logs within log files that have the.DAT extension of DJI Phantom 3. Similarly, in [23], [24], [96], [97], [99],

[197]–[199] studies show that many types of drone keep and store GPS data and highlight the importance of recovering GPS tracks in UAV forensics.

3.1.4 IP Addresses

IP addresses are personal identifiers that employ various technologies to link people's physical locations to their IP addresses. The importance of IP addresses was highlighted in a recent digital forensics framework by Dimitriadis et al. [200] that focuses on investigating and reviewing cyber attacks. Furthermore, according to [201], using consecutive IP addresses by hackers can help investigators decipher geospatial and temporal patterns by revealing their digital fingerprints, leading to their identity.

According to [150], [151], the literature showed that mapping IP addresses to their geolocation has been thoroughly studied; however, the researchers in [120] have discussed how it has not yet been applied to digital forensic tools. The authors have demonstrated that IP address preservation can help researchers predict important locations in applications that keep these records. Although geocoding IP addresses requires additional effort and is not accepted by digital forensics software, valuable information has been demonstrated, including location-relevant information [120]. In this case, the authors demonstrated a connection between two different digital forensic images by highlighting that both have the same IP address, which brings them to the same geographic location, as verified by the spatial technique they followed.

Furthermore, researchers in [2] have illustrated that IP addresses can be recovered from applications such as WhatsApp, Telegram, and TextNow, as well as many others. According to [120], these applications use IP addresses to approximate the user's position even when the device's GPS is disabled, which endangers the user's privacy if it is preached. Research in [149] has discussed how crucial but challenging it is to use IP addresses as digital evidence in different investigations due to their complexity. Researchers in [202] discussed how the IP address is important in identifying the location of criminals and illustrated through a digital forensic case that applications such as Skype, which records local and public IP addresses, can be used to investigate a case further. Although researchers in [202] discussed how no

GPS data were recovered from the Whatsapp application, researchers in [2] could recover the IP address that helped them locate the user on Whatsapp. IP addresses were recovered from Instagram, Threads, WhatsApp, Skout, Telegram, Imgur, TextNow, Gallery Vault, and Skype on Android 10. Investigators can estimate the geographical extent of the case using recovered IP addresses along with other geodata. Many digital forensic tools do not currently enable geocoding of IP addresses, but it has been shown to provide important information, including geographical data [120].

Despite the fact that there are around 4 billion potential IPv4 addresses expressed in human-readable notation [203], there is a newer protocol called Internet Protocol version 6 (IPv6) that effectively replaces IPv4 and is widely used by many devices such as IoT [204]. According to [120], this will lead to new challenges in geocoding these IP addresses. Furthermore, a new academic study in [146] has discussed earlier concepts and designs for an edge management system produced by Oriwoh in [205] and emphasized how IP addresses from IoT devices can be recovered as evidence. Furthermore, a researcher in [195] discovered that the IP address is stored in a smart light bulb in the chip-off revered data as a result of his IoT forensic work.

3.1.5 EXIF data

The EXIF standard includes GPS tags, which are saved in a distinct IFD (Tag) from the rest of the EXIF data [206]. The EXIF data are embedded in the image file itself, and many modern devices (e.g., smartphones and digital cameras) are capable of embedding these data into the images taken. Moreover, many image editing software and readers can recognize and preserve EXIF data from the original image if it still has it. On the other hand, drones often have cameras to capture photos and videos, and these camera modules store GPS data from the GPS sensor on the body of the drone [199], [207], [208]. Therefore, the researchers in [197] found it essential to examine the two DJI Phantom 3 Professional and AR drone files using EXIF readers such as ExifTool [209].

3.2 General Gaps and Challenges

Since the public was first informed of the expanding importance of digital forensics, many years have passed [13], [14], and, over time and with the rapid advancement of digital devices, geodata are among the common challenges facing the digital forensics community.

With a volume of big data in certain cases, investigators are straying with investigations with large data [32] and if more than one case happens to be at the same time with big data, it is difficult for investigators to juggle them all effectively [11]. Other issues that have arisen as a result of technical improvements include, but are not limited to, lack of a road map for investigators, anti-forensic techniques, encryption, and visualization. Furthermore, digital mobile devices are increasingly ubiquitous with a wide range of hardware and software [59], which can create substantial obstacles to digital forensic investigations.

The literature shows that the use of geolocation and geospatial data has increased dramatically in the last decade; these rates have been directly influenced by smart devices and technology that enable data collection and usage. However, only a few digital forensic tools and frameworks have mimicked this increase and have begun to incorporate some capabilities and features to deal with this evolution. Garfinkel in [14], discussed the absence of standard abstractions and data formats; moreover, the author discussed that many existing digital forensic software is still following what he called the visibility filter and report model. This model is built on identifying the information and then presenting it to the investigator in an elegant way.

Garfinkel also mentioned in [14], that there is a need for digital forensic tools to overcome some of the challenges related to visual analytics by integrating techniques that help to guide investigations better. In addition, it is an enormous burden for the digital forensics community, where most current digital forensics models and processes lack comprehensive techniques to deal with geospatial data.

The following sections present an overview of the gaps and challenges related to geodata that affect the geo-contextualization efforts on data collected from mobile devices in digital forensic investigations.

3.2.1 Big data

Moreover, large amounts of data created from many sources are increasing challenges in the field of digital forensics [32], [210]. Despite the wide variety of definitions and distinctions, there are certain commonalities found in many definitions of big data, with at least one including size, complexity, and technology [211]. Therefore, according to [212], big data have many essential dimensions and characteristics; the following are some that can be found challenging digital forensics:

- Volume: large amounts of data that are generated and stored. This is one of the most challenging challenges in digital forensics, where the ever-increasing volume of data has to be evaluated.
- Velocity: this means many things, including the rate at which data are generated.
- Variety: Different types and formats of data.
- Veracity: Uncertainty and inherent inaccuracy of certain data sources.
- Value: With big data comes the question of how to create value from it. Therefore, data analysis yields excellent results when dealing with large data sizes.

3.2.2 Legal Issues

The challenges are not only limited to the complication of data recovery; the conduct of digital forensics is becoming increasingly difficult, time-consuming, and expensive as a result of a plethora of legal stumbling complications [213]. Due to the lack of defined methodologies and procedures, the importance of digital evidence is affected in judicial proceedings [28]. As an example, in *Bradley Cooper vs. the State of North Carolina*, the only irrefutable evidence came from the suspect's Google Maps-cashed search and pictures indicating exactly where the victim's corpse was recovered [28], [214]. However, due to the way evidence was handled, this evidence was in question in this trial [28].

In a court, the admissibility of evidence is critical [215]. Furthermore, according to [215], [216], the proliferation of mobile phones and their ongoing development of new capabilities

have made their admissibility increasingly difficult. The admissibility criteria are designed to ensure that any data kept in a digital format is not modified or altered in any way. The rate at which laws are modified and changed to keep up with the speed of change in the technological environment often falls behind the rate at which these technological devices advance [217]. Furthermore, [218] addressed how, rather than just being reactive in understanding and applying the law to new technologies, the law must play a more proactive role. When there is a lack of technical understanding, the law can be misapplied, and technological reasoning or evidence can be misused [219], [220]. Therefore, the approaches must be scientific and fairly hold forensic soundness to advance techniques that involve geo-contextualization and ways to deal with geodata.

Moreover, in the following subsections 3.2.3, 3.2.4, 3.2.5, and 3.2.6, we will explore the gaps and challenges in each of the mobile digital phases proposed by NIST [81], respectively.

3.2.3 Preservation

Evidence collection and preservation must be handled with care to protect its integrity throughout the investigation, as it is one of the most important aspects of the digital forensic process, and any mistake can have catastrophic consequences [221]. The acceptability and importance of each geodata data vary according to the situation and the environment of each incident. Therefore, starting from the crime scene, there are many challenges that first responders face with regard to the preservation of digital devices. Responders have to pay attention to the details and be careful when securing devices. The handling of mobile devices and IoT devices that are found and running at the time of the preservation stage must be carefully documented and preserved. Moreover, where and when it is applicable, many important elements are often not highlighted by digital investigators dealing with preserved devices later. For example, how exactly was the device found? Is there anything around the device that can help us gather some geographical information about where the victim was before the crime?

3.2.4 Acquisition

The use of geolocation and geodata has increased significantly in the past decade, and this has been attributed to the advent of mobile technology that allows the collection and use of such data. However, some forensic tools are trying to ride the wave of this trend by adding new capabilities and features to deal with it. According to [222], the lack of standards for a wide range of devices makes it impossible to access, extract, or retrieve data consistently. Therefore, to keep up with the latest technical advances, digital forensic tools try to include the most cutting-edge digital technologies from other sectors in the digital forebode system. Several high-end tools for digital forensics, both open source and proprietary, started to emerge as a result of this development, such as Autopsy [15], Cellebrite [17] and Magnet AXIOM [18]. Digital forensics has been classified into many sorts depending on the technology employed (e.g., computer forensics and mobile/IoT device forensics).

Yet, there are numerous issues to cope with since these technologies are always evolving. Forensics on mobile devices, for example, has become more complex because of the devices' increasing capabilities, and they have grown into small computers with significant storage, which is causing a lot of issues in the acquisition phase. Digital forensic tools are constantly searching for new ways to obtain access to, recover, analyze, and visualize geodata from these devices, as they are constantly changing. However, according to Barmpatsalou et al., [173], forensic tools focused their attention on acquisition processes rather than other aspects of the investigative process model. Furthermore, according to SWGDE in [223], the lack of available training, appropriate tools, research, and data collection methodologies impedes the capture of data from IoT devices.

There are many strategies and techniques that can be used at each step in a variety of ways. Many factors come into play, such as what kind of technologies and equipment are being investigated, the location of the evidence, and even the type of investigation. Mobile devices can provide a wealth of information about their owners. Garfinkel noted in [14] that there are no universally accepted standard abstractions and data formats. Furthermore, many current digital forensic tools still adhere to the "visibility filter and report approach,"

as described by the author [14]. Identifying the information and then presenting it in an attractive manner is at the heart of this methodology.

In this phase, the objective is to extract as much information as possible from the phone and storage. To achieve this goal, there are several ways to it, and the methods vary greatly depending on the exact smartphone in question (e.g., logical and physical) [81], [111]. However, when it comes to collecting and evaluating data, today's examiners and investigators face a wide range of challenges. Mobile devices have become increasingly involved in digital investigations and civil and criminal cases. Therefore, for investigators, knowing the difficulties they may face is essential. Geodata recovery is challenging, even with the most modern digital forensic equipment. Many of these programs rely significantly on EXIF tags, artifacts, or other file formats that may include and display encoded GPS coordinates, such as those found in digital photographs (e.g., audio, video, documents, spreadsheets, databases, etc.). The EXIF data are embedded in the image file itself, and many modern devices (e.g., smartphones and digital cameras) can embed these data in the images taken.

However, the researchers in [224] found that AXIOM autopsy and magnet forensic tools did not recover and report all EXIT data compared to ExifTool software. The ExifTool software was able to report more data, such as the speed and direction of the images [224]. Furthermore, in [225], researchers investigated images from the Pokemon Go app captured by the smartphone with timestamps. Although these images were clear that they were at some location, researchers were unable to find the GPS coordinates of the EXIT of these images. Therefore, they concluded that we could at least use the timestamp to determine that the user was at that location at that time. Therefore, the researchers used the Internet and search engines to find locations that are shown in the background of Pokemon or the arena shown in the image. It is fair to say that the researchers in this article have used OSINT to help identify the location of the image.

Volume, velocity, variety, veracity, and value

Although potential sources of geolocation evidence can be files that contain geotag or geolocation information on such devices, many other challenges pose investigators dealing with

today's technological advances. The challenges have not only changed, but they have anticipated five V's (i.e., volume, velocity, variety, veracity, and value) and increased complexity in all dimensions.

In addition, there is always the possibility that, with new updates for operating systems or applications, there may be a change in the file structure to where important and relevant data can be stored [225]. This is a considerable challenge facing all tools and investigators. In addition, there are millions of applications with many different mobile operating systems. These varieties of operating systems are proprietary or open-source, making it even more difficult for tools and procedures. Apple's iOS is the second most popular mobile operating system, after Android [226]. In June 2021, Android retained its status as the world's most popular mobile operating system, with a market share of close to 73 present [226]. On the other hand, IoT devices create a large amount of data, and this number is only increasing as IoT devices shrink in size [227]. Although analytical solutions could help and enable investigators to obtain valuable information from the large data generated by IoT devices that are stored within mobile devices, many digital forensic tools lack the capabilities for different reasons. The ability to quickly extract and analyze these data can reveal previously unknown facts, patterns, and connections that can be used to improve decision-making [228].

Encryption Encoding and Privileges

Due to the fact that there is a continuing movement toward privacy, many applications have started to use encryption mechanisms. There are many examples that demonstrate that the challenges related to encryption and geodata are not different from other types of data when it comes to importance. Therefore, there have been many attempts to preserve the privacy of the user or enable a type of encryption that makes it difficult for tools. Both encryption and cloud computing pose a risk to forensic visibility [213]. Additionally, due to the increasing usage of encryption, acquiring digital evidence is extremely difficult in cases where these files cannot be decrypted. For example, researchers in [23] were able to recover two formats of DJI Mini 2 flight logs on the mobile device that controlled the drone; however, they were encrypted and researchers had to use a special way to decrypt them

that is not currently available in the digital forensic tools they used in their study. Another example of geolocation stored as base64 encoding in [195], the researcher was able to recover the latitude and longitude of the IoT device stored in base64 format. On the other hand, on Android smartphones, the authors of [186], [229] presented methods to perform forensic analysis of geolocation data stored in a variety of location service applications. Google Maps and Pokemon GO are two examples of such applications. However, the device was rooted to collect these data.

Cyber security and Privacy Concerns of Geodata

Researchers in [230] found numerous vulnerabilities in the use of LBS while individuals actively posted check-ins on Twitter. The researchers focused on Twitter's privacy policies; however, little research has been done into how these check-in artifacts are stored on phones or whether they pose any additional privacy or security risks. Furthermore, researchers in [2], [231] found that when a user communicates with a location in real-time, several applications on different operating systems, including instant messaging applications (IMA) such as WhatsApp, Facebook Messenger, Instagram, and many others, these apps use the user's phone GPS data and store them in unencrypted format. When more accurate and precise data are collected, it has always been the case that results in better service outcomes for the user; however, users will lose their location privacy during this process. Although it is possible that location privacy can be reached by disabling services that use geodata or even permit using them, users will lose many beneficial daily applications, which are provided by LBS that offer helpful apps such as real-time maps, the ability to locate locations of interest nearby (e.g., businesses and restaurants) that many people search for daily.

Great efforts and research work have been made before, where many methods have been developed to address the problem of user privacy and identification concerns. However, most of the solutions developed previously help increase user privacy when the user requests a query and do not support real-time moving privacy solutions.

3.2.5 Examination and Analysis

The investigator's ability and the forensic tool play an important role in the examination phase. Currently, digital forensic tools are trying to cope with the advancement in technology and aid their capabilities with the latest and the greatest digital technology that has been used in other senses and try to adapt it to the digital forebode system. In addition, the digital forensic investigator must have the ability to think spatially to uncover and solve cases where geodata would be helpful in the investigation.

Digital forensic tools and techniques can occasionally fall behind rapidly emerging technologies, leaving them unable to deal with the issues that arise from these emerging technologies [210]. One of the many challenges related to tools, mentioned by Garfinkel in [213], is that current tools, instead of aiding investigations, are designed to make it easier for investigators to locate specific pieces of evidence, which is only half of the problem. Furthermore, most end users are unable to access and use open-source technologies provided by academic researchers [213]. Furthermore, there is a significant absence of modern technologies that allow correlation between various forensic events [232].

Therefore, better geocoding mechanisms and procedures can help investigators. Researchers in [230] found numerous vulnerabilities in using LBS, while individuals actively posted check-ins on Twitter. Researchers focused on Twitter's privacy policies; however, little research has been done into how these check-in artifacts can be used to build day-to-day stories of the user. Furthermore, researchers in [2], [231] found that when a user communicates with a location in real-time, several applications on different operating systems, including IMAs such as WhatsApp, Facebook Messenger, Instagram, and many others, use the user's phone GPS data and store it in an unencrypted format.

Implicit Geodata

Researchers in [143], have conducted a study to highlight the challenges and opportunities related to the use of the Service Set Identifier (SSID) as a geodata to be used in forensic investigations. The authors have highlighted the importance of SSID as a passive digital fingerprint that can help provide a location for captured 802.11 client devices. As a result,

the study proposed the use of SSID geolocation as a supplement to the discovery development process, but not as a key input that can be used alone [143].

Using Internet Protocol (IP) addresses as digital evidence is critical but difficult, due to the complexity they carry, according to researchers in [149]. It is possible to associate an individual's actual location with their IP address using a variety of different methods. Furthermore, according to [201], investigators dealing with hackers can benefit from analyzing location- and time-based patterns by using consecutive IP addresses, which reveals their digital fingerprint, leading to the identification of important clues related to hackers.

According to [150], [151], the geolocation of IP addresses has been extensively studied in the literature. However, researchers have explored the lack of implementation of digital forensic tools in [120], where the authors showed that the preservation of IP addresses can help researchers predict crucial locations from applications that save this information. The digital forensic tools used by the researchers in [120] did not support IP address geocoding but have been shown to provide useful information, such as general city-level geodata. Furthermore, the authors were able to find the connection between the two phones using their purpose-built spatial analysis.

Furthermore, the researchers in [2], discussed that there are many applications that are used by many people that store the IP address of the user, which can be retrieved to locate the user. In addition, they were able to recover the IP address that helped them locate the user on Whatsapp. IP addresses were recovered from Instagram, Threads, WhatsApp, Skout, Telegram, Imgur, TextNow, Gallery Vault, and Skype on a device running Android 10. Investigators can estimate the geographical extent of the case using recovered IP addresses and other geodata. Many digital forensic tools do not currently enable the geocoding of IP addresses but have been shown to provide important information, including geographical data [120]. The authors also mentioned that the user's privacy is at risk if these applications use IP addresses to estimate the user's location, even if the user deactivates the GPS on the device. Despite the fact that there are around 4 billion potential IPv4 addresses expressed in human-readable notation [203], there is a newer protocol called IPv6 that effectively replaces IPv4 and is widely used by many devices [204]. This, according to [120], will lead to new challenges in geocoding these IP addresses. Furthermore, a new study by academics in

[146] has discussed earlier concepts and designs for an edge management system produced by Oriwoh in [205] and emphasized how IP addresses of IoT devices can be recovered as evidence. Furthermore, a researcher in [195] discovered, as a result of his forensic work on IoT, the IP address stored in a smart light bulb in the data of the revered chip.

Furthermore, the EXIF standard includes GPS tags, which are saved in a distinct IFD from the rest of the EXIF data [206]. Compared to ExifTool software, [224] discovered that the AXIOM Autopsy and Magnet AXIOM digital forensic programs did not retrieve and report all EXIT data. The ExifTool program was able to provide additional data, such as the speed and direction of the image [224]. Therefore, these can pose challenges in the examination and would increase the process that investigators need to follow. Another scale of complexity arises when that location is represented in a text format and cannot be directly extracted as a location. Currently, investigators use location as a search term when dealing with cases where devices have large amounts of files or text-formatted artifacts.

The authors of [183] have looked at different mapping applications (e.g., Google Maps, MapQuest, Waze, Bing Maps, and Scout GPS) on Android and iOS OSs. Although they found valuable location information for the user's navigation requests, they were not able to recover the routes the user acutely took. Furthermore, researchers in [225] faced difficulties in converting the cell ID information recovered from the Pokemon Go application to GPS coordinates. Furthermore, the Life360 application was examined on an iOS-based device and the researchers in [73] found that the user's GPS coordinates were recoverable. Furthermore, they found that the iSharing app keeps the user location on Android devices [73]. Finally, in a comprehensive forensic analysis of two operating systems (i.e., Android and iOS), researchers in [2] found multiple applications that keep GPS-related PII on the device. A summary of some existing research on geodata forensics is provided in Table 3.1.

3.2.6 Documentation and Presentation

Garfinkel mentioned in [14], that there is a need for digital forensic tools to overcome some of the challenges related to visual analytics by integrating techniques that help guide investigations better. Additionally, it is an enormous burden for the digital forensics com-

Table 3.1. Summary of some of the existing research on geodata forensics

Reference	Year	Study Objective(s)	Limitations
[183]	2007	In this study, the researchers studied the most popular smartphone mapping programs for Android and iOS are examined, including Google Maps, Apple Maps, Bing, Waze, and Scout.	Only examined GPS and searched terms
[229]	2011	The Approach allows for the automated extraction and display of all essential geodata from Android devices	focused only on GPS and Text
[143]	2016	In this study, the authors determined whether the spatial dimension can be obtained from fingerprints based on the enumeration of the preferred network list (PNL).	Focused on only SSID
[233]	2018	Developed a mobile forensic investigation procedure and a tool that can recover and analyze GPS information stored in log files	Focused only on GPS
[120]	2021	In this study, the authors demonstrated the usefulness of geolocating IP addressed from mobile devices and then performed a spatial analysis that involved interacting IP locations with geotagged images	Focused on only GPS recovered from EXIF and IP geolocation
[225]	2021	Investigated Pokemon Go app investigated to extract location artifacts	Difficulty to geolocate Cell IDs

munity, where most of the current digital forensics models and processes lack comprehensive techniques to deal with geodata. Although the implementation and significance of the recovered geodata differ depending on the amount of data stored and collected for each case, even a slight hint or hint can help investigators make substantial leaps in complex investigations.

Moreover, researchers in [120], demonstrated the lack of IP geolocation in digital forensic tools and the lack of spatial analysis that in some cases can lead to major findings. As it is the same case, researchers in [97] highlighted considerable differences between the three digital forensic tools in the decryption and visualization of drone paths that are stored in an extension in *.DAT*. Furthermore, they found that the Cellebrite digital forensic tool displayed the incorrect altitude field.

3.2.7 Data Curation

Digital forensics is becoming more difficult due to the vast volumes of data that are generated from a variety of sources that may all happen to be in the investigation. Many definitions of big data have certain characteristics that include scale, complexity, and tech-

nology [211]. Despite the range of definitions and differences, the problem of how to obtain most of the data is what digital forensics is about. In addition, there are millions of apps available for a wide range of mobile platforms, and current tools fall behind by much more challenging structures and data analysis mechanisms.

Therefore, according to [29] big data curation plays an important role in the whole big data value chain, as seen in Figure 3.1. Materials selection and classification, content transformation, preservation, and validation are examples of data curation activities [29]. It is important to think about everything from a multidimensional perspective to choosing the standards and technologies that are needed to implement data curation strategies [29]. Data curation is described as the active and ongoing management of data throughout its life cycle in the context of research, science, and education [234], [235]. Moreover, the ability to identify and retrieve data through data curation is feasible due to the various operations, such as data archiving and data management, and the additional value and usability that they offer whether they were for management or visualization.

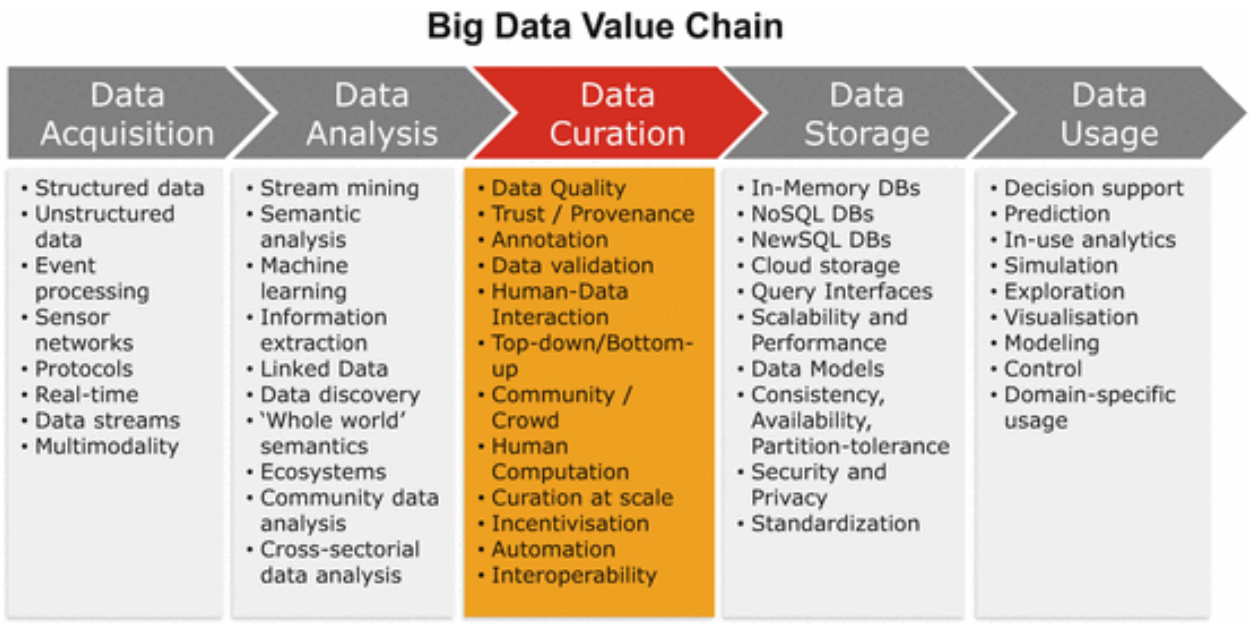


Figure 3.1. Big data value chain [29]

Figure 3.2 is from [236] that provides an overview of the data collection life cycle model, helping to better understand the entire life cycle of a project's activities. It provides a

high-level overview of the phases necessary for effective data curation and preservation, from the time it is first conceptualized or received to the time it is archived. For example, an organization might use the model for planning activities to ensure that all relevant steps are completed in the proper order. As a result of the model, a framework of standards and technologies can be developed and implemented to define roles and responsibilities and provide granular functionality [236]. Although there are many challenges that work against these defined steps in digital forensics, they can help provide an understanding of additional activities that are not necessarily currently in use in the digital forensics community due to challenges to the forensic source of the retrieved evidence. However, in specific circumstances, disciplines, and investigations, these additional steps could help the investigation process by finding additional steps that can be taken to build forensic intelligence and future mitigation plans.

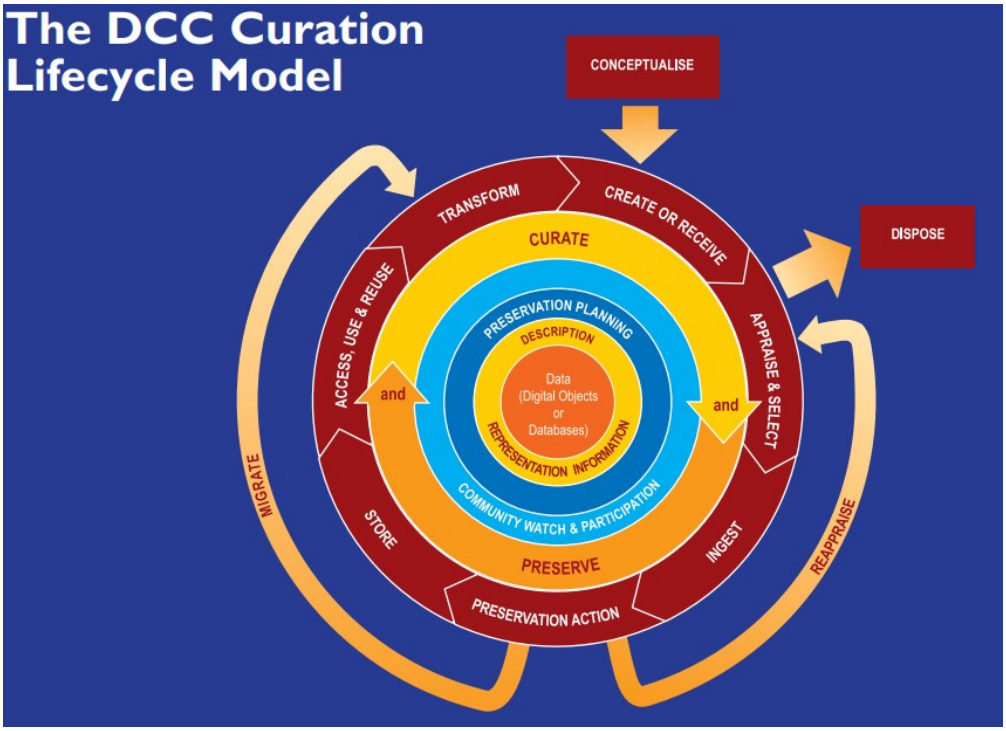


Figure 3.2. Data curation lifestyle model [236]

Furthermore, according to [48], more and more personal information is being used in the services and functions that digital devices provide to help achieve satisfactory operations.

Therefore, many parts of the user's daily life may depend on the truth and integrity of their personal information. For example, if the user wants to search for a nearby gas station, they will reveal their approximate location if they are using mapping services that relay the user's GPS location. As a result, these devices are collecting a considerable amount of data that can be used and help law enforcement if something bad happens; moreover, some digital forensic investigations may have certain big data that are magnetites of terabytes, which can hinder digital forensic investigators [237]. Digital forensic examiners heavily rely on the preservation or missing data in some cases to make their decision-making process; therefore, giving data such that the right amount of accurate description may result in the rise of valuable information that can help build knowledge.

3.2.8 Geodata Curation

Numerous research projects provide investigators with detailed instructions and recommendations but often fall short of highlighting all sorts of geodata and best practices to work with them. With the most advanced digital forensics technologies, geodata may be difficult to identify. For these tools to work, GPS coordinates must be kept in EXIF tags, artifacts, or other file formats that may include and display embedded GPS (e.g., audio, video, documents, spreadsheets, databases, etc.). Despite this, certain digital forensic systems dealing with a large number of GPS records, such as in Unmanned Aerial Vehicle (UAV) flight routes that may also be encrypted, still have difficulties dealing with basic GPS data [24]. When it comes to encrypted flight record data, digital forensics solutions (such as those from Autopsy, Cellebrite, and Magnet AXIOM) do not meet the necessary detail to provide full recovery and visualization, according to [23], [24].

Furthermore, it is clear that not all geodata types are evaluated when populating mobile devices for research use. Only a few forms of geodata are mentioned in the "Quick Start Guide for Populating Mobile Test Devices," which is regarded as one of the most essential publications for populating mobile devices, published by NIST [30]. Section 8 [30], talks about location data and provides limited examples for types of geodata, for example, GPS-related applications and routes were the main focus. Therefore, current research is limited

when it comes to investigating all types of geodata, and it is evident that there are more than simply the mentioned factors to take into account.

According to [29] fundamental principles of data analysis argue that the quality of an analysis is intimately tied to the quality of the data being investigated. Furthermore, concerns about data integrity can have a substantial influence on operations, particularly when making critical decisions [238]. Although current digital forensic tools are coping with advancements, they lack technologies that were designed from the ground up for more complicated geodata curation procedures. Therefore, in order to achieve good geodata curation, in this research we are going to use generic data curation solutions that are built on dealing with such data; moreover, we are going to provide two case studies that we will use for data curation that are briefly presented in their investigation to show the current dynamics and future demands in digital forensics.

3.2.9 Threats to the Validity of Geodata Curation

Many threats can encounter the validity of the geodata curation process in digital forensics. The following subsections are going to dive into advancements in security and privacy measures along with anti-forensics techniques area, making it harder for data curation in digital forensics.

Advancements in Security Measures

Many applications now use encryption techniques as a result of the growing trend toward privacy. Attempts to protect user privacy by enabling encryption of sensitive personal indefinable information make it harder for digital forensic tools to keep up with the constant advancements in decryption methods. As a result, forensic visibility could be compromised by encryption according to [213], increasing the difficulty of obtaining digital evidence in circumstances where encrypted data cannot be decrypted and is exacerbated by the growing use of encryption.

On the other hand, there is a need for the device to be rooted or jailbroken in order to collect valuable sensitive data. These procedures are not part of many digital forensic

workflows when dealing with mobile devices such as Android, smartphones, and iPhones to enable full privilege to extract as much as possible. This is always a challenge in the real world and for digital forensics researchers.

In an interesting research [23], researchers demonstrated that flight records were retrieved from the mobile devices that were used to control the drone, but the researchers had to employ a special approach that is not currently available in digital forensic tools to decrypt these records. Therefore, the researchers in [23] had to use a program that is not intended for digital forensics work to be able first to decrypt the encrypted *.DAT* files, then used the service of the tool to visualize the drone path.

Although encryption has helped users obtain more privacy and make applications more secure, it affects how developers structure and develop their apps, resulting in many different structures, and there is no single standard for the data to be represented with. This is a great problem for digital forensic tools.

Anti-forensics techniques

Current research efforts have focused on providing clear general guidelines and standards. Recently, NIST pointed out the challenges related to the identification phase of digital cloud forensics, where geodata have been considered an essential component that can help find evidence [101]. However, not many frameworks have highlighted that there could be fabricated data that investigators need to be aware of. Also, not much research has been done on this topic.

According to Harris [239], there has been an increase in criminals using anti-forensic measures to thwart the forensic process and manipulate the evidence itself. The fact that forensic techniques may be circumvented by simple technologies was also noted by Garfinkel [240], who presented an overview of some types of anti-forensics technologies (e.g., traditional data hiding, tampering, etc.). One of the early works that has been done in regard to anti-forensics taxonomy was proposed by Rogers in [241] that included data hiding (e.g., encryption and stenography), artifact wiping, and trail obfuscation. Furthermore, Dahbur and Mohammad in [242] also discussed the difficulties associated with anti-forensic techniques

and rated the efficiency of using such processes, procedures, and strategies based on their effectiveness in combating forensic evidence. However, according to [243], academic research on anti-forensics has not received the same attention as other subjects related to forensics. Furthermore, according to their findings during their stay, the authors found that only 2 of the data they collected among the 500 publications on digital forensic research focused on anti-forensic [243]. They assumed that this could be because most anti-forensic advancements occur outside of academic publications [243].

There is an enormous amount of danger that anti-forensics can potentially pose, such as ensuring that no evidence is collected, prolonging the duration of the investigation, which could result in wasted time; the entire investigation could be jeopardized if fraudulent or misleading evidence is collected; and it can also prevent the detection of crucial artifacts or digital evidence [239], [244]. In addition, the authors in [239] also pointed out that organizations that deal with such problems; must decide up front what information to collect and how to retain it in a forensically sound manner. Furthermore, according to [245], anti-forensics prolongs and increases the cost of digital forensic investigations. Due to the fact that criminals may use such anti-forensic techniques or software that allows them to erase evidence from digital devices in the same way that they would eliminate evidence from physical crime scenes [245].

In mobile phones, researchers in [246] found it possible to stalk WeChat users in a certain location anywhere on the planet. The authors used WeChat's People Nearby feature and found that it can be exploited using a fake GPS application installed on an Android emulator [246]. Furthermore, researchers in [26] examined how to quantitatively identify location spoofing on social networks, as well as how to investigate the various reasons and uncertainties of this growing activity. The authors argue that although location spoofing is true and is a kind of location inconsistency induced by faulty positioning ambiguity or even a user's operational mistake, most technical models and techniques do not look at how human incentives affect the quality of these data [26]. Moreover, they also mentioned that there are two main components of location spoofing, where the quality of geographic data must be evaluated from a human and technological perspective rather than just a technological

perspective [26]. Therefore, this can mean that there could be positive or negative use of GPS spoofing, which can pose issues for digital forensic investigators.

On the other hand, researchers in [247], [248] discussed anti-forensic techniques that focused on abnormal flight patterns that indicated an unlawful change in flight direction, such as GPS spoofing and structural failures. This can make the evidence misleading and confusing to investigators. Furthermore, the authors in [249], [250] focus on numerous anti-forensic tactics for drones, as well as the challenges of drone forensic discovery and the link between these approaches and aspects such as use, environment, attack vector, and level of skill. These challenges can present great challenges for investigators if they are dealing with devices that have been compromised.

On the other hand, GPS is included in the EXIF standard and is stored in a distinct IFD from the rest of the EXIF data. The EXIF data associated with a photograph are kept inside the image file itself, and this feature is accessible on a wide variety of contemporary devices and software (such as smartphones and digital cameras). Depending on whether or not the EXIF data is still there in the original photo, it may be maintained in different image-editing programs and readers. Drones, rather than cameras, are often fitted with GPS sensors on their bodies, which enable these camera modules to preserve position data from the drone's GPS sensor as an alternative to shooting photographs and filming. Therefore, it is necessary to examine the DJI Phantom 3 Professional and AR drone two files using EXIF readers such as ExifTool [209] to determine their authenticity.

Digital forensic tools can plot these coordinates on a geographical map. However, these EXIF tags can be manipulated and changed. Therefore, there are major challenges in determining whether the location is the correct location or whether it has been fabricated. The digital forensics investigator must understand that some of these data are not straightforward and can be misleading. Moreover, they also need to make judgments about whether the data are real or have been manipulated.

3.3 Frameworks and forensic technologies that used Geo-spatial Techniques

The following subsection discusses frameworks and forensic technologies that use geospatial techniques.

3.3.1 Text

Another scale of complexity occurs when that location is represented in a text format and cannot be directly extracted as a location. Currently, investigators use location as a search term when dealing with cases where devices have large amounts of files or text-formatted artifacts. Therefore, researchers in [251] have thoroughly investigated the best approaches with respect to geoparsing, geotagging, and geocoding to extract locations from social media posts. Although the authors mentioned that there is a considerable chance that well-known locations can be extracted from the text and matched with their respective locations or coordinates, they found that many of these top algorithms struggled with some geosemantic that either were continuing the complex location description or unpopular locations that could not be accurately matched with a precise location.

3.3.2 Video

Video forensics on a large amount of data is considered challenging; Deng et al. in [252] have presented an advanced video forensics retrieval system based on a geospatial computing framework. The presented system enables effective geospatial index techniques that can help query a massive amount of video data quickly and efficiently. Although this work focused on one type of data, researchers have found that integrating geospatial data when indexing has benefited the retrieval process.

3.3.3 Technology and Techniques

Authors in [252] have discussed and emphasized the importance of contextual knowledge that is combined with their framework, which in their case is extracted from TIGER-Line data [253] for more accurate and specialized forensic examination inquiries. Although

Vincent in [254] discussed how Google Street View is mainly used for street visualization purposes, Harrington and Cross in their book [175] discussed how Google Earth has helped digital forensic investigators in using maps and street photographs to integrate it into the process of seizing, acquiring, examining and reporting.

Moreover, many social networking services nowadays have integrated this type of geotagging mechanism. In a recent survey, Karabiyik et al. have investigated the use of geolocation metadata in online social networks (e.g., Twitter and Facebook) and how it can help aid in spatial analysis of crimes committed in such services [255]. Furthermore, researchers in [176] have disused geospatial forensic tools that can be incorporated into digital forensics and GIS methods. In addition, they proposed a GIS environment for forensics. They mentioned that there is a substantial need for customized tools that use GIS to meet investigator requirements [176].

Another survey by [256] has presented geolocation prediction to help geolocation-based services expand their capabilities provided to users. The authors discussed three main ways, including the Global System for Mobile Communication (GMS), GPS, and wireless data (e.g., WiFi and Bluetooth), to obtain geolocation trajectory data. Although the proposed model focuses mainly on geolocation prediction and where the user will go next from an application perspective, it can be easily applied to digital forensic investigations in cases where the suspect is still roaming. At the same time, law enforcement has a connected device filled with appropriate geospatial data that can be recovered and analyzed.

3.3.4 Legal Effects of Geospatial Technologies in the Courtroom

Like other applications, geolocation has double edge complexity. It increases the likelihood of regulatory assistance building networks around the suspect and enhances the shape and connectivity of that suspect and their movements and various trends and outliers. Geolocation has aided many law enforcement agencies in catching bad guys, as it can be used as a significant tool in understanding misuse use or catching trends.

In terms of cases, the admissibility of evidence is crucial [215]. According to [215], [216], the proliferation of mobile phones and their continued development of new capabilities

have made it more difficult from an admissibility perspective. The rules of admissibility are intended to ensure that any data stored in a digital format is not changed or altered in any way. The pace of technological innovation often outpaces the rate with which laws are changed to keep up with the pace of change in the technological environment [217]. In addition, [218] discussed that rather than being proactive in understanding and applying the law to new technologies, the law acts more as a reactive rather than a proactive actor. Furthermore, when there is a lack of technical expertise, legislation can be applied incorrectly, and technological reasoning or evidence can be used erroneously [219], [220].

According to [219], the lack of familiarity with digital evidence by both the prosecution and defense in many parts of the United States is a problem. Despite the fact that law enforcement says that almost every crime today involves a digital device; law schools give little or no training on the nature of digital evidence [219]. Therefore, the legal implication of using digital devices and GPS evidence stored in them has become a growing area of study within academic research. Researchers in [257], [258] demonstrate how the use of mobile devices and artifacts from GPS evidence influences judicial procedures; however, they mentioned that it is crucial for digital forensic experts to demonstrate the legal relevance of recovered evidence in a forensically sound manner, so they can use it to prove or disprove a case.

The researchers of Cole et al., in [259], evaluated some of the many challenges that occur during the prosecution of digital forensic investigations in the USA. The authors used the FindLaw database to investigate 100 cases from different federal appellate courts with the aim of finding the core of the appeal with regard to digital evidence [259]. To evaluate the challenges, they used a theme analysis consisting of four primary categories: search and seizure, data analysis, presentation, and legal problems [259]. Although the scope of this research is restricted to only 100 instances found in the FindLaw database during the last decade, many of the cases analyzed were categorized into at least one kind of category.

Moreover, Berman et al. in [258] investigated the impact of GPS evidence in the legal setting for civil and criminal cases in the UK, although investigating the Lexis Nexis, Westlaw, and the British and Irish Legal Information Institute legal databases. The authors found that in the past decade, the use of GPS evidence in court cases has increased, and it seems to

be playing an increasingly important role in the courtroom. According to preliminary empirical research [258], in which researchers looked at data from 83 separate incidents, including GPS evidence that occurred between 1 June 1993 and 1 June 2013, in the UK and Europe, the use of GPS evidence in court cases is increasing and the vast majority of those instances were criminal in nature. Therefore, given the further advancement of GPS technology, which is becoming more incorporated into other devices and becoming more accessible, the authors suggested that GPS data could have a greater influence on court proceedings in the future.

As a result, many data, including sensor data (e.g., GPS), may be useful in determining the user's context in certain crimes [152]. These types of data not only help in the investigation, but can also provide context, which may be crucial for law enforcement authorities in a digital investigation, both for the detection and sanctioning of crime, as well as for the prevention of crime [152].

The authors in [260] discussed how anti-forensic tactics, such as obfuscation and misdirection, must be taken into account while verifying and validating geodata. Therefore, it is critical that digital evidence is explained and defended using systematic and agreed-upon procedures [28], because legal concerns have been raised concerning digital forensics, including concerns about the certifications needed, standards, analysis, and challenges with the admissibility of digital evidence [261]. As a result, the authors in [28] discussed that there are criteria that can be used to assess the validity of digital evidence that uses nations as being under good science, which differs from other forensic investigations. Furthermore, the authors mentioned that these criteria are under the control of many factors, such as the existence of testable hypotheses, repeatable findings, verifiable procedures, peer review, widespread acceptance, standardization, realistic explanation, and application of exact methodologies [28].

4. METHODOLOGY

This chapter presents the methodology used in this study to provide a comprehensive strategy to produce a transdisciplinary approach by integrating DFIR, intelligence, and geography, providing a comprehensive solution to forensic investigations containing geodata in digital format. The approach to research methodology to come up with the holistic framework aims to accomplish the following:

- Propose factors from identified shortcomings that must be addressed in the developed framework.
- Infusing and dissolving parts of a combination of disciplines to deal with geodata in an investigation.
- Conduct a comprehensive cyber forensic investigation of multiple cases. This cyber-forensics investigation aims to:
  - Identify common and uncommon types of geodata (i.e., explicit and implicit) that could be present in the cyber forensics of mobile devices.
  - Utilize the factors identified to improve the digital forensic process.
- Use intelligence domains and GIS frameworks to help geo-contextualization efforts and develop a transdisciplinary approach:
  - Geo-contextualize geodata using geo-coding and geo-processing.
  - Examine the recovered geodata and geo-contextualized efforts for validation using the transdisciplinary approach by incorporating GIS analysis tools to verify the validity of data recovered from mobile devices.
  - Discover and examine what spatial consolidation methods can be used for geodata cases.
  - Provide guidelines for geodata visualization in cases containing geodata.

This research bridges and dissolves disciplines to fill the current gaps and produces a comprehensive framework to create a transdisciplinary framework adapted to geodata in

Cyber Forensics. The following sections are divided into parts that focus on different aspects and go through the study methodology in detail. Figure 4.1 shows the three main phases followed in this study and provides an overview of the goals, tactics, and techniques used in this investigation, including all the procedures and components used. The details of the stages are as follows.

- Phase One: Propose factors based on shortcomings of previous frameworks, research, and studies. At the same time, materializing the principles that were taken into account while creating the framework to fill the gaps in the NICE and digital forensic frameworks (i.e., NIST, SWGDE).
- Phase Two: Conduct comprehensive forensic investigations. This phase will play an important role in stylizing the developed framework.
- Phase Three: Create the framework elements based on the feedback loops in the second phase and then test and validate the framework.

4.1 Highlighting Shortcomings of Mobile Forensic Tools and Frameworks

This section discusses the factors that are proposed to be considered when performing this study's comprehensive cyber forensic examination, which will contribute to developing the geo-contextualization framework of the geodata in digital forensics.

These factors will also be used in the research to examine, clarify, and explain the gaps in current methods that many practitioners face when dealing with geodata. Moreover, the author intends to present technical opportunities as potential solutions to these limitations and demonstrate the importance of utilizing the new framework.

The creation of four ACPO principles highlighted in [262] was an attempt to provide the entire digital forensics industry with broad and general guidance. Furthermore, the SWGDE has contributed several best practices to the digital forensics community, such as the widely recognized best practices for mobile phone forensics [83] and guidelines for collecting and acquiring evidence from mobile devices [84]. These were created in response to the growing demand for digital forensics frameworks, standards, and guidelines. Furthermore,

the National Institute of Standards and Technology (NIST) has developed well-defined digital forensic processes for various devices, including mobile devices, which are outlined in NIST Special Publication 800-101 [19]. Although the SWGDE and NIST guidelines are widely used and considered best practices by many practitioners, they lack comprehensive instructions and procedures for dealing with different types of geodata. Furthermore, there are numerous other guidelines, such as ISO / IEC 27037:2012 [87], ESDFIM [88], Electronic Crime Scene Investigation: A Guide for First Responders developed by the DOJ with NIST [90], and Interpol [91], which does not provide adequate details on how to handle, analyze, and examine various types of geodata.

Despite the significant progress made by the digital forensics community in recent years, with the development of multiple frameworks and standards to help investigators address the distinctive challenges of digital device investigations, there are still some gaps and challenges when it comes to dealing with geodata.

Furthermore, as presented in Section 3, many studies highlighted several open issues and research challenges for geodata in digital forensic studies. Since the investigation focuses only on the stages after the digital evidence identification and collection phases, the proposed elements of the investigation are divided into three main parts (i.e., examination, analysis, and reporting). This aims to systematically evaluate the author's progress in building the framework. These shortcomings are synthesized and identified from the leading mobile forensic tools and frameworks in dealing with geodata concerning the three categories as follows:

1. Examination:
    - Knowledge of geodata file types (e.g., explicit and implicit).
    - Tools and techniques to minimize the amount of data that must be examined to find information from geodata quickly (i.e. geodata triage).
2. Analysis:
    - Data decoding and coding using geocoding and reverse geocoding.
    - Evaluation of the accuracy of the recovered geodata.

- Geoprocessing, geospatial analysis, and the use of OSINT.
- Geoanalysis of life patterns.
- Consolidation

3. Reporting:
    - Visualization of geodata.

Although the factors proposed do not cover all aspects of the mobile forensics process, they are intended to be considered when conducting the forensic investigation in this study. Furthermore, this study and research used best practices to obtain and analyze digital forensic images of related devices, which were then used in subsequent analyzes. In addition, multiple well-known forensic tools were used in this investigation to cross-validate and determine whether both could obtain the same information from the same images. With all this, the author used the factors to examine and explain what current methods lack when dealing with geodata in digital forensics, along with technical opportunities and challenges.

In addition, feedback from this will help identify the potential tactics, techniques, and details needed to develop the new framework. Therefore, the author proposes adding a geographic perspective to forensic techniques (see Figure 4.2 for the enhanced model). This will enable the geo-contextualization of data to take shape in the process. Although the model includes the complete digital forensic process, this study focuses on the Forensic Processes in the Analysis Phase (i.e., Examination, Analysis, and Presentation). This does not mean that there is no need to incorporate geospatial thinking and inclusion into the first steps, but it is beyond the scope of this study.

The following perspectives were taken into account to establish the fundamentals of the framework and the integration of different disciplines and processes.

1. First, digital forensics, and more specifically mobile forensics. The author adapted the forensic procedures created by NIST, SWGDE, and GDFM [86].
2. Second, geography and geospatial thinking using the GIS framework and approaches.
3. Third, intelligence tools and approaches.

Significant factors are shared between the three domains. All three need people with the unique knowledge and skills required to perform each of them. This is also one of the reasons why this study aims to create a transdisciplinary approach. Moreover, each domain deals with data and requires technology (e.g., hardware, software) and procedures (i.e.g., analysis). Figure 4.3 shows that these fields share the same factors but with different attributes.

4.2 Comprehensive Cyber-Forensic Investigation

This section describes how the author will create and then forensically examine devices to harvest the needed information to develop the new model, providing a road map to produce the geo-contextualization framework. To answer the questions stated in this research, an in-depth forensic study of two different forensic cases and several images obtained for each case is performed. The following subsections describe the comprehensive cyber forensic investigation methodology in detail.

4.2.1 Experiment Design

The first piece of this puzzle is to identify the parts that need to be investigated that already exist in mobile forensics. Figure 4.4 shows the design of the experiments. In real-world incidents, digital evidence could be the only connection between a crime and its perpetrator when devices are seized and their contents evaluated. However, filtering through a lot of data, particularly with regard to considerable storage capacity and unfamiliar file formats, might be a challenge. This study and research used best practices to obtain and analyze digital forensic images of related devices, which were then used in the subsequent analysis. Furthermore, this study follows a well-defined digital forensic procedure for various devices provided by NIST. The NIST mobile device guidelines [19] have four primary steps, as indicated in Figure 4.5. Furthermore, since this study aims to enhance and build a framework based on GDFM [86], it utilizes the principles of different forensic clients, elements, and processes by adding the geographical perspective to the 3D dimensional matrix (see Figure 4.2).

Furthermore, according to [263], in digital forensics, three principles (i.e., acquisition, authentication, and analysis) are fundamental because they ensure that the integrity of the evidence remains intact throughout the investigation process. It is essential to ensure that the evidence is reliable and can be used in court, if necessary, by acquiring digital evidence from the original source without altering or modifying it to preserve its integrity. Second, ensure that the acquired data are authentic and unchanged from the original source through various verification techniques. Third, analyze the data obtained without making any modifications to draw conclusions and make informed decisions based on evidence.

The process starts with the preservation phase, which covers many sub-phases, such as search, identification, and evidence collection in the NIST framework. In all parts of the preservation phase, the evidence must be retained in its original state, and a failure to do so can result in the destruction of a part of the entire evidence. Additionally, many instructions are provided in the acquisition, examination, and documentation steps to facilitate the process.

Therefore, the author followed best practices to collect and analyze forensic images of related devices in this study and research to ensure the highest quality of data extraction. A brief description of the NIST mobile device guidelines [19] for each step that was followed in this investigation is as follows.

1. Preservation: In this step, the goal is to secure the device from the crime sense in a manner that it will not interfere and will not cause any data tempering (i.e., seizure protection and control of mobile devices). This step encompasses all the responsibilities that fall under the first responders. A mistake in this step can jeopardize the entire process [221], [261]. Since this research does not deal with real criminal or civil cases, all the cases were produced for research purposes. This has helped control the variables to conduct more accurate tests of the hypothesis and techniques. However, it is essential to note that not all hypothetical instances adequately mirror real-world cases. Figure 4.6 demonstrates the procedures taken from [19], [86].

2. Acquisition: This step aims to collect as much information as possible from the device storage. Therefore, the acquisition process preserves evidence for later analysis and

interpretation. Depending on the device or system being studied and the investigation's needs, the acquisition process may use various methods and technologies. Due to the criticality of this step, all acquired images were taken from trusted parties in the digital forensics community or were done by the author while taking extreme measures to adhere to common and well-known guidelines.

3. Examination and Analysis: This step examines and analyzes the recovered data to identify and extract relevant information. In the research, the author has used multiple tools and techniques (e.g., keyword searches, data carving, and timeline analysis) to reconstruct events and extract information. In addition to the well-known guidelines, the author has taken extra steps to analyze, examine, and interpolate the data to identify relevant patterns, correlations, and anomalies. Although, in the NIST Guidelines on Mobile Device Forensics, this phase combines examination and analysis, in this study, the author has chosen to follow the framework proposed in GDFM [86], where this is considered as two separate steps.

4. Reporting: Report results and other significant findings comprehensively and efficiently. The author has documented the effects of the examination and analysis steps in various formats (e.g., descriptions, tables, timelines, diagrams, and maps).

4.3 Testing Environment

The set of devices, computers and tools that were used to carry out research and investigations are explained in this section. Although testing environments mimic real-world circumstances to test digital forensic investigation tools and methodologies, to eliminate hardware bias throughout the study, all data obtained were examined using at least two independent digital forensic tools and two different forensic workstations equipped with identical tools to guarantee the precision of the results and eliminate hardware restrictions.

Furthermore, to confirm the findings and rule out any software restrictions, three digital forensic tools were used, the first being Autopsy [15], which is an open-source tool, Magnet AXIOM [72] and Cellebrite [17] as proprietary products. All three are well-known software

that law enforcement agencies and practitioners around the world commonly use. Therefore, as a precautionary measure, all collected data were evaluated using at least two digital forensic software solutions.

In addition, open-source tools such as CyberChef [264], Apple Pattern of Life Lazy Output'er (APOLLO) [265], Plaso [266], [267], and iOS Logs, Events, And Plists Parser (iLEAPP) [268], were used as additional valuable tools to examine and analyze digital forensic images.

4.3.1 Main Workstation: Windows and Kali Linux

The first computer was used as the main workstation in the study. The latest device specifications described in Table 4.1 and the details of the latest Windows OS [269] of this machine are highlighted in Table 4.2. This workstation was used to acquire the cases that were populated in this study, along with analyzing all the cases. Furthermore, the machine was set up and equipped with Kali in a Windows Subsystem for Linux (WSL) environment that enables the use of a Linux distribution natively on Windows without the need for a virtual machine. This has helped run tools and commands in Kali easily and directly on the data [270], [271].

Table 4.1. Workstation 1 (Main Machine) Specifications

Property	**Value**
Processor	AMD Ryzen 9 3900X 12-Core 4.00 GHz
Installed RAM	64.0 GB
Graphics Card	GeForce RTX 2060
Drive 1 (Windows OS)	2TB M.2 SSD
Drive 2 (Data Storage)	2TB M.2 SSD

4.3.2 Secondary Workstation: Windows

The second computer was mainly used to eliminate hardware bias and validate the results. The specifications of the device and the details of the Windows OS of this machine are highlighted in Tables 4.3 and 4.4, respectively.

Table 4.2. Workstation 1 Windows OS Information

Property	Value
System Type	64-bit operating system, x64-based processor
OS Edition	Windows 11 Education*
OS Version	22H2
OS Build	22621.1413
Device ID	582E16F2-FC1C-428B-971B-4925A3694376
Product ID	00328-00263-48519-AA037
Experience	Windows Feature Experience Pack 1000.22639.1000.0

* Originally Equipped with Windows 10 Education, then upgraded to Windows 11 Education

Table 4.3. Workstation 2 (Secondary Machine) Specifications.

Property	Value
Processor	Intel(R) Xeon(R) Gold 6238R CPU @ 2.20GHz
Installed RAM	96.0 GB
Graphics Card	Nvidia RTX A4000 16GB
Drive 1 (Windows OS)	1TB M.2 SSD

Table 4.4. Workstation 2 (Secondary Machine) OS Information.

Property	Value
System Type	64-bit operating system, x64-based processor
OS Edition	Windows 10 Pro
OS Version	22H2
OS Build	19045.2728
Device ID	9792ECA4-AFC6-484D-80EE-7A09DFB00F62
Product ID	00331-10000-00001-AA059
Experience	Windows Feature Experience Pack 120.2212.4190.0

4.3.3 MacBook Pro Laptop

Since the study deals with iOS devices, it was initially recommended to use MacOS for jailbreak operations. Table 4.5 provides the latest specifications of the device and includes information on the operating system.

Table 4.5. MacBook Pro

Property	Value
OS	MacOS
OS Build	13.3 (22E261)
Processor	2.9 GHz 6-Core Intel Core i9 with Intel UHD Graphics 630 1536 MB
Installed RAM	32 GB 2400 MHz DDR4
Product ID	MacBookPro15,1 (15-inch, 2018)

4.3.4 Tools

This research does not take into account the speed and performance differences between the two digital forensic workstations or the tools used; instead, they were used to validate and verify the forensic procedures. It is important to note that the companies that provided digital forensic software produced updates throughout the research and investigations. The author has considered the updates to the tools during this study and recorded all the versions used. The tools used in this research are not necessarily the same tools that other researchers might use. The specific trade names, company products, commercial equipment, instruments, or materials identified in this research are used to specify the experimental procedure adequately. Therefore, in no case is such identification intended to imply recommendation or endorsement by the researcher, nor is it intended to indicate that the materials or equipment identified are necessarily the best available for the purpose. Instead, they were chosen for their availability to the researcher and his capability.

Table 4.6 shows the tools that the main workstation had at the beginning of the study, and Table 4.7 shows the same tools that were updated throughout the study, along with their updated version number and update date. Note that the secondary machine was equipped with the latest versions. Later in the study, a complete description of the tools that were subsequently included due to the need for research will be highlighted.

Table 4.6. The set of tools and applications used to conduct the research.

Software Name	**Version**	**Usage**	**Availability**
Autopsy	4.19.3	Examination and Analysis	Open-source
Magnet ACQUIRE	2.52.0.30234	Acquisition	Free Software
Magnet AXIOM (Process & Examine)	5.7.0.27176	Processing, Examination and Analysis	Proprietary
Cellebrite Physical Analyzer	7.42.0.50	Processing, Examination and Analysis	Proprietary
Cellebrite UFED	7.42.0.82	Processing, Examination and Analysis	Proprietary
Binwalk	2.3.2	Entropy measurement	Open-source
7-Zip	22.01	Unpacking and extracting compressed files	Free Software
CyberChef-Cyber Swiss Army Knife [264]	v9.55.0	Examination, Decoding, and Encoding	Open-source
iLEAPP [268]	v1.15.8	Examination and Analysis	Open-source
Plaso [266], [267]	v20221229	Examination and Analysis	Open-source
APOLLO [265]	v1.4	Examination and Analysis	Open-source
ArcGIS Pro	2.8.0	Data curation, Mapping and accuracy validation	Proprietary
https://ipgeolocation.io	Online	IP geolocation locator	Free version
https://earth.google.com	Online	Checking surroundings and images	Proprietary
SAS	9.4	Statistical Operations	Proprietary
checkra1n program	0.12.1 Beta	Jailbreaking the iPhone	Freely available
ExifTool	12.36	Reading meta-information	Open-source
Hex Editor	HxD	2.5.0.0	Free Software
DCode™ - Timestamps Decoder	5.5.21194.40	Timestamps Decoding	Free Software
plist Editor Pro	2.5.0	A software for reading and editing plist files	Trial Free Software
DB Browser for SQLite	3.12.2	SQLite Database Browser	open-source

Table 4.7. Software used and their versions.

Software Name	Version	Updated After the Release on
Autopsy	4.20.0 (Latest Version Used)	02-12-2023
Magnet ACQUIRE	2.61.0.33597 (Latest Version Used)	02-26-2023
Magnet AXIOM (Process & Examine)	5.8.0.27495	12-14-2021
	5.10.0.30634	02-25-2022
	6.1.0.31400	04-29-2022
	6.2.0.31740	05-31-2022
	6.3.0.32040	06-27-2022
	6.4.0.32382	07-26-2022
	6.5.0.32778	08-29-2022

Table 4.7 continued

	6.6.0.33061	09-20-2022
	6.7.1.33408	10-18-2022
	6.8.0.33712	11-14-2022
	6.9.0.34051	12-13-2022
	6.11.0.34807	02-21-2023
	6.11.0.34807 (Latest Version Used)	02-21-2023
Binwalk	2.3.3	09-10-2022
	2.3.4 (Latest Version Used)	02-01-2023
ArcGIS Pro	2.9.0	11-11-2021
	3.0	6-23-2022
	3.0.1	8-11-2022
	3.0.2	9-22-2022
	3.0.3	11-29-2022
	3.1.1 (Latest Version Used)	02-23-2023
ExifTool	12.42	06-01-2022
	12.51	11-21-2022
	12.60 (Latest Version Used)	04-05-2023
iLEAPP	1.18.0	10-19-2022
	v1.18.1	11-03-2022
	v1.18.2 (Latest Version Used)	02-05-2023

4.3.5 Accessories

In the study, a physical SIM card was used, and the operator was Mint Mobile [272], with the most affordable plan that includes 1) unlimited nationwide talk and text and 2) 4GB of 5G per month, which in May 2023 increased to 5GB per month.

4.3.6 Reproducibility

In the process of conducting a digital forensic investigation, reproducible results are essential. If more than one investigator cannot obtain the same findings, it must be concluded that the evidence is unreliable from a forensic point of view. Digital forensic investigation tasks may include imaging and analyzing storage media, reviewing and extracting data from various file systems and applications, and conducting network and OSINT investigations. Forensic workstations have specialized software and hardware tools explicitly designed to examine and analyze digital evidence. The use of a forensic workstation allows for a controlled and secure environment to perform forensic examinations, ensuring the preservation and integrity of the evidence being analyzed.

Although the use of virtual machines (VMs) can enable easily replicated results due to similar hardware setups, there are several reasons why the author chose not to use them in the study. One of the most common reasons was the limitations of the resources and the limited access to physical memory. Additionally, there is a lack of native hardware integrations. However, the choice ultimately depends on the specific requirements and objectives of the research and the nature of the digital forensic investigation being conducted. There is no one-size-fits-all approach, and each case can require a different methodology based on factors such as the nature of the evidence, the type of analysis needed, available resources, and legal considerations.

4.4 Test cases in the study

Research starts initially with two main cases.

- Case 1: Containing seven digital forensic images of three different iPhone devices that are publicly available for researchers and students
- Case 2: Digital forensic images made by the author to experiment with some of the settings and applications

4.4.1 Devices and Setup

This section contains a description of the devices and their setup in each of the cases.

Case 1

In total, seven images were included in this Case 1; five digital forensic images were taken from [273] and the other two were images from the Magnet Forensics Capture the Flag (CTF) competitions [274], [275]. These digital images were created with the aim of digital forensic research in mind and made available to the public. All images except the latest (iOS 16) are hosted by the NIST Computer Forensic Reference Datasets project, which has a collection of digital forensic test data sets that can be used by researchers, educators, tool developers, and practitioners [276]. These images provide valuable information and insight to researchers, as they provide a glimpse into the inner workings of different devices, operating systems, and applications. Therefore, researchers can use these images to study artifacts left behind by various applications or to test and validate new forensic techniques, frameworks, and tools.

Using these images allows one to replicate the experiments and results presented in the research and ensures the reliability and validity of the findings, which also helps cross-research validation. Images were obtained from a trusted and well-known source in the digital forensic community and used according to best practices for research and educational purposes.

The six images, which will be treated as scenarios, are as follows.

1. iOS 13.3.1 [277], [278].
2. iOS 13.4.1 First acquisition [277], [278].
3. iOS 13.4.1 Second Acquisition [279].
4. iOS 14.2 [279].
5. iOS 14.3 [279].
6. iOS 15.0.2 [274], [275].
7. iOS 16.1.1 [280], [281].

Table 4.8. Device Information and Specifications for Scenarios 1-5 in Case 1

Property	Value
Make	iPhone SE
Model	A1662 (Rose Gold)
Order Number	MLXL2LL/2
RAM	2 GB
Storage	64 GB
Carrier	Google Fi
Serial	DX3T126VH2XV
Wi-Fi MAC	A0:D7:95:79:DD:A1
BT MAC	A0:D7:95:79:DD:A2

According to the documentation published by the owner of the first five digital forensic images (i.e., iOS 13.3.1, iOS 13.4.1, iOS 13.4.1 Second Acquisition, iOS 14.2, and iOS 14.3) used in this case, the same device was used in all images. Table 4.8 provides the device information taken from the documentation provided by the owner of the digital forensic images.

For Image iOS 13.3.1, the device was wiped by restoring it to factory settings. Then the owner of the device installed Apple 13.3.1. For the iOS 13.4.1 images, the device was updated with previous data kept on the device. The device owner takes another image before updating the device to 14.2. Then he resets and wipes all data, and then installs iOS 14.3 for the fifth image (iOS 14.3). Regarding cellular connectivity, the owner used a Google Fi account number for all scenarios.

Since the iPhone device was connected and paired with other devices during the population, Table 4.9 provides a detailed description of the devices used while running iOS 13.3.1 and 13.4.1. Although the same devices were used in iOS 14.2 and 14.3, the Apple Watch was updated to watch OS 7.2 and build 18S563. Additional devices were included and are shown in Table 4.10.

The other two images, iOS 15.0.1 and iOS 16.1.1, on the other hand, offered little documentation due to the way in which they served as digital forensic images for Magnet Forensics CTFs. However, image 15.0.1 has a detailed document that was produced by the acquisition

Table 4.9. Paired Devices with iOS 13.3.1 and iOS 13.4.1 Images.

Device Name	Property	Value
AppleWatch (Series 4)	Size	40 mm
	Color	Space Grey
	Name	This Iss AppleWatch
	Model	A1975
	Order Number	MTUG2LL/A
	S/N	D92XF148KDT2
	Wi-Fi MAC	F8:6F:C1:4B:99:B5
	BT MAC	F8:6F:C1:4E:FF:6A
	watchOS	6.1.3
	Build	17S811
AirPods	Model	A1523
	Order Number	MMEF2AM/A
	S/N	FWYT1CJWH8TT
	Firmware Version	6.8.8
	Hardware Version	1.0.0
AirPods Pro	Model	A2084
	Order Number	MWP22AM/A
	S/N	GX5CCJMLLKKT
	Firmware Version	6.8.8
	Hardware Version	1.0.0
Nissan Rogue	Name	Rogue
	Bluetooth MAC	b4:ec:02:73:ff:93

Table 4.10. Additional Paired Devices with iOS 14.2 and iOS 14.3 Images.

Device Name	Property	Value
Forerunner 35	Model	A02990
	Unit ID	3329145769
	MAC	C1:D1:71:67:AC:4E
Fitbit Versa 3	Model	FB511
	Version	36.128.4.17
	MAC	F0:51:EA:86:0E:73

Table 4.11. Device Information and Specifications for images 6 and 7 in Case 1.

Property	Value
Make	iPhone 8 (Global)
Model	D20AP [iPhone10,1]
Serial	FFMC855HJC6C
Wi-Fi MAC Address	e0:eb:40:8f:46:2b
Bluetooth MAC Address	e0:eb:40:8f:cd:04

software used (GrayKey v1.7.3.19461530). Table 4.11 provides the device information taken from the documentation provided by the GrayKey forensic tool. Unfortunately, for a digital forensic image 6, in this case, there is no clear documentation for setup.

Case 2

Devices used in the case scenarios of this study were populated according to the NIST Special Publication (SP) 800-202 [282]. However, an important note is that the author greatly expanded the population tactics provided in 800-202 publications due to the lack of coverage of all geodata types. Three different devices were used in this case. The devices were the iPhone 6s, iPhone 7, and iPhone X. 1) Table 4.12 highlights the device specifications and information of the iPhone 6s; 2) Table 4.13 highlights the device specifications and information of the iPhone 7; and 3) Table 4.14 highlights the device specifications and details of the iPhone X. Furthermore, Table 4.15 provides an overview of the DJI Mini 2 Drone connected to the iPhone 6s and 7 and outlines the specifications and features of the DJI Mini 2 Drone. Figure 4.7 displays the drone, controller, and iPhone.

Table 4.12. Device Information and Specifications for Device 1 in Case 2.

Property	Value
Make	iPhone 6s
OS version	iOS 14.1
Model	iPhone8,1 N71AP
Serial	DNPQMYRWGRY5

Table 4.13. Device Information and Specifications for Device 2 in Case 2.

Property	Value
Make	iPhone 7
OS version	iOS 13.3.1
Model	iPhone9,1 D10AP
Serial	F71SW8DLHG6X
Wi-Fi MAC Address	F8:62:14:3F:87:31

Table 4.14. Device Information and Specifications for Device 3 in Case 2.

Property	Value
Make	iPhone X
OS version	iOS 14.3
Model	iPhone10,3 D22AP
Serial	DNPWC3JQJCLF

Table 4.15. Paired Drone Details with iPhones 6s and 7.

Device Name	Property	Value
DJI Mini 2	Model	MT2PD
	Device ID	3Q4CHBN3A3B1FX
	Drone Camera Model	FC7303
	Drone Camera ID	1SFLH870AB0K6X
	Drone Gimbal ID	3QCCHC3P23EKJK
	Flight Controller Version	3NZCHBS003C5MF
Drone Remote Controller	Model	RC231
	Device ID	396CHBR00194WJ

4.4.2 Data Population

Data population steps are discussed in the following subsections for images in case 1 and case 2.

Case 1

The first five iPhone digital forensic images in Case 1 are well-documented digital forensic images created for research use; therefore, the author relied on the research documentation found with the images [277], [279].

A critical aspect of using these images for research is ensuring that they are adequately acquired and handled to maintain the integrity of the evidence. Binary Hick follows strict protocols and procedures to ensure that the images he provides are forensically sound and can be used in a legal context if necessary.

Additionally, researchers can use these images to study the different types of data and information that can be found on a device, how it is stored, and how it can be accessed. This can include analyzing file systems, studying the structures of different types of files, or identifying patterns of usage or activity on a device. By studying these images, researchers can better understand the digital landscape and develop new methods to acquire, analyze, and interpret digital evidence.

Since all the data collected and populated during this case are freely available to other researchers, it will allow cross-research examination and allow others to replicate. Therefore, the objective is to highlight and provide the best possible details so that other researchers can perform a complete evaluation from the beginning to the end without requiring additional procedures. Table 4.16 details the population duration of the four images.

Furthermore, the additional two CTF digital forensic images did not have documented population steps. Still, they were used for their newer iOS to combat the growing demand to analyze newer iOS versions.

Table 4.16. Duration details of the images 1-5 in Case 1.

Image name	Property	Value
iOS 13.3.1	Start	03-21-2020
	End	04-12-2020
	Duration	23 Days
iOS 13.4.1	Start	03-21-2020
	End	04-16-2020
	Duration	27 days, and only four days were used as iOS 13.4.1
iOS 13.4.1 Second Image	Start	03-21-2020
	End	12-12-2020
	Duration	Around 9 Months
iOS 14.2	Start	12-12-2020
	End	12-13-2020
	Duration	Around Day and a half
iOS 14.3	Start	01-17-2021, after update from iOS 14.2 that lasted turned on for around 2 hours
	End	02-19-2021
	Duration	34 Days

Table 4.17. Duration details of the images 1-3 in Case 2.

Image name	Property	Value
Image1 iPhone 6s iOS 14.1	Start	05-19-2022
	End	05-26-2022
	Duration	7 Days
Image2 iPhone 6s iOS 14.1	Start	03-03-2023
	End	03-07-2023
	Duration	4 Days
Image3 iPhone 6s iOS 14.1	Start	05-01-2023
	End	05-06-2023
	Duration	6 Days

Case 2

Data population steps were regressive in testing missing parts that were apparent in case 1. This includes imaging the device multiple times after populating new data and testing applications from the app store.

For iPhone 6s and 7, a DJI Mini 2 drone was flown using the devices as a supplementary screen to the controller for these digital forensic images. The population and the flights occurred on 03-03-2023 and 05-04-2023 for the iPhone 6s and 03-26-2021 and 04-10-2021 for the iPhone 7 in a safe flight zone just outside West Lafayette, Indiana, USA. The drone was flown for approximately 15 minutes, recording high-resolution video and capturing photos at various altitudes and locations. The scenarios aim to discover techniques for recovering significant geodata and PII that can help investigations involving a drone controlled by an iPhone. DJI Fly app v1.3.1 controlled the drone on the iPhone 7 and v1.5.10 on the iPhone 6s. DJI Fly is a flight operation app for DJI drones, and is used to manage the drone's flight path and camera settings. The flights were intended to have varying altitudes and other important telemetry data. Lastly, the iPhone X running iOS 14.3 was used mainly to test sending and receiving different geocoded and geohashed messages and files and experiment with the accuracy of GPS indoors. Table 4.17 provides details on the images for the iPhone 6s.

Table 4.18. Case 1 first five digital forensic images acquisition details.

Image Name	MD5 Hash Value	Magnet Acquire Version	Date
13-3-1.tar	0806f1105231f12108838de2c3142600	2.25.0.220236	04/12/2020
13-4-1.tar	c2a733e6db7af9be6bd0437fd7c765f8	2.25.0.220236	04/16/2020
iOS 13-4-1.tar	c2999833eb1fc338285776696babbd12	2.34.0.23504	12/12/2020
iOS 14-2 - Post Update - No Activity.tar	a1c6e673ca5fa71ea2f9d9cf97f48f79	2.34.0.23504	12/13/2021
iOS 14-3 - Apple iPhone SE.tar	7e7cb4d7e6204089758bf41d5d2c5efc	2.36.024403	02/19/2021

4.4.3 Acquisition

Two well-known forensic tools were used in this investigation to cross-validate the acquisitions. In case 1, the creators of the digital forensic images already acquired them using Magnet Acquire and GrayKey tools; however, in the author's digital forensic images, Magnet Acquire and Cellebrite were used to acquire the devices. Figure 4.8 demonstrates the structure of the drive of all acquisitions.

Case 1

The documentation supplied with the digital forensic images by the owner [277], [279], who obtained the image, shows that the iPhone was acquired with Magnet Acquire software for all images. Furthermore, iOS 13.3.1 and 13.4.1 were successfully jailbroken using checkra1n v0.10.1 beta, and iOS 14.2 and iOS 14.4 were jailbroken using checkra1n v0.12.1 beta.

All downloaded images were verified to have the same hash sum values provided by the owners of the images highlighted on the website or/and in the documentation. Table 4.18 provides MD5 image hash values, the version of Magnet Acquire used, and the date of acquisition (Eastern Time (ET)) for each image.

For CTF digital forensic images, the iOS 15.0.2 image was acquired on 02-14-2022 with GrayKey software version 1.7.3.19461530 and an MD5 of 448db62270f86a773788f5d07 b899f6f; and the sixth iOS 16.1.1 image has an MD5 of 067606649297d7adcf6082e5ed0acbb9; however, it is not clear which Graykey version was used to acquire this image.

Case 2

As Magnet Acquire does not provide jailbreak capabilities without the use of external hardware by the investigator, jailbreak steps were required unless the iPhone was obtained using Cellebrite, which provides jailbreak for defined types of devices and OSs.

The iPhone 7 was acquired by two different forensic software; the extraction time of the first image was 03-31-2021 using Cellebrite UFED v7.42.0.82; the second image was acquired after the second day of drone testing using Magnet Acquire V2.37.0.24776. In the first image, there was no need to jailbreak the iPhone since Cellebrite provided jailbreak mechanisms within its software. However, for the second image, the device needed to be jailbroken using the Checkra1n application (version beta 0.12.2) on the MacBook Pro laptop because Magnet Aquire took the acquisition.

For the iPhone 6s running iOS 14.1, the Checkra1n Program version Beta 0.12.3 was used to jailbreak the iPhone 6s every time Magnet Acquire was needed to acquire the device. Therefore, the device was acquired three times, each on the day of the end of the population.

For iPhone X running iOS 14.3, Cellebrite software was used, which has the checkm8 exploit (that is, Checkra1n beta 0.9.6) to provide privileged access to iOS data. This exploit enables the device to be jailbroken and is incorporated into the Cellebrite acquisition process. The outcome of this process is an image of the Advanced Logical Full File System in the form of a `.dar` file, which is then processed by the Cellebrite Physical Analyzer version 7.42.0.50. Figure 4.9 provides an overview of the steps taken for the devices used in Case 2.

4.4.4 Examination and Analysis Stages

Three well-known forensic tools were used in this investigation to cross-validate and determine if both could obtain the same information from the two images used. The first piece of software is an open-source tool developed by Basis Technology named Autopsy [15]. On the other hand, proprietary software, Magnet Axiom [18], and Cellebrite [17] were used. These tools are known and used by many law enforcement agencies worldwide. The complete examination and analysis are discussed in detail in the next chapter. After that, the author will dive deeper by performing several different forms of analysis, including a keyword search,

the results of ingested modules, an analysis of file type, a timestamp analysis, and an analysis of deleted files.

Categorization of Geodata

Many file types can contain and present embedded spatial data (e.g., pictures, audio, video, documents, spreadsheets, data-based). In addition, other types of data can represent and hold geospatial data when investigated (e.g., IP address, WiFi, SSID, and text inside images). Furthermore, currently, many devices store and use geolocation and spatial data, including, but not limited to, smartphones, cars, tracking devices, watches, computers, laptops, cameras, drones, robots, and many more.

Current digital forensics guidelines and tools rely significantly on standard GPS coordinates stored in EXIF tags, artifacts, or other file formats (e.g., audio, video, documents, spreadsheets, databases, etc.). However, including primary GPS data can affect specific digital forensic tools, which cannot handle large amounts of such data. Additionally, not all data formats representing geospatial or geolocation information are considered when populating mobile devices. In the "Quick Start Guide for Populating Mobile Test Devices," considered one of the essential documents for populating mobile devices that NIST has developed, Section 8 talks about location data; however, only a few types of geolocation data are discussed [30] for example, GPS-related applications, routes, check-ins, and geotagged information. There are more than just these to consider when dealing with geolocation data.

Therefore, Figure 4.10 demonstrates the categorization of these types of geodata, which the author defines. In other words, Figure 4.10 describes the kinds of geodata that can be directly implied to find a location and those that require additional investigation techniques to locate the associated location. This categorization will be expanded in the research to help build the framework.

4.5 The Framework

In the cases where geodata are present, they can guide the investigation or give it an extra space dimension as a reference over time. There are multiple scenarios in which location data

can be quite valuable; however, many guidelines fail to emphasize the importance and provide best practices for dealing with various types of location data. Even with the most modern digital forensic tools, geodata is incredibly challenging. Although the implementation and significance of the recovered geospatial data differ depending on the amount of data stored and collected for each case, even a slight hint or clue can help investigators make great leaps in complex investigations. Therefore, it is critical to undermine every possible technique that can be used to present geodata to provide accurate and relevant information that can later be used to help the investigator in a given case, as geolocation information of all types would be considered tremendously valuable potential clues and evidence for digital forensic investigators. The argument for extensive examination, comprehensive analysis, and good documentation and presentation comes to another level when dealing with evidence containing a large number of geodata because recovering, analyzing, reporting, and displaying these types of data require analytical and categorical skills to convey precise information.

In addition, in recent years, digital forensic tools have been used in various fields. In this study, the author investigated and demonstrated missing geodata in forensic tools such as autopsy and AXIOM, which lack the identification, examination, and presentation of some geodata. This has led to the use of functional extraction methods and tools that parsed and preserved relevant GPS data for further examination by investigators. This helped the author apply and prove that spatial analysis techniques and geodata curation methodologies can help uncover hidden knowledge for investigators for both cyber forensics and cyber investigations in general, which will also help clarify whether maps can provide a rich source of information for investigations. Therefore, (H_1) examined whether a comprehensive cyber forensic investigation can result in the construction of a cyber forensics transdisciplinary geo-contextualization framework.

In addition, to answer the hypotheses of validating and verifying geodata collected using geographical perspectives H_2, the author used GIS (the ArcGIS Pro software geoprocessing framework) to test the altitude data stored in each record to test this hypothesis. There could indeed be a column that indicates the accuracy for altitude; however, perform both the accuracy check and determine whether there are substantial differences between the recorded

and real-world values. Therefore, there is a need for geodata that could be easily used for this geoprocessing task.

Moreover, during the technical analysis and examination of the cyber methods in this study, the objective was to answer H_3. Furthermore, to help answer this hypothesis, the author investigated how to geo-contextualize geodata and other data objects. Therefore, the author worked on geocoding and geoprocessing different geodata formats recovered from the cases, giving geo-contextualized meaning to other collated data. Then the author aimed to highlight what can be possible using the transdisciplinary framework infused with geographical perspective and used spatial analysis techniques to determine whether they support hypothesis H_4. Therefore, multiple questions that involve spatial geoprocessing were answered, of which GIS tools are capable but not cyber forensic tools yet. It is an operation that starts with an input data set, performs a function on it, and then returns the output data set, also known as derived data, as the result of the operation [283]. Therefore, this highlighted the importance of the geo-contextualization process for both cyber forensic investigations and cyber forensic intelligence purposes.

Since creating a transdisciplinary framework is a complex process, the author used interactive feedback loops that can provide insights and help consolidate and construct a regressive framework while performing the analysis. This provides a better approach to understanding the whole by understanding the parts and their connections. Additionally, explore the current gaps and challenges that prevent it from advancing and then shed light on possible opportunities that can help enhance cyber forensics investigations and digital forensic intelligence processes.

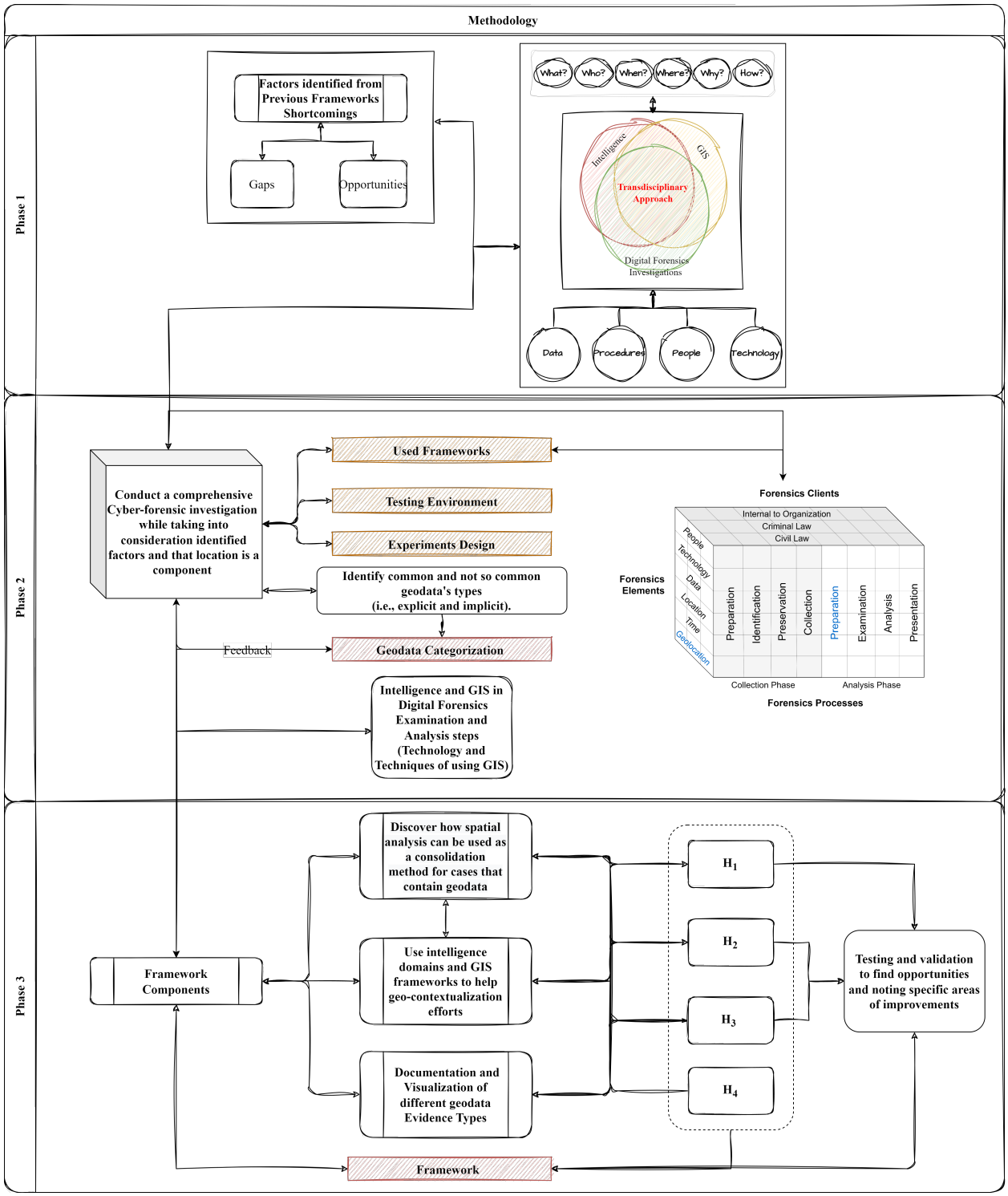


Figure 4.1. Research Methodology and Workflow of the Study.

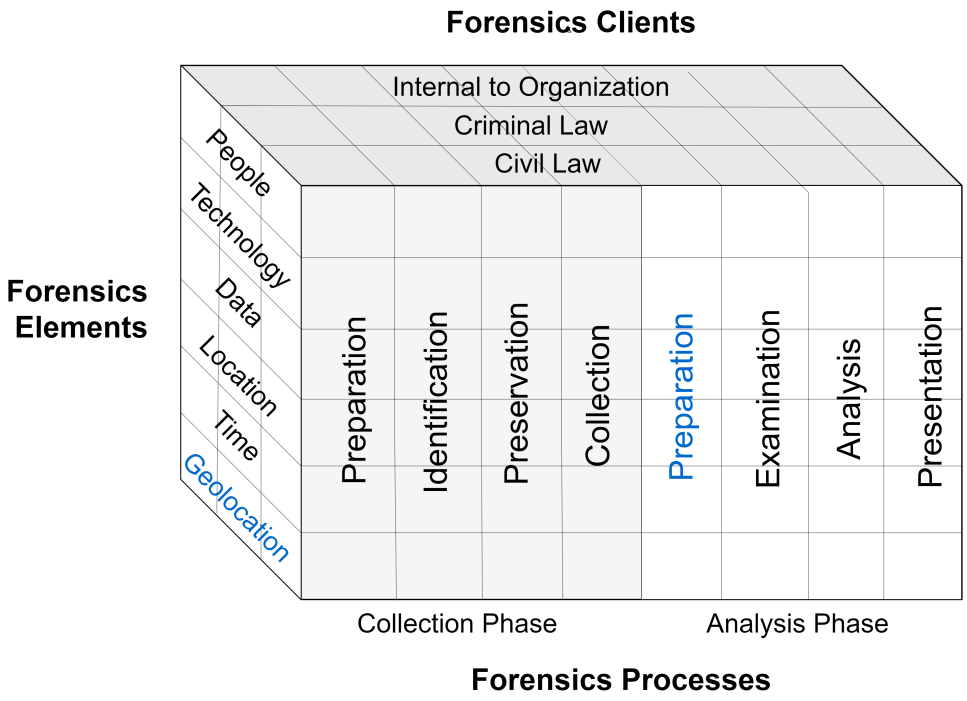


Figure 4.2. Enchanced cube with geolocation forensic element and Analysis Phase Preparation step.

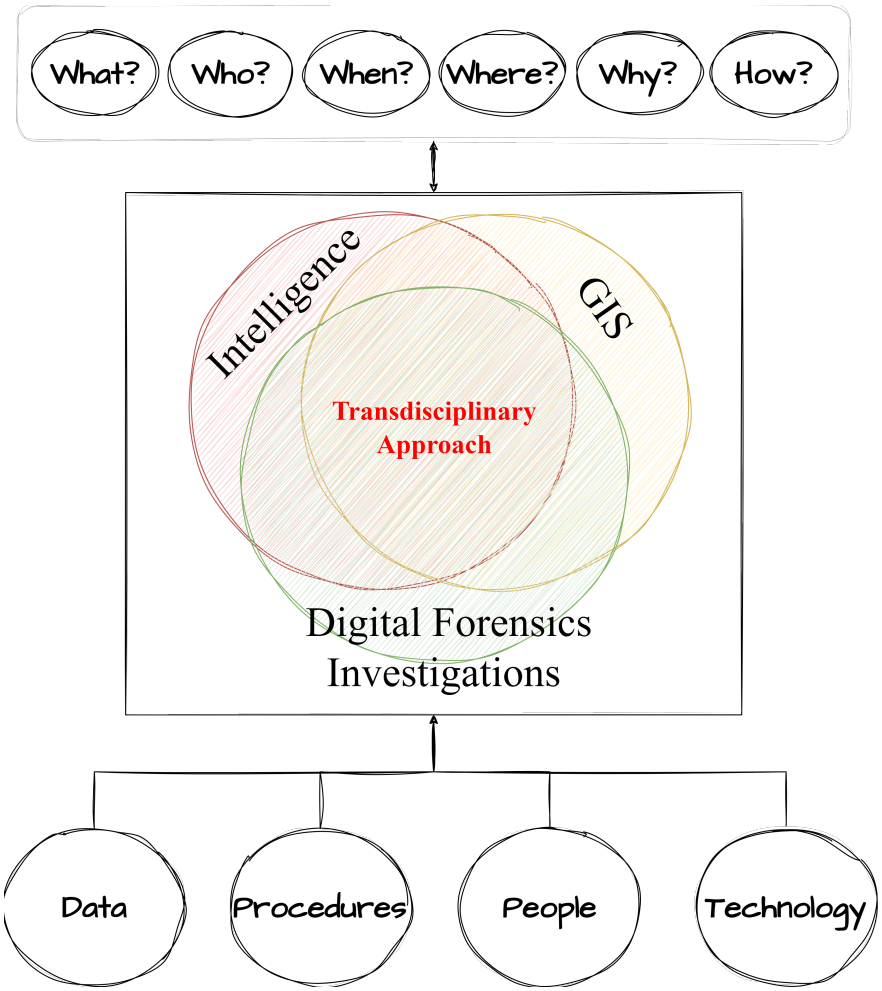


Figure 4.3. Factors and Fundamentals of the Approach

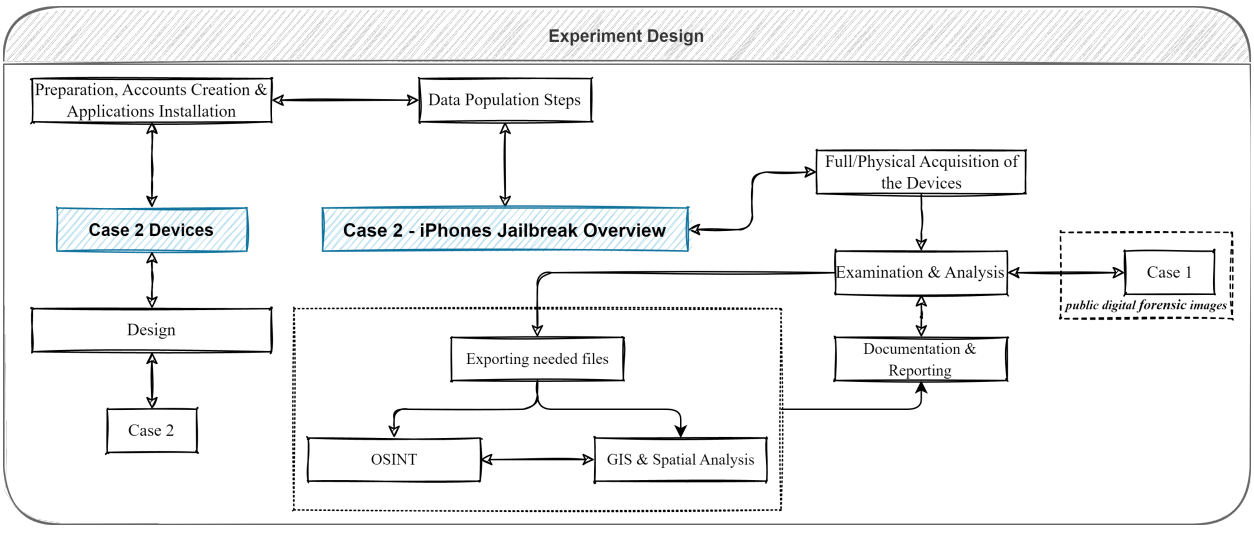


Figure 4.4. Experiment Investigation Methodology and Workflow.

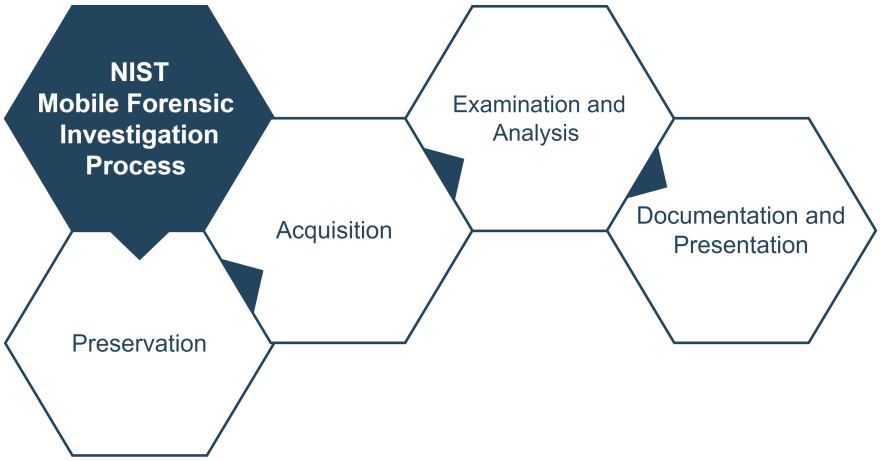


Figure 4.5. NIST high-level guidelines on mobile device forensics in [19].

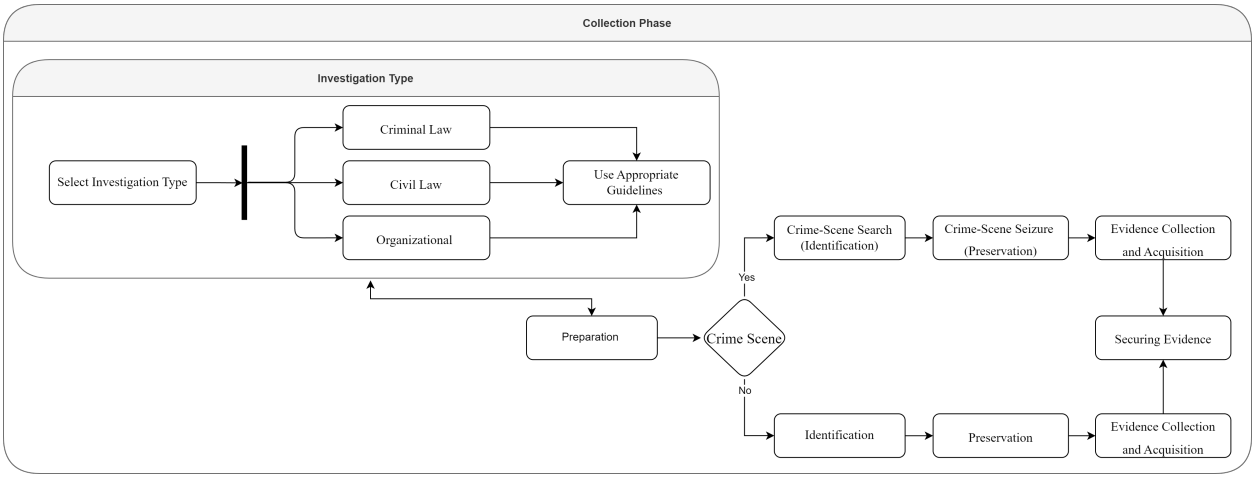


Figure 4.6. Collection phase procedures [19], [86].

Figure 4.7. DJI Mini 2 drone, Conrtoller, and iPhone.

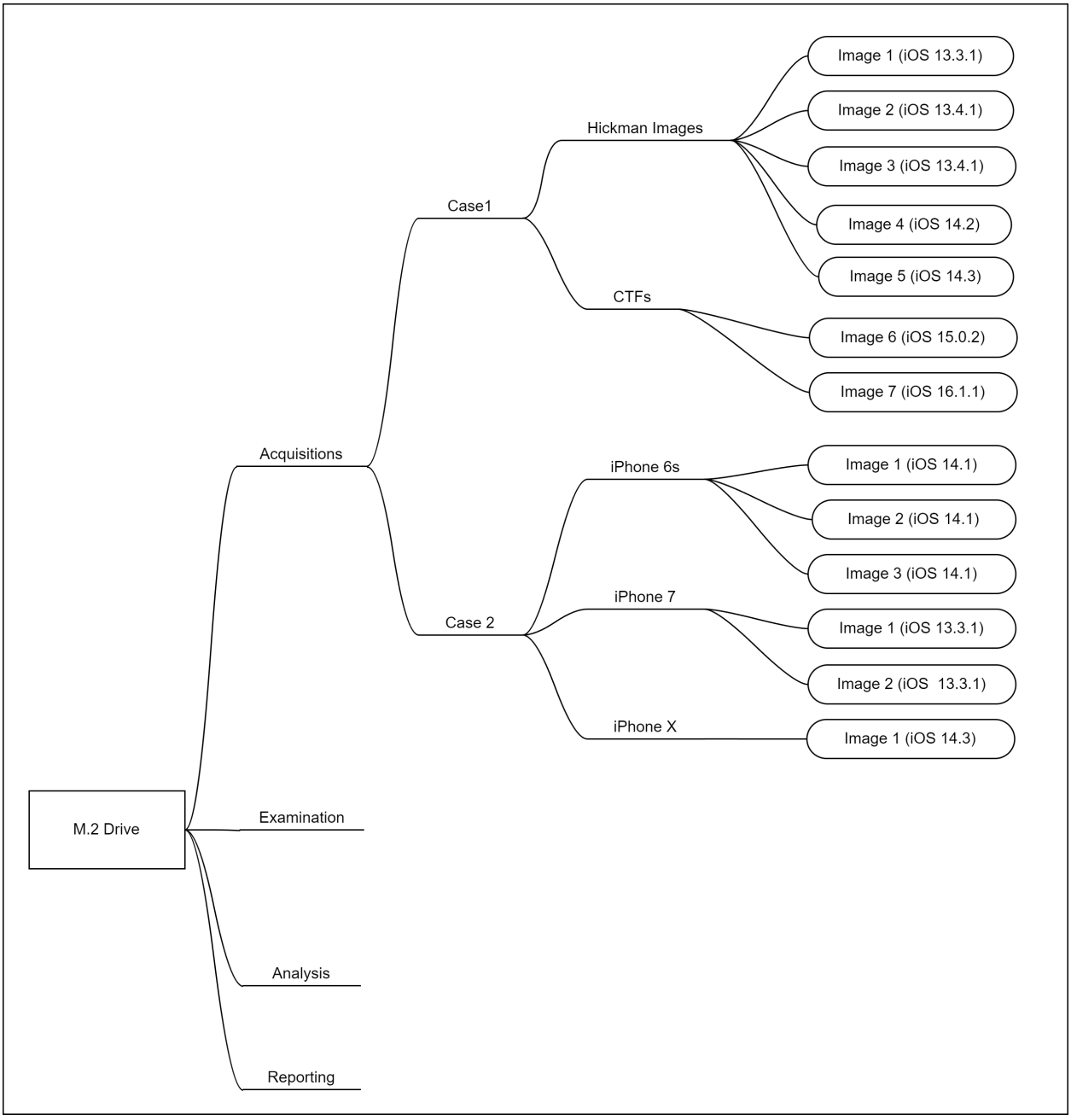


Figure 4.8. Structure of Acquisitions images on the drive

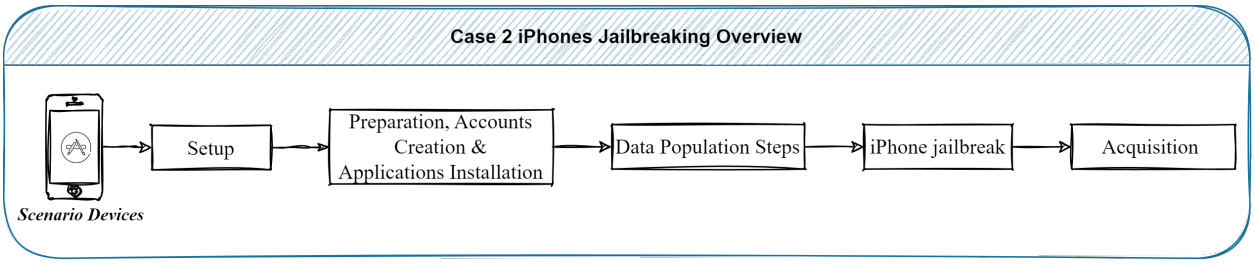


Figure 4.9. Acquisition and overview of the Jailbreaking after data population.

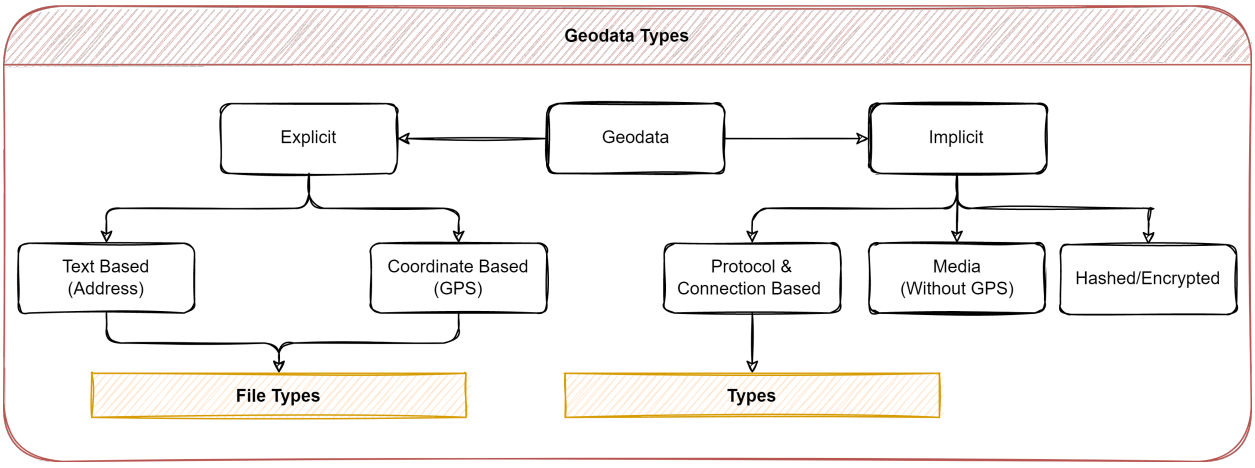


Figure 4.10. The Classification of Different Types of Geodata.

5. EXAMINATION AND ANALYSIS

At the start of the comprehensive mobile forensic examination phase, acquired and extracted digital forensic images were ingested into at least two digital forensic tools. In addition to creating a case for each digital forensic image, similar images of the same iPhone have been added in a single case. By adding similar images to a single case, investigators can access and examine digital evidence with better management and ease of use. However, proper high workstation hardware and specs are necessary as adding multiple digital forensic images into the same case may result in a large number of artifacts.

Figure 5.1 shows the structure of the cases created for the images in the study. This approach facilitated efficient data investigation, allowing comparison of results obtained from different tools and ensuring that no information was overlooked.

Furthermore, the use of multiple tools and cases also increased confidence in the findings, providing an opportunity to validate and cross-check the results. The process of ingestion of digital forensic images into Magnet Axiom and Autopsy involved selecting standard settings and running all possible modules. This was done to ensure a complete examination of the acquired and extracted data. Running all available modules, the software tools were able to automatically identify and extract as much data as possible from the digital forensic images. This approach allowed for a more thorough examination of digital forensic images and provided a better chance of discovering relevant information. Furthermore, the examination process was conducted without a time frame limit for all possible data, ensuring a thorough examination.

While conducting the comprehensive mobile forensics examination and analysis, iterative loops-based feedback and collected notes were used to build the framework, which is presented in Section 4. The process involves collecting evidence, exporting it, and then analyzing it to gain a deeper understanding of the data. This iterative process allows for refining the framework and understanding of the cases and the data they have, which can lead to a more robust and useful framework.

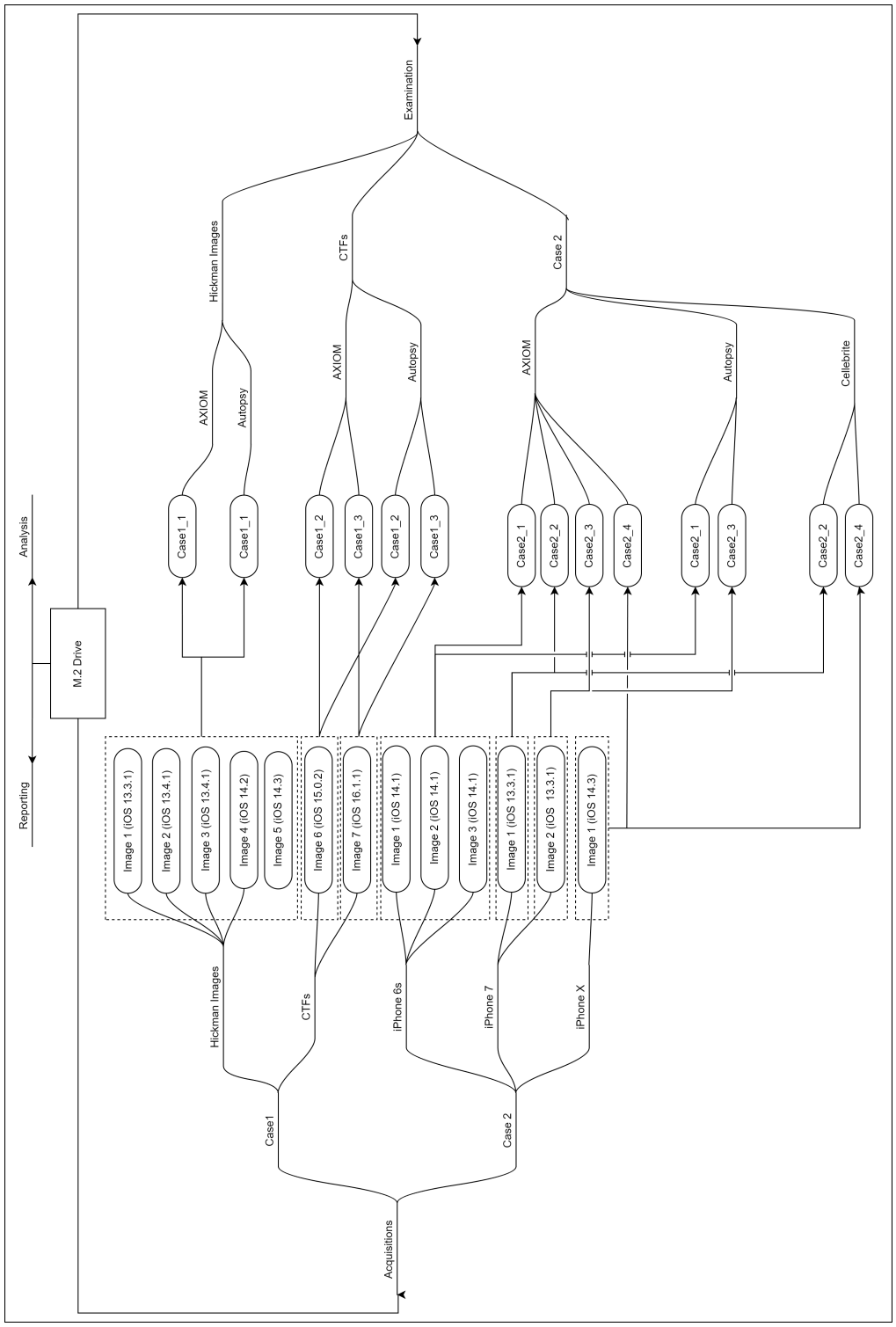


Figure 5.1. Structure of Examination cases on the external drive

5.1 Characteristics of Geodata Digital Evidence

Many file types can contain and present embedded spatial data (e.g., pictures, audio, video, documents, spreadsheets, data-based, etc.). In addition, other types of data can represent and hold geospatial data when investigated (e.g., IP address, WiFi, SSID, and text inside images). Furthermore, many devices store and use geolocation and spatial data, such as, but not limited to, smartphones, cars, tracking devices, watches, computers, laptops, cameras, drones, robots, and many more.

Therefore, it is evident that not all data formats that can represent geodata/geolocation information are taken into consideration when populating mobile devices. In the "Quick Start Guide for Populating Mobile Test Devices", which is considered one of the most critical documents for settling mobile devices that NIST develops, Section 8 talks about location data; however, only a few types of geolocation data are discussed [30], for example, GPS-related applications, routes, check-ins, and geotagged information. There are more than just these to consider when dealing with geolocation data. The classification model proposed in the methodology is used as a general classification of geodata. In other words, each time geodata is found in the cases, they are accordingly classified based on the data types that can be directly implied to find a location and the other type where there is a need for more investigation techniques to find the associated location. In the coming subsections, examples of important recovered artifacts that can be used to help with geo-contextualization.

5.1.1 Global Positioning System (GPS)

GPS coordinates can be crucial in digital forensic investigations, especially when a suspect's or victim's whereabouts, past locations, and movements are significant to the investigated case. Modern digital forensic tools can retrieve and display GPS data. These can include information such as the latitude and longitude coordinates of the device at specific times, as well as other location-related metadata such as altitude, speed, and direction, which provide valuable case insights. Moreover, digital forensic investigators must know how to recover GPS data and preserve and analyze it according to legal and ethical standards.

One of the most critical databases that holds GPS points for the iPhone at very high frequency is `Cache.sqlite` database. This database is located at `\private\var\mobile\Library\Caches\com.apple.routined\` and has more than 15 tables with valuable geodata, such as GPS points.

First, a table named `ZRTCLLOCATIONMO` inside the `Cache.sqlite` database contains accurate information along with GPS points. It contains a detailed location for the user with almost a week's worth of data. On the other hand, the table is known to keep records for around 7 days; however, examining and analyzing Image3 within Case1, the table contains data that go back more than 7 months. This was an extreme case, but more studies are needed to highlight why such behavior would happen. Figure 5.2 illustrates the table along with the columns, including:

- `Z_PK`: a unique identifier
- `ZALTITUDE`: Altitude, measured in meters,
- `ZVERTICALACCURACY`: Altitude accuracy measured in meters,
- `ZCOURSE`: direction, measured between 0-360 if it is populated, and -1 if not,
- `ZSPEED`: speed measured as meters per second,
- `ZLATITUDE`: Latitude in degrees,
- `ZLONGITUDE`: Longitude in degrees,
- `ZHORIZONTALACCURACY`: Horizontal accuracy measured in meters, and according to Apple developer documentation [284], this value indicates the radius of that circle of uncertainty for the location,
- `ZTIMESTAMP`: The timestamp in apple format.

Although the digital forensic tools tested have done a great job recovering this information, it was not as impressive as displaying them in the World Map View. Furthermore, it was lagging, and sometimes the entire software crashed when trying to plot the locations

SQLITE VIEWER

Select table ZRTCLLOCATIONMO

FIND BUILD QUERY EXPORT SHOW / HIDE COLUMNS

#	Z_PK	Z_ENT	Z_OPT	ZALTITUDE	ZVERTICALACCURACY	ZCOURSE	ZSPEED	ZLATITUDE	ZLONGITUDE	ZHORIZONTALACCURACY	ZTIMESTAMP
7562	49755	2	1	787	12	45.59375	0.75	35.654820750011 6	-78.8345787752826	5	635117654.025375
7563	49756	2	1	100.50099945068 4	55.3586578369141	-1	-1	35.6699890757404	-78.852833787072	3000	635117648.740757
7564	49757	2	1	100.26000213623	186.4000030756	-1	-1	35.6601882936088	-78.8508254997555	165	635117301.585325
7565	49758	2	1	133.1120262146	8	90.703125	0.75	35.6548242504109	-78.8344209362556	10	635117656.022689
7566	49759	2	1	127.773769378662	6	87.890625	1.37000000476837	35.6548860250373	-78.8343483489741	10	635117661.015876
7567	49760	2	1	133.571804046631	6	87.5390625	0.519999980926514	35.6548857735802	-78.8343414758135	10	635117667.010229
7568	49761	2	1	129.401699066162	6	91.0546875	1.55999994277954	35.6548779365007	-78.8343830500532	10	635117658.01967
7569	49762	2	1	132.722805023193	6	87.5390625	0.150000005960464	35.6548841810186	-78.8343529590208	10	635117666.011002
7570	49763	2	1	132.43087387085	6	87.5390625	0	35.6548807863478	-78.8343607541908	10	635117665.011824
7571	49764	2	1	132.045375823975	8	90.703125	1.55999994277954	35.6548761343915	-78.83437986493	10	635117659.018329
7572	49765	2	1	131.236415863037	6	87.5390625	0.150000005960464	35.6548807863478	-78.8343607541908	10	635117664.012701
7573	49766	2	1	131.328456878662	6	87.890625	0.680000007152557	35.6548749609251	-78.8343448285748	10	635117663.013662

Figure 5.2. Cached locations recovered from the device that recorded the user's movements for around a week.

on the map for the cases where it contained combined iPhone images. However, the performance is outside the scope of this investigation. Still, it shows the lack of capability of digital forensic tools in handling many GPS points.

Second, the `\private\var\mobile\Library\Caches\com.apple.routined\Cloud-V2.sqlite` database contains multiple tables of interest. The following are some important tables:

- `ZRTDEVICEMO`: The table contains devices that were set up and connected to the same iCloud account (see Figure 5.4; it shows duplicate device information for older setup times for older images). For iOS 14.3, the iPhone is registered as 1 and the Apple Watch as 7.
- `ZRTADDRESSMO`: Table with addresses,
- `ZRTMAPITEMMO`: Table contains GPS locations for frequent places, and

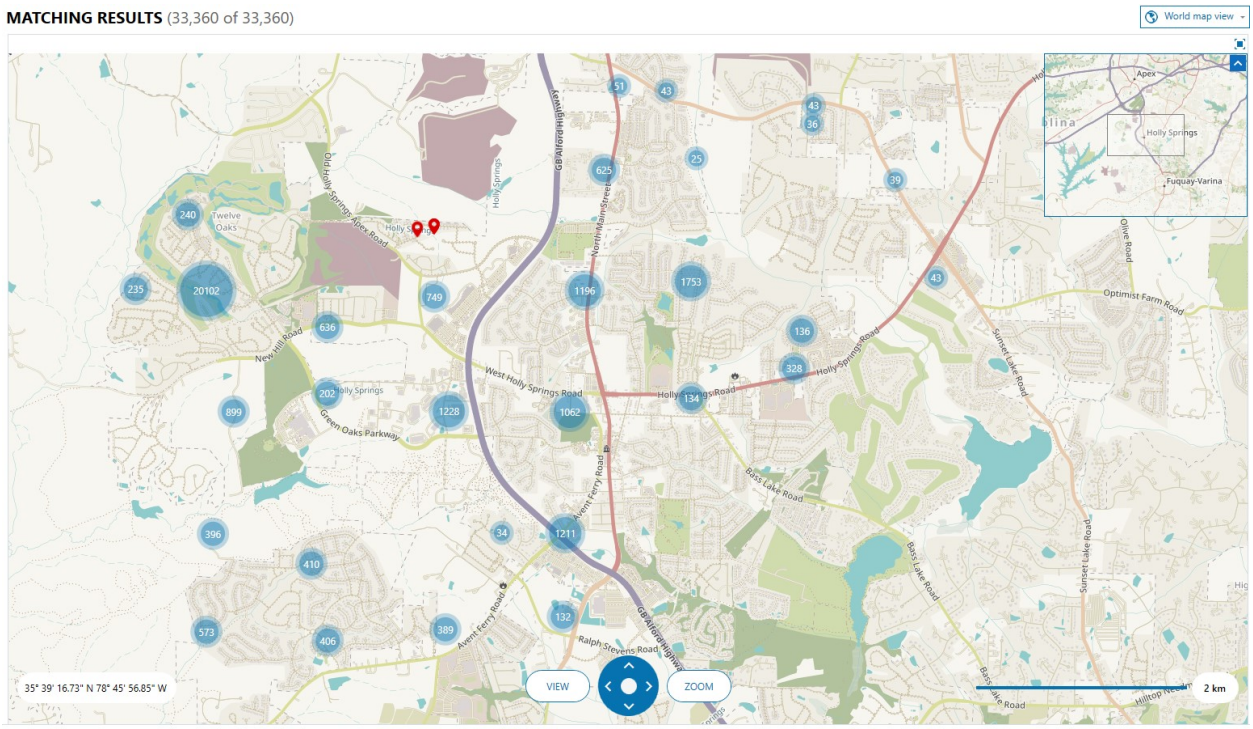
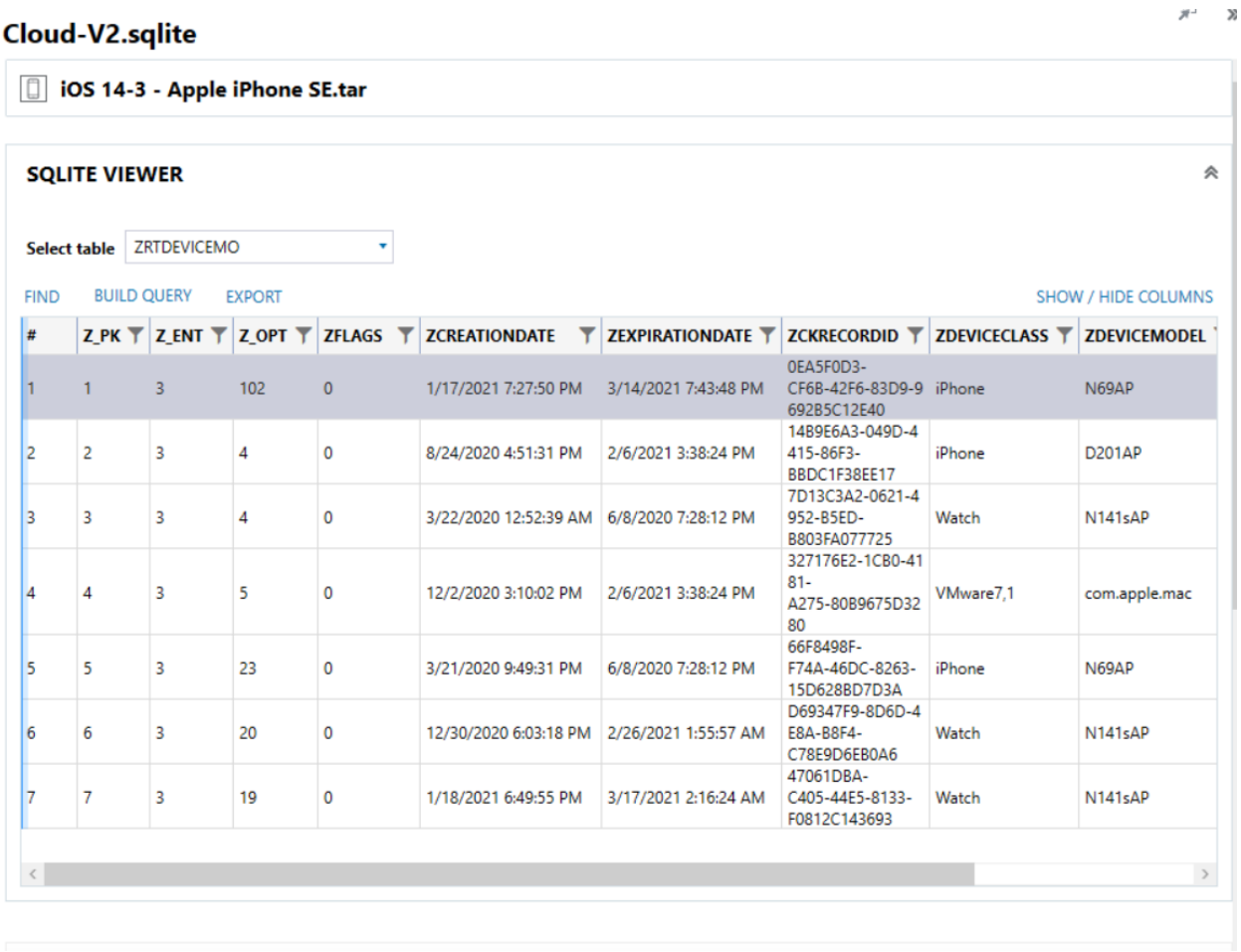


Figure 5.3. Aggregated Locations in the World Map view

- `ZRTLEARNEDPLACEMO`: Table contains locations with the type of device and map location (see Figure 5.5 for significant locations learned from 1 and 7, iPhone and Apple Watch, respectively)

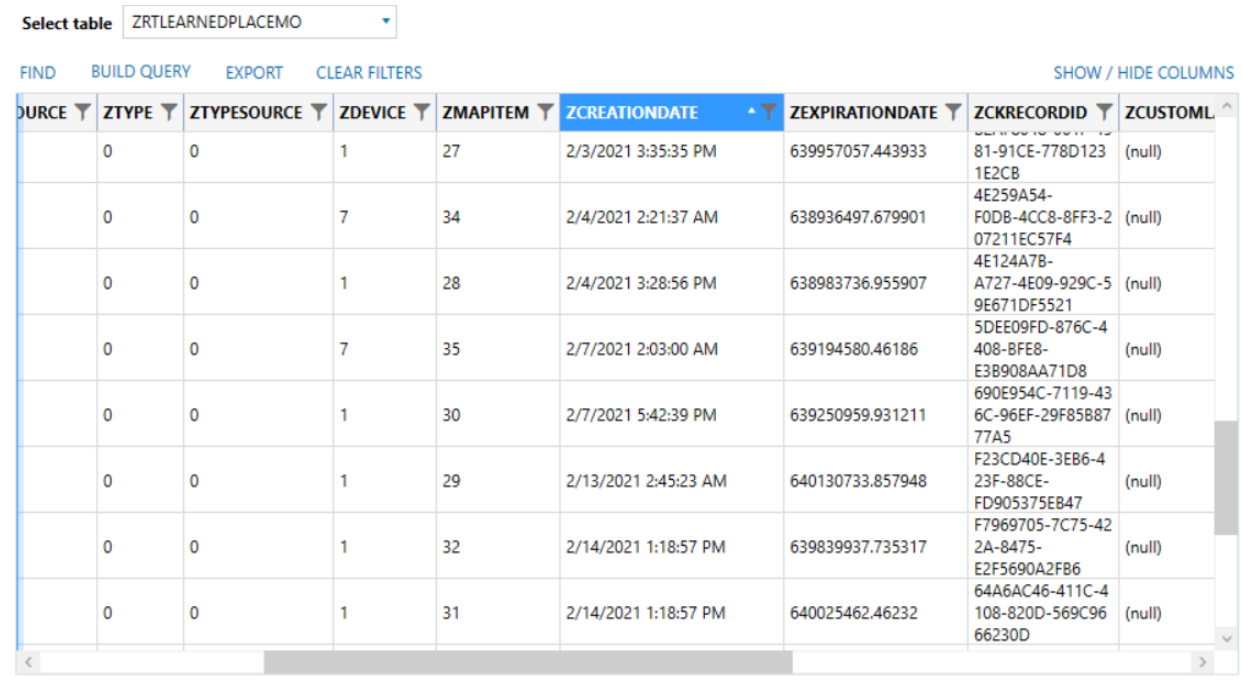
Moreover, similar to `ZRTCLLOCATIONMO` table, the `ZRTLEARNEDLOCATIONOFINTERESTVISITMO` table, which is located within the following SQLite database `\private\var\mobile\Library\Caches\com.apple.routined\Local.sqlite` contains significant location visits and the duration the user stayed at these locations. Figure 5.6 demonstrates the recovered details and highlights the entry and exit times. Although this information is not categorized into what this location represents to the user, it is essential to be linked when creating a day in the life of the user type of analysis. Figure 5.6 shows that Magnet AXIOM aggregates the data.

Other vital artifacts associated with FindMy services are located within `\private\var\mobile\Library\Caches\com.apple.findmy.fmipcore\Devices.data`. This information includes the device's name, last GPS location, last Address, and other columns associated



#	Z_PK	Z_ENT	Z_OPT	ZFLAGS	ZCREATIONDATE	ZEXPIRATIONDATE	ZCKRECORDID	ZDEVICECLASS	ZDEVICEMODEL
1	1	3	102	0	1/17/2021 7:27:50 PM	3/14/2021 7:43:48 PM	0EA5F0D3-CF6B-42F6-83D9-9692B5C12E40	iPhone	N69AP
2	2	3	4	0	8/24/2020 4:51:31 PM	2/6/2021 3:38:24 PM	14B9E6A3-049D-4415-86F3-BBDC1F38EE17	iPhone	D201AP
3	3	3	4	0	3/22/2020 12:52:39 AM	6/8/2020 7:28:12 PM	7D13C3A2-0621-4952-B5ED-B803FA077725	Watch	N141sAP
4	4	3	5	0	12/2/2020 3:10:02 PM	2/6/2021 3:38:24 PM	327176E2-1CB0-4181-A275-80B9675D3280	VMware7,1	com.apple.mac
5	5	3	23	0	3/21/2020 9:49:31 PM	6/8/2020 7:28:12 PM	66F8498F-F74A-46DC-8263-15D628BD7D3A	iPhone	N69AP
6	6	3	20	0	12/30/2020 6:03:18 PM	2/26/2021 1:55:57 AM	D69347F9-8D6D-4E8A-B8F4-C78E9D6EB0A6	Watch	N141sAP
7	7	3	19	0	1/18/2021 6:49:55 PM	3/17/2021 2:16:24 AM	47061DBA-C405-44E5-8133-F0812C143693	Watch	N141sAP

Figure 5.4. Table ZRTDEVICEMO showing different devices linked to the iCloud account



Select table ZRTLEARNEDPLACEMO

FIND BUILD QUERY EXPORT CLEAR FILTERS SHOW / HIDE COLUMNS

URCE	ZTYPE	ZTYPESOURCE	ZDEVICE	ZMAPITEM	ZCREATIONDATE	ZEXPIRATIONDATE	ZCKRECORDID	ZCUSTOML
	0	0	1	27	2/3/2021 3:35:35 PM	639957057.443933	81-91CE-778D123 1E2CB	(null)
	0	0	7	34	2/4/2021 2:21:37 AM	638936497.679901	4E259A54-F0DB-4CC8-8FF3-2 07211EC57F4	(null)
	0	0	1	28	2/4/2021 3:28:56 PM	638983736.955907	4E124A7B-A727-4E09-929C-5 9E671DF5521	(null)
	0	0	7	35	2/7/2021 2:03:00 AM	639194580.46186	5DEE09FD-876C-4 408-BFE8-E3B908AA71D8	(null)
	0	0	1	30	2/7/2021 5:42:39 PM	639250959.931211	690E954C-7119-43 6C-96EF-29F85B87 77A5	(null)
	0	0	1	29	2/13/2021 2:45:23 AM	640130733.857948	F23CD40E-3EB6-4 23F-88CE-FD905375EB47	(null)
	0	0	1	32	2/14/2021 1:18:57 PM	639839937.735317	F7969705-7C75-42 2A-8475-E2F5690A2FB6	(null)
	0	0	1	31	2/14/2021 1:18:57 PM	640025462.46232	64A6AC46-411C-4 108-820D-569C96 66230D	(null)

Figure 5.5. Table ZRTLEARNEDPLACEMO showing the learned location from the devices used in iOS 14.3 image in case 1

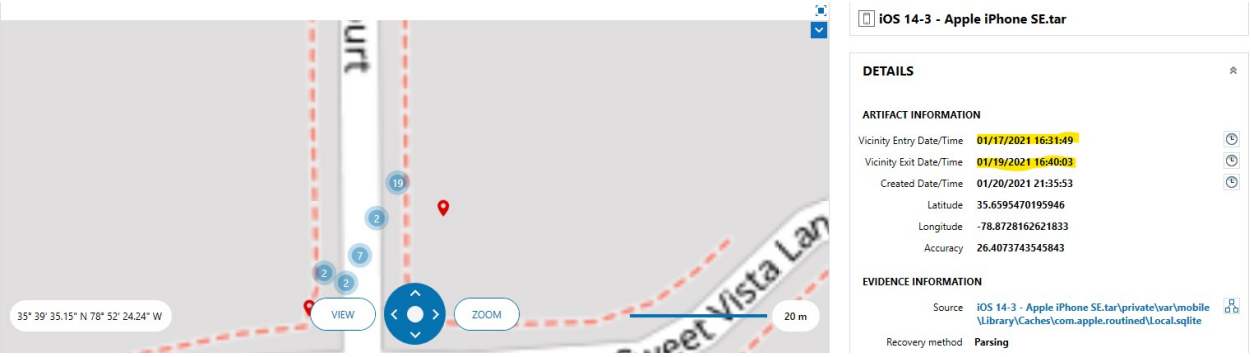


Figure 5.6. Location visits (entry and exit time)

with wiping the device's status. Other information regarding Airtags trackers can be found within `\private\var\mobile\Library\Caches\com.apple.findmy.fmipcore\Items.data`. The iPhone also records locations for car parking when the device loses connection with the car infotainment system in the `ZRTVEHICLEEVENTHISTORYMO` within the `\private\var\mobile\Library\Caches\com.apple.routined\Local.sqlite` database (see Figure 5.7 for an example of GPS locations). Moreover, iOS keeps track of geofences created to serve many apps, which are stored in table `Fences` within `\private\var\root\Library\Caches\location\consolidated.db` database. This table contains BundleID (the service), timestamp, GPS, and fence radius.

Geo-tagged Photos and Videos

Recently, there has been an increase in smartphones that can capture additional data (e.g., GPS tags) when taking a photo. Responders and digital forensic investigators often consider photos an essential source of information, especially when dealing with mobile investigations, as photos could be embedded with the corresponding GPS data. There were images in most of the cases; images were taken using the phone while GPS tags were enabled. These geotags are embedded in the EXIF data. These images were recovered from `\private\var\mobile\Media\PhotoData\` and `\private\var\mobile\Media\DCIM\100APPLE\`. Figure 5.8 is an example of one of these images and its location and metadata shown in AXIOM Examine. Although general GPS information would be satisfactory in some cases, other

SQLITE VIEWER

Select table ZRTVEHICLEEVENTHISTORYMO

FIND BUILD QUERY EXPORT SHOW / HIDE COLUMNS

#	Z_PK	Z_ENT	Z_OPT	ZDATE	ZLOCDATE	ZLOCLATITUDE	ZLOCLONGITUDE	ZLOCUNCERTAINTY	ZIDENTIFIER
1	1	19	1	1/27/2021 10:00:34 PM	1/27/2021 10:00:34 PM	35.6668583578249	-78.831158544128	5.00990664958954	1834B0E1-3BEE-43E4-BE2F-3A344E3909C7
2	2	19	1	1/27/2021 10:26:16 PM	1/27/2021 10:26:16 PM	35.6588646026924	-78.8741056768165	6.25766617059708	D24DC9C1-7CC2-4064-8508-A14306DB405C
3	3	19	1	1/28/2021 10:04:08 PM	1/28/2021 10:04:08 PM	35.6668587103987	-78.8312116719422	5.50276470184326	D3185E4E-D3AB-4303-85E2-DB27F479066E
4	4	19	1	1/28/2021 10:31:24 PM	1/28/2021 10:31:24 PM	35.6590503769463	-78.873765373966	5.11200726032257	DC8694E5-377C-410B-B802-D3B25453889B
5	5	19	1	1/28/2021 10:31:24 PM	1/28/2021 10:31:24 PM	35.6590503769463	-78.873765373966	5.11200726032257	DC8694E5-377C-410B-B802-D3B25453889B
6	6	19	1	1/28/2021 10:31:24 PM	1/28/2021 10:31:24 PM	35.6590503769463	-78.873765373966	5.11200726032257	DC8694E5-377C-410B-B802-D3B25453889B
7	7	19	1	1/29/2021 10:04:31 PM	1/29/2021 10:04:31 PM	35.6668387173766	-78.831155705659	5.30437099933624	83B460F1-2047-46E3-A89A-B7D89BF5000D
8	8	19	1	2/3/2021 5:02:33 PM	2/3/2021 5:02:33 PM	35.6591692330891	-78.8365191222319	5.09732842445374	19ABD50E-B8B3-4B5D-910F-90A7EA15F5FB
9	9	19	1	2/3/2021 5:18:00 PM	2/3/2021 5:18:00 PM	35.6593427356253	-78.8727545463182	7.16816370020462	46F20116-3FD3-42A7-AC17-6A2D89A34BAA
10	10	19	1	2/3/2021 5:18:00 PM	2/3/2021 5:18:00 PM	35.6593427356253	-78.8727545463182	7.16816370020462	46F20116-3FD3-42A7-AC17-6A2D89A34BAA
11	11	19	1	2/3/2021 5:18:00 PM	2/3/2021 5:18:00 PM	35.6593427356253	-78.8727545463182	7.16816370020462	46F20116-3FD3-42A7-AC17-6A2D89A34BAA
12	12	19	1	2/3/2021 5:18:00 PM	2/3/2021 5:18:00 PM	35.6593427356253	-78.8727545463182	7.16816370020462	46F20116-3FD3-42A7-AC17-6A2D89A34BAA

Figure 5.7. Table ZRTVEHICLEEVENTHISTORYMO that contains car parked locations and timestamps

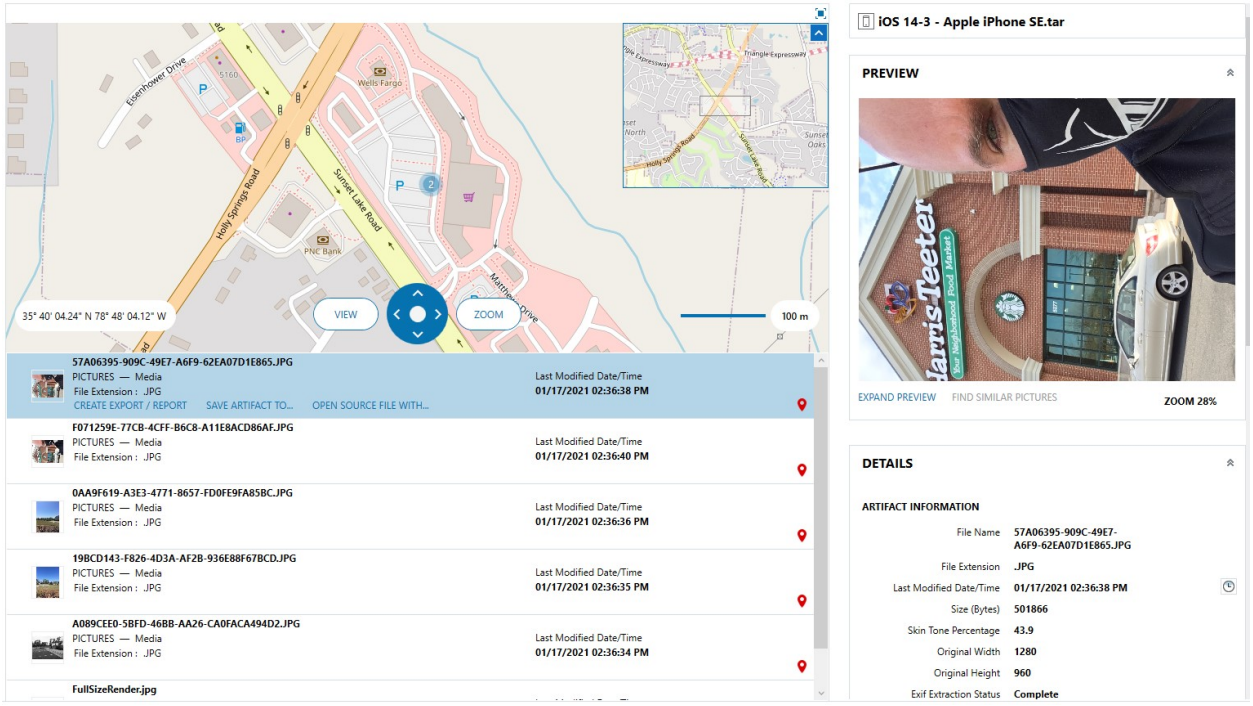


Figure 5.8. AXIOM World Map View of the recovered photos.

EXIF data induce image direction and speed that might aid investigators and can be helpful in many investigation settings. However, these tools only present limited EXIF data related to geolocation (i.e., latitude, longitude, and altitude). Therefore, extracting these images and then using EXIFTool to check other metadata is necessary. This recovered more information using EXIFTool, and Figure 5.9 shows other metadata that can be recovered, such as `GPShorizontalpositionerror,GPStimestamp,anddirection`. This information will be essential to an investigation and may lead to better conclusions. For example, looking at the GPS timestamp may indicate whether the photo has been modified or if the timestamp has been changed.

5.1.2 IP Addresses

To recover IP addresses, it is suggested to use regular expressions (regex), patterns used to match and manipulate text based on specific rules and criteria and run them over the

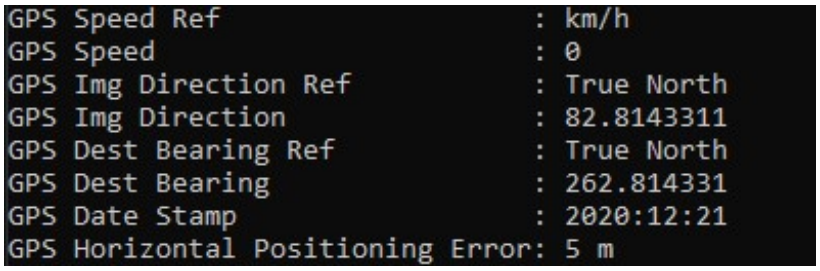


Figure 5.9. GPS Horizontal Positioning Error of a photo recovered using EXIFTool

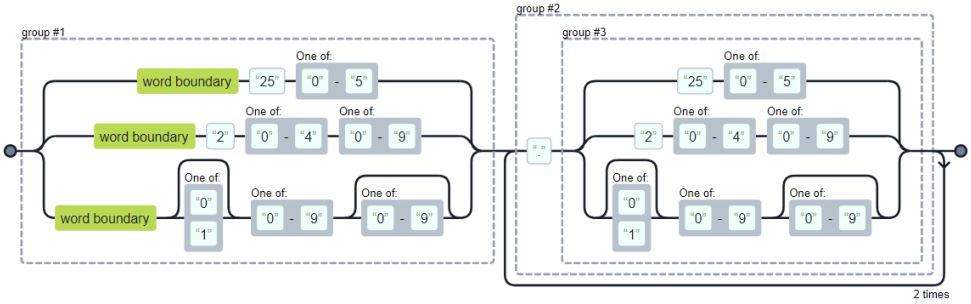
regex for **ip address(ipv4)**

match an ipv4 address

```
(\b25[0-5]|\b2[0-4][0-9]|\b[01]?[0-9][0-9]?)(\.(25[0-5]|2[0-4][0-9]|
[01]?[0-9][0-9]?)){3}
```

show matches

Matches an ip address(version 4)



regex for **ip address(ipv6)**

match an ipv6 address

```
(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|
([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:
[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4})
{1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]
{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]
{1,4}){1,6})|:((:[0-9a-fA-F]{1,4}){1,7}|:)|fe80:(:[0-9a-fA-F]{0,4})
{0,4}%[0-9a-zA-Z]{1,}|::(ffff(:0{1,4}){0,1}:){0,1}((25[0-5]|(2[0-
4]|1{0,1}[0-9]){0,1}[0-9])\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}
[0-9])|([0-9a-fA-F]{1,4}:){1,4}:((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-
9])\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9]))
```

Figure 5.10. Regular Expressions for IPv4 and IPv6 From ihateregex.io [285], [286].

case. Figure 5.10 illustrates the regular expressions for IPv4 and IPv6 that were used and taken from ihateregex.io [285], [286]. Figure 5.11 illustrates the regular expression search mechanism in Magnet Axiom and Autopsy, and Figure 5.12 is an example of what Magnet AXIOM was able to recover. In particular, regular expressions are a powerful way of searching for particular patterns, which can be used for many things.

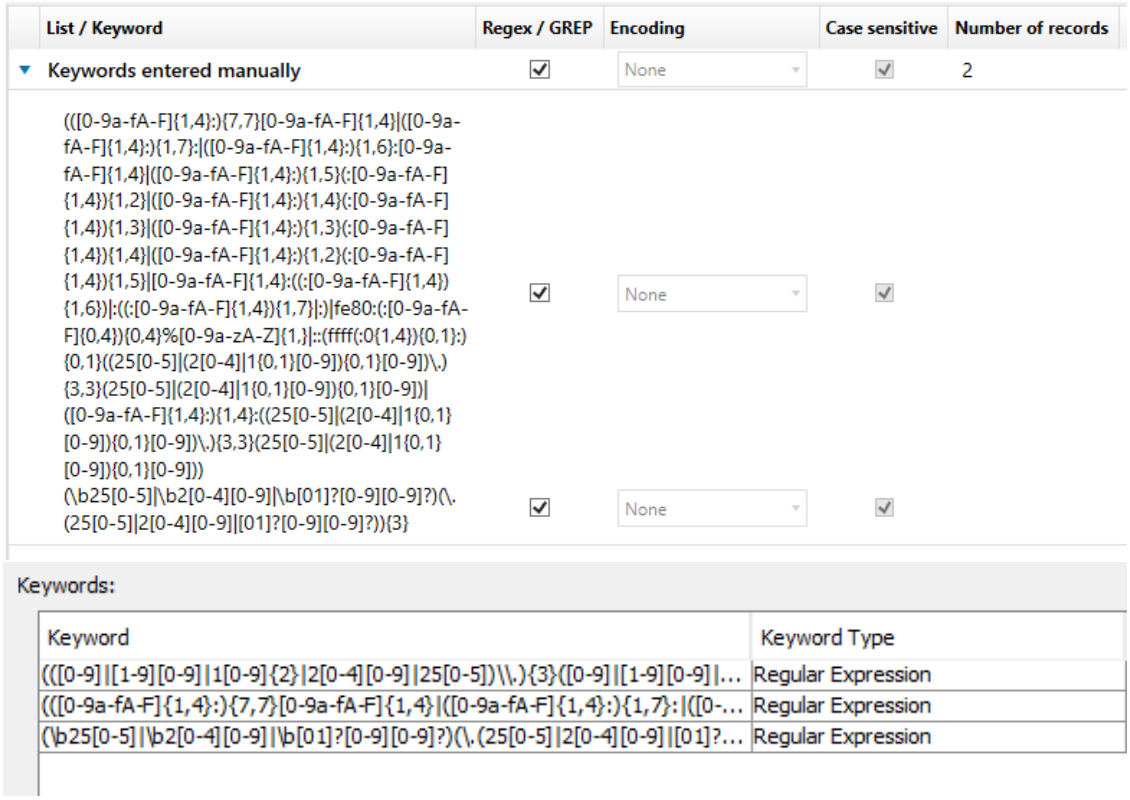


Figure 5.11. Search by Regular Expression in AXIOM and Autopsy.

Although not all cases may yield critical IP addresses, in Case 1, within the five images, the tools using the regular expression recovered critical recovery snippets of carved data with valid IP addresses (e.g., not internal IP addresses). Using Autopsy enabled to export the recovered IP addresses with the number of hits in the case. Digital forensic tools have yet to get IP mapping functions; therefore, these data will be analyzed using OSINT. Moreover, incoming email headers revealed IP addresses that could be important to determine the relative location of other people at the time of the email.

5.1.3 Cell Site Location Information (CSLI)

CSLI is a type of data that can be requested by law enforcement from cellular carriers (providers) using subpoenas or search warrants that are supported by probable cause. Cell towers generate these data and can provide information on the approximate location of

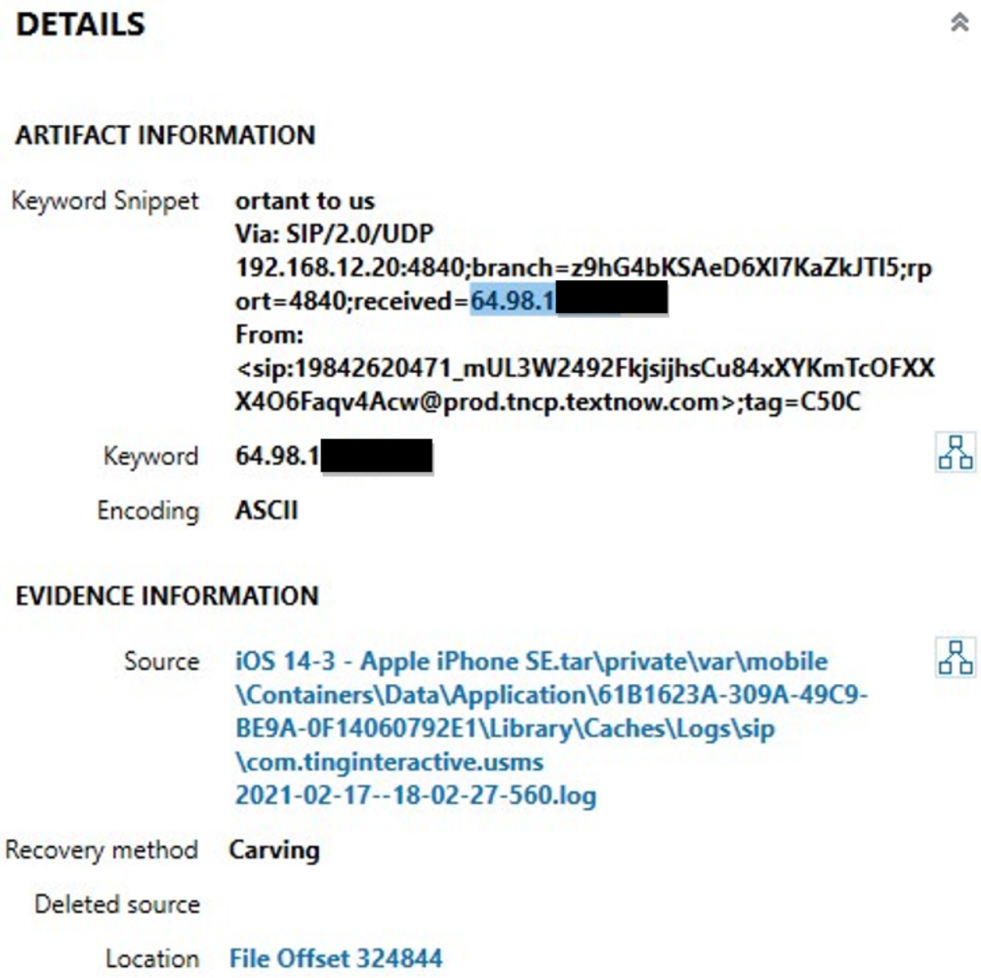


Figure 5.12. Recovered IP address using regex.

nearby devices at a given time or in other wards; these data are generated each time a mobile phone connects to a nearby cell tower [287]. Moreover, this information can approximate the location of the device in the present and the past (i.e., historical data), which is commonly used. Therefore, law enforcement and digital forensics investigations using these data enable them to track the movements of a suspect's mobile device over time. Unlike data on the phone, the user cannot erase or alter the CSLI as the carrier stores it. However, there are significant drawbacks to relying on CSLI alone. The data provide only a coarse approximation of the location rather than a precise location. Therefore, this information must be compared, cross-examined, and analyzed in conjunction with other sources of information,

such as geodata within the same device if available, so the data can be correlated, producing more accurate information.

iPhone devices are known to store such data, which is valuable in cases where CSLI is required to correlate with stored and cached data. This can provide more accurate measurements. The examination revealed that such data could be recovered from a table named `LteCellLocation` within the `\private\var\root\Library\Caches\locationd\cache_encryptedB.db` database (see Figure 5.13 shows the recovered table). The examination also revealed that the horizontal accuracy of the GPS plots differs between images, meaning that the range generated and measured by the iPhone.

EVIDENCE (521) Column view

CellID	Loca...	Mob...	Mob...	Timestamp Date...	Latitude	Longitude	Range	Confide...
34896446	31734	311	490	02/18/2021 04:15:39 PM	35.55601119	-79.02896881	5329.0	70
19210242	31734	310	260	02/18/2021 04:15:39 PM	35.53649902	-79.02610015	3347.0	70
19210497	31734	311	490	02/18/2021 04:15:39 PM	35.60044479	-79.08650207	5562.0	70
19210813	31734	311	490	02/18/2021 04:15:39 PM	35.60009765	-79.07634735	9454.0	70
195603629	10010	313	100	02/18/2021 04:15:39 PM	35.5915718	-79.03292083	6226.0	70
19148546	31734	311	490	02/18/2021 04:15:39 PM	35.58890533	-79.0668106	4529.0	70
263367904	39933	311	480	02/18/2021 04:15:39 PM	35.59432983	-79.01428985	11065.0	70
31494425	31734	311	882	02/18/2021 04:15:39 PM	35.53411483	-79.0348587	4215.0	70
263710069	39933	311	480	02/18/2021 04:15:39 PM	35.56682968	-79.02785491	1414.0	70
263928263	39933	311	480	02/18/2021 04:15:39 PM	35.56682968	-79.02777099	1414.0	70
19210242	31734	311	490	02/18/2021 04:15:39 PM	35.54468154	-79.02571105	18137.0	70
264510524	39924	311	480	02/18/2021 04:15:39 PM	35.55770492	-79.08480072	1414.0	70

Figure 5.13. Cell Towers geolocation recovered from the iPhone.

5.1.4 Wi-Fi

WiFi MAC addresses (BSSID) and SSIDs can provide geographical information in digital forensic investigations. Investigators can use the MAC addresses of recovered encountered nearby Wi-Fi access points and their latitude and longitude to locate a device at a specific time and date. Moreover, they can be used to establish suspect movements or detect recently visited locations, revealing essential insights. These data can be recovered within a table named `WifiLocation` within `\private\var\root\Library\Caches\`

EVIDENCE (21,472) Column view

MAC Ad...	Chan...	Timestamp Date/Time	Latit...	Longi...	Accuracy (meters)
00:04:96:C9:35:A0	6	02/16/2021 11:45:40 AM	35.64082717	-78.83914184	86.0
00:04:96:C9:35:A0	6	02/16/2021 11:57:40 AM	35.64082717	-78.83914184	86.0
00:04:F3:1D:A2:E4	6	02/19/2021 12:09:53 PM	35.66999435	-78.87699127	85.0
00:04:F3:1D:A2:E4	6	02/19/2021 12:14:28 PM	35.66999435	-78.87699127	85.0
00:0E:C6:20:B4:CD	11	02/15/2021 10:50:07 AM	35.66022491	-78.88262939	39.0
00:0E:C6:20:B4:CD	11	02/19/2021 04:51:21 PM	35.66024017	-78.88262939	39.0
00:0F:00:57:B8:CE	1	02/18/2021 02:46:45 PM	35.65522766	-78.83513641	39.0
00:11:32:6C:35:2C	10	02/15/2021 10:50:42 AM	35.66209411	-78.88029479	36.0
00:11:32:6C:35:2C	10	02/18/2021 02:34:57 PM	35.66209793	-78.88028717	34.0

Figure 5.14. Wi-Fi access points geolocations recovered from the iPhone.

`locationd\cache_encryptedB.db`, and table `ZACCESSPOINT` within `\private\var\root\Library\Caches\com.apple.wifid\ThreeBars.sqlite` database.

The table contains data on the MAC address, channel, latitude, and longitude of the Wi-Fi access points encountered, timestamp, confidence, and accuracy level measured in meters. Examining the timestamps of the recorded MAC address of Wi-Fi happens to be stored in bulk if the user is moving. Moreover, suppose that the user encounters the same access point twice. In that case, it will register twice because the examination revealed that the same access point MAC addresses were stored but with different timestamps for each encounter. Figure 5.14 shows the columns and some recovered records of the 21,472 records. Moreover, Figure 5.15 shows three encounters of the same MAc address within the same digital forensic image, and the blue highlights are the similar encounters between different images in Case 1.

On the other hand, when the device is trying to acquire a location using A-GPS, it scans for nearby Wi-Fi signals. This information, including BSSID, timestamp, Received Signal Strength Indicator (RSSI), and channel, are stored within table `ZRTWIFIACCESSPOINTMO` in the `private\var\mobile\Library\Caches\com.apple.routined\Cache.sqlite` database (see Figure 5.16). Although it does not have GPS locations for the scanned and stored Wi-Fi BSSIDs, it can be used to prove that the device was near these access points at some point,

MAC Ad...	Source	Timestamp Date...	Chan...	Latit...	Longit...	Accu...	Confidence
78:29:ED:A5:5C:36	iOS 14-3 -...	02/16/2021 04:46:42 PM	1	35.65838241	-78.87897491	106.0	50
78:29:ED:A5:5C:36	iOS 14-3 -...	02/17/2021 06:29:07 PM	1	35.65838241	-78.87897491	106.0	50
78:29:ED:A5:5C:36	iOS 14-3 -...	02/18/2021 04:38:36 PM	1	35.65838241	-78.87897491	106.0	50
78:29:ED:BF:5B:3A	iOS 14-3 -...	02/18/2021 02:31:22 PM	6	35.66685867	-78.87758636	47.0	50
78:29:ED:BF:5B:3A	13-3-1.tar\...	04/12/2020 10:21:21 AM	5	35.66685955	-78.87760463	63.0	50

Figure 5.15. Similar Wi-Fi BSSID Encounters.

SQLITE VIEWER

Select table ZRTWIFIACCESSPOINTMO

FIND BUILD QUERY EXPORT SHOW / HIDE COLUMNS

#	Z_PK	Z_ENT	Z_OPT	ZCHANNEL	ZRSSI	ZFINGERPRINT	ZAGE	ZDATE	ZMAC
5128	28045	22	1	1	-66	686	0.487	4/16/2020 11:51:54 AM	f8:bb:bf:90:a8:f9
5129	28046	22	1	11	-83	686	6.691	4/16/2020 11:51:48 AM	74:83:c2:77:fd:92
5130	28047	22	1	1	-42	686	0.411	4/16/2020 11:51:54 AM	f8:bb:bf:1e:fa:ef
5131	28048	22	1	6	-92	686	13.955	4/16/2020 11:51:41 AM	d8:32:14:bd:2e:41
5132	28049	22	1	6	-77	686	0.274	4/16/2020 11:51:55 AM	7c:db:98:c2:30:33
5133	28050	22	1	6	-91	686	14.147	4/16/2020 11:51:48 AM	b6:7c:9c:26:a7:f0
5134	28051	22	1	1	-63	686	0.711	4/16/2020 11:52:01 AM	f8:bb:bf:8d:b9:c5

Figure 5.16. Table ZRTWIFIACCESSPOINTMO within Cache.SQLite database showing used Wi-Fi signals for A-GPS

which can be mapped and correlated with other tables or OSINT to find the location of these BSSIDs.

Moreover, the file `com.apple.wifi.plist` is stored in a property list (plist) format, a structured data format commonly used by Apple software. This file is within the `\private\var\preferences\SystemConfiguration\` folder. It is essential because it is a configuration file that stores information about the Wi-Fi networks to which the device has connected or attempted to connect in the past. It also contains details such as the SSID and MAC address of the access points and other settings. Although this file does not have GPS data, digital forensic investigators can analyze it to determine a device's Wi-Fi network usage history. Furthermore, some new cars have Wi-Fi Carplay functionality, and information can be found if the device was ever connected to a car that has this functionality within the `\private\var\mobile\Library\Preferences\com.apple.carplay.plist` file.

5.1.5 Bluetooth

Bluetooth artifacts play an essential role in digital forensic investigations, particularly in cases involving mobile devices or other devices that enable Bluetooth. Bluetooth artifacts

refer to digital evidence of Bluetooth communication and left-over interactions. The following are significant Bluetooth artifacts and their relevance in the field of digital forensics:

- Paired Devices: This Bluetooth pairing information can reveal valuable insights into the connections established between devices with which the device owner might own or have a close connection. A list of paired devices provides evidence of device interactions and is found in `\private\var\containers\Shared\SystemGroup\<GUID>\Library\Database\com.apple.MobileBluetooth.ledevices.paired.db`. This database contains information including device names and Bluetooth MAC addresses. Moreover, the `\private\var\containers\Shared\SystemGroup\<GUID>\Library\Preferences\com.apple.MobileBluetooth.devices.plist` file records information about the devices that have been paired and the timestamps of their last detection. Figure 5.17 shows the AirPods that have been connected to the device highlighted in table 4.9.

- Other Encountered Devices: Public MAC Bluetooth identifiers of other devices with which the device came into close proximity are stored in `\private\var\containers\Shared\SystemGroup\<GUID>\Library\Database\com.apple.MobileBluetooth.ledevices.other.db` with a table named `OtherDevices`. These can be used as proximity data, which can help establish the physical presence of devices and individuals in specific locations. Although these encounters do not have timestamps, they can be helpful in cases where the investigator wants to approximate whether the user has come into close contact with another known Bluetooth address.

Bluetooth MAC addresses, device names, last seen, last connected, and other identifiers are crucial to identifying devices and linking them to their owners or users in complicated cases. Although they do not have geolocation information, this can be valuable for establishing connections between devices and encounters or last-seen timestamps. This can help investigators understand when and where devices were connected to establish timelines, track device movements, and identify potential associations between devices. Figure 5.18 shows the device names and Bluetooth addresses recovered using AXIOM.

```
<key>UserNameKey</key>
<string>Josh's AirPods</string>
<key>AACPVersionInfo3</key>
<string>FWYT1CJWH8TT</string>
<key>AppleDevFeatures</key>
<integer>134234367</integer>
<key>ServiceGATT</key>
<string>Unknown</string>
<key>AACPVersionInfo4</key>
<string>6.8.8</string>
<key>AppleDevFeaturesVersion</key>
<integer>1</integer>
<key>AACPVersionInfo10</key>
<string>6.8.8</string>
<key>AACPVersionInfo5</key>
<string></string>
<key>InEarDetection</key>
```

Figure 5.17. AirPod Bluetooth connection within *com.apple.MobileBluetooth.devices.plist*

EVIDENCE (125) Column view

Device Name	Bluetooth Address	UUID	Source	Recovery
[LG] webOS TV OLED65B6P	Public A0:6F:AA:3D:6E:D7	80476EA4-C821-4902-A285-31F0F37DDDF7	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
[TV] Samsung 7 Series (65)	Public 68:27:37:4E:42:C1	72E2D7B8-9BB8-9267-D410-F048BD554959	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
[TV] Samsung 7 Series (75)	Public B8:BC:5B:4C:ED:ED	B488040C-1B6A-4D7D-32A5-B79727C61EE8	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
ALAM (23:E2:6C)	Public B8:3A:9D:23:E2:6D	9471B85A-F223-2E9A-B96E-62E7741887DE	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
ALAM (72:0E:E4)	Public B8:3A:9D:72:0E:E5	7592EFB0-5E0A-84FB-70E9-6DBAEB94D0F7	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
AugPHP4	Public 78:9C:85:00:51:F8	07CF3AF1-7A9B-A47E-4601-EC3E9C8FEC6E	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
Forerunner 35	Random C1:D1:71:67:AC:4E	CC1E9F08-060A-8E73-34E3-65D67437AAE5	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
Josh's AirPods	Public 7C:04:D0:89:89:A0	34F07271-02CF-AD57-6670-1856A278CCC0	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
N11G9	Random F0:EF:86:EC:68:1B	7EF0B573-95BC-0061-7BCC-5A166433F7F8	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
This Is's Apple Watch	Random 70:2F:48:ED:AE:91	CA6F8505-537F-6CDA-9E93-4BF792127804	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
Versa 3	Random E8:F0:58:00:C0:FB	0F2183F0-376C-7083-4998-E2F8A75ADB11	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing
	Random DC:04:71:5F:AA:AB	DB589A6D-9F12-923C-E1DD-FDFCBA472623	iOS 14-3 - Apple iPhone SE.tar\private\var\container...	Parsing

Figure 5.18. Bluetooth devices and their addresses recovered from Case 1 iOS 14.3

5.1.6 Map Tiles

Map tiles can be found as digital evidence in various forms, such as cached map tiles stored on devices or extracted from digital forensic images of populated apps. These map tiles are typically associated with location-based apps, navigation software, or online mapping services. They consist of pre-rendered, small-sized image files representing specific geographic areas at various zoom levels. As a result, map tiles can be crucial to digital forensics investigations as they provide a visual representation of geographic locations, offering a binding context for analyzing digital evidence. Moreover, by examining these map tiles, investigators can determine the locations accessed or viewed by the user, including details such as street names and landmarks. Therefore, analyzing map tiles aids investigators in uncovering user browsing patterns, movements, and interaction insights. On the other hand, comparing map tiles with other digital artifacts, such as GPS coordinates, timestamps, or geotagged photos, can aid in verifying the authenticity and accuracy of location-related information.

These map tiles can be recovered within multiple apps, and `\private\var\root\Library\Caches\locationd\cache_encryptedB.db` database has a table named with tile geolocations for the native Apple Maps app. Moreover, `\private\var\mobile\Library\Caches\com.apple.geod\MapTiles\MapTiles.sqlitedb` contains Apple Maps app tiles, which are generated when the user uses the app and starts navigating the map or starts looking for nearby locations.

Other apps also keep map tile information; Google Maps is one of these apps. The app keeps information regarding the tiles in two different locations, the first can be found in table within `\private\var\mobile\Containers\Data\Application\<GUID>\Library\ApplicationSupport\GMSCacheStorage-Tiles\Tiles.sqlite` database that contains x,y, and zoom level (see Figure 5.19). The second are carved network caches stored on the device within the `\private\var\mobile\Containers\Data\Application\<GUID>\Library\Caches\WebKit\NetworkCache\Version16\Records\` folder, which can be blobs, URLs, or JSON files.

Moreover, creating a collage of map tiles can be valuable for understanding the extent of a user's browsing activities and gaining a better understanding of their geographic interaction.

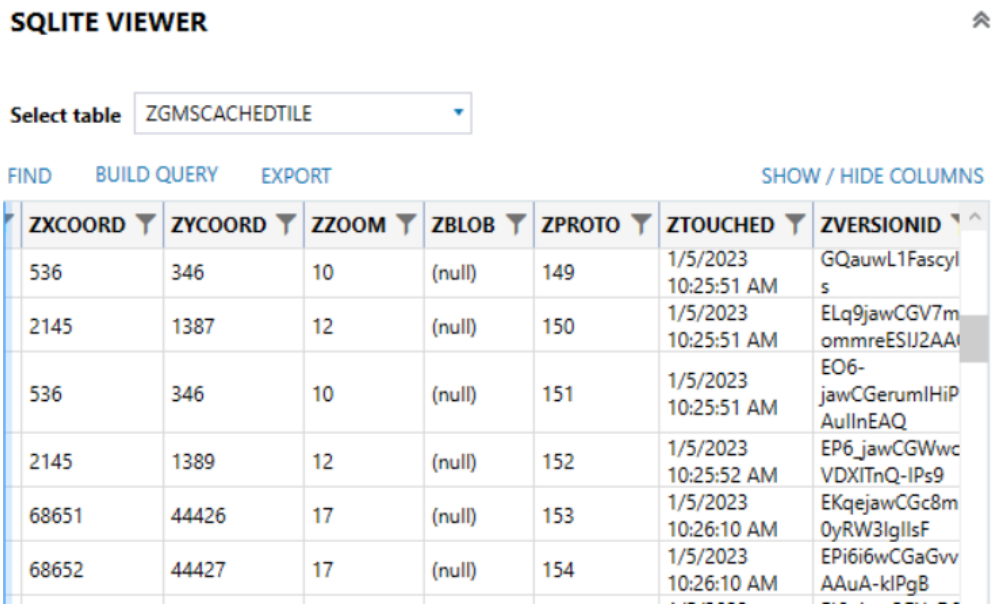


Figure 5.19. Google Map Tiles from iOS 15 Image Recovered Using Magent AXIOM

This technique involves assembling multiple map tiles into a single visual representation, providing a comprehensive view of the areas the user explores. Moreover, it is important to differentiate between zoom levels, which is crucial in this process because it can provide a spatial context to the browsing activities. By considering multiple zoom levels, investigators can distinguish between higher zoom levels that provide finer details, allowing for a closer examination of specific locations. In comparison, lower zoom levels provide a broader overview of larger areas. Therefore, examining, visualizing, and interpreting the user's spatial browsing activities and behavior contribute valuable insights to the forensic investigation process. However, it is crucial for the investigator to know which mapping service is being used in the app to accurately map the tiles.

5.1.7 Addresses

Although text addresses can be found anywhere in the device (e.g., messages and social media), significant locations for user addresses and GPS locations were recovered from the `Cloud-V2.sqlite` file inside the tables `ZRTADDRESSMO` and `ZRTLEARNEDPLACEMO` on the following path `\private\var\mobile\Library\Caches\com.apple.routined\`. Figure 5.20 displays the column names and highlights a location of type "Home" but without a complete address. The rows without addresses appear to be pulled from a different table named `ZRTLEARNEDLOCATIONOFINTERESTMO` within a file named `Local.sqlite` from `\private\var\mobile\Library\Caches\com.apple.routined\` folder.

Furthermore, this home location appears 2009 times in an SQLite database named `DeviceAnalyticsModel` on the following path `\private\var\root\Library\ApplicationSupport\com.apple.wifianalyticsd\`. This file was found using custom AXIOM artifacts. Figure 5.21 shows GPS locations within 500 meters of the recovered home GPS address from the `Cloud-V2.sqlite` file.

Moreover, iOS devices have a function that takes a snapshot of applications that can be used for app-switching background placement. Many apps do not blur their background when showing the app when the user is switching apps. Although recovered snaps might not have valuable information every time, looking at these artifacts as they leave behind

EVIDENCE (38)

Location Name	Address	City	Count...	State/P...	ZIP/...	Location Type	Created Date/Ti...	Latitude	Longitude
Ancient Oaks Dr	508 Ancient Oaks Dr	Holly Springs	United States	North Carolina	27540	None	01/13/2021 09:13:44 PM	35.66046825	-78.8786222
Ancient Oaks Dr	505 Ancient Oaks Dr	Holly Springs	United States	North Carolina	27540	None	02/06/2021 09:03:00 PM	35.66030885	-78.8775496
Ancient Oaks Dr	508 Ancient Oaks Dr	Holly Springs	United States	North Carolina	27540	None	02/19/2021 07:54:25 PM	35.66046825	-78.8786222
Cleveland & Holly Springs Ace Hardware	509 N Main St	Holly Springs	United States	North Carolina	27540	None	02/12/2021 09:45:23 PM	35.659641187503	-78.83696826892 19
Climbing Tree Trail	208 Climbing Tree Trail	Holly Springs	United States	North Carolina	27540	None	01/24/2021 10:16:17 PM	35.6596317	-78.88386705
Holly Springs Vehicle Service	205 Thomas Mill Rd	Holly Springs	United States	North Carolina	27540	None	02/04/2021 10:28:56 AM	35.655405	-78.858669
Linksland Dr	4914–4926 Linksland Dr	Holly Springs	United States	North Carolina	27540	None	02/19/2021 10:36:46 AM	35.6581929857116	-78.8101338923405
N Main St	601 N Main St	Holly Springs	United States	North Carolina	27540	None	02/03/2021 10:35:35 AM	35.66098745	-78.83667585
N Main St	301 N Main St	Holly Springs	United States	North Carolina	27540	None	02/18/2021 08:10:43 PM	35.65531655	-78.8350335
Purfoy Rd	7629 Purfoy Rd	Fuquay-Varina	United States	North Carolina	27526	None	01/11/2021 09:02:15 PM	35.58927075	-78.77259185
S Main St	242 S Main St	Holly Springs	United States	North Carolina	27540	None	01/14/2021 09:05:17 PM	35.6492506	-78.8339382
South Park Village Center	301 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	12/31/2020 07:16:49 AM	35.640513	-78.83740305
South Park Village Center	330 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	01/10/2021 08:58:06 PM	35.6397869	-78.8391385
South Park Village Center	301 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	12/30/2020 09:43:06 PM	35.640513	-78.83740305
South Park Village Center	330 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	01/08/2021 10:32:31 PM	35.6397869	-78.8391385
South Park Village Center	330 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	01/17/2021 02:53:05 PM	35.6397869	-78.8391385
South Park Village Center	330 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	02/15/2021 10:44:42 AM	35.6397869	-78.8391385
South Park Village Center	301 Village Walk Dr	Holly Springs	United States	North Carolina	27540	None	02/14/2021 08:18:57 AM	35.640513	-78.83740305
Sweet Maple Ct	101–199 Sweet Maple Ct	Holly Springs	United States	North Carolina	27540	None	01/06/2021 07:29:55 AM	35.6595836158773	-78.8729178376389
Sweet Maple Ct	101–199 Sweet Maple Ct	Holly Springs	United States	North Carolina	27540	None	12/17/2020 10:30:58 AM	35.6595836158773	-78.8729178376389
Sweet Maple Ct	101–199 Sweet Maple Ct	Holly Springs	United States	North Carolina	27540	None	02/19/2021 04:26:44 PM	35.6595836158773	-78.8729178376389
Thai Thai Cuisine	108 Osterville Dr	Holly Springs	United States	North Carolina	27540	None	02/14/2021 08:18:57 AM	35.6781301122007	-78.8324017742386
Thomas Mill Rd	201 Thomas Mill Rd	Holly Springs	United States	North Carolina	27540	None	02/03/2021 09:21:37 PM	35.6554256	-78.8585341
Town Hall Burger & Beer	301 Matthews Dr	Holly Springs	United States	North Carolina	27540	None	02/07/2021 12:42:39 PM	35.6646694852719	-78.7947675571463
Trayesan Dr	352 Trayesan Dr	Holly Springs	United States	North Carolina	27540	None	01/08/2021 09:32:06 PM	35.6671388	-78.83092815
Trayesan Dr	352 Trayesan Dr	Holly Springs	United States	North Carolina	27540	None	12/31/2020 07:16:49 AM	35.6671388	-78.83092815
Trayesan Dr	352 Trayesan Dr	Holly Springs	United States	North Carolina	27540	None	02/19/2021 07:54:24 PM	35.6671388	-78.83092815
						None	02/19/2021 07:54:29 PM	35.6667979588494	-78.83124443679131
						Home	02/19/2021 07:54:29 PM	35.6595364953513	-78.8728529852168

Figure 5.20. Locations that recovered from the iPhone were the device registered them as significant to the user

critical leads is a good practice. This artifact is stored as a `.ktx` photo extension within most applications. Figure 5.22 shows two recovered `.ktx` screenshots of the iOS 14.3 case 1 image, Skpye app 5.22a and for the native maps app with reference to the parked vehicle 5.22b.

Another location that might hold address information is calendar invites or events. the `private\var\mobile\Library\Calendar\Calendar.sqlitedb` database has a table for locations associated with events and a table for participants of the event, which can help build connections between different participants. In addition, voice recording using the native app (Voice Memos) may name the recording based on an address if enabled by the user.

EVIDENCE (2,009)

Date/Time	Latitude	Longitude
01/17/2021 03:45:56 PM	35.6593711233882	-78.8728257018747
01/17/2021 04:27:25 PM	35.6593289366324	-78.8729066123058
01/17/2021 04:27:31 PM	35.6593205966388	-78.8727067039151
01/17/2021 04:27:40 PM	35.6593378705511	-78.8730985124947
01/17/2021 04:28:17 PM	35.6594203379048	-78.8730693637504
01/17/2021 04:28:31 PM	35.6594203379048	-78.8730693637504
01/17/2021 05:42:13 PM	35.6595058933064	-78.872887276311
01/17/2021 05:49:32 PM	35.6595392596713	-78.8728445092189
01/17/2021 05:59:29 PM	35.6595737516299	-78.8728400798541
01/18/2021 02:37:05 AM	35.6594756870789	-78.8730309021416
01/18/2021 02:37:09 AM	35.6594757118163	-78.87303089511

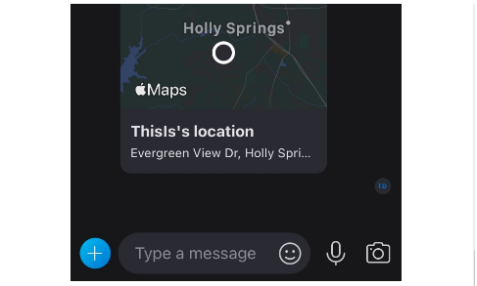
Figure 5.21. New custom artifacts that were recovered for Wi-Fi analytics

5.1.8 Encrypted, Encoded and Hashed Geodata

Data in various formats were analyzed and visualized by entropy analysis. This technique, initially proposed by Claude Shannon [288], involves a formula explained in Table 5.1. The calculation of the maximum Shannon entropy equation consists of determining the probability of each symbol in a data set and using this probability to compute the entropy. The formula (5.1) is represented as follows:

$$SE(X) = -\sum_{\mathrm{i}=1}^{N} p(x_{\mathrm{i}}) log_2(p(x_{\mathrm{i}})) \tag{5.1}$$

It is calculated by adding the product of the probability of each possible value of a variable and the logarithm of that probability [289]. When using Binwalk, it automatically divides the result by 8 to return the calculated data in bytes. This formula helped examine and interpret files that were heavily encrypted. Essentially, the Shannon entropy formula calculates the amount of uncertainty or randomness in a dataset, with a higher entropy indicating more randomness and less predictability. Using this formula in entropy analysis,



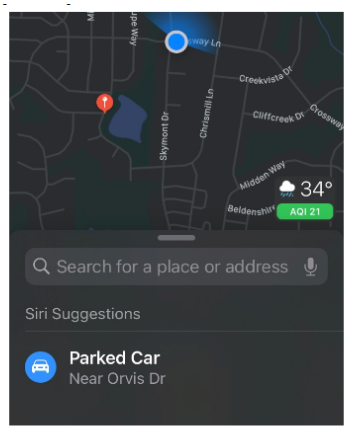
EXPAND PREVIEW ZOOM 80%

DETAILS

ARTIFACT INFORMATION

Application Package Name	com.skype.skype
File Name	E7DDD01D-29D3-4C9B-A188-1ECA43A43266@2x.jpeg
File Extension	.jpeg
Last Modified Date/Time	02/18/2021 03:43:48 PM
Size (Bytes)	103099
Skin Tone Percentage	0.0
MD5 Hash	682c8aa5639ba009d544dcc317806be4
SHA1 Hash	73764dc0ffd8b5e1aff8a141162115dbd117577f
Artifact type	iOS Snapshots

(a) Skype App Screen



EXPAND PREVIEW ZOOM 80%

DETAILS

ARTIFACT INFORMATION

Application Package Name	com.apple.Maps
File Name	8BA9BFE2-93DA-4211-84C0-73280CB3782C@2x.jpeg
File Extension	.jpeg
Last Modified Date/Time	02/19/2021 08:11:29 AM
Size (Bytes)	113508
Skin Tone Percentage	0.1
MD5 Hash	2b1e95d0d39a8fa03ee1b0b7c25cc92a
SHA1 Hash	def9b0b142e025f63c994e8fde9e65e8e8a07081
Artifact type	iOS Snapshots

(b) Maps App Screen

Figure 5.22. .ktx screen snaps showing geolocation information

Table 5.1. Explanation of Variables in The Shannon Entropy Formula

Variable	Explanation
SE(X)	The Shannon Entropy of the dataset X
Σ	Sum of variable 1 to N
N	Number of possible outcomes in the dataset encountered for each possible byte value (0-255)
$(p(x_i))$	The probability of each possible value of a variable x (bites)
$log_2(p(x_i))$	Log base 2, to calculate the amount of information in bits that are needed to represent each possible outcome

we can measure and visualize the data in different formats to gain insight into the underlying patterns and structure of the dataset.

Autopsy has a default encryption file detection using the entropy score threshold of the files ingested. This module has helped detect heavily encrypted files, which were cross-validated using the formula. Unfortunately, for the digital forensic images in Case 2 that contained scenarios for a flying DJI Mini 2 drone, the digital forensic tools used in the examination, such as Autopsy and Magnet Axiom, were unable to decrypt the flight record files stored in either `.DAT` or `.txt` formats. These encrypted `.DAT` and `.txt` files were heavily encrypted and detected for their high entropy score. Moreover, as shown in the literature, usually these types of files hold flight records in the case of a phone that was connected to a drone, and they were recovered from `\private\var\mobile\Containers\Data\Application\<GUID>\Documents\FlightRecords\MCDatFlightRecords\` and `\private\var\mobile\Containers\Data\Application\<GUID>\Documents\Flight\Records\`, respectively. However, the examination of the app led to the retrieval of the location where the iPhone was first connected to the drone, which in this case was the location for the setup. This is a critical and significant piece of PII that can help in investigations.

In other cases with the iPhone 6s, the author tried encoding geolocation in different formats. Table 5.2 explains some of the many encoding formats that can be used. The author tested and populated these formats to determine which format the tools could easily detect. However, none of the digital forensic tools tested could detect these as geolocations, which puts tremendous pressure on investigators who deal with large amounts of data to figure out what they might mean if found in text messages. Although it is very challenging for digital forensic tools to decode these encoded geolocations, using [290], [291] can revere

and decode the geohash to a cell or location on the Earth. Furthermore, Plus codes can be easily decoded using [292], [293].

Table 5.2. Explanation of some geo-encoding types used in testing.

Type	Explanation
What3Words	A proprietary geocoding system that divides the world into a grid of 3m x 3m squares and assigns a unique three-word address to each square
Geohash	Using a brief alphanumeric string (base32), a geohash is a practical approach to describing a location anywhere globally.
DMS	A format that uses degrees, minutes, and seconds to represent the latitude and longitude coordinates
Plus Codes (Open Location code)	Geocoding system divides the world into grids and assigns a unique code to each grid to represent and communicate geographic coordinates in a concise and user-friendly manner

Understanding the drone's flight and the operator's actions can help investigators reconstruct events, establish timelines, and gain valuable context for investigations that deal with drones operated with a smart device. Recovering critical information can provide insights into the intentions and motivations behind the drone's movements and help identify any potentially illegal or unauthorized activities. Through data analysis, during the investigation of the iPhones 6s and 7 that operated a DJI Mini 2, the author, using forensic tools, recovered encrypted flights. However, this valuable information, which can reveal the flight behavior of the drone and the actions of its operator, were not decrypted by Magnet AXIOM and Autopsy. Examining this information using other tools that are designed for drone operators, such as the website `airdata.com` [294], the author was able to decrypt the flight records and download them as Keyhole Markup Language (`KML`) and `CSV` files, which revealed GPS coordinates, flight records and timestamps. The analysis using the data stored in the iPhone provided a comprehensive understanding of how the drone was operated, including its flight path, changes in altitude and speed. It also revealed important actions taken by the operator. For example, in a criminal investigation, analysis of drone data could help determine the exact location and time of the crime and identify any accomplices, vehicles, or parties involved, as in *Kyle Rittenhouse v. Wisconsin* case [295]–[297].

5.1.9 Other

Data from sensors (e.g., GPS) may be valuable in detecting the context of a user's mobile phone in certain crimes [152]. Both the discovery and investigation of criminal activity, as well as crime prevention, may be made possible through the use of this kind of data. Therefore, they are precious when found in an investigation. As a result of the increasing usage of mobile devices and the IoT, they can be used as substantial evidence in criminal prosecutions. For example, they can be instrumental in describing a victim's behavior or physical condition in the moments leading to death. Moreover, they may contain related information that could also be useful in determining the suspect's activities and movement in spatiotemporal dimensions. Therefore, it is important for digital forensics frameworks and tools to expand their current capabilities with more functions and methods to deal with such data, and more importantly, there is a need for investigators to understand all aspects that circulate geodata data because when they are found, they can be of critical value. Of course, these methods must be adaptive to the parameters of the case in which the investigator is dealing and must be bounded by location-relevant analysis. In a criminal investigation, it is evident that a detailed history of location data with timestamps might be helpful [298]. For example, some cases require the investigator to prove or disprove that the user was at a certain location at a given time. In contrast, other cases may require the investigator to determine and quantify some patterns. Furthermore, this can help investigators gather information to build a profile of user behavior or pattern, as few studies have considered the problem from a geographical and technological perspective.

Therefore, accessing detailed and specific user and application usage data is invaluable in forensic investigations, offering a wealth of insights. PoL data is significant, providing a comprehensive narrative about users and their devices. The `\private\var\mobile\Library\CoreDuet\Knowledge\knowledgeC.db` and `\private\var\containers\Shared\SystemGroup\<GUID>\Library\BatteryLife\CurrentPowerlog.PLSQL` databases are handy and valuable in contextualization efforts, as they provide a wealth of data regarding the user. Moreover, new files called `Biomes` within `\private\var\mobile\Library\Bioms\` subfolder are in a proprietary formatted binary file structure. These files store some user experience,

app-related actions, and OS. According to [299], iOS 16 started to migrate some of the data from KnowledgeC into this format. However, during the examination of this study, they still appear in older iOS versions (i.e., iOS 14). Magnet AXIOM does parse some of these and displays them as new Bioms artifacts.

PoL data allows investigators to gain a deep understanding of how the device user interacts with their devices, including which apps they use, how frequently they use them, and the duration of each activity. This information sheds light on the user's digital behavior and habits. Moreover, by analyzing PoL data, investigators can reconstruct accurate timelines of events, activities, and user interactions. This chronological sequence is pivotal in establishing the order of actions and determining the timeline for specific activities. In addition, analyzing PoL data enables the creation of detailed user profiles, revealing insights into their preferences, routines, vital signs (health data), and habits. These data can uncover behavioral patterns, including regular usage patterns, deviations from the norm, and anomalies in activity. Furthermore, because the multiple devices in this study were connected to at least one IoT device (e.g., three different watches in case 1 of Joush Hickmen Seanrios), the examination led to the retrieval of some of the user's vital signs, such as heart rates, movement, exercise done, and steps taken. Data were found in the following database`\private\var\mobile\Library\Health\healthdbsecure.sqlite`. However, there were no records of where these events occurred.

PoL also enables the detection of unusual or suspicious behavior and aids investigators in identifying potential evidence or indicators of illicit activities. This profiling enhances investigators' understanding of the user's digital presence and provides valuable context for interpreting their actions. During the examination and analysis, the author aimed to extract some of this information to be used later as data to be consolidated and correlated using the geo-contextualization approach with other geodata.

5.2 Enhancing Analysis Phase (Examination, Analysis, and Presentation) for Geodata Digital Evidence

The examination and analysis showed that it is possible to obtain more accurate information about the iPhone user and the environment's surroundings by integrating multiple

pieces of information. For example, cached GPS points, Bluetooth, geolocated Wi-Fi access points, geotags within pictures taken, and address data found in the smartphone. Additionally, combining data sets may increase the efficiency of data validation and verification. It can also help investigators understand the geographical extent of the case they are dealing with, which can help detect outliers and strange information that can be inaccurate or manipulated. The authors of [131] validate the collected data from the suspect device using alternative sources; for example, they used location data from Wi-Fi MAC addresses accordingly to validate, when possible, the GPS locations.

Furthermore, this research aims to use all sources possible to validate, verify, and consolidate the device's location evidence with other types of evidence. Likewise, open-source data was beneficial in some cases, which may not be accurate in every digital forensic investigation. However, when possible, digital forensic investigators should make every effort to use intelligence and open-source data, which can help them prove the main points and understand the various aspects of the case.

The examination of this study involved the analysis of various geodata sources to better understand the user's behavior and surroundings. However, digital forensic tools lacked the advanced functionalities needed to examine and analyze many types of geodata. The absence of these is also apparent in well-known digital forensic frameworks and guidelines. Therefore, the ability to gain spatial insights and make informed decisions based on geospatial patterns is enhanced by examination, analysis, and visualization using GIS software to analyze and present spatial data. Some of these functions and limitations are:

- Inadequate support for multiple images within a case: cannot easily distinguish between distinct digital forensic image geolocations displayed on the world map.

- Inadequate support for spatial queries: The tools lacked robust spatial query capabilities, which are essential for performing targeted searches and filtering based on geographic criteria. This limitation restricted the ability to extract specific geodata subsets and identify relevant information based on spatial relationships.

- Limited support for geodata formats: The tools lacked the ability to handle and analyze all types of geodata formats effectively. This limitation restricted the ability to extract

meaningful information from diverse geodata sources, such as mapping IP recovered automatically.

- Insufficient geospatial analysis capabilities: The tools lacked robust geospatial analysis functionalities, making it challenging to perform in-depth spatial analysis on the collected geodata. This limitation hindered the ability to uncover complex patterns, relationships, and anomalies within the geospatial data.

- Lack of integrated mapping and visualization features: The tools lacked comprehensive mapping and visualization functionalities, making it difficult to visually represent and interpret geodata, especially for displaying a large number of geolocated geodata.

After reviewing the digital forensic evidence (images), using well-known digital forensic tools that have been verified and validated by the community, there is a need to search for relevant data, extract it, and examine and analyze it using other methods to gather insights and evidence while maintaining the integrity of the original evidence throughout the examination process to ensure that any findings are admissible in court. This can be done while storing evidence and maintaining integrity, which are critical and standard practices in digital forensics, ensuring that the original evidence is not compromised or altered during the investigation. Therefore, to investigate the data and apply more advanced examination and analysis techniques, evidence that needs more examination is exported from digital forensic tools and secured and controlled in an environment where digital evidence can be stored, analyzed, and examined using other tools or techniques. By being open-minded and resourceful, investigators can leverage various tools and techniques to overcome obstacles and uncover critical information that may have otherwise remained inaccessible. This flexibility and willingness to explore alternative solutions are essential to ensuring comprehensive and successful digital forensic investigations.

To enhance the ability to deal with geodata and help the geo-contextualization approach, multiple approaches and tools were employed to help build the framework in the stages of examining, analyzing, and visualizing geodata. However, a critical step must be incorporated into the framework to enable robust examination, analysis, and reporting outcomes,

which is the `Strategic~Planning~Phase` (see Figure 5.23 for the enhanced overview of the framework).

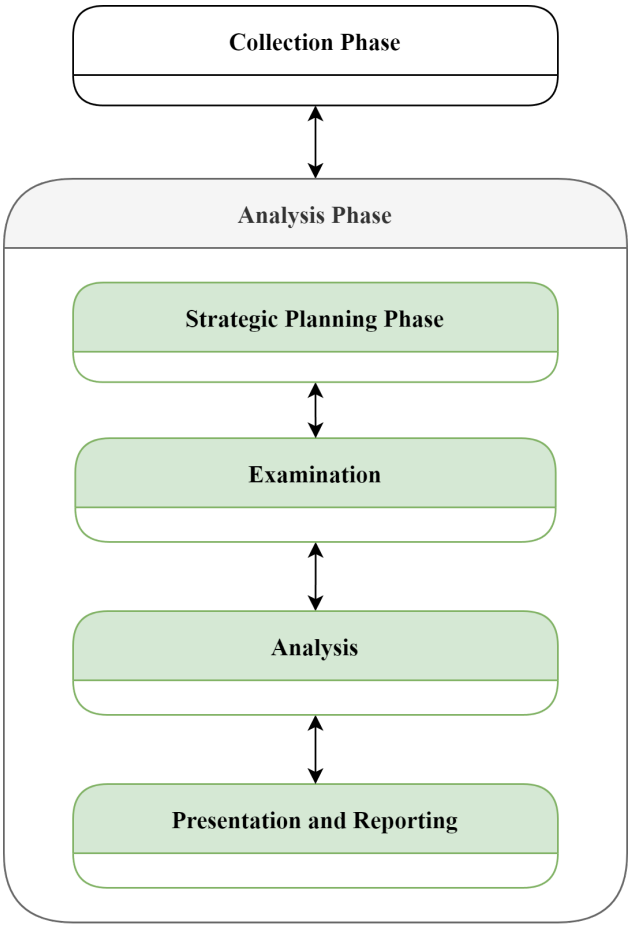


Figure 5.23. Enhanced Framework

Since the framework is transdisciplinary and is built on top of [86] cube. Therefore, procedures, people, data, and technology are essential for the strategic planning phase (see Figure 5.24). The significance of each element is as follows:

- There is a need for Well-defined procedures and protocols, which are crucial for conducting effective and efficient digital forensic investigations. These procedures outline the step-by-step processes to be followed during evidence collection, analysis, preservation, and reporting. Establishing standardized procedures ensures consistency, accuracy, and adherence to legal and ethical guidelines.

- Skilled and trained personnel are critical in digital forensic investigations. Forensic examiners' and investigators' expertise, abilities, and knowledge are essential for conducting thorough examinations, interpreting findings, and drawing valid conclusions for geodata.

- Data is the foundation of any digital forensic investigation. Proper handling, preservation, examination, and data analysis are essential to maintain its integrity and ensure it is admissible as evidence. Data management practices, such as maintaining a chain of custody and implementing secure storage systems, are vital considerations.

- Digital forensics heavily relies on advanced technology and specialized tools. Digital forensic software, hardware, and analysis tools enable the acquisition, examination, and analysis of digital evidence. These technologies (i.e., commercial and open source) aid in data recovery, decryption, data carving, and various other tasks. Staying updated with the latest technologies and utilizing appropriate tools can significantly enhance the efficiency and effectiveness of digital forensic investigations.

- Data location within the evidence, time (e.g., created timestamp, last modified timestamp), and geographical location are critical for investigations.

Digital forensic investigators can establish robust processes, assemble skilled personnel, manage data effectively, and leverage appropriate technologies by considering and integrating these components during the strategic planning phase. This comprehensive approach enhances the quality, reliability, and success of digital forensic investigations dealing with geodata. This study incorporated three types of fields that share the same components to help build a transdisciplinary approach to geo-contextualize efforts for data along with geodata in digital forensics; however, the possibility to enhance is open and needed as there are many things it is not covering. In addition, further research and studies can build on top of approaches and enhance this module component to cope with evolving challenges.

The strategic planning phase is an overarching module that covers investigation requirements, approaches, objectives, and the environment based on the investigation type and the collected digital forensic images. Figure 5.25 demonstrates the components of this phase. It

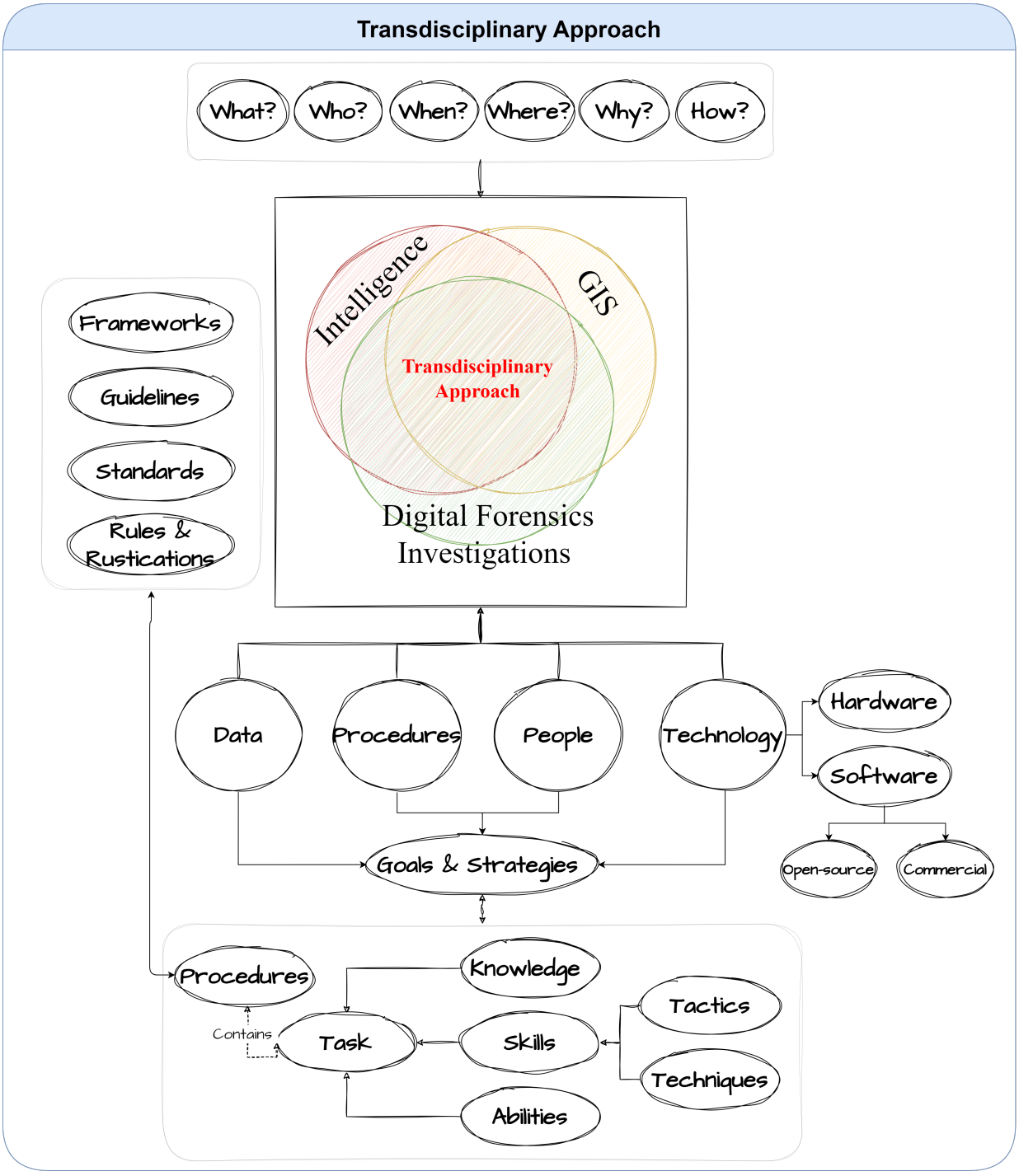


Figure 5.24. Components of the Transdisciplinary Approach

is necessary to provide structure, guidance, and organization to digital forensics investigations. Moreover, it serves as a stage where the objectives, goals, scope, and desired outcomes of the investigation are clearly defined. In addition, it helps in determining the necessary resources for the investigation, such as personnel, tools, technologies, and budget.

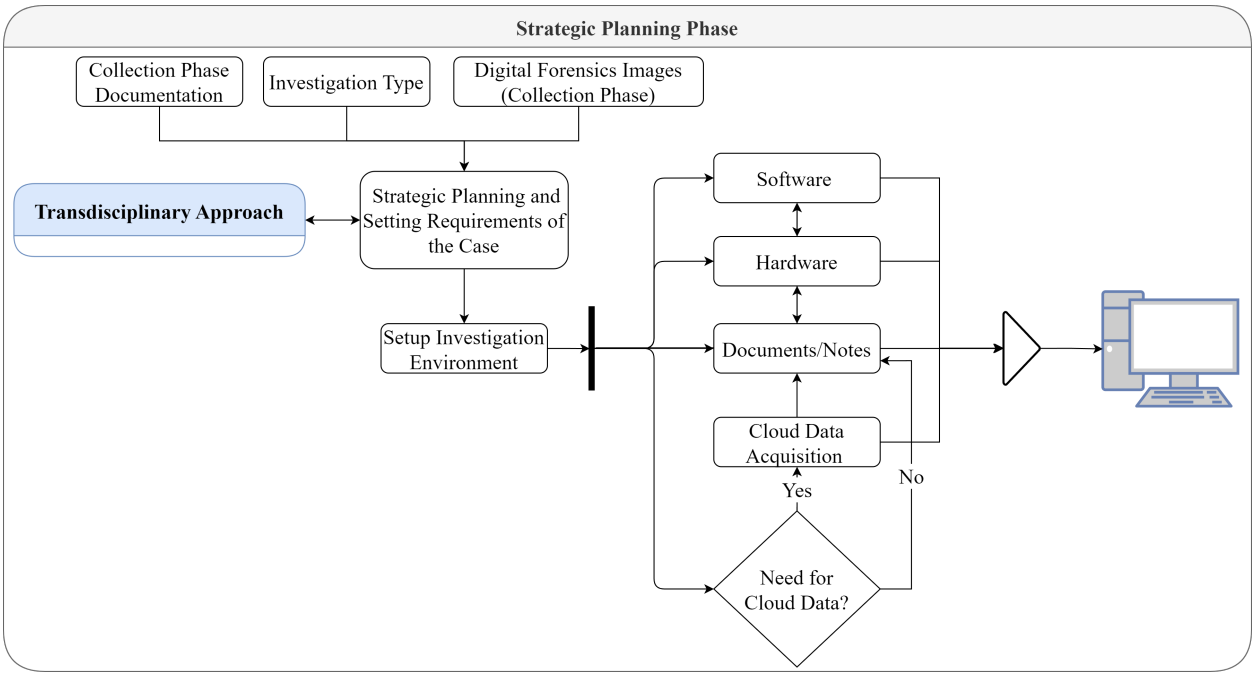


Figure 5.25. The Strategic Planning Phase

Although this study focused on enhancing the geo-contextualization of things after digital evidence collection, it can also be applied to the collection phase. For example, the investigator dealing with the scene has to link physical and digital objects, elements, and evidence at the scene to geo-contextual documentation and description that tells the story when possible. On the scene, if digital evidence is found, many essential elements are often not highlighted to the digital investigators that might help with the geographical thinking of the case. For instance, how exactly was the device found? Is there anything around the device that can help us gather some intel information about where the victim was before the crime?

In digital forensics, the geospatial information inside seized devices found at crime scenes or devices used in committing crimes is omnipresent and can provide many valuable clues

when analyzed. This description has to not only describe the location of the object and their pictures at the scene but even try to link them with a geo-related context. For example, suppose at the scene, there is a coffee cup that is relatively hot, and that cup is from a well-known store. In that case, this has to be given to the digital investigator before they dig into other digital evidence found at the scene. This can be a good starting point to see if the location of where the victim picked the coffee is essential in the case. Moreover, other digital devices (e.g., IoT devices) surrounding the evidence might come in handy and can contain clues and value leads. Another example is linking geoforensics sciences, which deals with the application of geology to criminal investigations [300]. This information is helpful to digital investigators when it is provided and clearly stated in the crime scene report because it might help build stings between objects and evidence found at the scene and the digital evidence.

5.2.1 Examination

The first step in the `Analysis~Phase` is the examination module to ensure that all relevant information for the investigation is acquired and ready. This can include data from various sources such as computers, mobile devices, network logs, cloud storage, and other relevant digital media to the investigation. In addition, before or during the examination, if other potential sources of evidence need to be acquired, investigators need to identify them and justify why they are relevant to the investigation.

When all relevant information is available and ready, the investigators must process the collected evidence using appropriate tools and techniques. The investigators carefully examine the collected evidence, preferably using at least two trusted and verified tools. Moreover, if there is more than one acquired evidence, it is up to the investigator and the capability of the tools to decide if they all can be in one case or separate cases. In this study, the author has tested and tried both ways.

After the tools extract data, investigators might employ different tactics for the examination involving manual inspection of files and folders, recovery of deleted files, system log artifacts, and the verification of encrypted and hashed data (see Figure 5.26 for the decryp-

tion module). Moreover, it is equally important to know the forms in which geodata data can be preserved and their location on devices (see Figure 5.27 that was the outcome of the categorization of geodata encountered in the comprehensive examination of cases in this research). Also, depending on the case and the recovered files, other advanced technical examinations might be needed, such as metadata and timestamp examinations. These are important to establish timelines, track user activities, and validate the integrity of the data. Throughout the comprehensive examination phase, investigators maintain documentation of the steps taken, the tools used, and the findings obtained.

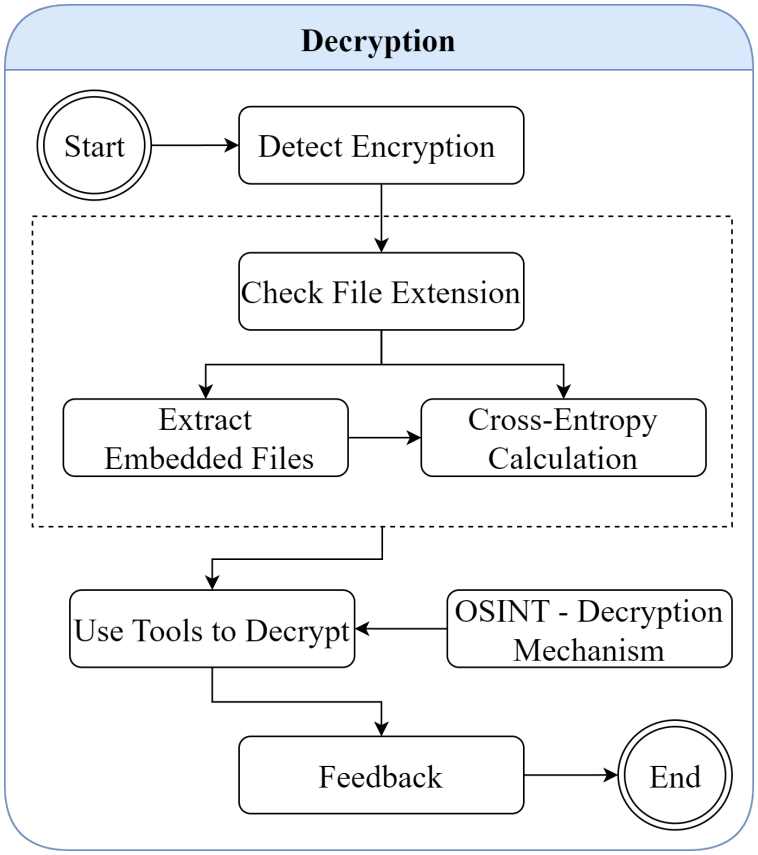


Figure 5.26. The decryption module.

Since current digital tools lack many functionalities to deal with spatial analysis and to better deal with geodata recovered from the case, there is a need to extract information to be interpreted using specialized software. All relevant data must be extracted and stored within a secure case container. This container will be a crucial part of the analysis phase;

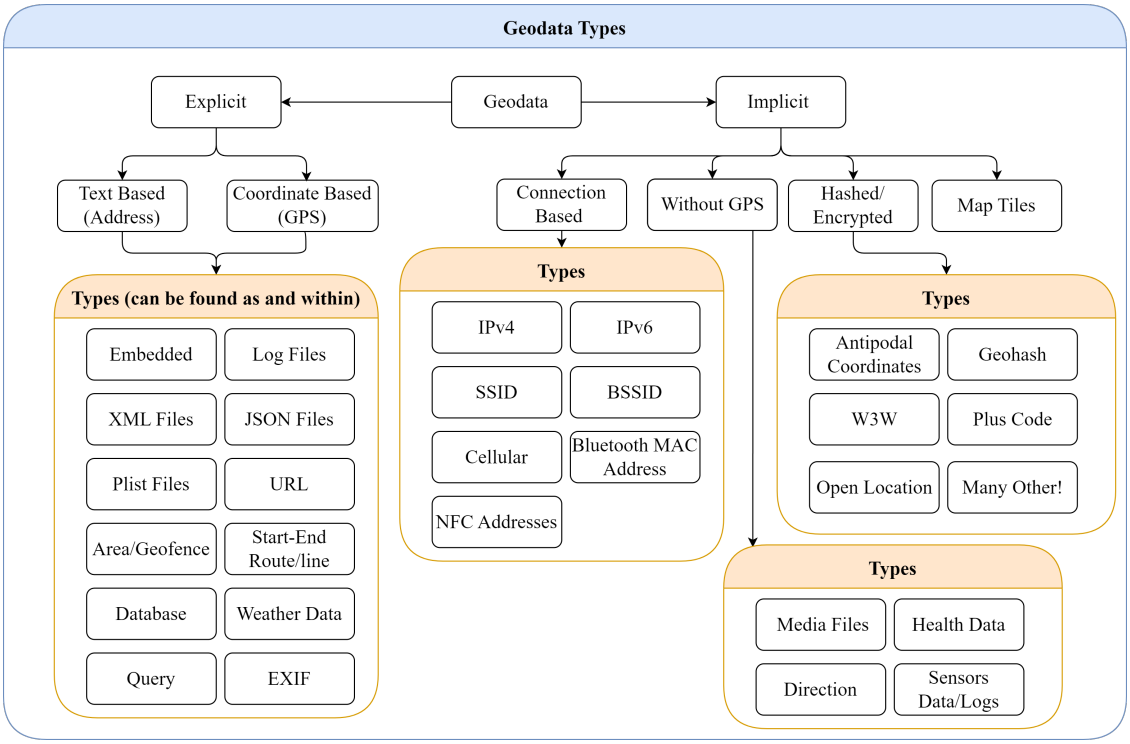


Figure 5.27. Geodata types categorization.

moreover, this repository ensures that a copy of the evidence is processed for analysis. Figure 5.28 depicts the complete examination module.

5.2.2 Analysis

The analysis phase is where the investigators' knowledge, skills, and abilities play a significant role. Digital forensic tools are currently adapting cutting-edge digital technology from other disciplines in an effort to keep up with the rapid pace of technological development and improve the system's predictive capabilities. Furthermore, digital forensics investigators must be able to think spatially to uncover and solve cases where geodata and spatial analysis are deemed to be valuable and would aid the investigation.

Although potential geolocation evidence sources can be files containing geotag or geolocation information on such devices, investigators face many other challenges in today's technological advancements. Challenges have not only changed but have anticipated the

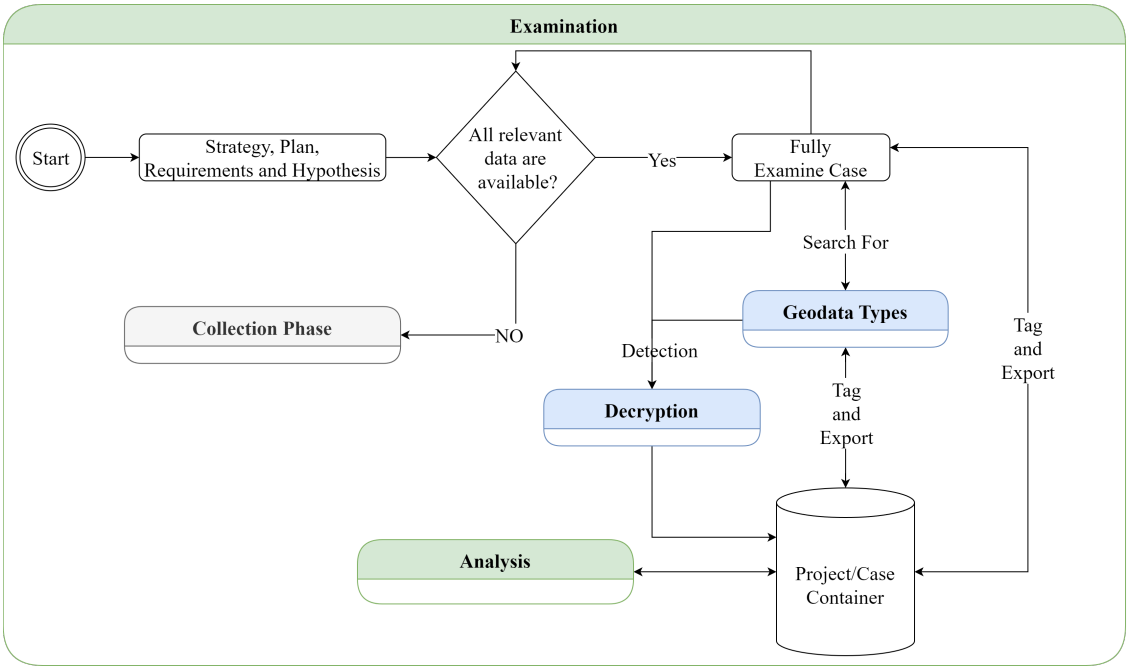


Figure 5.28. The Examination module.

five Vs. (i.e., volume, velocity, variety, veracity, and value) and increased complexity in all dimensions. Many techniques can be used to help investigate these geodata and even help with implicit geodata. Geocoding is one of the most widely used processes, which starts by taking information and turning it into its geolocation. This process aims to take any information that can be tied to a location and turn it into the latitude and longitude of that location so that most tools can easily recognize it. For example, change an IP address to the actual location. Figure 5.29 demonstrates the analysis module that aims to help with geodata and geo-contextualization.

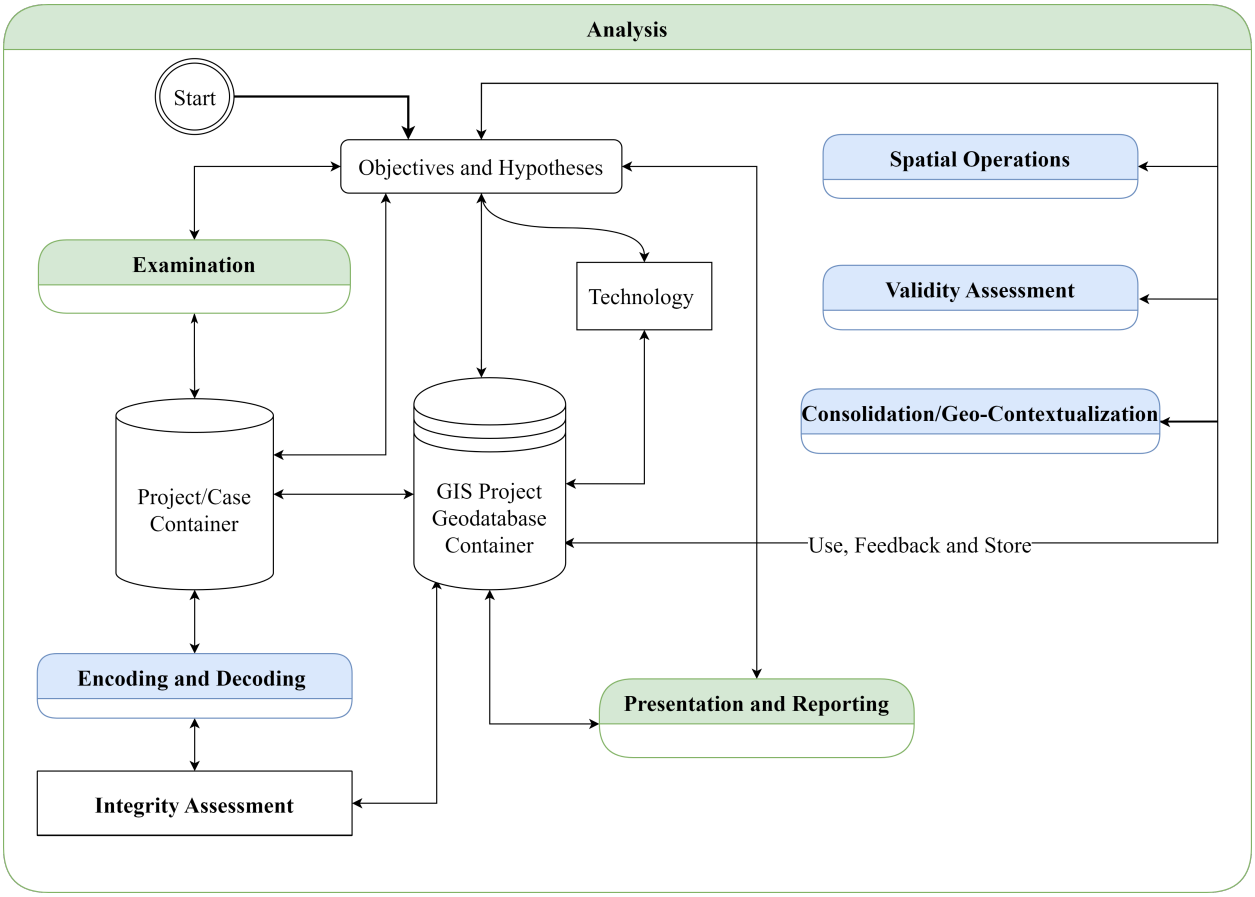


Figure 5.29. The Analysis Module

The following sections are divided into different aspects and approaches to be incorporated into the analysis module.

Objectives and Hypotheses

In the analysis phase of digital forensics, the formulation of clear objectives and hypotheses is crucial. This phase focuses on interpreting and analyzing the processed evidence to derive meaningful insights and draw conclusions. The purpose and the importance of the goals, objectives, and hypotheses in this phase are highlighted by the following:

- Providing clear objectives can help define the scope and direction of the analysis.
- They help in structuring the analysis process. This can help investigators prioritize the investigation of relevant artifacts, employ appropriate analysis techniques, and allocate resources accordingly.
- Hypotheses in digital forensics are educated assumptions based on the available evidence about what might have occurred. Formulating concise hypotheses allows investigators to generate plausible explanations or theories about the events under investigation. These hypotheses guide the analysis within the scope of the investigation by providing a starting point for analyzing evidence, identifying patterns, and testing alternative scenarios.
- They promote efficiency and focused objectives by staying far from unnecessary distractions and concentrating on the relevant evidence and analysis techniques.
- They can serve as a framework for evaluating and interpreting the evidence.
- They provide a context for understanding the significance of the findings and help investigators assess the strength and relevance of the evidence in relation to the case.
- They play a vital role in formulating and helping document and report the analysis process and findings.

Of course, goals, objectives, questions, and hypotheses must be adaptive to the parameters of the investigator's case. For example, some cases require the investigator to prove or disprove that the user was at a specific location at a given time. On the contrary, others

require the investigator to determine and quantify some patterns. This can also help investigators gather information to build a user behavior or pattern profile, as few researchers have considered the problem from a geographical and technological perspective. Many questions can help in an investigation; a few examples are the following.

- How long has the person been there?
- Identify how frequently the user has been there.
- Identify the route the user took to go there.
- Identify what the user did after going there.
- What is the most visited location of the user?
- Is there an abnormal geolocation activity of a user that can be considered an outlier behavior?

In addition to all the above, to take advantage of geodata, the analytical powers that provide extended geospatial analysis are still not integrated into digital forensic tools and processes. Therefore, geospatial information technologies have an important forensic role to play here. One of the most widely used technologies in this context is GIS, which consists of tools that incorporate a wide range of different types of data layers that leverage geographic location-based data structures and are a handy tool to use when the data have a spatial dimension. Choosing the right technology and creating a geodatabase for the case part of the process is essential for effective management, analysis, and visualization of geospatial data; moreover, it facilitates data integration, spatial analysis, and presentation of findings, ultimately contributing to a comprehensive and robust investigation.

Processes for using GIS and Intelligence

This subsection discusses the procedures designed to examine and analyze the recovered data using OSINT and GIS approaches. Using the established fundamentals (see Figure 5.30 shows the way of thinking when using GIS and OSINT approaches in general). The following perspectives were the result of the process needed for using GIS and OSINT:

1. For using the GIS framework. The author created the following steps.

    - Planning and requirements: Based on the digital forensic question and what is already known (e.g., raw data), set and establish specific GIS requirements. It is also important to determine the objectives by:
        - Identification of the relevant data that are needed to solve the question.
        - Breaking down the requirements and procedures into steps.
    - Collection of Raw Data: The collection of raw data (e.g., vector, raster, non-spatial data) associated with the planning and requirements phase
    - Project Creation & Data Mapping: Maintain all data inside a geodatabase. Moreover, add spatial and other attribute data to the geodatabase.
    - Data operations: Perform joint operations while maintaining the integrity and admissibility of evidence.
    - Geoprocessing and spatial analysis, then evaluate and interpret results. There might be a need to refine the parameters or data.
    - Maintenance & Custody: According to [301], a strong chain of custody is maintained throughout the identification, acquisition, examination, and analysis of digital data through digital forensic science.
    - Feedback: reports, statements, or visual maps of results for the intended audience.

2. For intelligence tools and approaches, the life cycle of this process is very similar to the GIS, and it is as follows.

    - Planning and requirements: Based on the digital forensic question and what is already known (e.g., raw data), set and establish specific intelligence requirements. Moreover, depending on the question asked, different intelligence domains will be required (e.g., open source, location intelligence). Therefore, a well-stated purpose, requirement, or intended use case directs the following steps and defines the success of successful intelligence efforts.

- Identification and Collection of Raw Data: The identification and collection of raw data from the case (e.g., user names, email, location, address).
- Data Search and Collection: Search and collect information and data from publicly available sources.
- Data Integration, Process, and Analysis: Enable integration with other data in the study.
- Maintenance & Custody: Documentation and complete traceability.
- Feedback: results as reports, statements, or visual maps for the intended audience.

In digital forensics investigations, intelligence domains can be essential in delivering valuable insights using geodata retrieved from cases. For instance, leveraging a user's smart device's location intelligence might shed light on their whereabouts and actions during an investigation. The investigation usage of IoT devices is also on the rise. Information acquired from the IoT devices like Fitbits, smart homes, and even vehicle telemetries can be beneficial for investigation. In numerous cases, for instance, police have used Fitbit data to track a suspect's whereabouts and activities. Vehicle telemetries data can also shed light on a criminal's movements and routines.

Moreover, intelligence domains such as location and open-source intelligence can provide valuable insights to investigators using geodata recovered from cases. By leveraging these insights, investigators can comprehensively understand a suspect's movements and behavior, helping to identify other potential suspects, gather more evidence, and build insightful reports; even a slight hint or lead can help investigators brake great leaps in complex investigations. OSINT allows investigators to leverage publically available information to find leads, compile evidence, and write informative reports. For instance, a suspect's social media accounts may yield valuable clues about his or her whereabouts, relationships, and actions that can be utilized to verify or disprove an alibi. Moreover, OSINT may help provide a rich source of information that can help geo-contextualize the events.

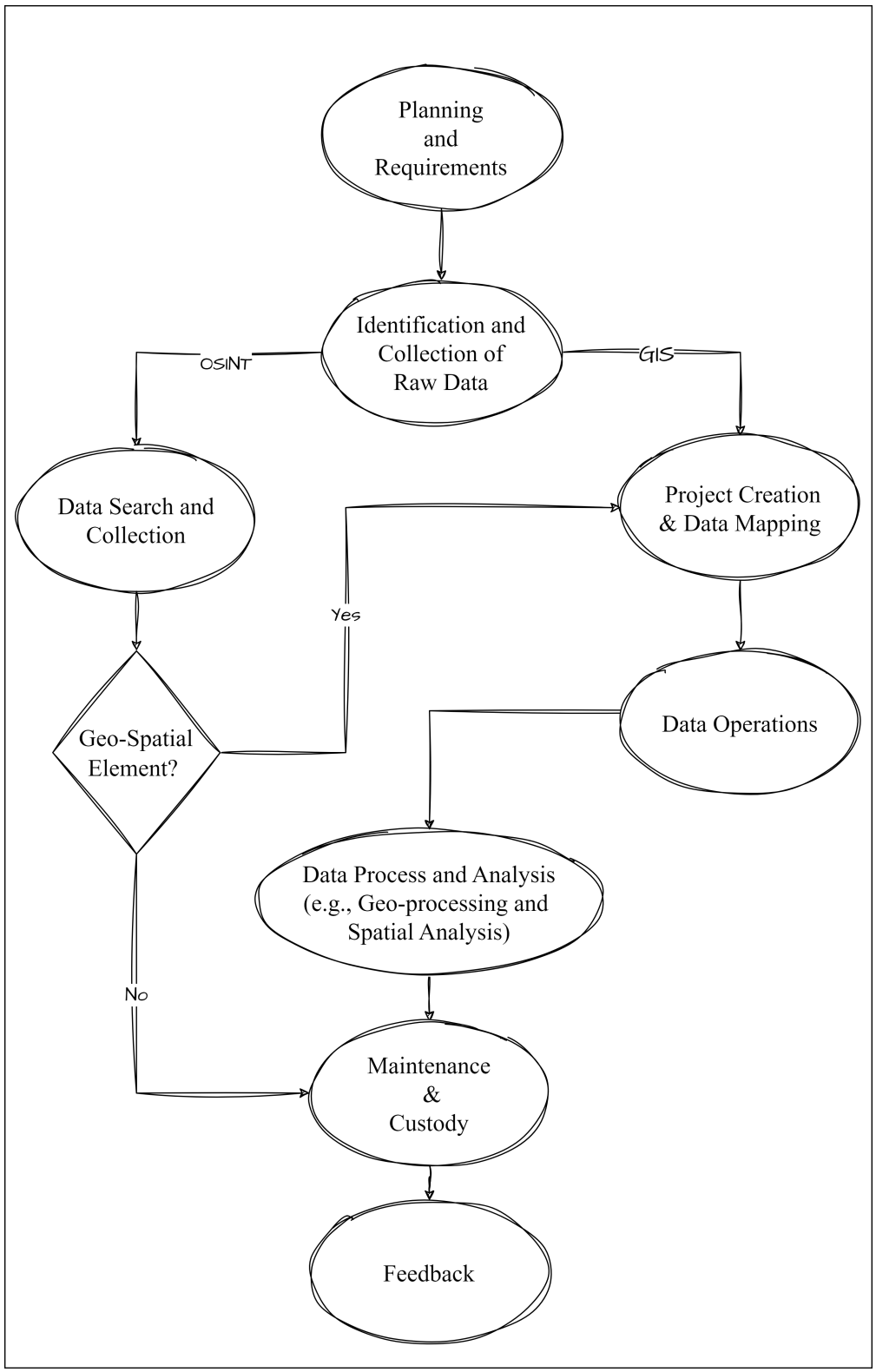


Figure 5.30. General Processes design for the use of GIS and OSINT approaches

Encoding and Decoding

This module focuses on the conversion and interpretation of suspected geodata obtained from various sources within the case. It involves encoding raw geodata into a standardized format for analysis and decoding it back into a human-readable form for interpretation and visualization. OSINT is included in this phase within the encoding and decoding module to provide investigators with possible ways to approach a problem because current digital forensic processes and tools are not well-optimized to deal with all types of geodata. In civil and criminal cases, it would be very beneficial for the investigator to use publicly available data to help build relationships and discover unknowns that can lead to better connections between evidence pieces. Moreover, it is critical to validate encoding and decoding to ensure accuracy and reliability. This might involve cross-referencing and verifying against known reference points within the case. Figure 5.31 illustrates general steps that can be taken in this module.

Geodata Integrity Assessment

In digital forensics, "forensically sound" is often used to characterize a particular forensic method or approach and qualify and, in some cases, justify its use [302]. Moreover, it refers to the forensic process's reliability, integrity, and credibility, ensuring that the evidence collected and the methods employed are valid, defensible, and in accordance with established legal and ethical guidelines, principles, and standards.

Moreover, the procedure follows the 3A's of digital forensics proposed by [263]: by ensuring that the acquired evidence was acquired without modification or corruption, authenticating that the retrieved evidence is the same as the originally seized data, and analyzing the data without modification. For this reason, all procedures performed during the forensic investigation must be appropriately documented. Establishing a clear and unbroken trail of custody from the initial collection to the presentation in court requires recording the chain of custody, specifying who has had access to the evidence and when.

In addition, forensically sound practices involve validating and verifying forensic tools, techniques, and methodologies. This can be inherited from the Daubert standard in digi-

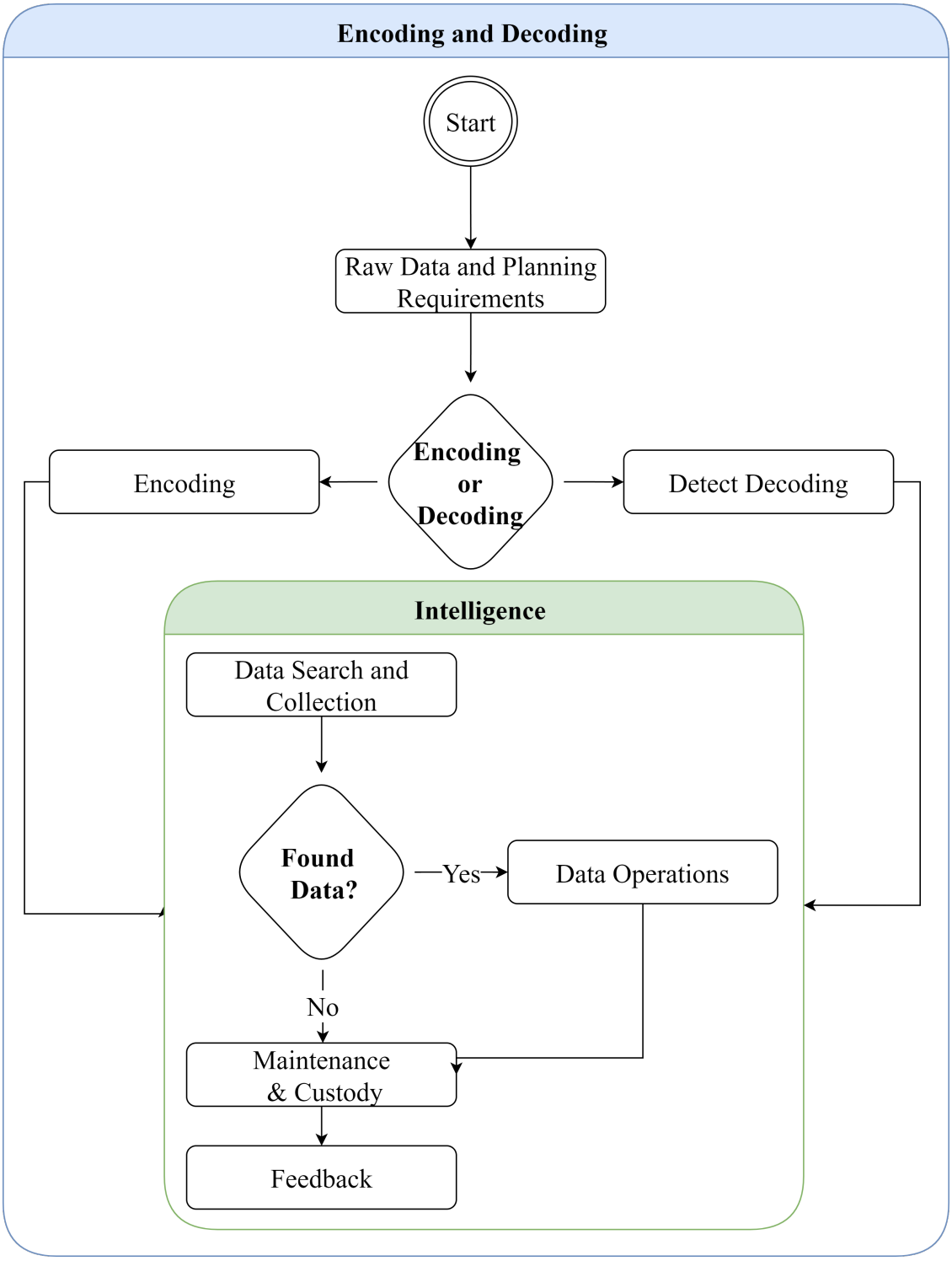


Figure 5.31. The Analysis Module

tal forensics, which evaluates the scientific validity and reliability of forensic methods and techniques presented as evidence in court. The US case *Daubert v. Merrell Dow Pharmaceuticals* in 1993 has established guidelines for expert testimony admissibility, and the Daubert standard requires digital forensics methods to be scientifically valid and reliable [303], [304]. The criteria include the following:

- Empirical testing: The forensic method or technique must be rigorously tested and validated to demonstrate its reliability and accuracy. In geo-contextualization, it is crucial to demonstrate that the methods and techniques consistently produce accurate results. This includes testing geospatial algorithms, data collection methods, and analysis tools. Testing, validation, and quality control should verify the geodata and its methods.
- Peer review: Experts should have reviewed the methodology to ensure that it meets scientific standards. Using the same data and methods, multiple researchers can produce the same results. This gives the geospatial evidence more credibility.
- Error rate: The method or technique's potential error rate should be quantified, and any limitations or uncertainties disclosed.
- Standards: The methodology should follow scientifically accepted methods. Furthermore, the methodology documentation should include data sources, processing steps, and analysis procedures to ensure reproducibility.
- Acceptance: The relevant scientific community must accept the method or technique.

Although it is essential to prioritize forensically sound practices in nearly all circumstances to maintain the integrity and admissibility of the evidence, there may be occasional situations where forensically sound practices may be less of a concern. For example, conducted investigations for internal or administrative purposes, such as internal audits, incident response within an organization, or private investigations; moreover, performing research, experimentation, and preliminary or exploratory investigations, legal admissibility may not be necessary for these situations. Despite these exceptions, it is still essential to take precautions

to ensure that any digital forensics techniques or procedures used are ethical, transparent, and in line with industry best practices.

Spatial Operations

Spatial operations and geodata mapping are efficient methods of visualizing and analyzing information geographically. In contrast to a tabular or textual depiction of the data, it can assist in uncovering patterns, correlations, and trends. By plotting them on a map, investigators can learn more about the spatial features of a case and the relationships between pieces of evidence. In digital forensic investigations, when a suspect's movements and actions may be analyzed, this can be pretty helpful.

Visualizing, analyzing, and interpreting geodata and other data collected from digital devices that have undergone geo-contextualization requires the application of a vast array of techniques and technologies. GIS software, which allows investigators to generate, analyze, and present spatial data, is one of the most common methods for mapping geodata. Additionally, this sort of software makes it possible. To perform spatial analysis, such as buffer analysis, network analysis, and spatial statistics, which can provide deeper insights into the data. The GIS also enables the integration of additional data types, such as demographic, critical locations, or crime data. Doing so makes it easier to recognize trends and connections. Figure 5.32 demonstrates the module.

Many mapping techniques can be used in digital forensics. For example, heatmaps are graphical representations of data to represent the intensity of a specific variable using color-coded representation. These heat maps can represent the density of geodata collected from a case. The digital forensics heatmap analysis helps to visualize and analyze geospatial data. Heatmaps reveal patterns, hotspots, and exciting data. They can also assist detectives in pinpointing areas for additional inquiries. In a tracking investigation, a heatmap might highlight a suspect's most frequented locations. The heatmap can help investigators focus on high-activity and frequency locations. Heatmaps can analyze many users' activities in a specific place. Investigators can identify suspects and witnesses by overlaying the geolocation data of different users on a heat map.

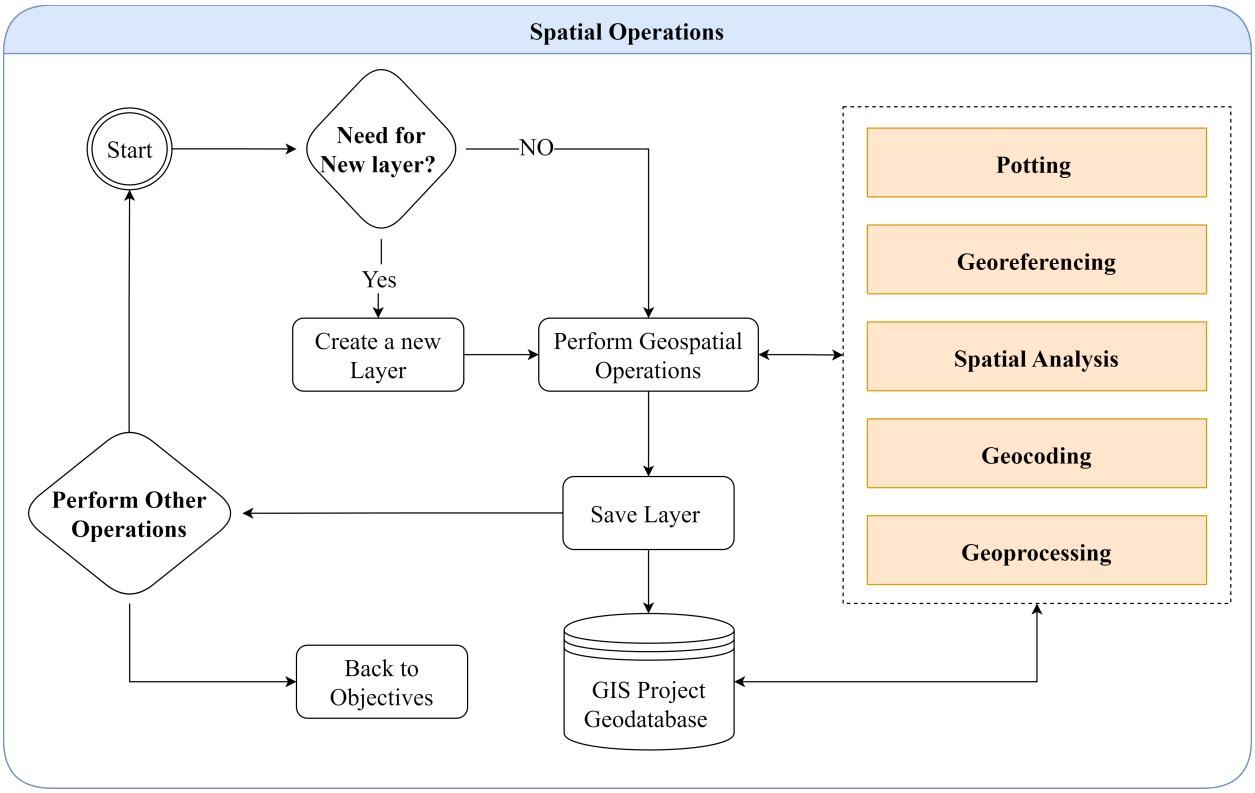


Figure 5.32. The Spatial Operations Module

Performing spatial operations on recovered digital forensics can be a powerful tool for investigators, providing them with new insights and a deeper understanding of the evidence obtained from digital devices. It also helps investigators visualize patterns and connections that may not be immediately apparent when looking at raw data. For example, mapping the locations of multiple devices and their different connections can reveal prospective relationships and networks between individuals, for example. This is particularly helpful in cases involving organized crime or terrorism. Furthermore, mapping geodata can help to present evidence to a jury or other decision-makers. Maps and visualizations can be easier to understand than tables of data or written descriptions and can help convey the significance of specific locations or connections.

Validity Assessment

Validity assessment for the geodata of GPS points found within a case can be an essential step in digital forensics to ensure the accuracy and reliability of the information. Since the longitude, latitude, and altitude information were recovered from the cases within the `Cache.sqlite` database, checking the consistency of the x, y, and z coordinates involves examining if the values fall within the expected range and conform to the defined coordinate system is one way to do it. This can help detect inconsistencies or outliers in the data, indicating potential errors or tampering, which can require further investigation. Moreover, geodata with accurate x, y, and z coordinates to ensure the spatial accuracy of the information. It allows for precise mapping and analysis, enabling investigators to determine the exact location of an event, object, or individual. This accuracy is crucial in digital forensics to establish the spatial context of the case and draw informed conclusions. On the other hand, by comparing multiple data points or cross-referencing with other sources, investigators can ensure the reliability and consistency of the information. Further investigation or verification may be necessary in cases with conflicting data to resolve the discrepancies. Figure 5.33 demonstrates the procedures needed to perform x,y, and z validity assessment of points recovered from a case.

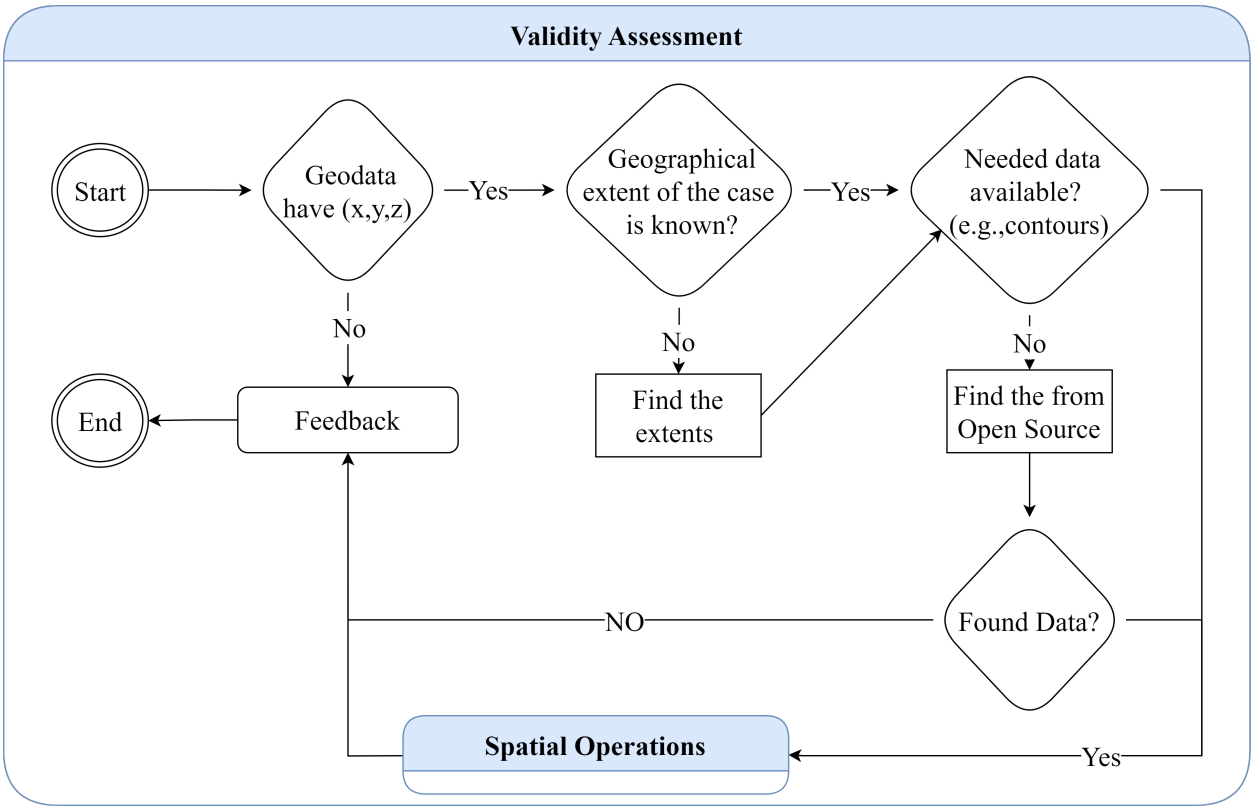


Figure 5.33. The Validity Assessment Module

Geo-Contextualization

The sense of data in digital forensics has always been horizontal and followed mainly one axis: timeline analysis based on timestamp analysis. In other words, time-based timeline analysis has traditionally been the focus of data interpretation in digital forensics. It provides a chronological sequence of events that can help investigators reconstruct the sequence of activities on a digital device. This method has proven helpful in many situations, especially those involving the investigation of hacking, data theft, and cyberbullying. However, the proliferation of data sources and the growing complexity of digital devices means that the conventional timeline analysis method may not always be adequate. Challenges to traditional timeline analysis are presented by data sources such as social networks, mobile devices, geodata, and sorted cloud-based data.

Due to this, digital forensic investigators increasingly need more approaches to data analysis that can consider multiple data axes. Metadata analysis, network traffic analysis, and other data mining techniques could be used in this investigation. The concept of data layers analysis that goes beyond simple timestamp analysis can help law enforcement officials better understand what happened on the devices and who was responsible for it, leading to more efficient investigations and prosecutions. Therefore, the framework aims to add data in different layers to highlight the extent of space and time by trying to add a geo-contextualized meaning.

Figure 5.34 demonstrates the procedures of geo-contextualization. The following points explain the main items within the module:

- Data Preparation: Both continuous geodata and case data needing geo-contextualization must be identified from the investigation data container. At this stage, the hypotheses and the objectives guide the investigator in data selection. Moreover, the continuous geodata's oldest and most recent timestamp must be known, as this will help frame the geo-contextualism duration of other case data chosen.

- Import and data cleaning: The chosen data must be imported to the case GIS project using the suitable import functions. On the other hand, it is essential to thoroughly

check imported data to identify and eliminate any issues or outliers when needed. This cannot be done without a deep understanding of the data sources, which enables the investigators to adapt to their case-specific characteristics and objectives. This checking process can be done using the Vilidity Assmentment module and conducted for continuous geodata sources that will be used. This ensures that low precision and faulty data are eliminated.

- Data Processing and Fusion: There are two primary approaches to consider in data processing and fusion, where data, availability of precise timestamps, and analysis requirements determine which method to use.
  - Matching Timestamps: One way to analyze data from multiple sources is to align it based on corresponding timestamps. This synchronization creates a unified timeline that directly compares data points. Although this method is advantageous when precise temporal alignment is necessary for data integrity, it will miss many data points that might be very close to each other.
  - Similar Near Timestamps: The second strategy involves finding and matching data points with the same or nearby timestamps (e.g., using a threshold between timestamps). Therefore, this method comes in handy when the data sources do not contain precisely synchronized timestamps. By clustering together data with similar timestamps, data that share temporal proximity can be analyzed and fused to take advantage of their commonalities.
- Consolidation: This involves the analysis of geo-Spatiotemporal and geo-contextualized data. Multiple sources of evidence can be combined and analyzed to comprehensively understand phenomena and patterns influenced by geographic and temporal factors and other specific contextual variables within the case.

5.2.3 Reporting/Presentation

There is an urgent need for digital forensic tools to overcome some of the challenges associated with visual analysis by incorporating techniques that help improve the investiga-

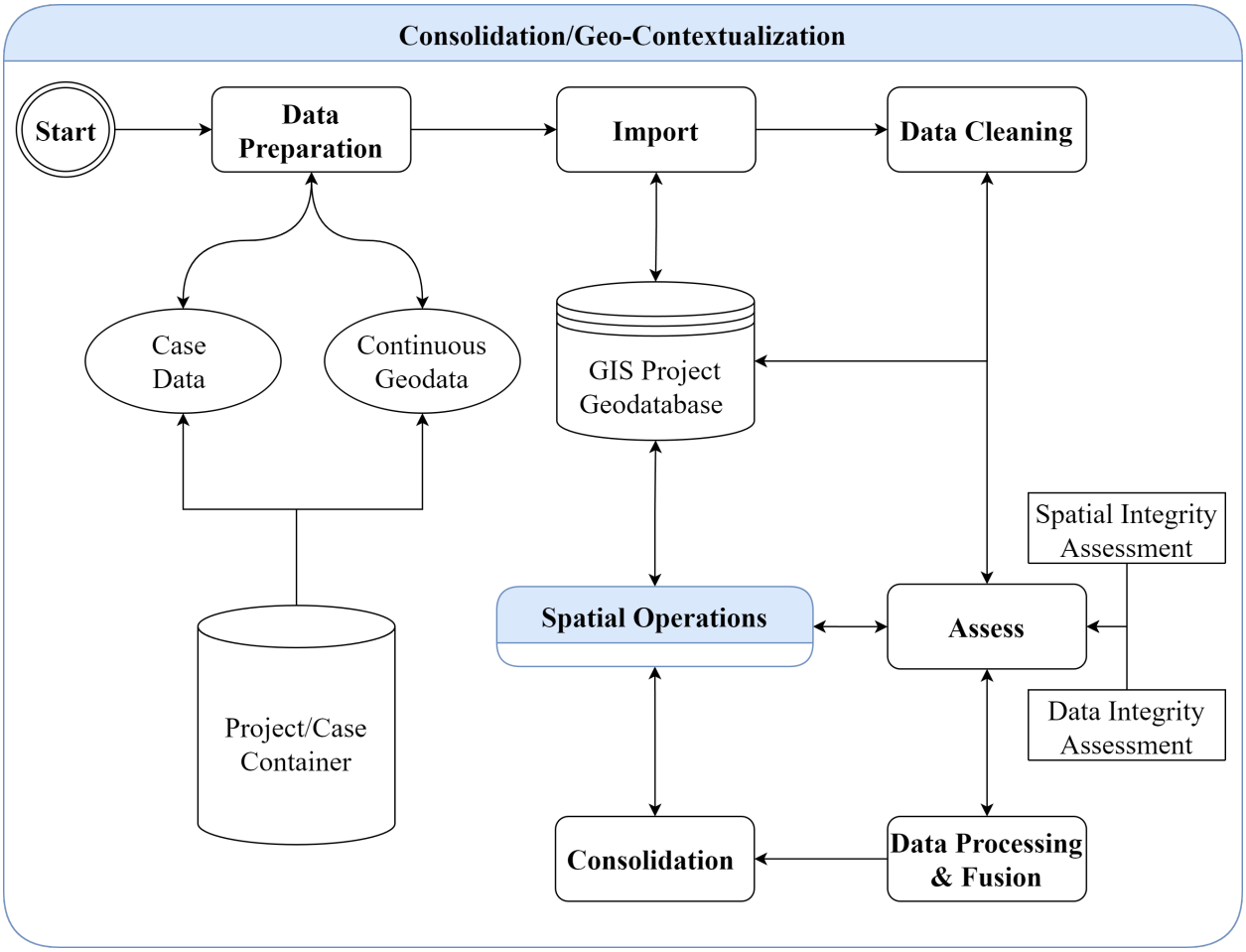


Figure 5.34. The Geo-Contextualization Module

tion guide [14]. Furthermore, these challenges represent a significant burden for the digital forensics community, as most existing digital forensics models and methods do not include complete strategies for dealing with geographical information.

Many people have expressed concerns about the eventual quality of cartographic output, which includes concepts such as accuracy and completeness [305]. Furthermore, the authors in [305] mentioned that geospatial data processing platforms have made it easy to integrate and convert a wide variety of data sources, resulting in results that vary from "raw" to "final" in quality. Similarly, [306] discussed how the variety of data types could raise issues in geodata curation and geodata processing in GIS due to the need for considerable effort from organizations to understand the different files and how to make them meaningful by grouping them in a driven way. Furthermore, according to [25], several fields are adopting strategies for obtaining, processing, editing, analyzing, and presenting geodata. However, digital forensic procedures and tools have been slow to adapt to this type of situation, especially regarding geocoding, geoprocessing, and spatial analysis techniques. Enormous geodata in investigations may be challenging for investigators under certain circumstances. Suppose that several cases have a large amount of geodata. In that case, it will be difficult for investigators to efficiently manage them all, as they are not like any other type of data and need to be dealt with carefully.

Investigators can use GIS tools to visualize and analyze data in a spatial context, allowing them to understand better relationships and patterns that might not be immediately apparent when the data are presented in a tabular format. However, to present the findings in court in a forensically sound manner, investigators must write clear and concise reports that thoroughly detail their search strategy, procedures, and results. Expert testimony from investigators is sometimes required to clarify their methods, findings, and conclusions and ensure their work is credible, consistent, and admissible in court. They need to have an answer to the concepts, data, and map elements chosen to be demonstrated in court.

In digital forensics, the Daubert standard ensures that court evidence is scientifically sound and legally admissible. In addition, it ensures that the tools used are reliable, suitable for the purpose, and produce consistent and repeatable results. It also involves cross-validation of findings by multiple investigators or peer review processes. As a result, it

promotes justice and digital forensic integrity. The Daubert standard can be applied to geodata in digital forensics by evaluating the scientific validity and reliability of the methods and techniques used to collect, analyze, and interpret geospatial information as evidence in legal proceedings. First, the geospatial methods and techniques used to collect and process the geodata should be empirically tested and validated. Second, the geospatial methodology should have undergone peer review by experts in the field. Third, documenting geospatial analysis's uncertainties and potential errors is essential to understand their impact on the results. Fourth, geoprocessing and geospatial analysis should adhere to established standards and best practices. Finally, expert witnesses or individuals who present geospatial evidence should have the necessary expertise and qualifications in geospatial analysis. Their knowledge, training, and experience should be relevant and reliable, and they should be able to explain and defend the methodologies used.

The digital forensic tools tested and used in this research lacked reporting and presentation capabilities. Therefore, when dealing with geodata, investigators usually export data in KML format and visualize them on Google Maps. Although this might be sufficient in some cases, this limitation can have significant implications for investigators and forensic examiners who need to present their findings in a clear, organized, and professional manner.

Therefore, visualizations, graphs, charts, and other means of summarizing complex data are needed to present findings in a visually appealing and easily understandable format. These can effectively present the findings, improving the clarity and impact of the investigation results and making it easier for stakeholders to comprehend the information. GIS allows for this, as they are specialized tools designed to provide maps. In this study, ArcGIS was used to help with presentation and reporting. Moreover, other services such as ArcGIS StoryMaps [307], and ArcGIS Experience Builder [308] can be used effectively to display and present data to stakeholders or in court.

In addition, adequate documentation and presentation become even more crucial when dealing with evidence that contains a large amount of geodata. Presenting and visualizing such data requires analytical skills and the ability to convey precise information. In cases where geodata is available, it can provide an additional dimension of reference, enabling investigators to gain insights into the investigation's spatial and temporal aspects. There-

fore, emphasizing the importance of clear and comprehensive reporting and display methods becomes essential, as they facilitate a better understanding of the geospatial context and enhance the overall investigative process. Therefore when creating maps, they need to follow best practices and some general guidelines [309], [310] for geodata visualization in cases containing geodata, including:

- Various software packages and tools are available for geodata visualization; however, these tools need to follow the basic requirements of the case based on the type of data and the level of detail required to be presented.
- Using appropriate scales and projections for displaying the geodata accurately is important; for example, if the data covers a large area, use a small scale to show the entire area and a larger scale to show details of specific regions. Moreover, the North arrow and scale bar need to be present.
- Same goes for the symbology used to represent different types of geodata. For example, different colors, sizes, and shapes can be used. Moreover, labels and annotations need to provide context without affecting their appearance.
- Clear legends and explanations help the audience understand the geodata and their meaning.
- Data sources need to be mentioned.

Overall, geodata visualization and presentation will depend on the specific case and the goals of the visualization. However, following these general guidelines can help ensure that the visualization accurately represents the geodata and is helpful for the intended audience.

5.3 Summary

This chapter provides a comprehensive overview of various geodata in cyber forensics, particularly emphasizing the integration of geodata concepts. Firstly, it delves into the importance of conducting thorough cyber forensic examinations and analyses to uncover crucial evidence in complex cases. Then the chapter highlights the significance of considering

geodata as part of this process, as it can provide valuable insights and aid in understanding the spatial and temporal aspects of the investigated events.

Furthermore, the chapter explores different types of geodata that are relevant in cyber forensics, emphasizing their significance and potential as evidence. Then, discussed examples and case studies showcase how geodata information, mapping data, and other geodata artifacts can contribute to the investigative process and provide valuable clues.

Lastly, the chapter focused on integrating geodata and geo-contextualization concepts into the cyber forensic process, highlighting the need to enhance and infuse traditional methodologies with geospatial techniques. As a result, it is proven that a comprehensive cyber forensics investigation resulted in building a cyber forensics transdisciplinary geo-contextualization framework (H_1). In addition, it emphasizes the importance of leveraging geodata analysis tools, mapping technologies, and visualization techniques to interpret and present geospatial information in a meaningful way effectively. For example, the geo-contextualization module can help reconstruct the spatial-temporal dimensions of events or activities.

Overall, this chapter serves as a comprehensive guide, highlighting the crucial role of geodata in cyber forensics investigations. It underscores the importance of considering geospatial aspects, exploring various geodata types, and integrating geospatial concepts into the forensic process, ultimately enhancing investigative capabilities and providing a deeper understanding of the digital evidence examined.

6. FINDINGS, VALIDATION, AND RESULTS

In this chapter, the author discusses and addresses the proposed hypotheses through rigorous framework testing. Furthermore, the author aims to evaluate the effectiveness and validity of the framework for the stated hypotheses. Therefore, throughout the chapter, the author uses Case1 images, especially well-populated and documented images (i.e., images 1-5), to present the framework's effectiveness.

Furthermore, the author comprehensively analyzes the results obtained from the testing process that resulted in creating the cyber forensics transdisciplinary geo-contextualization framework. The findings using the new framework are examined with the proposed hypotheses:

- H_2: The transdisciplinary approach fosters techniques to complement and validate recovered geodata.
- H_3: The transdisciplinary approach enriches and geo-contextualizes different data, leading to a notable impact on cyber forensic analysis and more effective geo-contextualization than traditional investigative methods.
- H_4: The transdisciplinary approach assists in uncovering and identifying spatiotemporal information that can improve PoL analysis and add geo-added value to investigations.

A multidimensional technique was necessary to design a thorough investigation that produced a revolutionary transdisciplinary geodata forensic framework. In testing and validating the framework, there is also a need to explore how different intelligence domains (e.g., location intelligence and open-source intelligence) can add to existing guidelines by providing investigators with valuable insights using geodata recovered from crime scenes to help build insightful reports. Allowing for a critical evaluation and validation of the framework's ability to support or refute these hypotheses. The author discusses significant trends, patterns, or relationships from the data, highlighting their relevance to the hypotheses under investigation. By thoroughly examining the proposed hypotheses and subjecting the framework to rigorous testing, the author contributes to advancing knowledge in the field.

Therefore, the chapter serves as a valuable resource for researchers, investigators, practitioners, and other stakeholders in the cyber forensics community, providing insights into the applicability and effectiveness of the framework in addressing the research questions at hand. On the other hand, limitations and potential sources of difficulties in the testing process are acknowledged and discussed at the end of the chapter, offering possible explanations or avenues for further research along with suggested enhancements to the NIST NICE framework.

6.1 Prepration Phase

Case 1 images (specifically Joush Hickman digital forensic images 1, 2, 3, 4, and 5 [277]–[279]) were selected and utilized as test datasets to validate the framework. These images were carefully chosen to represent diverse scenarios and for their availability. Although utilizing cloud data could potentially provide valuable insights and data for the study, it is essential to acknowledge that its inclusion may be outside the scope of the current research. Recognizing the limitations and constraints of the study, the focus is primarily on the available geodata and critical user data that can be directly accessed and analyzed within the defined scope within the examined images.

Cloud data encompasses a wide range of information and resources stored and processed in cloud-based platforms or services. Geospatial, sensor, user-generated, and remote data can be included. Data access, security, privacy, and technical infrastructure must be considered when using cloud data in the study. Although cloud-stored data may offer valuable insights and enhance the analysis, it often involves complex data integration, API interactions, and potentially different data formats or access protocols. These factors may require additional resources, tools, time, and expertise beyond the scope and objectives of the current study. Therefore, it is essential to acknowledge the potential significance of cloud-stored data, but to focus on the available data sources and methodologies within the defined scope of the research. Future studies or follow-up investigations could consider incorporating cloud-stored data to further enhance the analysis and expand the scope of the study.

To aid in the investigation and the two main digital forensic tools (i.e., Magnet AXIOM and Autopsy) used, the author leverages two open-source tools: iLEAPP and APOLLO. These tools are specifically chosen for their capabilities in extracting critical user data that can be instrumental in using the geo-contextualization approach.

On the other hand, the Environmental Systems Research Institute (ESRI) ArcGIS Pro [311], one of the most complete GIS programs, enabled geodata and spatial analysis in the research. ESRI's ArcGIS Pro is a powerful GIS analysis tool with many features. The intuitive interface of ArcGIS Pro made geodata processing, analysis, and visualization more unobstructed. The software exhibited a comprehensive range of features that enabled the execution of spatial analysis, encompassing spatial statistics, geoprocessing, and data visualization. The software exhibited a comprehensive range of features that enabled the execution of spatial analysis, encompassing spatial statistics, geoprocessing, and data visualization. The sophisticated functionalities of the software facilitated the investigation by enabling the identification of patterns, correlations, and fluctuations within the spatial data, thus improving the comprehension of visible and hidden phenomena.

The software's capacity to efficiently process large datasets and its compatibility with file formats widely used in the industry effectively met the research requirements. Through the utilization of ArcGIS Pro, the power of geospatial analysis was harnessed, and the software's robust features were leveraged to conduct comprehensive investigations and generate significant insights from the geospatial data being examined.

6.2 Examnation Phase

Since some conditions have effectively challenged well-known frameworks and digital tools capabilities, these can be used as diverse scenarios and conditions to challenge the transdisciplinary framework to assess its performance. Moreover, the results obtained from testing and verifying the framework using these images provide valuable insights into its effectiveness and applicability to real-world scenarios.

To aid in identifying and extracting implicit geodata, keywords and regexes can be employed as powerful tools. By constructing appropriate regex patterns, one can effec-

tively search for and extract implicit geodata within textual data; moreover, many online tools enable easy creation, visualization, and sharing of regex, such as `regex101.com` [312], `ihateregex.io` [285]. Here are some ways in which regex and keyword searches can be utilized to find implicit geodata:

- Geographical References: To identify and capture references to locations, such as city names, country names, landmarks, addresses, IP addresses, or geographical coordinates (latitude and longitude). This can systematically identify and extract implicit geodata from the text by creating regex patterns that match specific naming conventions or coordinate formats.
- Geospatial Terminology: To identify domain-specific geospatial terms or keywords that indicate the presence of implicit geodata.
- Spatial Descriptors: To identify descriptive terms or adjectives that provide spatial context.
- Coordinate Formats: Regex can detect and extract different coordinate formats, such as DMS or UTM coordinates.

Tailoring regular expressions to the specific context and nature of the analyzed textual data is crucial. Regular expressions can be combined, modified, or refined to account for geodata representation or language usage variations. Additionally, iterative testing and validation of regex patterns against textual data are crucial to ensure accurate and reliable extraction of explicit and implicit geodata.

Moreover, the author extends the analysis by exporting the necessary files for future analysis in the same case examined previously. Recognizing the importance of preserving and utilizing data for subsequent investigations, the author ensures that the framework modules securely export relevant files and information for further examination and analysis. Upon completing a comprehensive examination of the available geodata and critical user data suitable for geo-contextualization, the next step involves exporting these data as CSV and KML files to the case container. This process ensures the preservation and organization of the data for future analysis and reference.

iLEAPP and APOLLO are known for their effectiveness in retrieving digital artifacts, enabling the author to gather valuable insights from the case data. The iLEAPP provides comprehensive support in extracting and analyzing iOS artifacts, assisting the author in uncovering relevant information from iOS devices. With its wide range of features and functionalities, iLEAPP facilitates the retrieval of crucial user data that may contribute to the geo-contextualization process.

Similarly, the author utilizes APOLLO, another open-source tool, to supplement the investigation by extracting critical user data from iOS devices. APOLLO is specifically designed to assist in retrieving and examining PoL artifacts from Apple devices, providing the author with valuable insights and evidence to enhance the geo-contextualization approach further. By incorporating iLEAPP and APOLLO into the investigative testing environment, the author cross-examined comprehensively and systematically the recovered artifacts to aid in gathering data that can be used for the framework for analyzing and geo-contextualizing critical user data. Moreover, Plaso was used for reducing the manual effort by automatic creation of timelines to generate a cohesive timeline of events by extracting timestamped entries and organizing them chronologically. This enables investigators to view a chronological overview of events.

By exporting the data in their original format and in CSV files to create a standardized format that is widely compatible and can be easily imported into various analysis tools or software. CSV files store tabular data, each row representing a data entry and each column containing specific attributes or variables. This format enables seamless data sharing and facilitates further analysis and manipulation of the data. Furthermore, generating MD5 hash values for the exported files is crucial as a best practice for data integrity and security. By comparing the MD5 hash values later, one can verify the integrity and authenticity of the exported files, ensuring they have not been tampered with or modified.

Therefore, exporting the geodata and critical user data as a database, CSV, and KML files to the case container and generating MD5 hash values establishes a reliable, well-documented, and organized data repository that preserves the data's integrity and enables further analysis.

6.3 Aalysis and Presentation

The first step involved importing the exported necessary databases and files from the case container. Once the required files were identified, the next step was to determine the optimal method for ingesting these files into ArcGIS Pro. One of the tables, namely `ZRTCLLOCATIONMO`, is inside the `Cache.sqlite` database that contains numerous columns where location information is stored in latitude, longitude, and altitude, along with many other information. As stated in the prior examination, this table contains one week's worth of very high-frequency geolocation of the device.

There are two options, 1) import the CSV file of the table or 2) import the whole database. For the first option, a minor issue where the software initially failed to recognize the timestamp as a date field was successfully resolved by converting the text-formatted field into a date field through a conversion process. The investigator must remember that this technique changed the ingested file, which may affect its admissibility in court. Each file change was recorded and compared to the original to ensure accuracy and openness. This conversion was needed to perform a time series analysis later on; however, if the analysis did not need a time series analysis, this step can be skipped. On the other hand, the second option imports the entire database and then imports each table into the map to perform operations. This will import the tables in their original state, meaning that the timestamps are in Apple format. Therefore, to display timestamps in UTC format, there is a need to create a new field and apply a Python function to display timestamps in UTC. Figure 6.1 demonstrates a new field calculation for the timestamps in UTC format.

Mapping the extracted data led to discovering some apparent discrepancies for the exported SQLite database `Cache.sqlite` that contains `ZRTCLLOCATIONMO`. The following are the observed behaviors for Case 1 image 5:

- If exporting the SQLite database alone using Magnet AXIOM `saveasfile/folderto`, presented that `ZRTCLLOCATIONMO` table only has 32,940 points (see table 6.26.2a). Furthermore, it has the same MD5 hash value `97aa83a07f6e7988b2b46d1c6eb49e86` as presented in Magnet AXIOM with a size of 4,317,184 bytes.

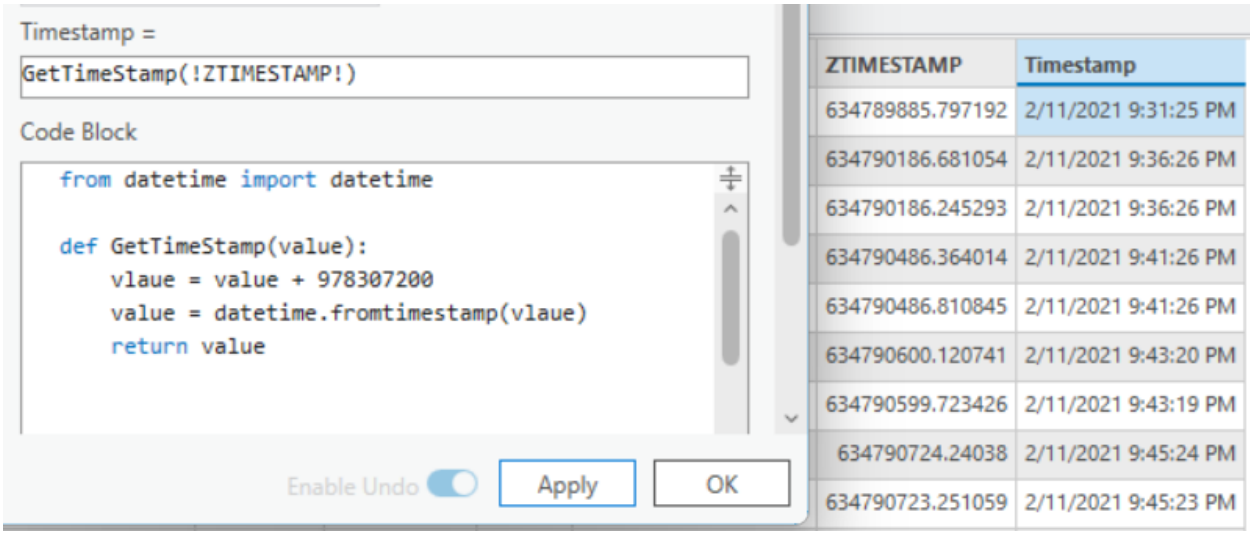
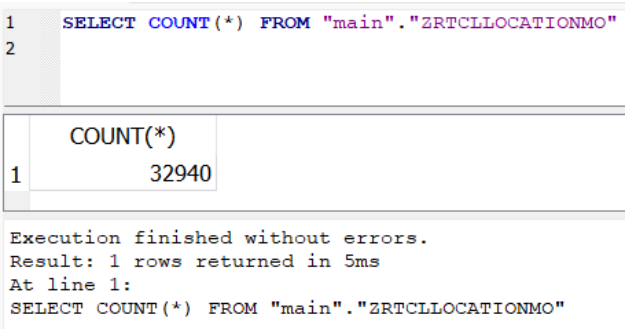


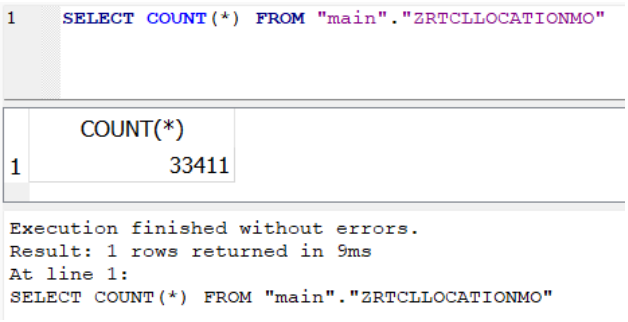
Figure 6.1. New field calculation for the timestamps in UTC format.

- Exporting the database with its associated Write-Ahead Log (WAL) and Shared Memory (SHM) files, then navigating to `Cache.sqlite` database and opening it shows that it first has a different MD5 hash value of `47020379CC48D91D346A1EF8EBCFF36D` and a size of 4,399,104 bytes. Second, it has 33,411 GPS points within `ZRTCLLOCATIONMO` table (see 6.26.2b to see that the table contains 33,411 rows). This is due to the WAL and SHM files.
- Using the exported CSV file from Magnet AXIOM, there were 33,411 GPS points; even the iLEAPP (V1.15.8) extracted 33,411 points (see 6.26.2c).
- On top of all of this, Magnet AXIOM was only able to map 33,360 GPS points (see 6.26.2d).

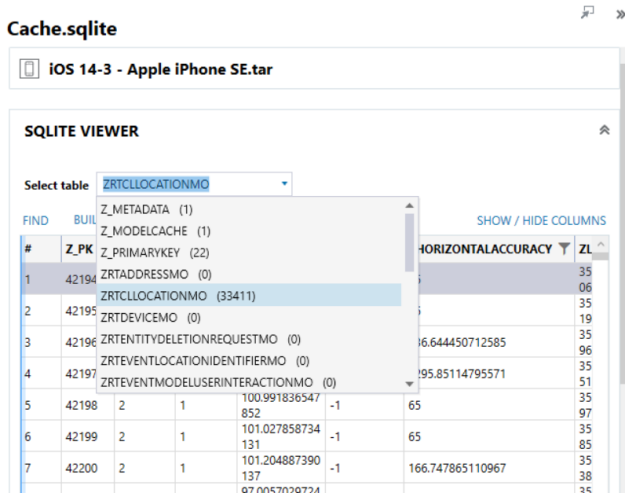
This was not a solo case; other databases have a different hash value if investigated together with their WAL and SHM files. Table 6.1 displays the information observed for the cache database tested up to Magnet AXIOM v7.0.0.35443 with the number of rows in the `ZRTCLLOCATIONMO` table in the original file, the number of Magnet AXIOM mapped rows, and the number of rows in the exported file.



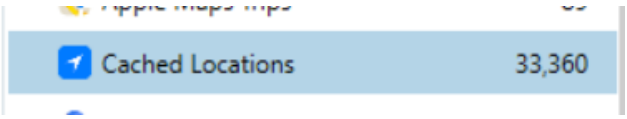
(a) Expoted SQLite database alone from Magnet AXIOM count function showing only 32,940 rows



(b) SQLite database after ingesting the WAL and SHM files count function showing 33,411 rows



(c) 33,411 of rows showing in Magnet AXIOM and the same number is when the table is exported as CSV file



(d) Magnet AXIOM only mapped 33,360 GPS points

Figure 6.2. GPS points discrepancy between different extractions

Table 6.1. Discrepancies during the examination and exporting of Cache.SQLite database.

Image	Original MD5 Hash	Rows	AXIOM Mapped	AXIOM Exported db MD5 Hash	Rows
1	3038AB2F4E330D360F6510F58758730C	89,662	88,479	a3529239117fa648c6960aa1321255a5	87,620
2	68D2C062A8E8F64136B8FE957376B997	106,863	104,549	3e70f0b0a5bea1863ed07560af130dad	104,668
3	8711E214A75F011F8D5F893A91D49559	135,736	132,389	cb3c6e9ccbd16a4b7c0f6f2f8bc482b1	135,582
4	AAA93959184EE1AC569F125BDC212874	853	851	68ba77093f8524cbff9e65fb78177ef5	839
5	47020379CC48D91D346A1EF8EBCFF36D	33,411	33,360	97aa83a07f6e7988b2b46d1c6eb49e86	32,940

Axiom, in the ingestion, uses the WAL and the SHM files to present data in the SQL Viwer; however, the tool does not indicate that the results in the table are from this operation because the hash changes once this is done, and they are not indicating this hash change. The disappearance of WAL and SHM files after opening a database can be attributed to the expected behavior of the database management system (DBMS) and its transactional nature. Many DBMSs use WAL files to ensure data integrity and durability. These records track all modifications made to the database, ensuring retrieval of lost data and the undoing of transactions. On the other hand, SHM files facilitate the communication and management of shared memory between processes. When the database is accessed, the DBMS performs several tasks, such as checkpointing, storing data on the disk, and deleting temporary files. This may entail eliminating redundant WAL and SHM files that have already been incorporated into the database. The absence of these files doesn't suggest any concerns or complications with the database. It is a regular process of the DBMS to guarantee effective and dependable data management. Still, it is essential to remember that the exact behavior could differ depending on the DBMS utilized and its setup.

Therefore, given the discrepancies during the examination and export process, investigators must be vigilant and cautious. They should investigate the exported database alone and another time with associated files. This can ensure that data are investigated closely in an attempt to map and capture as many data points as possible. By doing so, investigators can mitigate the impact of any potential discrepancies and ensure a more comprehensive and accurate representation of the data. These additional mapping efforts will enhance the integrity and reliability of the exported data, allowing for more robust analysis and interpretation. On the other hand, this is a huge issue for digital forensic tools, as the examined file did not maintain its original shape without any modifications or mention to the investigator that the file has been changed to log more missing data in the WAL file.

Furthermore, due to the lack of great visualization in digital forensic software dealing with a large number of points and the limitations of geodata querying, the use of GIS technology has made it easier to deal with geodata and map the five exported tables `ZRTCLLOCATIONMO` of the five different digital forensic images. This led to a more detailed examination and analysis of the data because ArcGIS Pro software enables queries (e.g., based on the attributes, space,

time, and spatial-temporal) while displaying the data. This is useful, for example, to visualize GPS locations with poor accuracy.

When examining and analyzing the data, the worst accuracy for horizontal (i.e., longitude and latitude) is observed to be 149 KM. Therefore, when performing the statistical analysis using the SAS program, some high outliers must be highlighted and dealt with when conducting further accuracy analysis. Figure 6.3 demonstrates the distribution for all 33,411 points; the outliers are clear. Furthermore, Figure 6.4 shows the interquartile range of the data set. It is good that it is a right-skewed distribution, which means the data will probably be accurate.

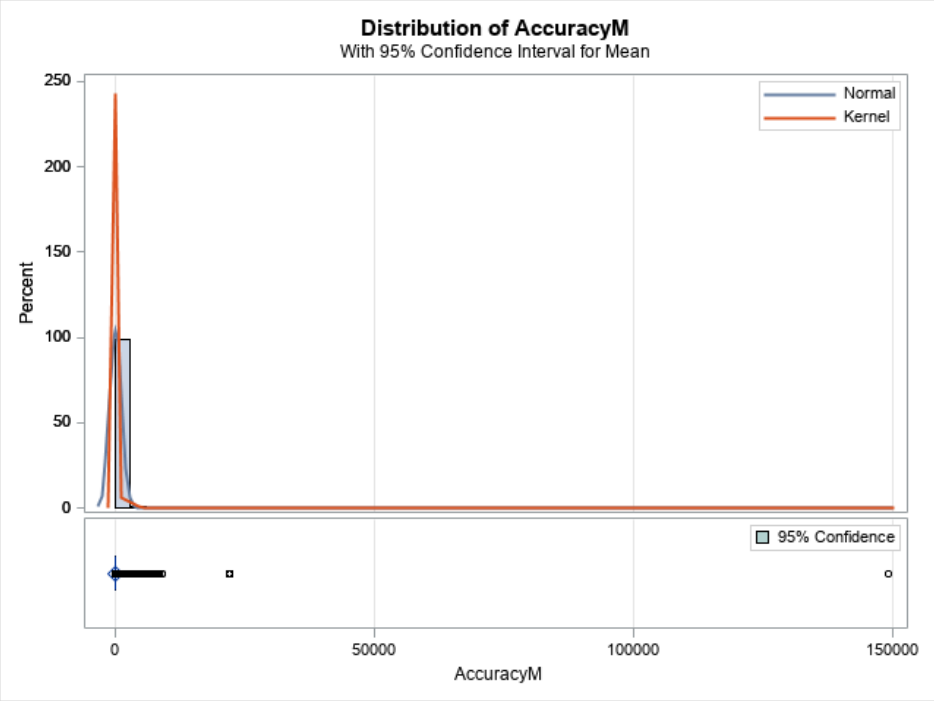


Figure 6.3. A right-skewed distribution for the accuracy of the horizontal positioning.

By performing a quick statistical analysis, the quartile showed that 90% of the recovered data had a longitude and latitude accuracy of 65 meters or less; 75% were 30 meters or less; 50% were 10 meters or better; and finally, 25% were 5 meters or better. This leaves one wondering why the accuracy of the GPS lock in 10 present is greater than 65 meters - assuming that there are reasons for these outliers. Therefore, with the help of the maps, upon further investigation and deeper analysis into the reasons behind the coarse accuracy

Quantiles (Definition 5)	
Level	Quantile
100% Max	149000.000
99%	3021.418
95%	245.732
90%	65.000
75% Q3	30.000
50% Median	10.000
25% Q1	5.000
10%	5.000
5%	5.000
1%	5.000
0% Min	5.000

Figure 6.4. SAS program output for the quartiles of the horizontal accuracy.

observed in the location and time analysis. The analysis revealed that this issue could be attributed to one or more of the following conditions:

1. The phone was stationary, which means that it remained fixed for an extended period. This resulted in limited location updates, leading to less precise location data.

2. The phone was set aside and no user interaction or movement on the phone was detected.

3. The phone was indoors and not in active use. When the phone was located inside a building and was not actively used, the available location data exhibited lower accuracy levels, primarily due to the limitations of indoor GPS signals.

4. The phone was on the charger and within a known frequent location visited, such as the home location.

Identifying and understanding these conditions provided valuable insight into the factors that contributed to the coarse accuracy observed in the location and time analysis. As a result, this knowledge serves as a foundation for interpreting the findings and considering the limitations of the data during the investigative process. Moreover, most of the points

occur late at night into the morning, when the device is on the side, and there is no direct interaction from the user; this means that it could be a saving battery function or low-performance mode. Although the phone appears to be connected to WiFi, it acquires poor accuracy for wired reasons and then moves to another location with better accuracy. More research in a controlled environment is needed to investigate this.

Therefore, Figure 6.5 shows the map displayed for all GPS points within `ZRTCLLOCATIONMO` table. Furthermore, to understand where the locations with an accuracy worse than 15 meters are, Figure 6.6 demonstrates the outcome of a query that selects the points with a latitude and longitude accuracy more significant than 30 meters. Furthermore, another query selects the latitude accuracy of GPS points that have worse than 10 meters accuracy (see Figure 6.7). It is noticeable that both locations with poor horizontal and vertical accuracy on both maps are closely matched at particular locations. Therefore, Figure 6.8 demonstrates the inverted where clause selection of `ZVERTICALACCURACY` >= 15 Or `ZHORIZONTALACCURACY` >= 15.

Moreover, using optimized hot spot spatial statistics analysis can discover if there are hot spots using statistical measurement; therefore, using an ArcGIS Pro predefined tool that can identify statistically significant spatial clusters of high values as hot spots and low values as cold spots. The result of this analysis for the horizontal accuracy column is shown in Figure 6.9. For an easier understanding of this map, the red colors are hot sports with low accuracy (i.e., a high number), which means that the accuracy was terrible.

In addition, one of the ways to get to know the general geographical extent of the case is to use cell tower locations and create a map with ranges. Again, there is a need to create a new layer for the cell tower and plot them on the map, then create buffers around each cell tower to estimate the case extent. By taking the `cache_encryptedB.db` database for the five digital forensic images, and taking the four tables `CellLocation`, `CellLocationLocal`, `LteCellLocation`, and `LteCellLocationLocal`, which for case 1 iOS 14.3 contains 120, 8, 393, and 3, respectively. For ArcGIS Pro, since this is .db, and the software cannot automatically import it, the created CSV files of these tables were needed. An important note is that these tables contain cell towers with null (-1) CI (Cell Identity) values, and there was a need to eliminate these since their range was greater than 149 km. Figure 6.10

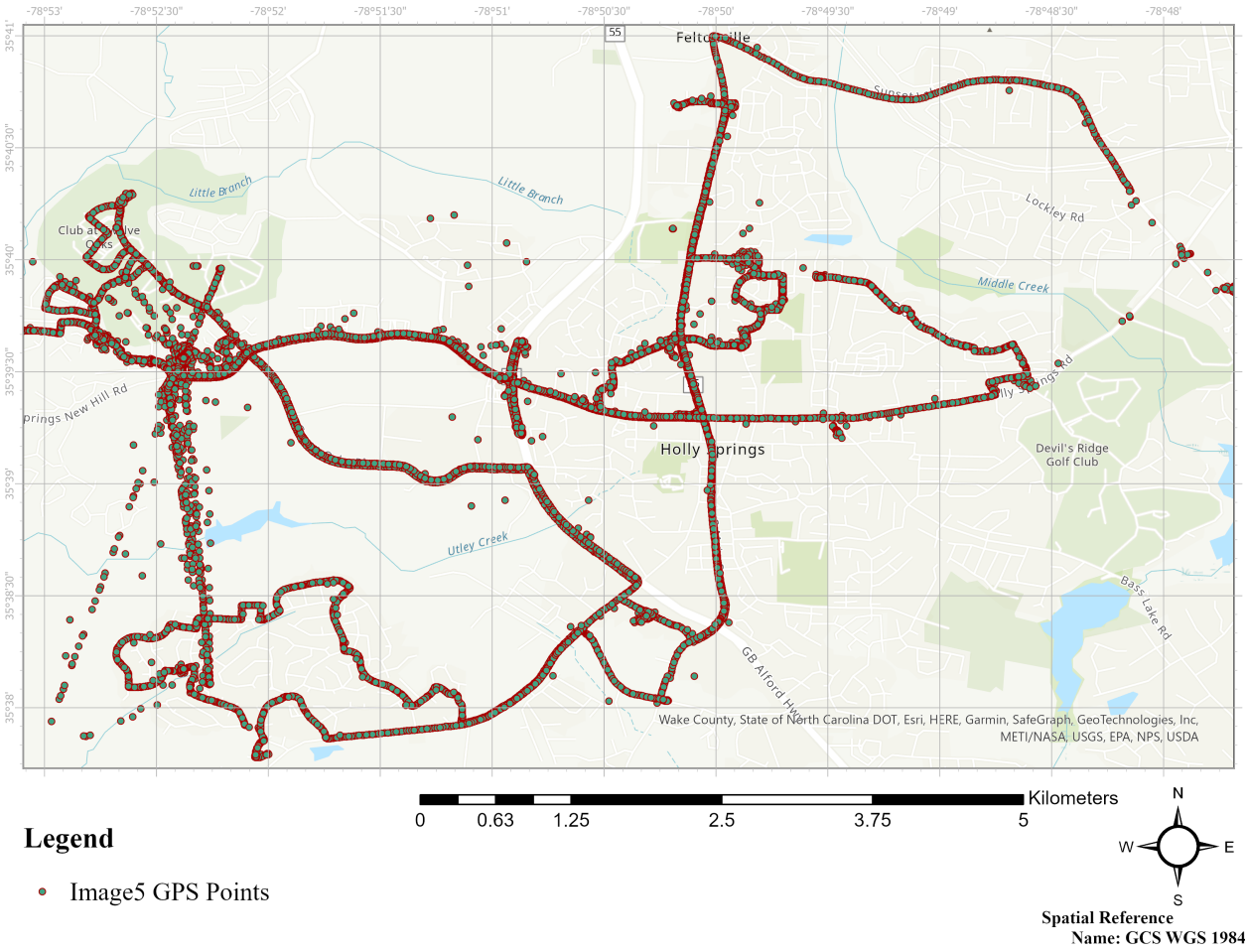


Figure 6.5. All cached geolocations recovered from ZRTCLLOCATIONMO table of Case 1 image 5

displays the GPS points and buffer zones around the cell towers within `CellLocation`, and `CellLocationLocal` tables, Figure 6.11 demonstrating `LteCellLocation`, and `LteCellLocationLocal` tables, finally, Figure 6.12 shows the extent of the case regarding the cell towers.

6.3.1 GPS Validation Using Geographical Prospective

To address hypothesis 1, which pertains to the utilization of spatial analysis, the author devised a methodology to compare the altitude values extracted from the case with real-world values. By leveraging these valuable open-source resources, the author could accurately derive and validate the altitude values associated with the digital evidence in

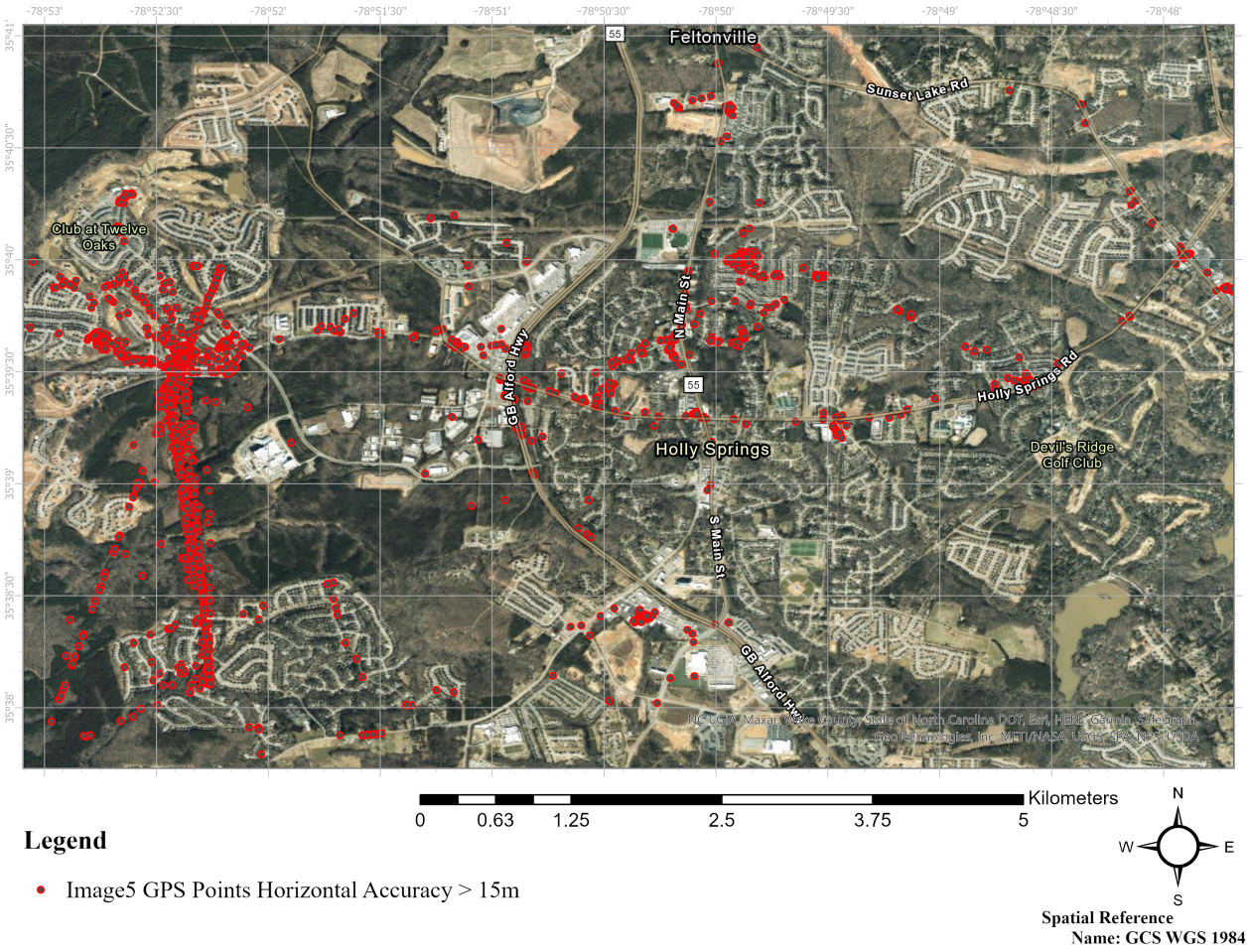


Figure 6.6. Cached geolocations with horizontal accuracy that is worse than 15 meters.

question. This approach ensured that the comparison and analysis of the altitude data were performed against a reliable and widely accepted reference, allowing a robust evaluation of the hypothesis and contributing to the overall credibility of the framework. To achieve this, the author used the state-wide 4-foot contour line resolution dataset publicly accessible as an open-source database [313]–[317]. The author downloaded the data and displayed them on the map. However, the author cannot use it directly to compare elevations because the counter data are a line feature. Therefore, the author had to create a raster layer out of this counter layer to be used as a reference to compare the elevations. The author uses the following procedures to accomplish this task:

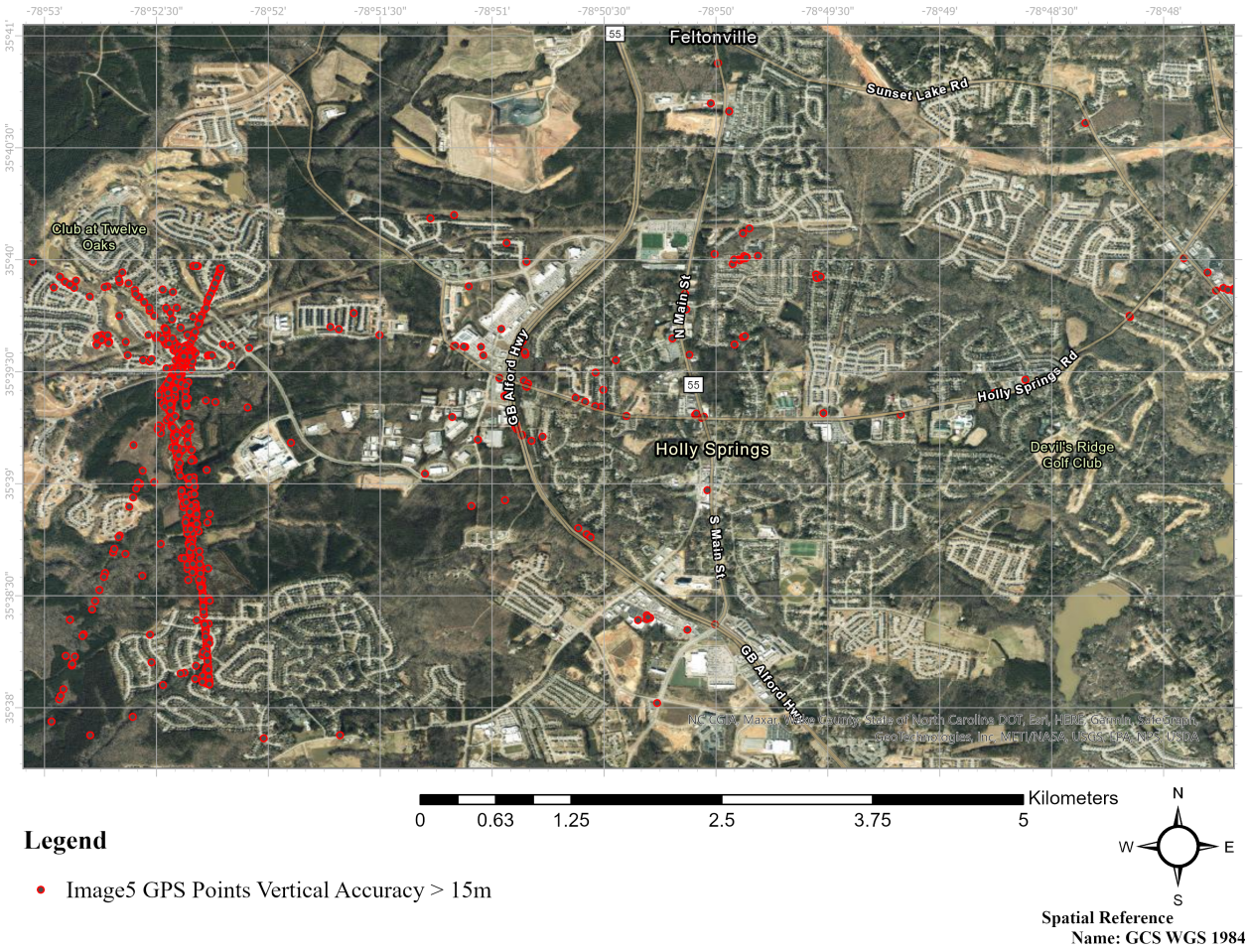


Figure 6.7. Cached geolocations with altitude accuracy that is worse than 15 meters.

1. Identify the extent of the GPS points in question.

2. Create a clip feature that will be used to clip the counter layer to the extent of the case locations. In this case, the extent of the encountered cell tower's dissolved layer was used for the clip feature.

3. Use the clip feature to clip only the contour lines that lie inside this feature and write (extract) the output to a new layer.

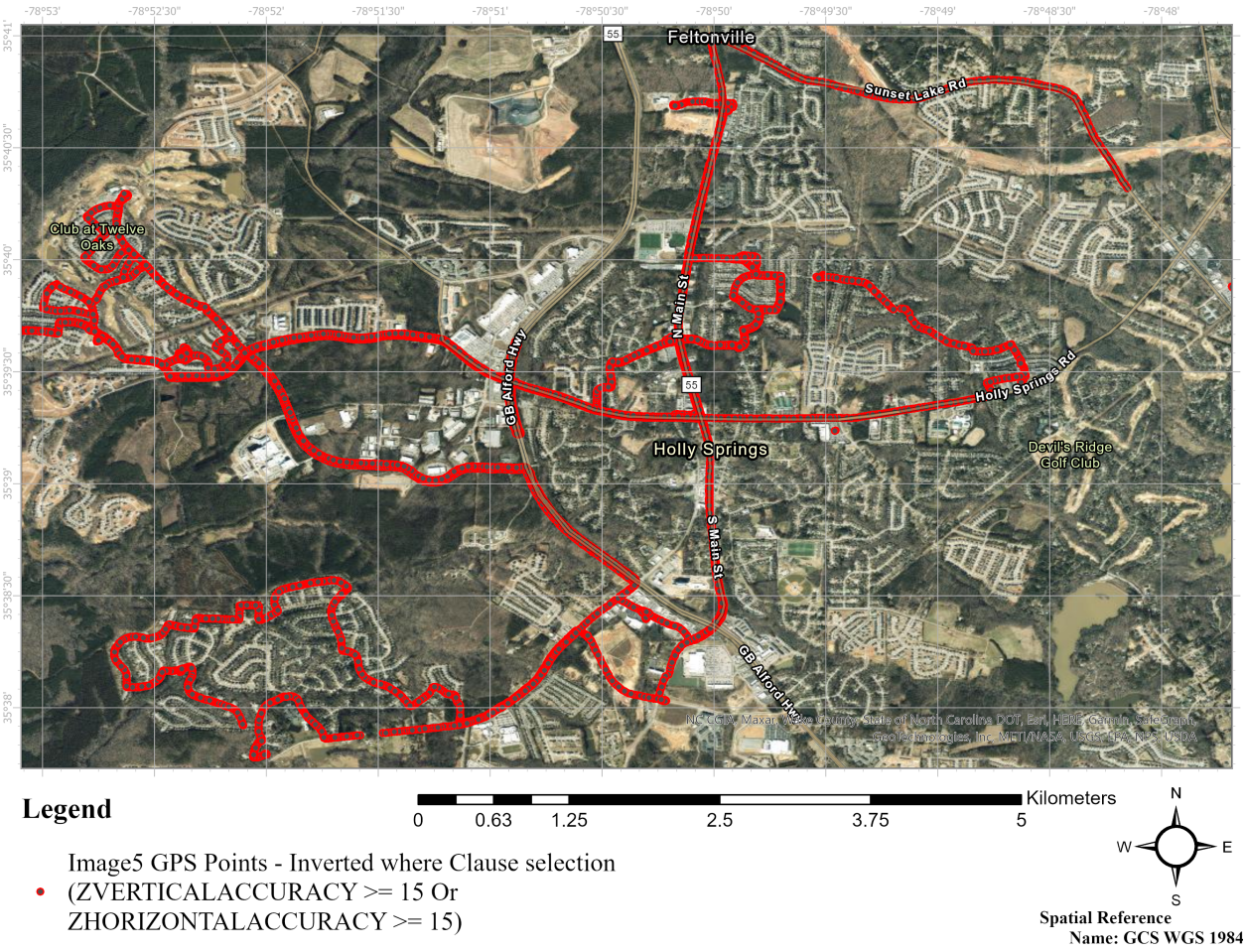


Figure 6.8. Geolocations with inverted where clause of ZVERTICALACCURACY >= 15 Or ZHORIZONTALACCURACY >= 15.

4. The downloaded layer data are in feet, and because there is a need to perform the analysis on meters, the author had to create a new column that calculates the values in meters (see Figure 6.13 for the outcome).

5. Transform the newly created layer into a triangular irregular network layer (TIN), commonly used as an elevation surface representing height values across an extent (see Figure 6.14 for the result).

6. Create a raster from this newly created layer (see Figure 6.14 for the result).

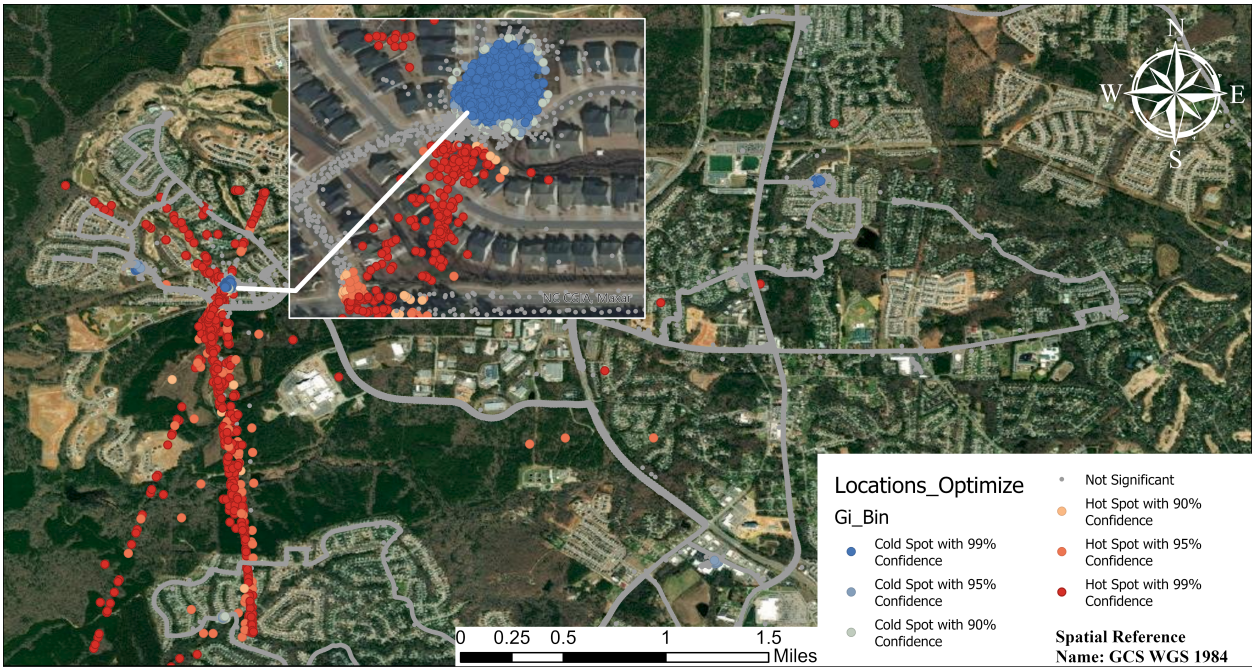


Figure 6.9. Map of statistically significant spatial clusters of high values and low values of the horizontal accuracy.

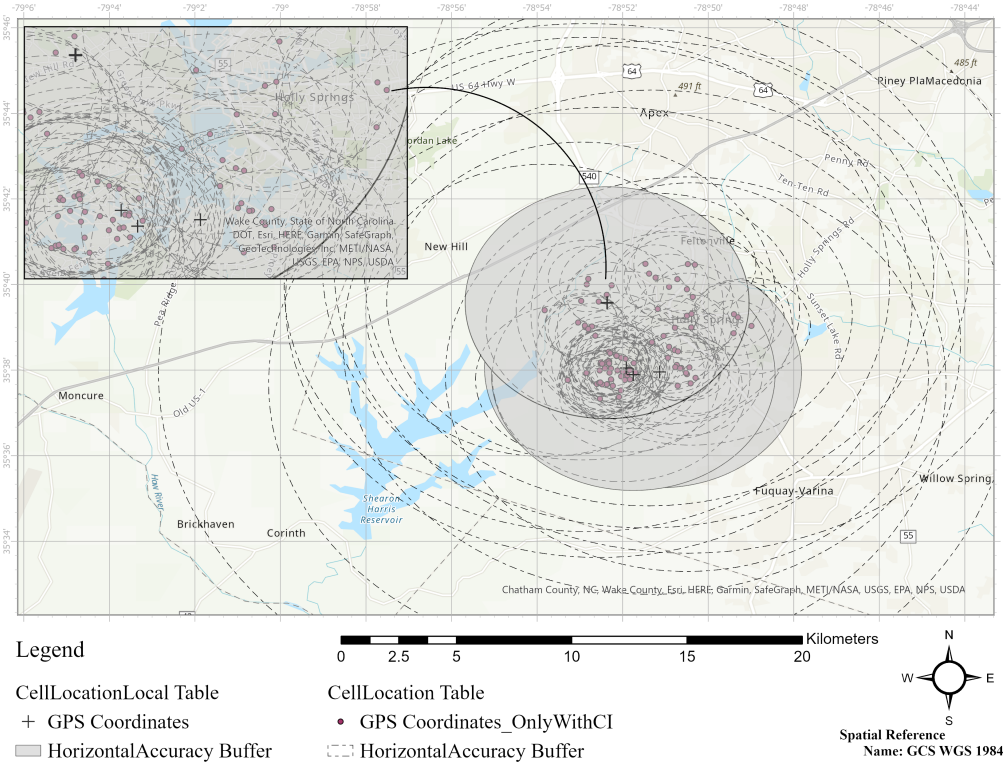


Figure 6.10. CellLocation and CellLocationLocal tables for Case 1 image 5 (iOS 14.3).

7. Now, either the TIN layer or the Raster 4-foot resolution layer can be used to compare the altitude of the GPS points. To do so, at each point where it lays on the TIN or the raster layer, its elevation is taken, and these values are then inserted as data into the newly created column for the data in question.

There is another more direct way, and it includes almost all of Earth's surface by using a 3D Scene, then use `https://elevation3d.arcgis.com/arcgis/services/WorldElevation3D/Terrain3D/ImageServer` ArcGIS service for world elevation 3D. This can be used as an input for the surface to interpolate the z values to extract elevation values. Figure 6.16 demonstrates the steps taken in ArcGIS Pro for using open-source data. The blue symbols represent the input data; the yellow symbols represent operations (i.e., geoprocessing operations); and the green symbols represent the output layers and data.

Once the newly created column is filled with new data, it is time to compare the results of the altitude taken from the raster layer with the altitude value taken by the iPhone. This

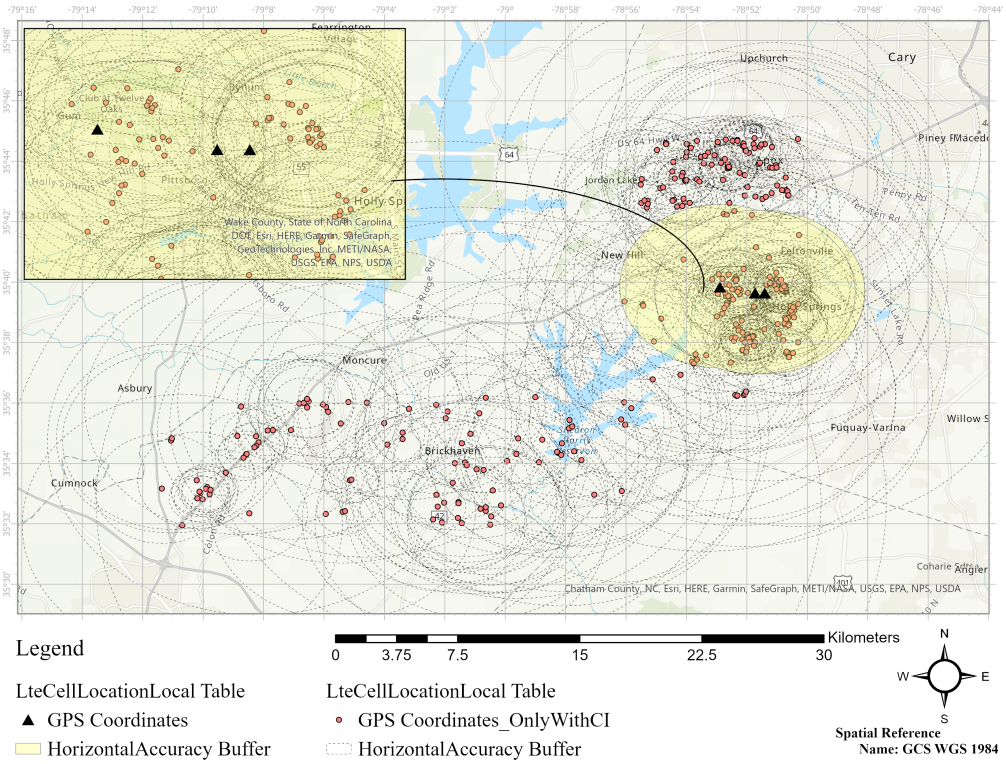


Figure 6.11. CellLocation and CellLocationLocal tables for Case 1 image 5 (iOS 14.3).

depends on the required error rate; in this case, the created new column will be populated with 0 if the difference between the two values is less than 10 meters and will be populated with 1 if the difference is 10 meters or more, -1 if the difference is -10 meters or less, and 0 for everything else. Then, all records with more than 10 meters of difference between the two points are selected and exported as a new layer, and the inverted selection, where the elevation between the raster layer and the GPS altitude is less than 10, is also exported into another layer to display them. Figure 6.17 shows the results. These two maps display and clearly state that the iPhone can obtain good altitude accuracy, and most of the points have good accuracy. Furthermore, the problems were either when the phone had a bad connection or signal that resulted in poor accuracy or when the user was inside the building at this location, which can lead to a bad connection, as discussed before. It also can mean that the device was not on the ground floor since the compared layers do not take buildings into consideration.

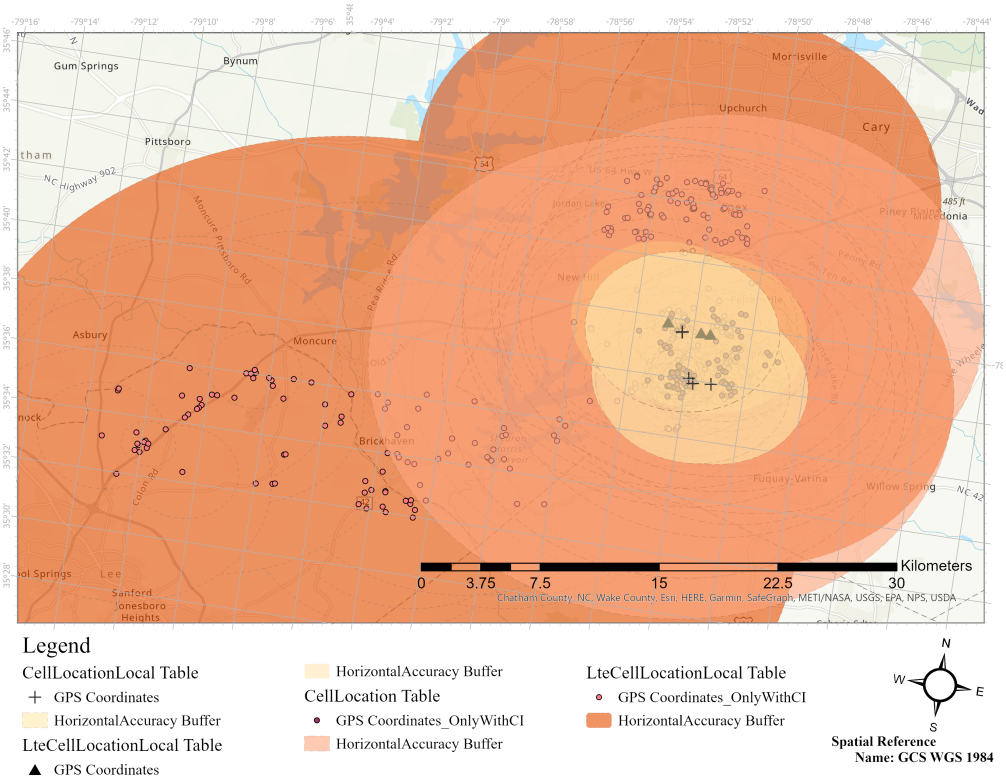


Figure 6.12. LteCellLocation and LteCellLocationLocal tables for Case 1 image 5 (iOS 14.3).

Moreover, Harrington and Cross, in their book [175], discussed how Google Earth had helped digital forensics investigators utilize maps and street photographs to integrate them into seizing, acquiring, examining, and reporting. Therefore, we used Google Earth to check the validity of the location in the images, and then Google Earth was used to verify the surroundings and see if the location was accurate. For example, we tested this using the image with a geotag shown in Figure 5.8; at the exact location, Google Earth has a street view represented in Figure 6.18. The Google Earth compass also indicates that `GPSimgdirection` shown in Figure 5.9 is very accurate. In addition, we can do the same process for all pictures and check the accuracy. This can help identify those for whom the phone had no problem finding and creating the correct GPS tags in the image.

As a result, validating GPS points collected using a spatial analysis methodology enabled:

- Providing general accuracy assessment (e.g., lowest, highest, average).

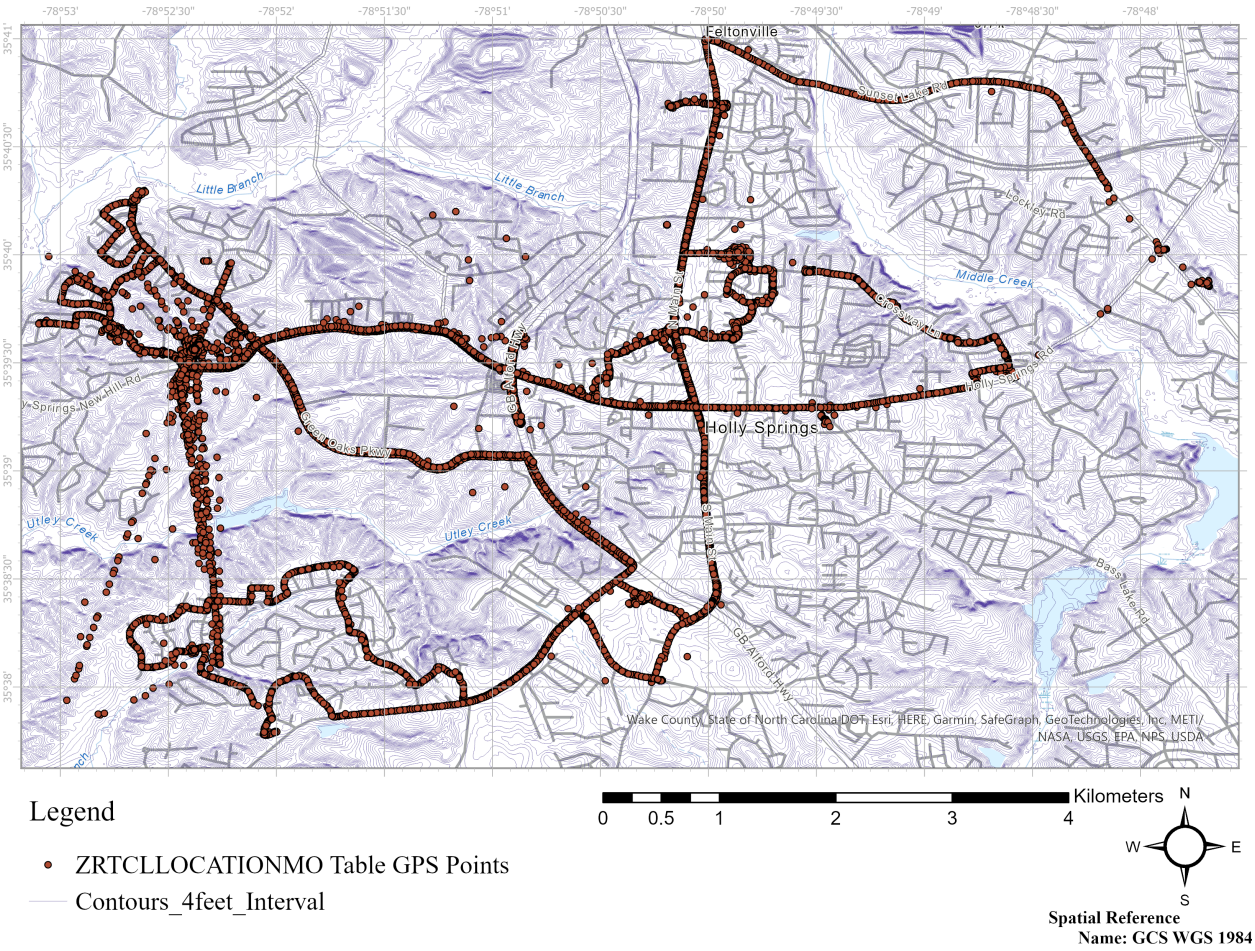


Figure 6.13. Map showing the 4 feet contour layer

- Can highlight locations with poor GPS signal or high error value.
- Error data elimination, if needed. For example, checking the image with the spatial analysis to check for geotag errors.

6.3.2 Geo-Contextualization

To effectively address and test the second and third hypotheses, the author formulated a series of investigative questions that necessitated the application of advanced geo-contextualization. These carefully crafted questions allow for a comprehensive exploration of the research question and aim to explore the intricate relationships and dependencies between

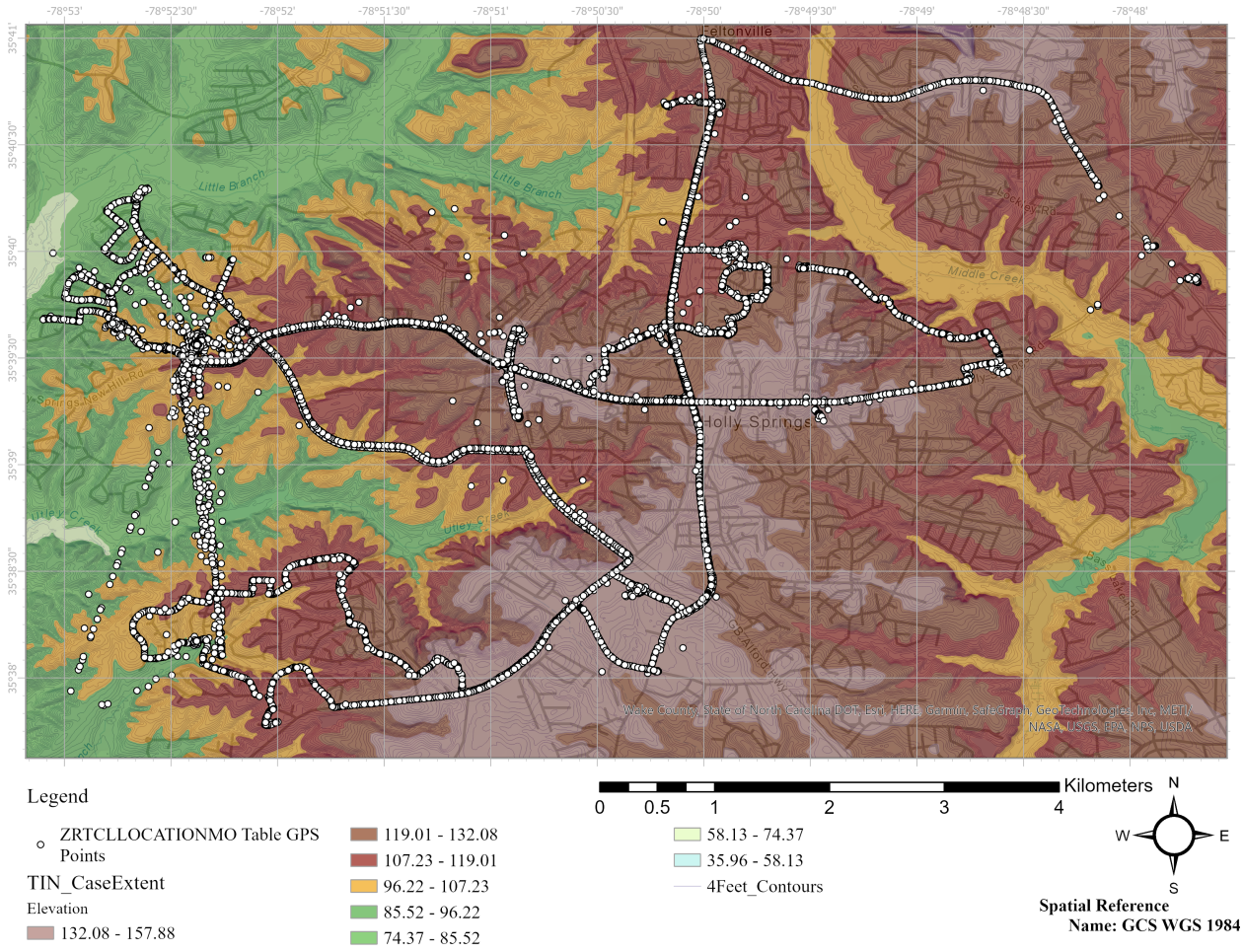


Figure 6.14. Map showing the TIN and the contour layers

geodata and the digital evidence under investigation. By incorporating geo-contextualization principles, the investigative questions delved into the spatial and temporal aspects of the evidence, seeking to unveil hidden patterns, correlations, and contextual information that could provide crucial insights into the case at hand. The utilization of advanced geo-contextualization techniques allowed for a comprehensive examination of the digital evidence within its geographical context, enabling a more thorough evaluation of the hypotheses and contributing to the overall validation of the framework.

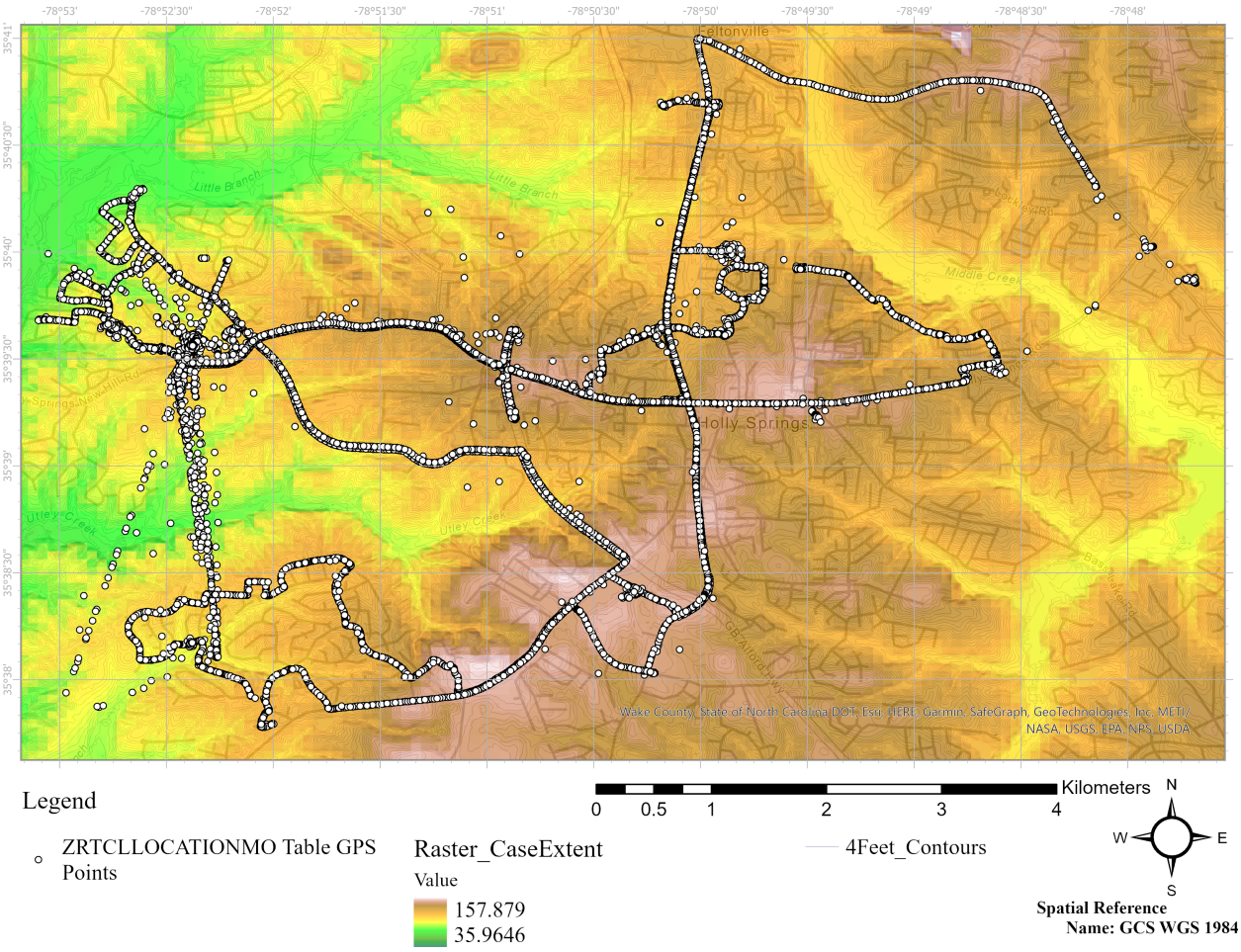


Figure 6.15. Map showing the raster and contour layers

6.3.3 Utilizing IP Geolocation and OSINT for GPS Mapping and Distance Analysis in Cyber Forensic Investigations

First, from the comprehensive examination, it is clear that there is a need to map the recorded IP addresses found in the case. Autopsy provided an easy way to extract recovered IP addresses and the number of hits. IP addresses are essential in cyber forensics to identify devices and trace evidence based on network activity. They can reveal necessary information about the user's device during internet activity and aid in identifying IP addresses that complement the user's physical location. However, there is still a gap in utilizing IP mapping and visualizing techniques in cyber forensic tools, resulting in the omission of valuable digital

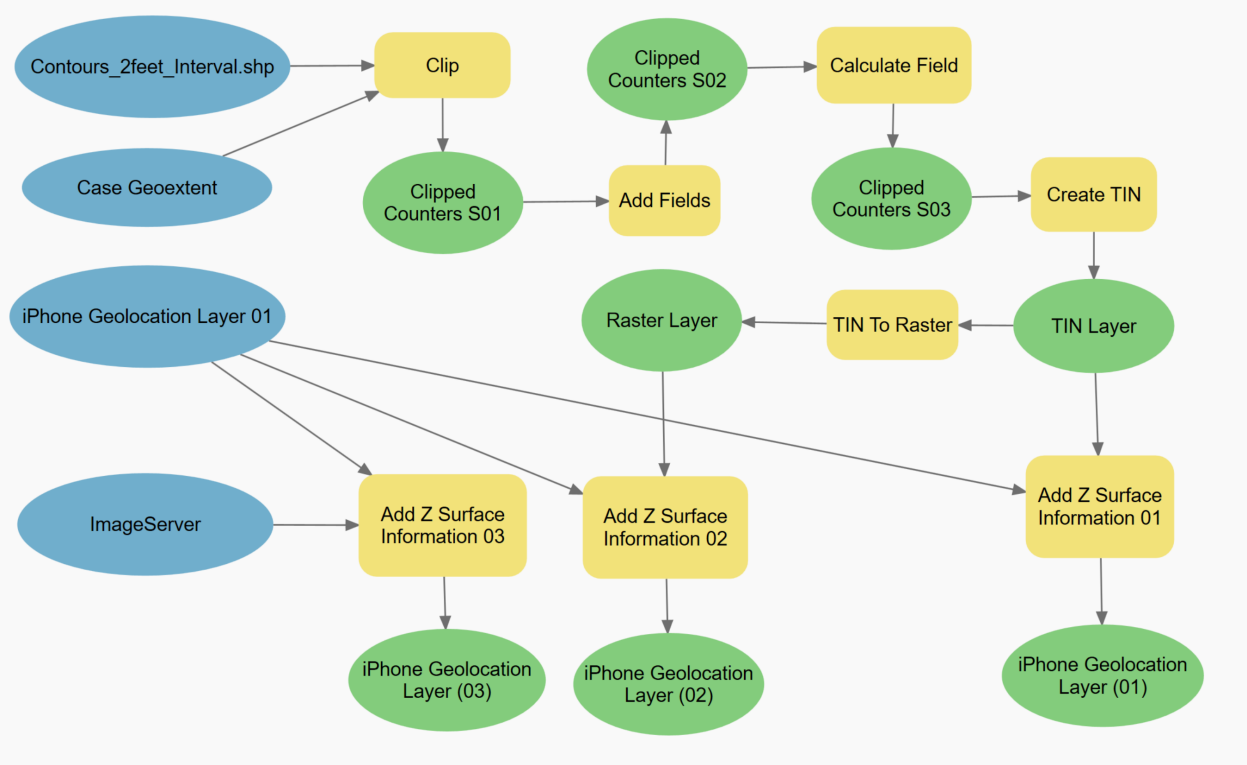


Figure 6.16. Geoprocessing model and workflow for horizontal accuracy validation of geodata collected

evidence. Therefore, there is a need to leverage the encoding module to use OSINT to locate recovered IP addresses.

The importance of IP as geodata in cyber forensic investigations can be achieved using visualization and presentation techniques, considering several sources of evidence from OSINT. This approach aims to enhance the speed of the investigation process concerning IP addresses and provide a better understanding of the relationship between IP addresses and physical locations within an investigation. Therefore, by utilizing IP geolocation mapping and visualization techniques, investigators can better analyze and understand the data generated by IP addresses, helping to identify potential suspects and establish their movements. This approach can help bridge the gap between using IP data for geolocation purposes and providing valuable information on cyber forensic investigations. By following the following methodology and harvesting the transdisciplinary approach, investigators can leverage IP

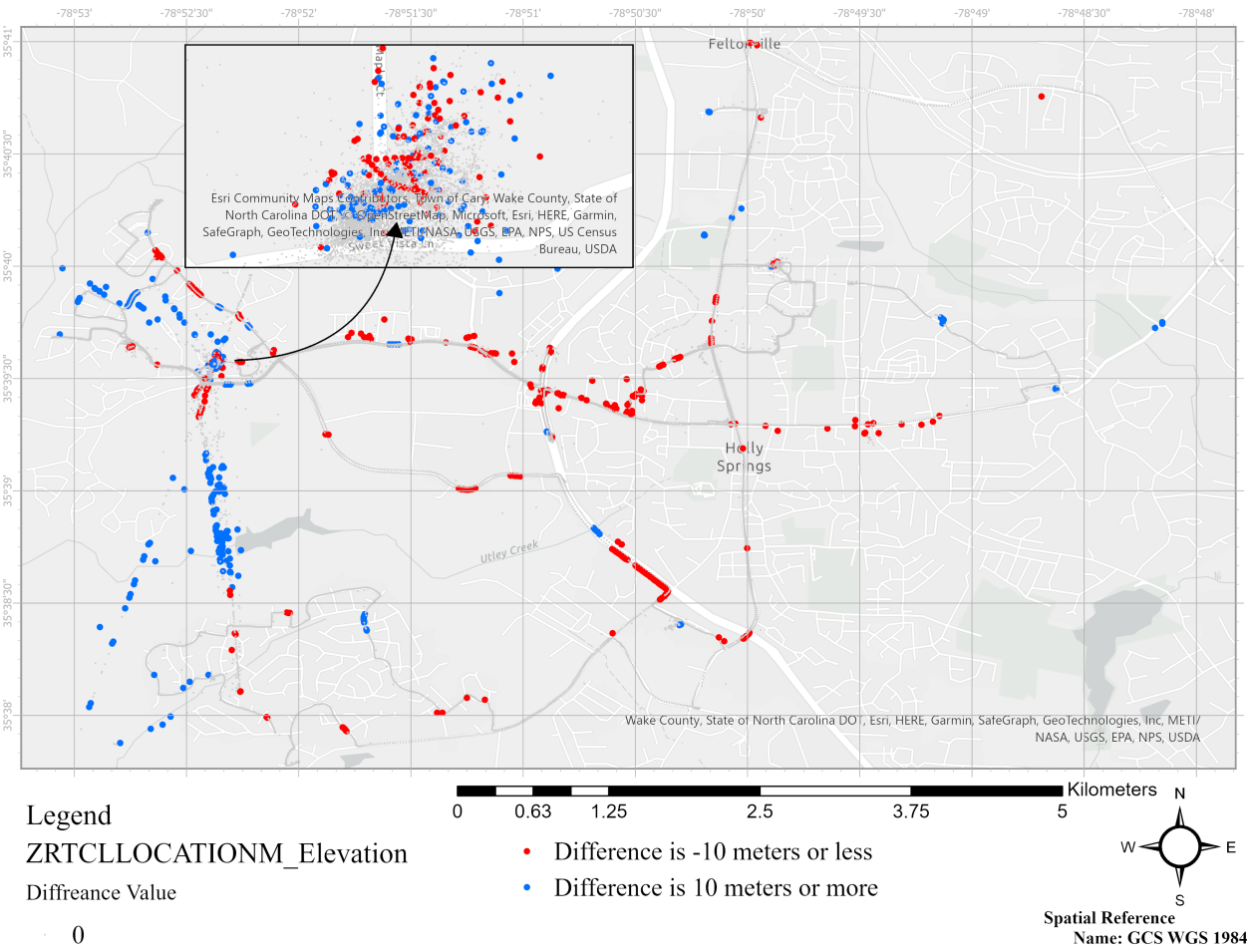


Figure 6.17. Map showing locations have more than 10 meters, and less than -10 meter altitude difference between the populate field by the phone and the TIN layer value

Figure 6.18. Google street view of the same rounding found in the photo presented in Figure 5.8

geolocation mapping, OSINT, and GPS data analysis to gain insights into the relationship between IP addresses and physical locations. The following are the steps taken to perform the analysis:

1. Collect IP addresses associated with the digital evidence under investigation using regex.

2. Encode the IP address using OSINT tools or services that offer IP geolocation mapping capabilities. In this test, `https://ipinfo.io/` [318] bulk upload was used.

3. Plot the mapped IP addresses into the GIS tool to obtain their corresponding physical locations.

4. Visualize IP addresses on a map to display their geographic distribution.

5. Perform geospatial distance analysis calculations between the mapped IP geolocation points and the case GPS coordinates.

6. Evaluate the proximity of IP addresses to the collected GPS data points, and identify any IP addresses that are in close range or overlap with the GPS coordinates, indicating potential correlations or connections.

7. Conduct further investigation and analysis to determine if there are any meaningful relationships or patterns between these IP addresses and the associated GPS coordinates.

8. Document the findings of the IP geolocation mapping, GPS data analysis, and distance analysis in a clear and comprehensive report.

9266 IP addresses got mapped to a location for Case 1 image 5 (iOS 14.3). Figure 6.19 demonstrates all IP addresses mapped and shows those within 30 KM of Cell Towers within the case. The 11 IP addresses can be related to the user and need further investigation.

6.3.4 Using Georeferencing Services to Map a Text-Based Address

Investigators might need to accurately georeference addresses found within digital evidence or entities of interest associated with the forensic investigation. An example of a table that contains an address as text is `ZRTADDRESSMO` within the `\private\var\mobile\Library\Caches\com.apple.routined\Cloud-V2.sqlite` database. Text-based geodata can be mapped using a georeferencing service, in this case, ArcGIS Pro georeferencing services that convert addresses into geographic coordinates; Figure 6.20 demonstrates the parameters used). The `ZRTADDRESSMO` table contains 31 addresses for case 1 image 5, and they are all successfully mapped to locations (see Figure 6.21). As a result, Figure 6.22 shows the mapped addresses and GPS points within the `ZRTLEARNEDVISITMO` table that stores GPS for frequent location functions with an expiration date of approximately 56 days.

6.3.5 Geo-PoL Analysis

PoL analysis is an analysis that evaluates all kinds of behavior in both temporal and spatial dimensions. As a result, this type of analysis can help create knowledge that can explain the actions and activities of the device user, which are not visible in traditional

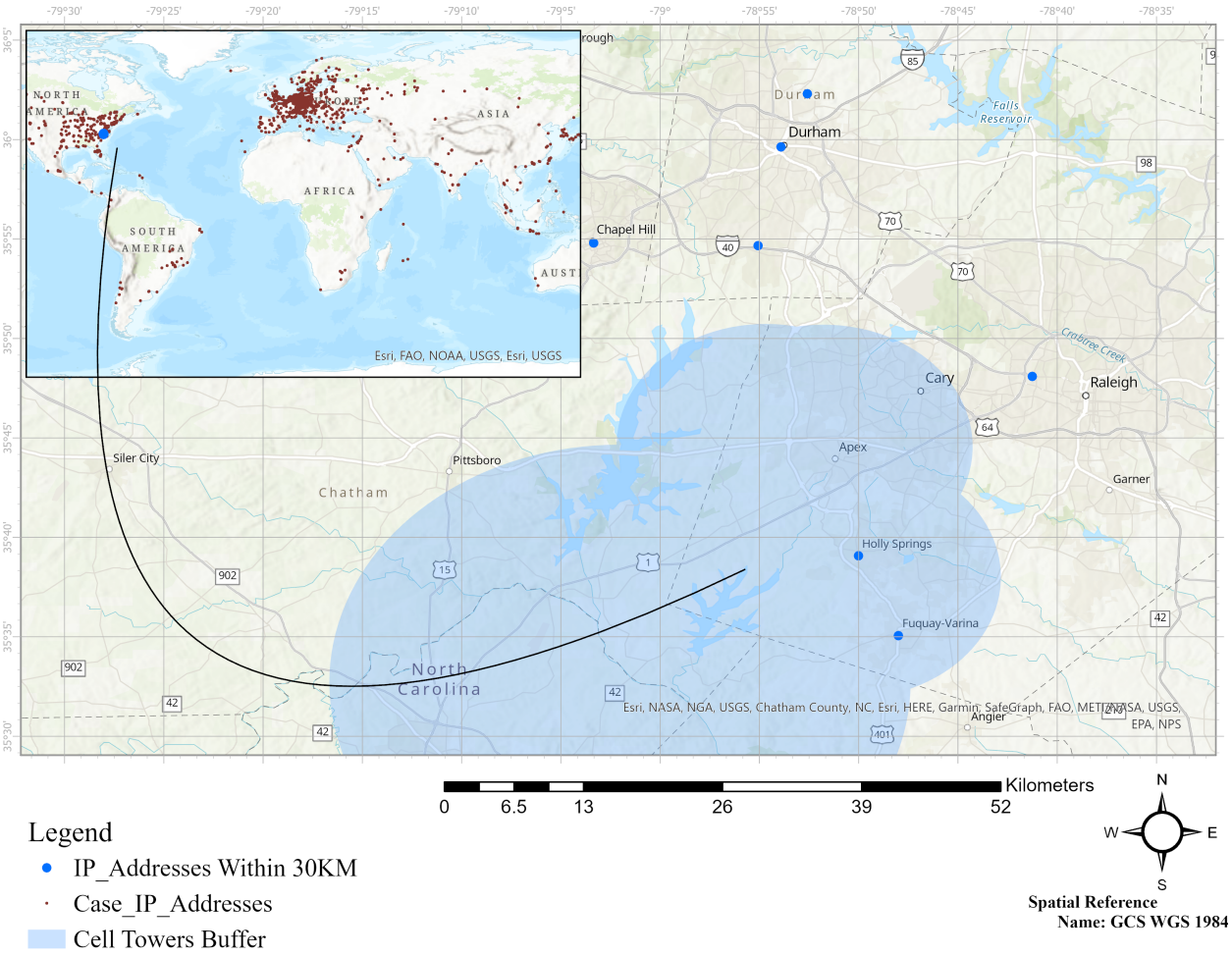


Figure 6.19. Case 1 image 5, IP addresses mapped, and showing IP addresses of locations within the case extent.

standard analysis (e.g., timeline). It is one type of intelligence technique that aims to aid investigation to uncover the story and quickly identify essential actions. PoL analysis has gained popularity in cyber forensics due to the need to use multiple approaches to improve the importance of information by giving it valuable meaning and creating reasoning behind what happened.

By incorporating the spatial aspect as layers of geodata by mapping locations and geographical patterns into the PoL analysis, investigators can further improve their ability to uncover the story behind the digital evidence and identify critical actions. Traditional temporal analysis alone may provide information on the timing and frequency of activities.

However, by considering the spatial dimension, investigators gain a more comprehensive understanding of how these activities relate to specific locations or geographic patterns. For example, mapping the locations where a device user accesses a service or makes specific messages or transactions can reveal potential hotspots or patterns of activity. The investigators can then analyze these spatial patterns in conjunction with the temporal aspect to identify connections, correlations, or anomalies that may be crucial to the investigation.

Investigators can use geodata present on the investigated devices to determine whether or not two or more devices were present at the exact location at the same time. This can be used to establish a spatial-temporal relationship between the investigated devices. A potential strategy involves examining geographic data collected from mobile devices, GPS logs, and other location-aware sources. Moreover, social network analysis techniques can be employed by investigators to ascertain possible links between the individuals using the devices. This may entail scrutinizing their social media profiles, email accounts, or other digital correspondences to identify shared contacts or communication trends.

Upon identifying potential connections between the individuals, investigators may utilize supplementary data sources to construct a more comprehensive description of their activities and associations. This may entail investigating surveillance recordings, conducting witness interviews, or gathering other supplementary evidence. By integrating various data sources, investigators can develop a more all-encompassing comprehension of individuals' behaviors and potentially establish spatial-temporal connections among them.

Moreover, visible geospatial phenomena, which refer to spatial information or patterns that can be directly observed or extracted from digital evidence, are usually detected by well-known guidelines and digital forensic tools. These visible geospatial phenomena are evident in geolocation data, such as GPS coordinates, Wi-Fi network information, or metadata embedded in digital files (see figure 6.23 shows located Wi-Fi access points and dissolved buffer using each Wi-Fi access point horizontal accuracy along with geo-cached data from the iPhone). Investigators can visualize and analyze these visible geospatial phenomena to understand the spatial aspects of a digital investigation, such as the locations where certain activities or events took place.

On the other hand, invisible geospatial phenomena in cyber forensics are spatial aspects or relationships that are not immediately apparent or accessible through visible geospatial data alone. These invisible geospatial phenomena may require specialized techniques, algorithms, or expertise to uncover or analyze. They involve hidden patterns, associations, or insights that are not readily visible or understandable without additional investigation or processing. There are many examples of invisible geospatial phenomena in digital forensics, which include 1) temporal-spatial correlations to uncover associations between timestamps of digital artifacts and their corresponding geolocation data to identify patterns of movement or activity, 2) geospatial clustering to identify clusters of geolocation data points to reveal potential hotspot areas or locations of interest related to the investigation, and 3) geofencing by defining virtual boundaries or geographic zones to determine if certain activities or events are occurring within specific geographical areas of interest.

These invisible geospatial phenomena require advanced data analysis techniques, algorithms, and tools to uncover meaningful insights and support the investigative process in cyber forensics. Through these techniques, investigators can acquire a more comprehensive comprehension of the spatial elements of digital evidence and reveal concealed connections or trends that could be imperative to the inquiry. It is worth mentioning that the detectability of geospatial events in cyber forensics varies depending on the data sources, investigative methods, and objectives. The technological progress and the emergence of novel geospatial analysis techniques in cyber forensics enable investigators to unveil and scrutinize previously hidden geospatial occurrences, yielding valuable findings for the pursuit of evidence and truth.

First, Table `ZRTCLLOCATIONMO` has the following columns: speed, direction, timestamp, and GPS locations. Therefore, they can be used to display the data based on each of these columns or a combination of these. For example, suppose that there is a need to know the user's direction of movement once data are in the direction columns. In that case, a query selects all records with data in the direction and then exports the results into a new layer to visualize direction and speed. This new layer now contains all records that do not have null data in the direction field. The direction number reflects the degrees that start at 0 and end at 359.99. To make it even more appealing, create a unique symbology for the direction by

choosing points in blue if the direction is between 0 and 90; points should be colored green if they are between 91 and 180; points to be colored yellow if they are between 181 and 270; and finally, points should be colored red if they are between 271 and 359.99. Figure 6.24 illustrates the outcome of these procedures.

Another example is very similar, but used the speed column to display the speed in colors. This can be done with the same methodology as selecting rows with speed and then exporting them to another layer that we will use to display the results. This table stores pace and measures it in meters/sec; to convert it to kph, the number must be multiplied by 3.6. Therefore, the data can be split based on the question's requirements; in this case, the data were divided into two main categories, speeds below 80 km/h (approximately 50 Mph) in green and speeds above 80 km/h in red. Figure 6.25 illustrates the symbology along with the points.

Moreover, conducting a geo-PoL analysis enhances the mapping and visualization of the collected information. The focus was to establish connections between related events or occurrences that took place in the same location or geographic context. By linking information that shares similarities in terms of location, time, and other relevant factors, the investigators can gain a deeper understanding of patterns and relationships within the data. In addition, in cyber forensic investigations, multivariate analysis can be precious when dealing with complex datasets that involve multiple factors, variables, and dimensions. It helps us uncover hidden connections, identify critical factors influencing the investigation, and make informed decisions based on a more thorough understanding of the data.

One example is correcting locations with the heart rate of the user of the device. Heart rate geo-mapping using contextualization techniques involves analyzing heart rate data in conjunction with spatial information and other contextual factors. A more comprehensive understanding of heart rate patterns and their underlying influences can be gained by incorporating spatial contexts, such as geographic locations, weather conditions, or physical activities. Moreover, other factors may contribute to changes in heart rate, such as stress, fear, and illness. Analyzing heart rate data in relation to these contextual factors, patterns, and correlations can be identified, allowing for a more comprehensive understanding of the underlying influences on heart rate.

Haret rates recovered are timestamped; therefore, joining them with recovered GPS locations timestamp allowed for few matching records. However, these records are minimal because there is no real sync between when the fitness trackers such as Apple Watch will take a heart rate measurement and when the device will take a location approximation. Therefore, for the per pose of investigation and extermination, the following was done:

1. Preform close timestamp matching using Pandas [319]; the `merge_asof()` function allows for merging two datasets based on their timestamps, matching the closest timestamps in each dataset.

2. 120-second tolerance was used to match the records, and the direction was set to nearest

3. It depends on what needs to be matched with what, 1) every heart rate matched with a location, or 2) every location needs to be matched with a heart rate.

4. Save the results into a new file, and then plot the GPS points on the map.

Although this manipulates the revitalization evidence, it provides the investigators with more insights that can later be used with the original data to find more forensically sound evidence. Both data timestamps must be preserved when merging, so each record has the left and right table timestamps. This will allow for easy traceability of original evidence. Multivariables were used as a symbology (i.e., speed and heart rate) for visualization; speed was split into three categories: 0 or below, between 0 and 1.24 meter/sec, and above 1.24, whereas for heart rate per minute, below 50, above 50 up to 95, and above 95. Figure 6.26 demonstrates the results from geo-contextualizing each heart rate with geolocation, and figure 6.27 demonstrates matching each geo-location with a responding heart rate.

As a result, leveraging spatial contexts and considering various influencing factors, heart rate geo-mapping with contextualization techniques enables researchers and practitioners to gain deeper insights into heart rate patterns and the complex interplay of factors that influence them. Another example follows the same geo-contextualization approach to geo-contextualize received messages. Figure 6.28 shows geo-contextualized messages within the case.

6.4 Results

The analysis and evaluation of the framework yielded compelling results that strongly support the three hypotheses in this study. The empirical findings confirmed the validity and effectiveness of the proposed framework in addressing the identified research gaps and challenges. These outcomes validate the importance of incorporating a geographical perspective into cyber forensic investigations and emphasize the potential value of geodata in enhancing the overall forensic process. Consequently, the null hypotheses hypothesized that the framework would have no significant impact or improvement were convincingly rejected. The positive outcomes and rejection of the null hypotheses affirm the proposed framework's significance and potential to enhance cyber forensic practices in handling geodata. Therefore, the results of using the framework have approved that geodata can help confirm or disprove alibis, establish behavior geo-patterns, and establish geospatial timelines.

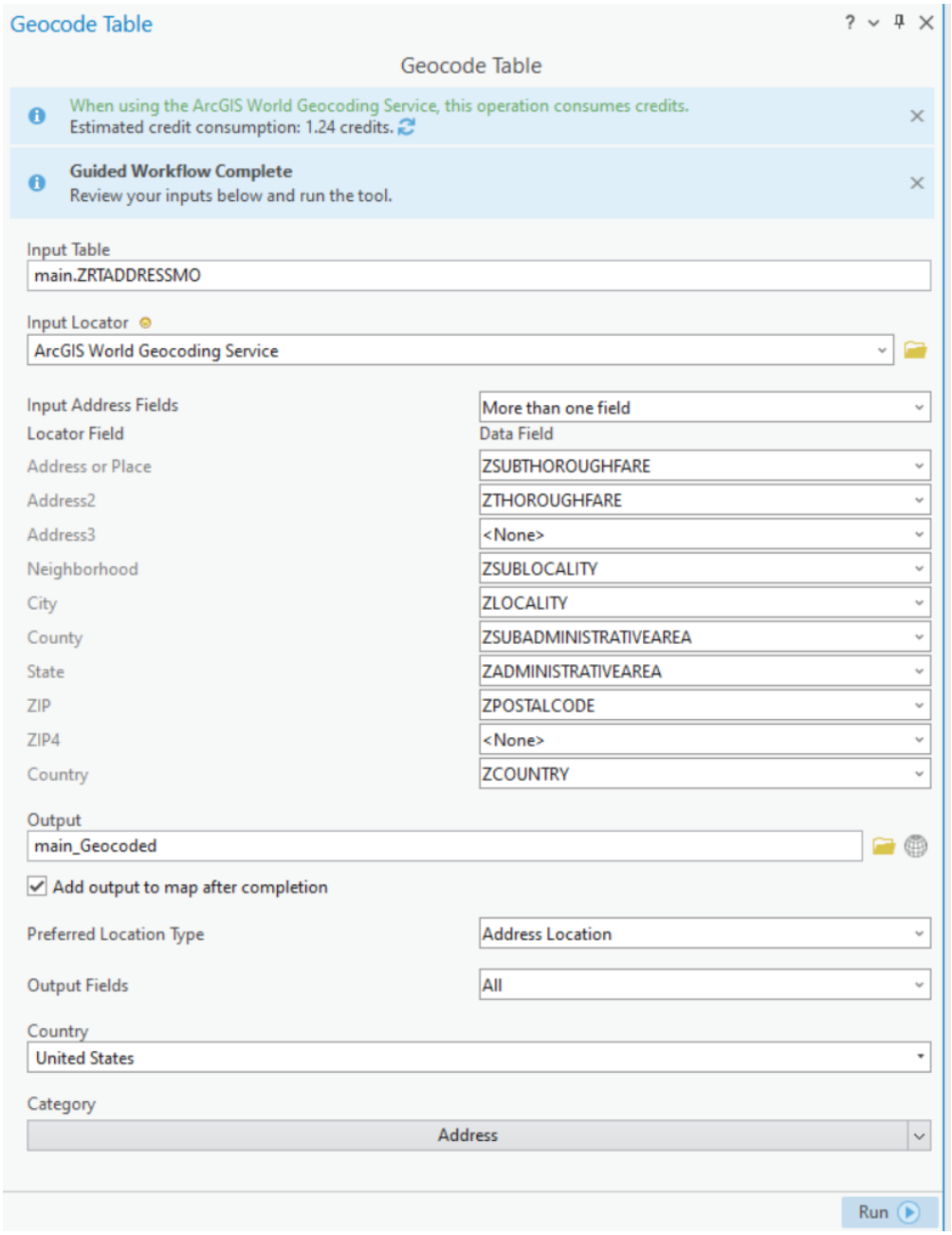


Figure 6.20. The parameters used for addresses georeferencing within ArcGIS Pro.

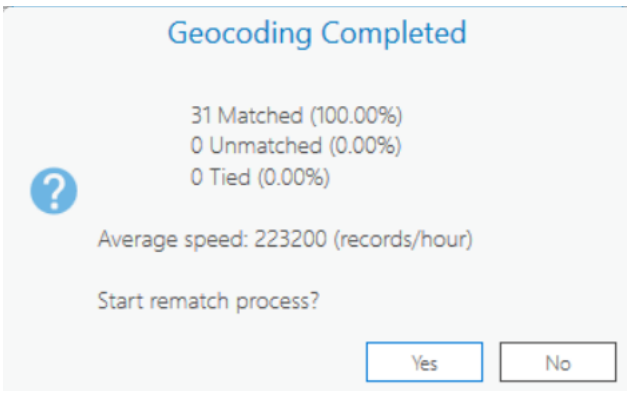


Figure 6.21. A successful georeferencing operation.

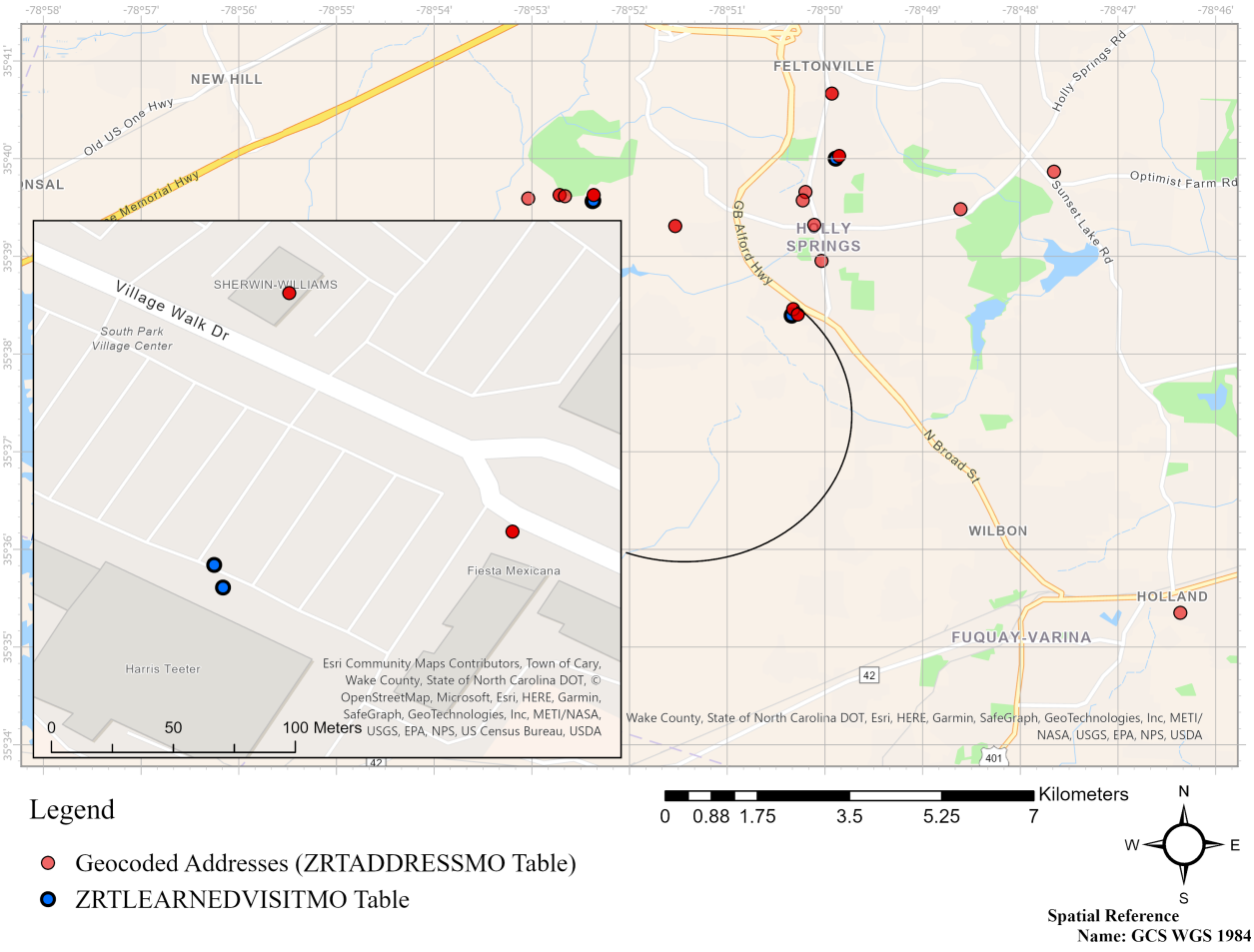


Figure 6.22. 31 mapped addresses in table ZRTADDRESSMO.

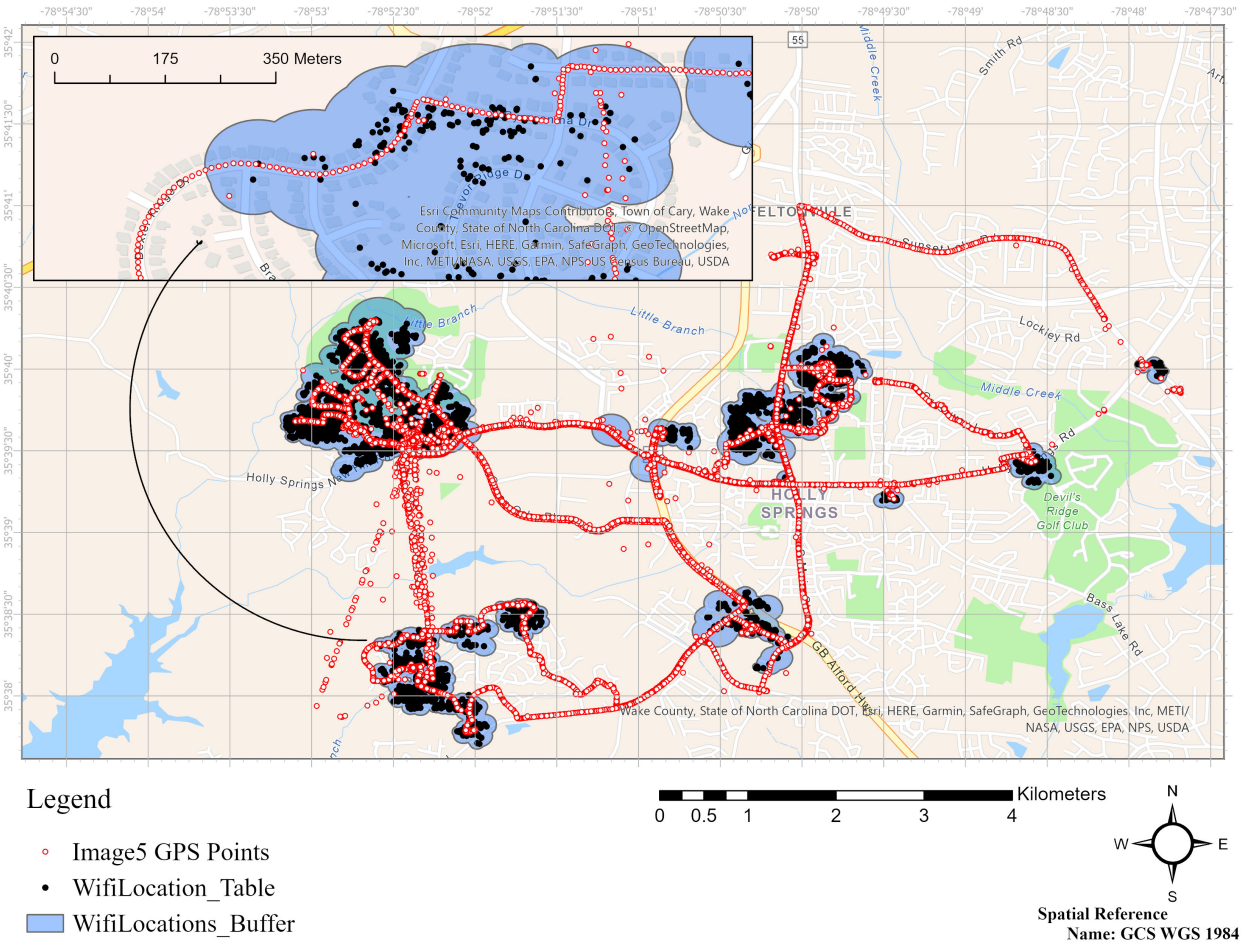


Figure 6.23. A map showing the device movement GPS points and locations of encountered Wi-Fi Access points.

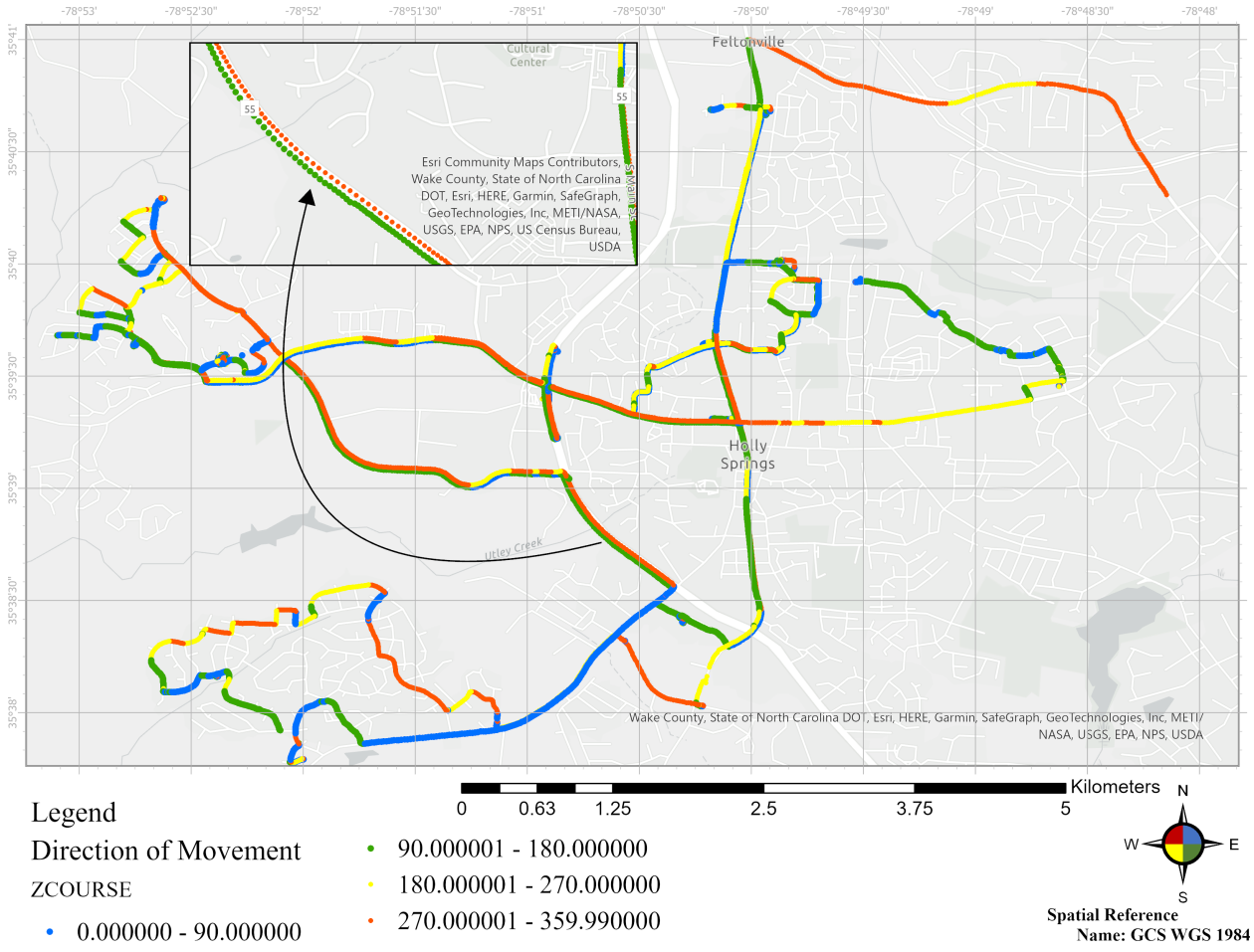


Figure 6.24. A map showing the device movement direction.

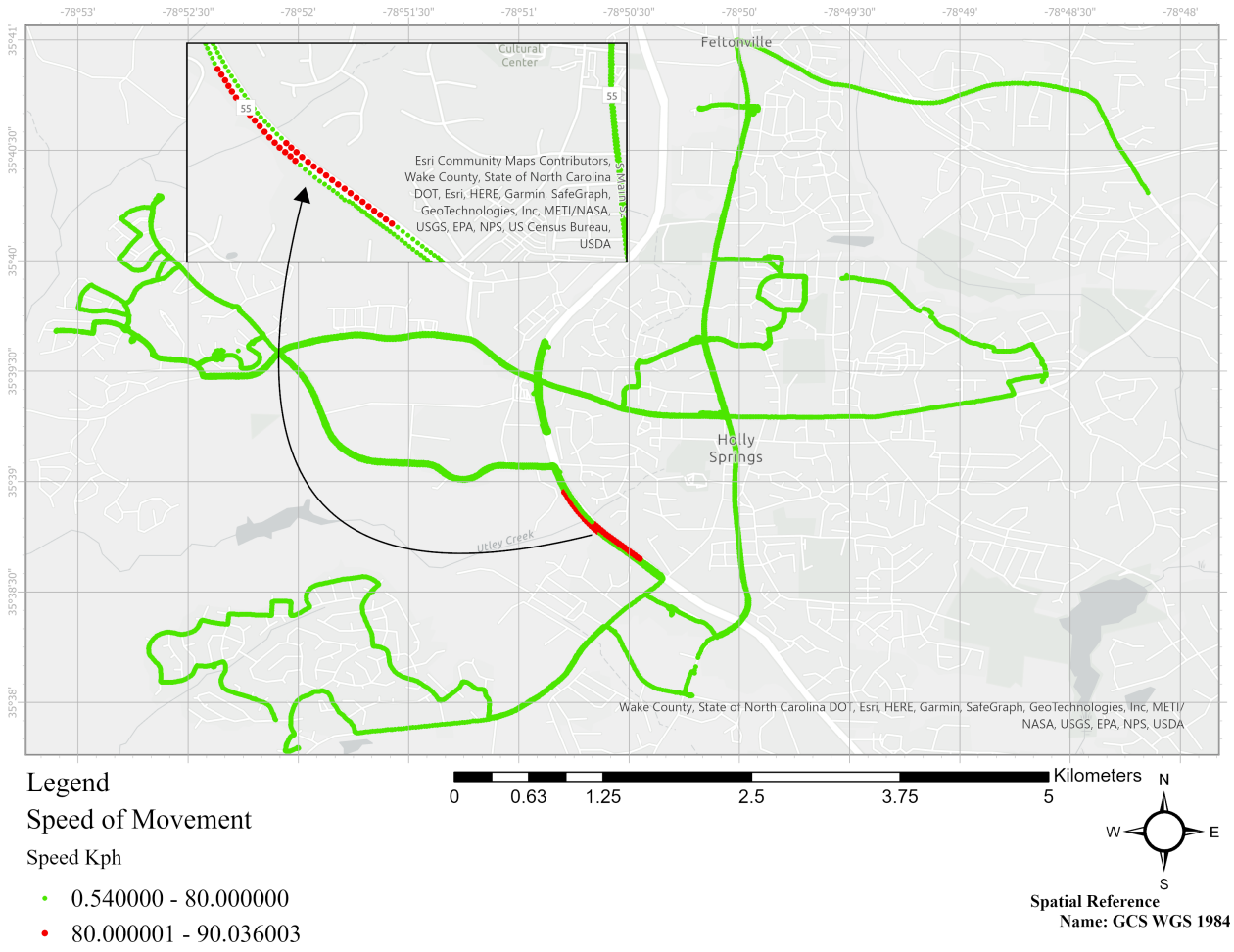


Figure 6.25. A map showing the device's movement speed.

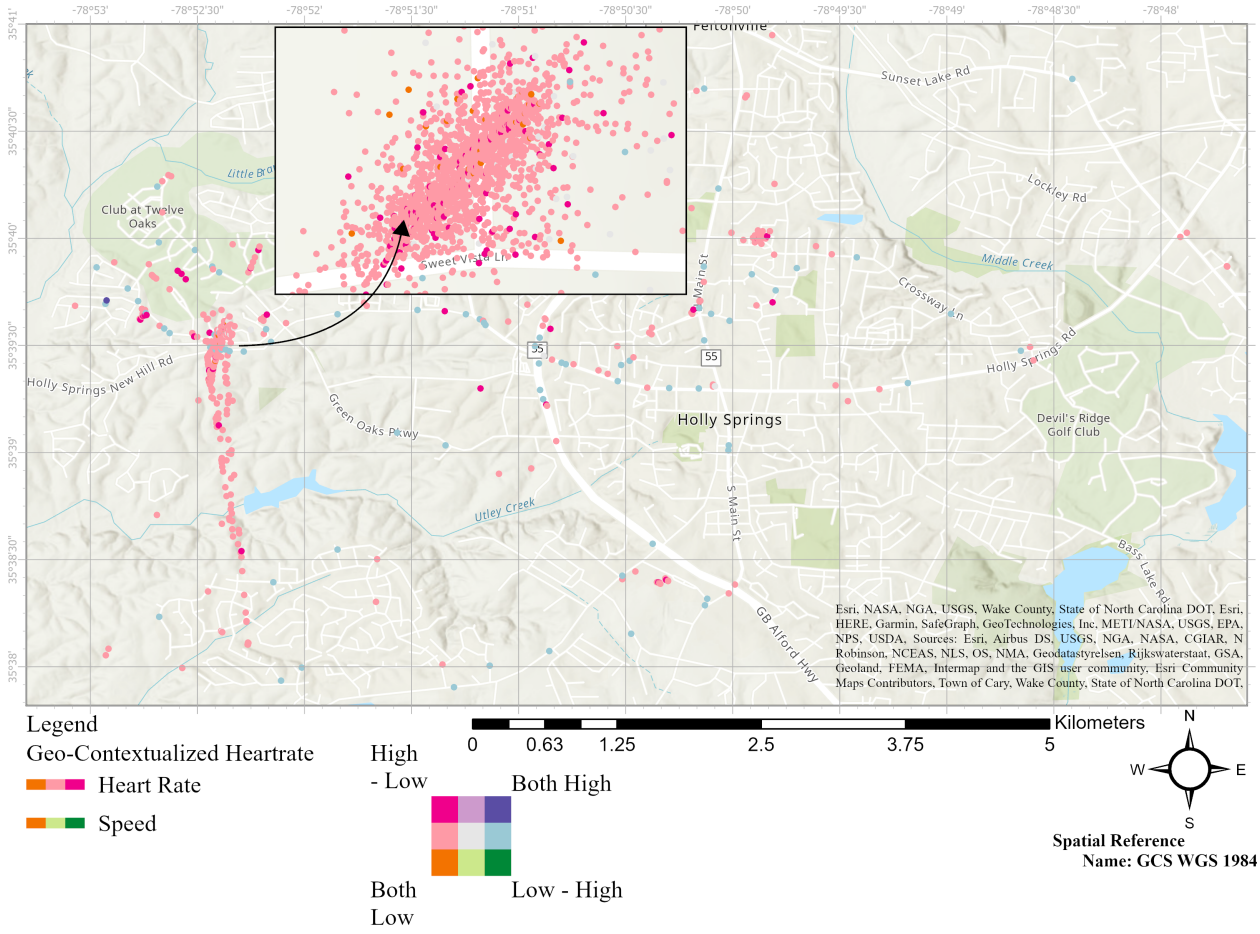


Figure 6.26. A map showing the geo-contextualizing of each heart rate.

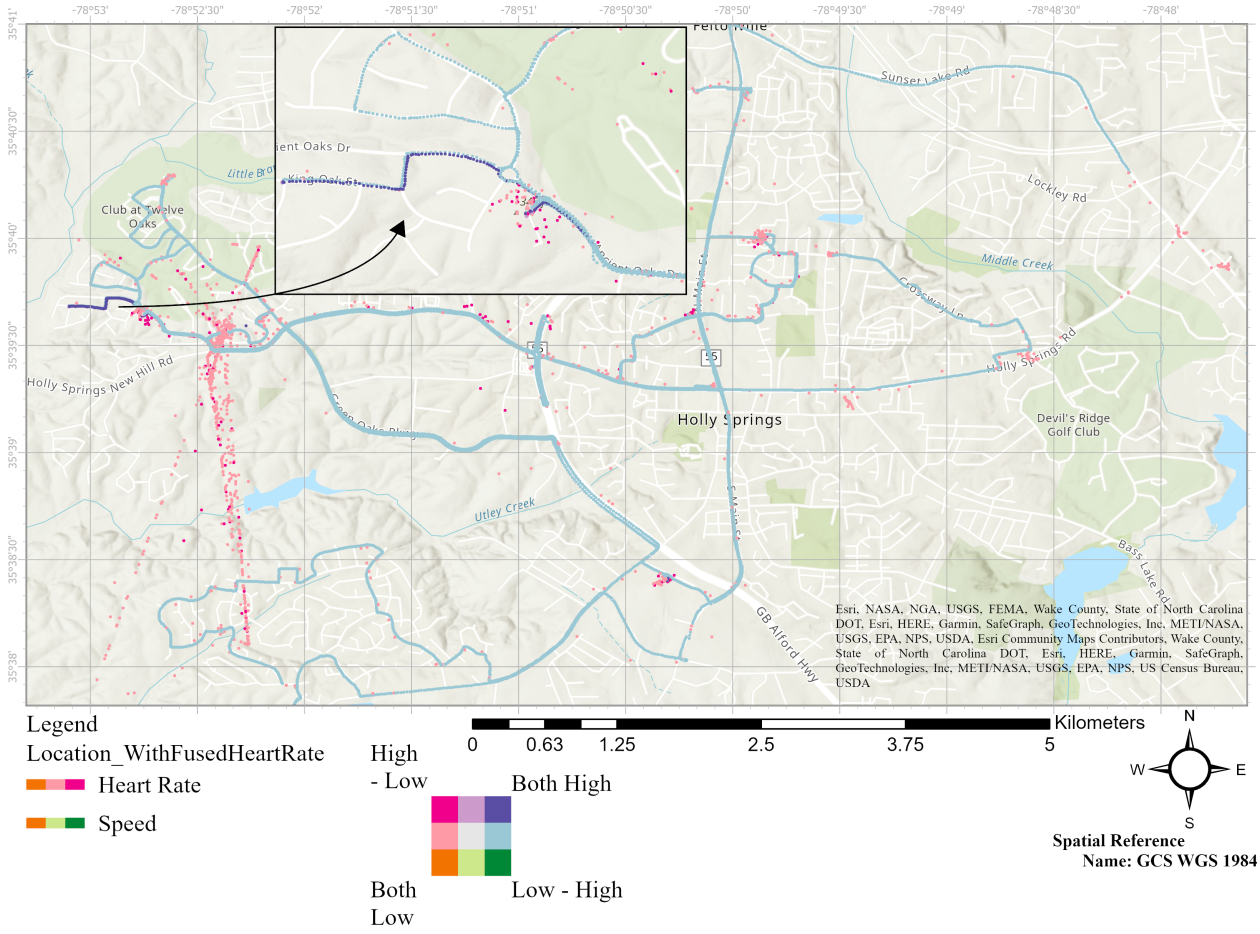


Figure 6.27. A map showing geo-locations with a responding heart rate.

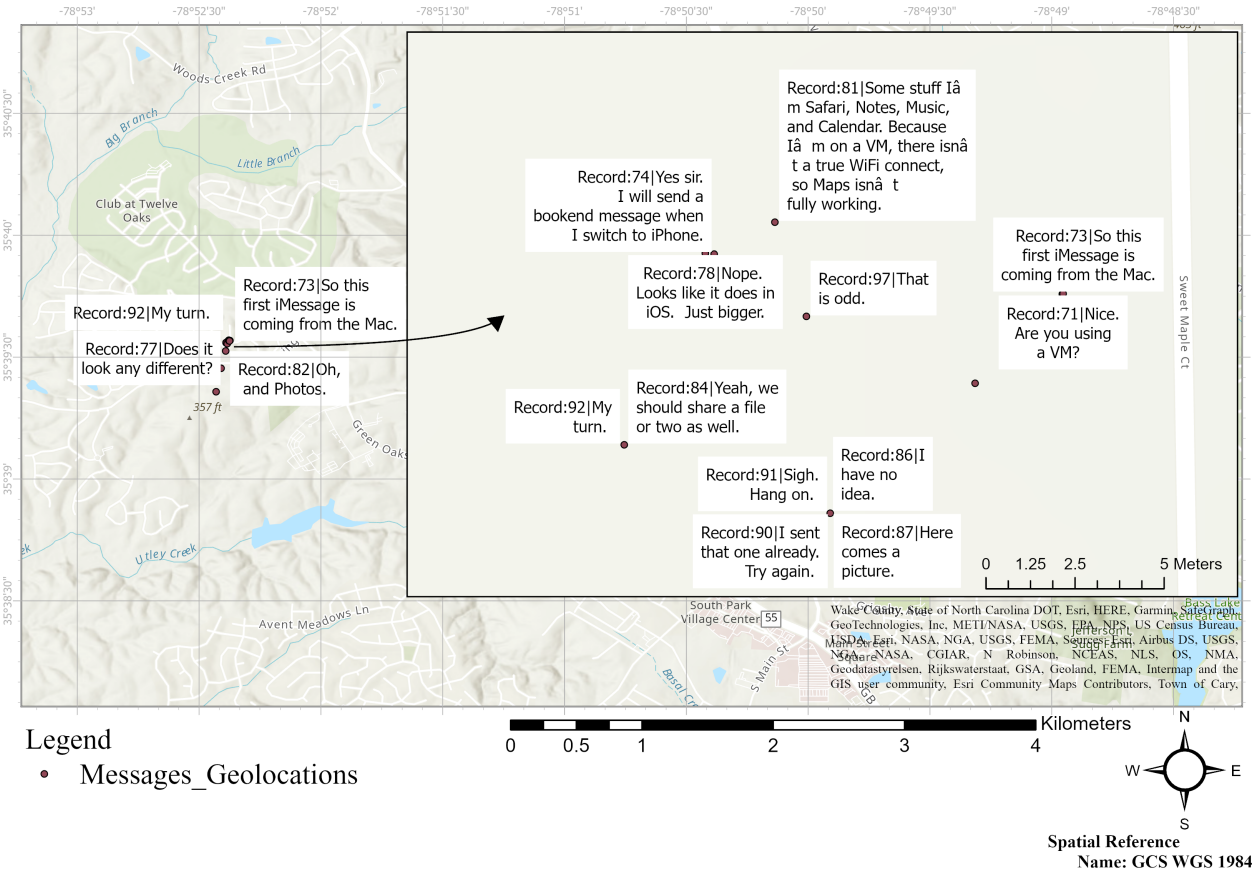


Figure 6.28. A map showing some locations of sent and received messages.

7. DISCUSSION AND CONCLUSIONS

In this chapter, the main focus is to discuss the outcomes of the three hypotheses and how the methodology and analyses have contributed to answering the primary research question. Furthermore, it discusses the implications of these findings for digital forensic practice and research, as the findings of this study demonstrate the potential value of geodata in digital forensic investigations when using the created transdisciplinary framework.

7.1 Technical Investigative Challenges

Apple devices like iPhones utilize proprietary operating systems (iOS) and have unique data structures, file formats, and encryption mechanisms. Therefore, digital forensic investigators can use Apple developer documentation to gain insights into the inner workings of these devices and effectively interpret the data they encounter during analysis. Moreover, this documentation may help with data interpretation and understanding the functionality of specific features and applications. The complexity of iOS and the constant evolution of Apple's software ecosystem necessitate ongoing reference to the Apple developer documentation to stay up-to-date with the latest changes and enhancements. By consulting the Apple developer documentation, investigators can better understand the purpose, format, and organization of different data artifacts stored on Apple devices. This knowledge aids in accurately interpreting and analyzing digital evidence, enabling investigators to uncover relevant information, establish timelines, identify user activities, and reconstruct events.

Many file types and extensions make examination and analysis challenging. Due to the diversity of data and storage types used by OSs and apps, digital forensic tools and practitioners may struggle to identify and comprehend evidence quickly. Using different file formats and extensions as technology advances hinders digital investigations. Furthermore, big data and various file formats and extensions make it difficult to manage and analyze evidence across devices and apps, so investigators need a broad understanding of digital technologies. On the other hand, encryption and other security measures might make some data or files unavailable without special software, complicating digital investigations and adding another layer of complexity to investigations.

Moreover, different time zones and timestamp formats can cause difficulties in digital investigations during examinations. When digital evidence is collected from devices located in different parts of the world, time zone differences can make it challenging to accurately establish a timeline of events. Additionally, other timestamp formats used by various OS versions or apps can further complicate the analysis of digital evidence. For example, iOS devices and apps may use Apple/Mac Absolute Time (measured in seconds or nanoseconds relative to the absolute reference date of Jan 1, 2001, 00:00:00 UTC), Unix Timestamps, WebKit/Chrome time, GPS time, etc.

Therefore, keeping up with digital forensic advances is important, as obtaining the correct tools to detect and analyze digital information during an investigation is challenging. It also stresses the need for digital forensics experts to work together to tackle these challenges and advance the discipline by combining efforts and knowledge, which was what this study aimed to do concerning geodata. Furthermore, to overcome these challenges, digital investigators must be skilled in filtering geodata linked to the user and converting between different timestamp formats and time zones, where specialized software tools can help. Furthermore, the presence and absence of data play a crucial role in any investigation or analysis, as they can provide valuable information and meaning to the overall findings. Therefore, it is essential to consolidate as many sources of evidence as possible and document any conversions made during the investigation to ensure the accuracy and reliability of the findings.

The Apple Developer Documentation serves as a valuable resource for understanding the functionality and behavior of Apple's native applications, frameworks, and services. This knowledge can help investigators make informed decisions when analyzing application-specific data, such as chat logs, call history, social media interactions, and location information. Additionally, digital forensic tools often face challenges in finding intersections or correlations between geospatial data from different devices, as shown in this study. This issue arises for several reasons, including varying data formats, incompatible data schemas, lack of functionality, and limited interoperability between different toolsets.

In addition, visualizing different geodata in digital forensic tools often fails to demonstrate responsiveness and interactivity. Analyzing and visualizing large volumes of geospatial data can be computationally demanding, and the tools tested in this study struggled to provide

smooth or real-time visualization experiences. This limitation can hinder the efficiency and effectiveness of forensic investigations, as investigators rely on responsive and interactive visualizations to gain insights from geospatial data.

Geodata curation and filtering are critical, and exciting artifacts were found called `WiFiLocation` within the following database `\System\Library\Frameworks\CoreLocation.framework\Support\factory.db`. This table contains geolocated access points; however, after a detailed investigation by plotting their locations, it turned out to be iOS stock and had no connection to the device user. Most of these WiFi access points are located in airports around the world; therefore, more research is needed to understand what they are used for. Figure 7.1 shows 71,078 Wi-Fi access points with their MAC addresses in `factory.db`. Moreover, the `\System\Library\PrivateFrameworks\CoreAnalytics.framework\marketMap.sqlite` database contains locations that are in stock with the system. Therefore, it is essential to differentiate between different types of artifacts generated during examination and analysis. The investigation came across multiple kinds, such as system default geodata (no connection to the user), OS-cashed geodata (stores user geodata), user-created geodata (e.g., geotagged photos), and other geodata linked to other people or services.

In addition, in the context of digital forensics investigations involving geodata, one recurring challenge is the creation of a consistent repository of continuous geodata for each case. Existing tools and methods often lack the necessary functionality to facilitate such repositories' easy and seamless creation. As a result, investigators face the cumbersome task of managing multiple schemas and appending tables with different columns, which can be time consuming and error prone. In this study, multiple times, creating a consistent repository of continuous geodata for investigated cases was hard. Investigators may need to extract geodata information from various sources, such as GPS coordinates, timestamps, and other location-based metadata, and consolidate them into a unified and coherent repository. However, this task becomes challenging without a streamlined solution and requires manual effort to ensure data consistency and integrity. It also depends on the investigators' experience and commitment to such cases.

Furthermore, the diversity of data formats and structures encountered in different cases exacerbates the difficulty of creating a consistent geodata repository. Each case may involve

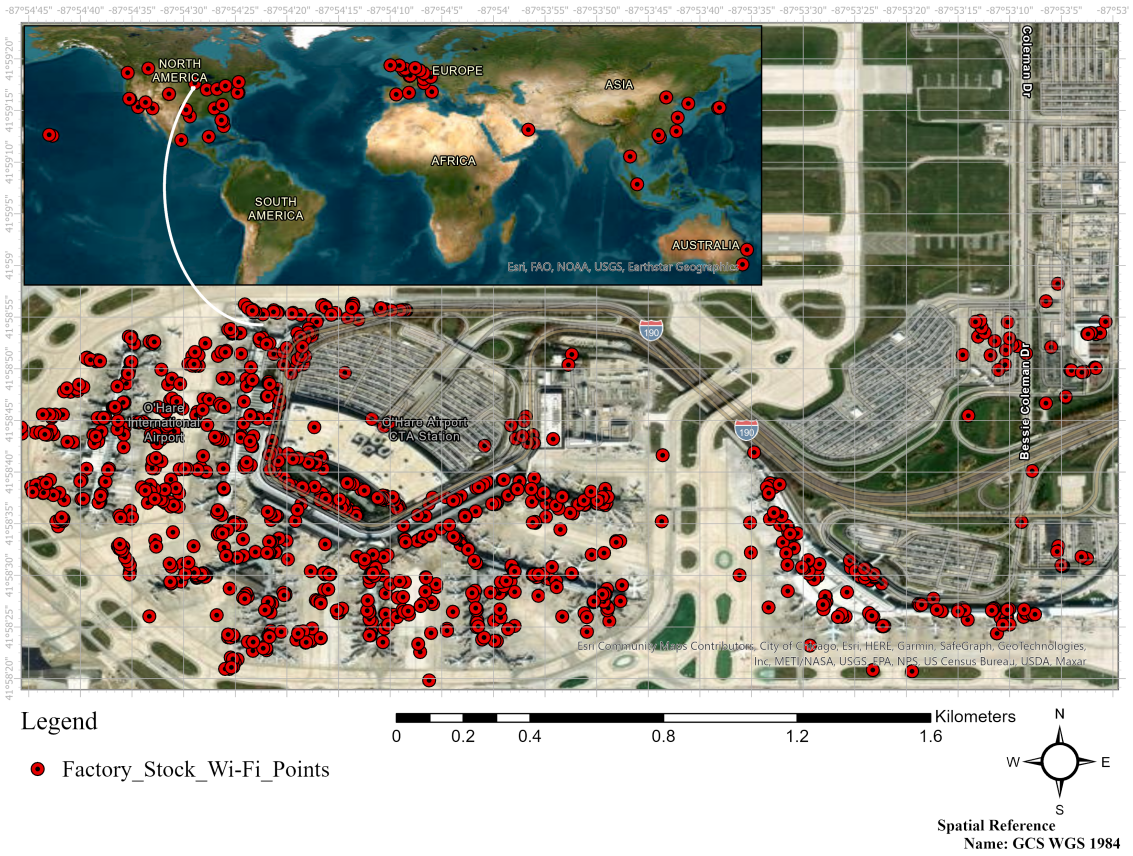


Figure 7.1. 71,078 geolocated Wi-Fi points recovered from Case 1 image 5 in a database named Factory.DB

different devices, platforms, or applications, each with its own data schema and representation of geodata information. The need to harmonize these disparate formats and reconcile their differences poses additional obstacles to investigators. Therefore, by streamlining this process, investigators can focus more on data analysis and interpretation rather than spending significant time and effort on data preparation and consolidation.

The expiration duration of geodata is a crucial factor that presents a significant challenge, especially when there is a considerable time gap between the incident and device acquisition. Geodata, such as GPS coordinates, timestamps, etc., are often subject to various factors that can lead to data loss or degradation over time, making them time-sensitive. Therefore, over time, geodata linked to past incidents may become inaccessible for forensic analysis as they may not be available anymore or may have been overwritten by newer data. Addi-

tionally, technological advancements and software updates may introduce changes in data storage formats or protocols, leading to compatibility issues and rendering older geospatial data incompatible with newer tools or systems. On the other hand, the challenge of geodata expiration is further exacerbated by legal and regulatory considerations. Data retention policies, privacy regulations, or law enforcement procedures may impose limitations on geospatial data storage and retention, potentially resulting in the deletion or loss of relevant information before it can be acquired for forensic analysis. To mitigate some challenges of geodata expiration, timely and proactive acquisition of devices is imperative. Investigators must strive to obtain digital forensic images of relevant evidence as soon as possible after an incident occurs to minimize the risk of data loss or degradation.

In addition, as shown in the literature, offenders have been using anti-forensic methods to impede the forensic process and manipulate evidence, which can significantly reduce precision. Current research efforts focus on developing a collection of clear rules and principles that investigators should follow. However, few frameworks have explicitly stated that investigators should be aware of the potential for falsified data, and there has also been little research. Therefore, things may be done, and there is a need to check for compromised, falsified, fabricated, or manipulated geodata using geo-contextualization detection and analysis approaches. In addition, geo-contextualization can help consolidate the evidence from multiple sources.

The author in [240] offered a review of certain types of anti-forensic technology that must be considered when dealing with digital evidence. The author also mentioned that simple technologies might evade forensic procedures (e.g., traditional data hiding, tampering, etc.). According to [239] and [244], anti-forensic techniques can pose a significant risk by ensuring that no evidence is collected, extending the duration of the investigation, which can result in wasted time, jeopardizing the entire investigation if fraudulent or misleading evidence is collected; and preventing the detection of critical artifacts or digital evidence.

In addition, [241] offered a taxonomy of anti-forensic techniques, including data concealment (e.g., encryption and stenography), artifact erasing, and trail obfuscation. Furthermore, the authors in [243] discussed that the academic study on anti-forensics has not received the same level of attention as other issues related to forensics. Furthermore, based

on their results during their study, the authors discovered that only 2 of the 500 articles in digital forensic research focused on anti-forensics [243]. They reasoned that this might be due to the fact that most anti-forensic advances occur outside of scholarly journals [243]. Furthermore, as mentioned in [32] and [11], investigators have difficulty handling investigations that involve large volumes of data in some scenarios and when more than one case uses enormous amounts of data at the same time. Moreover, what is worse than a large amount of data is the large number of these that have false information and encryption to deal with as an investigator. Although technology and digital forensic tools are making daily advances to deal with procedures, detect and counter anti-forensic tactics, and handle encryption, investigators face monumental tasks in the wake of these challenges and difficulties.

Moreover, investigators struggle with investigations that involve massive data volumes in certain circumstances, and if more than one case involves massive data at the same time involving massive data; furthermore, it is difficult for investigators to juggle large amounts of data at the same time efficiently [11], [32]. As a consequence of advancements in technology, investigators have been left without a road map that helps them deal with procedures, but also helps them detect anti-forensic tactics, deal with encryption, and provide helpful visualization. Furthermore, the enormous diversity of hardware and software available on digital mobile devices may pose significant challenges to digital forensic investigations. Again, there is always the possibility that, with new updates to operating systems or applications, the file structure in which essential and valuable data can be kept will change [225]. As a result, this affects processes, tools, and investigators, and they face this significant obstacle and have to adapt to it.

Many frameworks have been developed from past studies and the literature as a rigorous strategy for identifying data tampering and location counterfeiting. Most of them were related to research on the quality of geographic data. The authors of [320] argue that the quality of user-generated geospatial material can be assessed using crowd-sourcing, social networks, and geographic techniques. Furthermore, according to [321], most of the criteria used to determine whether geographic data (e.g., GPS locations) are correct or incorrect are based on understanding how the geographical world is formed. Therefore, many methods are geographical approaches, which is very important. However, according to [26], although

the evaluation of spatial data quality using geographic knowledge is already in place, a comprehensive theoretical framework that effectively detects spoofing events is needed.

On the other hand, researchers [322] discussed prevention measures against GPS spoofing, such as traveling viability checks, mock location app detection, malicious app detection, and jailbreak and root detection. Although the authors discussed these from the perspective of spoofing attacks, they can be relatively easily applied in digital investigations. The examiner can ensure that all recovered geodata are related to time and space. For example, someone cannot suddenly travel to another location in no time; therefore, checking for inconsistencies is crucial. Furthermore, scanning for malicious programs is a good practice in digital forensics to detect concerns and malicious conduct. Furthermore, the authors in [322] mentioned that users can easily change their GPS location after accessing the operating system by jailbreaking iOS or rooting Android. This is a crucial topic in digital forensics because, in some instances, there is a need to do so from the investigator's side.

7.2 Our Digital Footprints

Although this work is primarily concerned with investigative strategies and forensic methodology to understand the precision of geodata recovered directly from iOS-related artifacts, other artifacts on the device from different applications, as discussed in many other works, also play a significant role in consolidating user location. Furthermore, the author believes that users have major security concerns if the device gets hacked without knowing. A substantial amount of data can be breached and cause a considerable user data leak. People's physical whereabouts are considered highly sensitive personal information, where anything wrong can lead to significant issues that have implications in the physical world [323]. Furthermore, the available information that was found for the users of the investigated phones in the study using OSINT is sensitive, and the author argues that every user has to check their digital/cyber footprint to ensure that there is nothing available that can cause them harm.

Moreover, the devices (i.e., iPhones) we carry around collect a vast amount of data, as demonstrated in the examination and findings; these smartphones and the data they hold

can be used for reconnaissance purposes by attackers and malicious users without the need for any suspicious tools or hardware, which may pose risks to organizations and individuals.

7.3 Educational and Legal Awareness

According to [217], technology is advancing at a rate that routinely exceeds the rate at which the law changes to adapt to such advancements. Researchers in [324] believe that digital experts, legislators, judges, and lawyers lack common ground on the technical abilities that are essential to solving the challenges related to the intersection of forensic technology and law. Therefore, as the authors discussed in [220], it is necessary to shed light on how a general lack of knowledge of digital evidence can result in an innocent person being unfairly convicted of a criminal offense. Furthermore, there is a need for new practices in the law school curriculum to investigate and increase awareness of this injustice in the legal community when dealing with digital evidence. As stated by many previous researchers, the author of this study believes that there is a considerable need for combined efforts to understand digital evidence, especially geodata evidence.

In addition, according to [218], when understanding and applying the law to new technologies, the law is more reactive than proactive. Therefore, the author agrees with the researchers in [217] that the legal system's capacity to deal with new ideas that do not blend seamlessly is limited by its reactive nature. Therefore, efforts must be made to create proactive measures in the digital forensics community. On the other hand, according to [219], [325], many legal professionals, including judges and attorneys, lack the technical competence required to defend the present law or design new laws to respond to technological advancement adequately. As a result of a lack of technical expertise, there is always a risk of misapplication of regulations and technological justification/evidence [219], [220]. For example, recently, in *Kyle Rittenhouse vs. the State case*, Kyle's attorney claimed that the "pinch-to-zoom" function of the Apple iPad uses artificial intelligence to enhance what they see, which can involve fabrication in the eyes of the court; however, this may not be the case [295].

There must be some empirical proof when evaluating whether someone is guilty or innocent based on digital evidence. To ensure that digital forensic evidence is legitimate and competent, the Frye and Daubert standards provide some protection against the introduction of misleading scientific evidence or expert opinion [219]. The Daubert standards are now the standard for scientific evidence. According to [28], Daubert standards are acknowledged as "Good Science" to describe that evidence meets a set of standards for digital evidence to be categorized as scientific evidence. The author's attention in this research was drawn to the fact that the vast majority of geodata face difficulties if they are not proven using scientific methodology since many digital forensics investigation frameworks and tools provide limited functionality. Therefore, the author agrees with the argument made by [219] that it is a great responsibility for lawyers and judges to dispute inexact science at different stages of the case and to determine whether such evidence should be allowed based on their training, experience, and decision-making ability.

Therefore, the author emphasizes the importance of understanding the laws and using the correct procedures. The integrity of the data was preserved as much as the author could; however, for the use of external software, the examiner or the investigator needs to be aware of what they are doing to prove the science behind it. Furthermore, because the field of digital forensics is constantly expanding, the author agrees with [219] that there is a need for a thorough and strategic evaluation of laws and standards, together with a plan to improve them and keep them up-to-date.

On the other hand, anti-forensics tactics may be employed to change or later evidence, which can hurt accuracy and infuse false information. Although this research did not focus on falsified or inaccurate geodata detection, complete validation and verification of geodata must take into account anti-forensic methods, including obfuscation and misdirection, as highlighted by [260] as an excellent and prudent measurement that digital investigators should be concerned about. Therefore, the author believes that analysts and digital forensic investigators can profit from using geodata visualization tools; however, there are drawbacks if they ignore inaccurate information, which can lead to inaccurate representation of data and may lead to misinterpretation of the data.

7.3.1 Geodata Integrity and Court Data Collection

. Cybersecurity systems and practices are often criticized for not meeting the confidentiality, integrity, availability, and authenticity (CIAA) information security goals. To investigate security breaches and digital crimes, the CIAA often uses digital forensic processes and technology to investigate CIAA violations and incidents [49]. The field of digital forensics must evolve to meet the increasing complexity and amount of data. With the rise of mobile devices, social media, and cloud storage, digital forensics professionals now need to be able to acquire and assess a wide variety of types and locations of data in addition to traditional computer data. Therefore, digital forensic investigators must track the integrity of the data and ensure that they follow the correct data collection and visualization. This requires reliable records of data collection and analysis and chain-of-custody documentation.

Furthermore, to be admissible, digital evidence must first and foremost comply with the legal rules and standards applicable in criminal proceedings. It must also be complete and genuine, which means that it must be possible to positively link the evidence to the event in question being precisely as it appeared or claimed [131]. Additionally, the data must be reliable, which implies that they must have been gathered according to official procedures and can be reproduced. Furthermore, when performing forensic investigations, the connection of preserved digital evidence with an individual must be considered by showing the full methodology and legality.

7.4 General Benefits of Transdisciplinary Approaches For Cuber Forensics Investigations

Cyber forensics investigations, with the advancement of technologies, deal with different types of complex evidence. Thus, there are many advantages to integrating concepts to solve a complex problem or a case. Many cases need to be considered not only from different perspectives but also from a transdisciplinary approach, where transdisciplinary approaches involve integrating knowledge, skills, and methods from different disciplines to solve complex problems.

Some of the benefits of the transdisciplinary approach created in this research:

- Increased efficiency and productivity in dealing with data by enabling automated data analysis, streamlining data processing, and improving the data visualization processing workflow across multidimensional models.
- Enhanced measurement of the accuracy of recovered evidence by cross-validation of evidence using an integration of multiple techniques.
- Compliance and adherence to forensic standards span across disciplines and allow the development of operating procedures. It can also demonstrate the necessary shared knowledge and experience.
- Providing better decision support using a wide range of knowledge, skills, and methods from different disciplines, a more comprehensive and effective problem-solving process can lead to improved decision-making supported and measured by a consolidated perspective.
- Provide more profound insights into what the data hide and enable the detection of hidden phenomena. Moreover, geodata visualization was crucial in this research, and using visualizations, such as graphs, maps, and other visuals, to simplify data needs attention. This may help digital forensics experts spot patterns and data trends.
- Improved innovation and creativity for tools and techniques by combining approaches allows faster response time, lower cost, and time savings.
- Improved communication and collaboration among all stakeholders in a case when a piece of evidence can be justified using tested and consolidated techniques and technologies. For example, a digital spatial-temporal map that demonstrates the movement and actions of an individual or a group of different actors in a case map can enable a comprehensive and rich understanding of the extended extent of the case.

The value and practicality of a case are significantly impacted by the relevance of evidence, regardless of its admissibility. Legal professionals are crucial in providing direction on which evidence to gather during investigations, leading to better management of time and expenses incurred during the process.

In addition, it is imperative that digital forensic tools and methods also incorporate geospatial analysis. Using geospatial information technology in scenarios where data can be used in geographical dominions is essential. In this research, the author will use one of the most widely used technologies in GIS, which consists of many tools that include a wide range of data layers based on geographic location-based data structures. It is a handy tool when the data are of geographic dimension. This helped prove that these geodata curation methodologies can help investigators uncover hidden knowledge for both digital forensics and digital investigations.

7.5 Limitations and Recommendations

The research has presented an overview of the gaps and challenges related to geodata that affect the geo-contextualization efforts on data collected from mobile devices in digital forensic investigations. Moreover, the research discussed the opportunities that can enable geo-contextualization to help digital forensics investigations and digital forensics intelligence. This research revealed increasing opportunities; therefore, based on the study and discussion, the following is a list of future directions.

- This research only focused on the technical part, and there is a need to rethink the entire digital forensic process model considering all the concerns raised in this research. It is critical to reconsider each stage of the digital forensic process paradigm to enhance it with an infusion of related and supportive geodata analysis approaches.

- This research highlighted some limitations and challenges for digital forensic tools. However, there is a need for a comprehensive review to analyze and uncover the weaknesses in the current tools used by many law enforcement agencies regarding geodata.

- Due to the fact that geodata analysis and classification are still primarily performed manually, there is an urgent need for research into automated solutions for these tasks.

- There is a need to understand what to ask for in search warrants. This can help address security and privacy concerns about how not to compromise data privacy. Following a

clear and systematic approach is crucial for geo-reverse warrants to ensure compliance with legal requirements and obtain accurate and reliable information.

- This research did not investigate data stored in the cloud (e.g., iCloud services). Therefore, there is a need for further examination and analysis as an increasing number of users use cloud storage for their daily use and backups. This might involve studying the cloud infrastructure and analyzing how and what geodata are stored there. Moreover, during a digital forensic investigation, one may need to recreate events that occurred using smart devices that are linked with data that are housed on cloud-based platforms, where user data and actions could also be stored in the cloud v distributed across several services, leading to time-consuming operations and complicating the investigation process.

- The argument for good documentation and presentation for many geodata in digital forensic tools is needed.

- When reporting and displaying geodata, practitioners dealing with the case must have some analytical and categorical skills to convey precise information. In cases where geodata are present, there is a need for more detailed guidelines that can guide or give the investigation extra help, understanding and presetting the dimension of space as a reference to time.

- It does not matter how well current digital forensic technologies and tools are equipped to handle large amounts of data; they need to be able to compress them into easily digestible reports and insights.

- Many emerging technologies are considered promising, such as the use of GIS to help investigators with geodata analysis; however, substantial research is needed to study and explain current methods for the digital forensics community, along with technical opportunities and challenges.

- The value and practicality of a case are powerfully influenced by the relevance of the evidence collected during an investigation, irrespective of its admissibility in a court

of law. Legal professionals are vital in guiding investigators on the types of legally permissible evidence and are strategically valuable for building a solid case.

- The cost has always been a barrier to cyber forensics when it comes to tools; however, there is a strong case that the industry is transforming and the rise of open-source cyber forensics is evidence of that.
- Studies are needed to determine whether spatial intelligence and spatial thinking correlate with better geographic abilities in digital forensics.

7.5.1 Digital Tools Performance

This study reveals that no one tool can comprehensively analyze mobile devices forensically. Although this research does not evaluate digital forensics, commercial technologies improve with each release. These new versions incorporate more automation and automated artifact recovery, making the process more efficient. However, digital forensic tools still lack the analytical tools needed for geodata analysis. This examination highlights that these tools struggle with plotting multiple points on a map and do not offer spatial query functions. With geodata becoming increasingly crucial in digital forensic investigations, digital forensic tools must adapt spatial indexing and frameworks to handle and cope with the complexities of geodata analysis effectively. Furthermore, digital forensic examiners and practitioners must possess the knowledge and skills to work with and analyze geodata effectively to ensure that there are no blind spots in investigations.

In addition, digital forensic tools should prioritize the development of robust and responsive visualization capabilities. Advanced visualization techniques, such as interactive maps, spatial-temporal analysis, and data filtering, improve the exploration and understanding of geographic data. This would help investigators find trends, correlations, and anomalies for more accurate and insightful forensic analysis.

7.5.2 Potential Advancements

Machine learning and artificial intelligence have made their way to digital forensic tools recently and are proving to help investigators. In addition, digital forensics systems and tools that have the power of artificial intelligence are constantly improving and speeding up the analysis [326]. However, there are many challenges due to the various and complex types of data in digital forensics, and it can be challenging to collect and analyze using existing AI systems [327]. Therefore, there is a need to significantly modify many modern AI mechanisms to suit the needs of digital investigators. According to [326], current IA-based technology may only be used to assist in investigations, which a human must still supervise. The authors also mentioned that IA-enabled technologies are still in development and may not always provide accurate, complete, or robust information necessary for forensic investigations. Therefore, the correctness of the forensic conclusion depends on the talents of the human investigator performing the investigation [326].

Furthermore, according to [25], several fields are adopting strategies for acquiring, processing, editing, analyzing, and presenting geodata. However, digital forensics procedures and tools have been slow to adopt such a thing, especially regarding geocoding, geoprocessing, and spatial analysis techniques. Enormous geodata in investigations may be challenging for investigators under certain circumstances. If several cases have a large amount of geodata, it will be difficult for investigators to efficiently manage them, as they are unlike any other type of data. They need to be dealt with carefully.

In addition, many researchers have expressed concern about the eventual quality of cartographic output, which includes concepts such as accuracy and completeness [305]. Furthermore, the authors in [305] mentioned that geospatial data processing platforms have made it easy to integrate and convert a wide variety of data sources, resulting in results that vary from "raw" to "final" in quality. Moreover, [306] discussed how the variety of data types can raise issues in geodata curation and geodata processing in GIS due to the need for considerable effort for organizations to understand the different files and how to make them meaningful by grouping them in a geo-driven way.

Therefore, it is imperative that digital forensic tools and methods also incorporate geospatial analyses. It is essential to use geospatial information technology in scenarios where data have the potential to be used in geographical dominions. This research used one of the most widely used technologies in GIS, which consists of many tools that include a wide range of data layers based on geographic location-based data structures, and it is a precious tool when the data have a geographic dimension. This has helped to apply and prove the point that these geodata curation methodologies can help uncover hidden knowledge for investigators for cyber forensic intelligence, cyber forensics investigations, and digital investigation in general.

GIS combines a variety of data layers, many of which are geospatial in nature. Geospatial data is a substantial component of the geographic aspect of the data. GIS data comprise a base map that may be supplemented with photographs, locations that may be classified in various ways, and other data that are linked to a database. Therefore, this research examined geodata and GIS technologies, both of which have a cyber forensic application. In comparison, digital forensics has a wealth of geographical information stored on seized devices that may provide critical information while examining crime scenes or the devices used to conduct crimes. Using spatial analysis may improve our ability to analyze and anticipate our knowledge, grasp human activity patterns and their geographical representation, and use that information to make more informed decisions.

Geodata Triage

Digital forensics is constantly developing its methods and technologies to manage the variety and volume of data. Data production and maintenance methods and technologies can help digital forensics aid law enforcement and other organizations. Due to smartphones, computers, tablets, and cloud storage, the digital forensics community must increasingly evaluate more data. Therefore, geodata triage is crucial. Data triage can identify and prioritize investigative data, allowing digital forensics experts to focus on the most valuable data.

In addition, geodata triage can help with PoL and can be a valuable investigative tool, particularly when combined with geospatial metadata. By analyzing large amounts of observed data, this technique allows investigators to identify the habits and behaviors of individuals of interest and uncover hidden patterns that may reveal unusual activity. Moreover, investigators can better understand people's behavior by correlating their motions and behaviors using mapping and interactive visual analytics tools, which integrate activity-based intelligence and can be used in many use cases to recognize unexpected activities by creating a "typical" behavior baseline.

7.5.3 NICE Framework Suggestions

Digital forensic analysis aims to retrieve as much data as possible from any source. However, when dealing with large amounts of heterogeneous data, such as those found on mobile devices, these strategies often fail, especially in analysis and in providing valuable insights. Therefore, the skills and practicality of digital forensic examiners play a significant role in minimizing these issues. Although digital forensic tools are trying to add functionality to deal with such geodata types, they lack comprehensive spatial analysis and visualization techniques for these critical artifacts that can add geo-probative value while helping consolidate the evidence recovered.

The job positions are described in the NICE Cybersecurity Workforce Framework by the tasks, knowledge, and abilities necessary for numerous cybersecurity roles and are published by NIST [92] under the special publication number 800-181. A detailed explanation of how tasks, knowledge, and abilities can be used to establish positions in the cybersecurity workforce is provided in Revision 1 [93]. However, geospatial analysis, knowledge, abilities, skills, and tasks are not mentioned in descriptions of investigative roles such as cybercrime investigator, law enforcement/counterintelligence forensics analyst, and cyber defense forensics analyst [328].

This study emphasizes the need for digital forensic investigators to comprehend the needed skills to deal with geodata. Geographic skills and spatial thinking help investigators examine geodata. In many forensic investigations, geodata helps reveal digital evidence's

geographical and temporal characteristics. It underlines the need for digital forensic investigators to combine geospatial knowledge and methodologies into their skill sets to improve their skills and ensure thorough geospatial data analysis. In addition, geospatial capabilities will improve digital forensic investigations and enhance the capabilities to help investigators examine and understand GPS coordinates, location-based timestamps, and artifacts. Integrating digital and physical information helps recreate events and identify key investigation players.

These capabilities allow investigators to use GIS and geographical data visualization to improve the analysis and presentation of digital evidence. These tools allow investigators to visualize geographic data and find patterns, trends, and connections that standard analytical methods may miss. Geospatial approaches can help digital forensic investigators obtain significant insights and improve their results. This integration considers geographical data and enhances its investigative potential. This study extrapolates that digital forensic investigators need geospatial expertise.

In addition, investigators must employ various techniques and sources when conducting digital forensic investigations. For example, this study encountered a situation where files containing flight logs were not readily decryptable using conventional digital forensic tools. Although some of the tools used in this research may not have been specifically developed for forensic purposes, they proved invaluable in decrypting and examining data (e.g., encrypted flight logs), providing valuable insights for the investigation. This case serves as a reminder that digital forensic investigations often require thinking outside the box and considering unconventional approaches. Moreover, it emphasizes investigators' need to keep current on new tools and approaches, which may provide unexpected answers to digital evidence challenges. Therefore, it is essential to explore alternative solutions that could successfully decrypt and analyze these files, even though they were not initially designed for forensic investigations.

Spatial thinking and awareness are crucial for investigators and equally important when dealing with geodata cases. Understanding the spatial dimension of digital evidence and its implications can provide valuable insights and aid in the investigation process. Incorporating spatial thinking and awareness into the investigative process allows investigators to lever-

age the power of geospatial data and extract meaningful insights. It helps to understand the context, identify relevant patterns, reconstruct events, conduct geospatial analysis, and facilitate effective geo-contextualized understanding. By developing spatial thinking skills and utilizing geospatial tools and techniques, investigators can enhance their investigative capabilities and improve the overall results of their cases. This highlights the importance of adaptability and resourcefulness in digital forensics and that investigators must be willing to explore unconventional methods and tools to extract and analyze data effectively.

7.6 Conclusions

Technological breakthroughs profoundly impact our lives and the environment. Primary devices (e.g., a smartphone) are flooded with data, and geodata are among these data that are critical in any digital investigation. Moreover, digital devices and IoT devices will generate and feed our primary devices with even more data, since these devices are becoming increasingly commonplace in our daily lives. Furthermore, many devices and applications have seen an increase in geolocation use over the last decade; however, there are still significant gaps in the digital forensics community influenced by the lack of understanding of how to curate geodata properly.

This work has explored possibilities in dealing with geodata recovered from digital evidence by improving the way of maintaining geodata and getting the best value from them by creating a transdisciplinary approach tested on iPhone case studies. The findings have important implications for the practice and research of digital forensics, highlighting the need for the continued development of analytical tools and the importance of training practitioners in geodata analysis. Although the implementation, acceptability, and significance of each geodata and procedural legitimacy differ depending on the amount of data stored and collected for each case, investigators need to understand how they are stored on digital devices. In addition, it is equally important to know how to use them best in order to conduct the investigation. Many geospatial analytical techniques can help provide geo-contextual reasoning that improves digital forensics investigation and evidence representation for intelligence and forensics investigations. Finally, although the acceptability and importance of geodata

vary according to the situation and environment of each incident, there are many ways to preserve spatial and temporal information from smart devices, which add geo-probative value to other types of data recovered.

In conclusion, this research has explored the significance of a transdisciplinary geo-contextualization approach resulting from a fusion of different domains, including digital forensics, GIS, and intelligence, to help provide geo-added value to data recovered from cases and enhanced geodata curation. It also emphasizes the importance of incorporating other domains into the framework to enhance the outcomes and to break down barriers to effectively conduct cyber forensics analysis. Moreover, the research highlighted the need for integrating geospatial knowledge and techniques into the skill set of investigators. By recognizing the value of geodata and incorporating geospatial skills, investigators can uncover spatial and temporal patterns, identify key locations, and establish meaningful connections between digital evidence and physical locations. Furthermore, incorporating machine learning and artificial intelligence techniques into geospatial forensic analysis holds promising potential.

Through the utilization of advanced technologies, investigators can greatly improve their abilities in geospatial forensic investigations. The implementation of data analysis, pattern recognition, and predictive modeling techniques allows more precise and efficient examination of geospatial information. Future efforts should concentrate on further integrating geospatial knowledge and practices into cyber forensic investigations. This research area has immense potential to enhance the overall investigative process, increase the reliability of findings, and enable investigators to fully leverage geospatial data for comprehensive analysis and interpretation. Continued advancements in this field will empower investigators to extract valuable information and make informed decisions based on geospatial evidence, ultimately contributing to more effective and impactful forensic investigations.

REFERENCES

[1] N. Shirley M. Radack, *Guide to protecting personally identifiable information*, https://www.nist.gov/publications/guide-protecting-personally-identifiable-information, (Accessed on 01/05/2023).

[2] F. E. Salamh, M. M. Mirza, S. Hutchinson, Y. H. Yoon, and U. Karabiyik, "Whats on the horizon? an in-depth forensic analysis of android and ios applications," *IEEE Access*, vol. 9, pp. 99 421–99 454, 2021.

[3] S. Petroc Taylor, *Mobile network subscriptions worldwide 2028*, https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, (Accessed on 04/05/2023).

[4] S. ODea, "Number of smartphone users in the united states from 2018 to 2025 (in millions)," *Statistica. com, Number of smartphone users in the United States from 2018 to 2025/(accessed 30 November 2021)*, 2021.

[5] S. Federica Laricchia. "Number of smartphone users in the united states from 2009 to 2040." (Accessed on 02/28/2023). (), [Online]. Available: https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us//.

[6] Statista, *Number of internet of things (iot) connected devices worldwide in 2019 and 2030*, Accessed: 2022-12-22, 2022. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide-2019-2030/.

[7] F. L. Statista, *Smartphone unit shipments by vendor worldwide 2007-2022*, https://www.statista.com/statistics/271539/worldwide-shipments-of-leading-smartphone-vendors-since-2007/, (Accessed on 05/05/2023).

[8] S. Lim, *Global smartwatch shipments rise 1.5% in 2020:counterpoint research*, https://www.counterpointresearch.com/global-smartwatch-shipments-rise-1-5-2020-price-trends-going-premium/, (Accessed on 11/15/2021).

[9] I. Intelligence, *Drone industry analysis 2021: Market trends & growth forecasts*, https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts, (Accessed on 07/12/2021), Feb. 2021.

[10] S. E. Goodison, R. C. Davis, and B. A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, eng. RAND Corporation, 2015, ISBN: 0833091417.

[11] M. K. Rogers, "Psychological profiling as an investigative tool for digital forensics," in *Digital Forensics*, Elsevier, 2016, pp. 45–58.

[12] khaleda rahman, *Technology could place kohberger at scene of idaho murders: Ex-fbi agent*, https://www.newsweek.com/technology-could-place-bryan-kohberger-scene-idaho-murders-1780642, (Accessed on 02/28/2023).

[13] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digital Investigation*, vol. 11, no. 4, pp. 273–294, 2014.

[14] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, S64–S73, 2010, The Proceedings of the Tenth Annual DFRWS Conference, ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2010.05.009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287610000368.

[15] B. Technology, *Autopsy digital forensics*, https://www.autopsy.com/, (Accessed on 11/15/2021).

[16] Grayshift, *Graykey cell phone forensics tool*, https://www.grayshift.com/graykey/, (Accessed on 02/08/2023).

[17] Cellebrite, *Home - cellebrite digital intelligence for a safer world*, https://www.cellebrite.com/en/home/, (Accessed on 07/07/2021).

[18] M. Forensics, *Magnet axiom - digital investigation platform magnet forensics*, https://www.magnetforensics.com/products/magnet-axiom/, (Accessed on 03/30/2021).

[19] R. P. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics," Tech. Rep., 2014.

[20] NIST, *Digital forensics nist*, https://www.nist.gov/programs-projects/digital-forensics, (Accessed on 11/11/2021).

[21] N. S. Q. Group, *Mobile devices*, https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/mobile, (Accessed on 04/05/2023).

[22] M. H. NIST, M. Iorga, A. M. Salim, *et al.*, *Nist cloud computing forensic science challenges*, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf, (Accessed on 02/02/2022).

[23] M. Stankovi, M. M. Mirza, and U. Karabiyik, "Uav forensics: Dji mini 2 case study," *Drones*, vol. 5, no. 2, 2021, ISSN: 2504-446X. DOI: 10.3390/drones5020049. [Online]. Available: https://www.mdpi.com/2504-446X/5/2/49.

[24] F. E. Salamh, M. M. Mirza, and U. Karabiyik, "Uav forensic analysis and software tools assessment: Dji phantom 4 and matrice 210 as case studies," *Electronics*, vol. 10, no. 6, 2021, ISSN: 2079-9292. DOI: 10.3390/electronics10060733. [Online]. Available: https://www.mdpi.com/2079-9292/10/6/733.

[25] G. A. Elmes, J. Conley, and G. Roedl, *Forensic GIS: The Role of Geospatial Technologies for Investigating Crime and Providing Evidence* (Geotechnologies and the Environment), eng, 2014th ed. Dordrecht: Springer Netherlands, 2014, vol. 11, ISBN: 9789401787567.

[26] B. Zhao and D. Z. Sui, "True lies in geospatial big data: Detecting location spoofing in social media," *Annals of GIS*, vol. 23, no. 1, pp. 1–14, 2017.

[27] K. A. Wade, S. L. Green, and R. A. Nash, "Can fabricated evidence induce false eyewitness testimony?" *Applied Cognitive Psychology*, vol. 24, no. 7, pp. 899–908, 2010.

[28] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 346–376, 2018.

[29] A. Freitas and E. Curry, "Big data curation," in *New horizons for a data-driven economy*, Springer, Cham, 2016, pp. 87–118.

[30] R. Ayers, B. Livelsberger, and B. Guttman, "Quick start guide for populating mobile test devices," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-202, 2018. DOI: 10.6028/NIST.SP.800-202.

[31] what3words, *What3words the simplest way to talk about location*, https://what3words.com/clip.apples.leap, (Accessed on 09/20/2021).

[32] A. Guarino, "Digital forensics as a big data challenge," in *ISSE 2013 securing electronic business processes*, Springer, 2013, pp. 197–203.

[33] J. F. Flinterman, R. Teclemariam-Mesbah, J. E. Broerse, and J. F. Bunders, "Transdisciplinarity: The new challenge for biomedical research," *Bulletin of Science, Technology & Society*, vol. 21, no. 4, pp. 253–266, 2001.

[34] C. I. Med, "Multidisciplinarity, interdisciplinarity and transdis-ciplinarity in health research, services, education and policy: 1. definitions, objectives, and evidence of effectiveness," *Clin Invest Med*, vol. 29, no. 6, pp. 351–364, 2006.

[35] "Cross-disciplinary learning," in *Encyclopedia of the Sciences of Learning*, N. M. Seel, Ed. Boston, MA: Springer US, 2012, pp. 858–858, ISBN: 978-1-4419-1428-6. DOI: 10.1007/978-1-4419-1428-6_1476. [Online]. Available: https://doi.org/10.1007/978-1-4419-1428-6_1476.

[36] S. Mukhopadhyay, *Academics and research beyond the disciplines: Transforming the healthcare for a better india with interdisciplinary approaches!)* https://jwbuhs.in/issue/pdf/html?file_path=%2Fhtml-files%2F1674623380_editorial.html, (Accessed on 04/16/2023).

[37] A. R. Jesenius, *Disciplinarities: Intra, cross, multi, inter, trans*, http://www.arj.no/2012/03/12/disciplinarities-2/, (Accessed on 01/16/2023).

[38] A. Tolk, A. Harper, and N. Mustafee, "Hybrid models as transdisciplinary research enablers," *European Journal of Operational Research*, vol. 291, no. 3, pp. 1075–1090, 2021.

[39] Statista, *Smartphone users in the us 2009-2040*, https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/, (Accessed on 04/04/2023).

[40] Statista, *Number of mobile devices worldwide 2020-2025*, https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/, (Accessed on 04/04/2023).

[41] J. Byrne and G. Marx, "Technological innovations in crime prevention and policing. a review of the research on implementation and impact," *Journal of Police Studies*, vol. 20, no. 3, pp. 17–40, 2011.

[42] V. Jusas, D. Birvinskas, and E. Gahramanov, "Methods and tools of digital triage in forensic context: Survey and future directions," *Symmetry*, vol. 9, no. 4, p. 49, 2017.

[43] N. I. of Justice, *Digital evidence and forensics*, https://nij.ojp.gov/digital-evidence-and-forensics, (Accessed on 04/04/2023).

[44] N. Rana, G. Sansanwal, K. Khatter, and S. Singh, "Taxonomy of digital forensics: Investigation tools and challenges," *arXiv preprint arXiv:1709.06529*, 2017.

[45] C. M. Miller, "A survey of prosecutors and investigators using digital evidence: A starting point," *Forensic Science International: Synergy*, p. 100 296, 2022.

[46] R. McKemmish, *What is forensic computing?* Australian Institute of Criminology Canberra, 1999.

[47] A. Årnes, *Digital forensics*. John Wiley & Sons, 2017.

[48] J. L. John, *Digital forensics and preservation*. Citeseer, 2012.

[49] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, *et al.*, "Digital forensics subdomains: The state of the art and future directions," *IEEE Access*, vol. 9, pp. 152 476–152 502, 2021.

[50] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11 065–11 089, 2022.

[51] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Mobile forensics: Advances, challenges, and research opportunities," *IEEE Security & Privacy*, vol. 15, no. 6, pp. 42–51, 2017.

[52] K. Bhavsar, A. Patel, and S. Parikh, "Approaches to digital forensics in the age of big data," in *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, 2022, pp. 449–453.

[53] S. Achar, "Cloud computing forensics," *International Journal of Computer Engineering and Technology*, vol. 13, no. 3, 2022.

[54] F. Casino, T. K. Dasaklis, G. Spathoulas, *et al.*, "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," *IEEE Access*, 2022.

[55] E. A. Vincze, "Challenges in digital forensics," *Police Practice and Research*, vol. 17, no. 2, pp. 183–194, 2016.

[56] O. I. Abiodun, M. Alawida, A. E. Omolara, and A. Alabdulatif, "Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[57] S. Saharan and B. Yadav, "Digital and cyber forensics: A contemporary evolution in forensic sciences," in *Crime Scene Management within Forensic Science: Forensic Techniques for Criminal Investigations*, Springer, 2022, pp. 267–294.

[58] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions," in *2013 Information Security for South Africa*, IEEE, 2013, pp. 1–8.

[59] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," *IEEE Security & Privacy*, vol. 15, no. 6, pp. 12–17, 2017.

[60] K. Barik, A. Abirami, K. Konar, and S. Das, "Research perspective on digital forensic tools and investigation process," *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, pp. 71–95, 2022.

[61] H. Bowling, K. Seigfried-Spellar, U. Karabiyik, and M. Rogers, "We are meeting on microsoft teams: Forensic analysis in windows, android, and ios operating systems," *Journal of Forensic Sciences*, vol. 68, no. 2, pp. 434–460, 2023.

[62] M. Moreb, "Introduction to ios forensics," in *Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices*, Springer, 2022, pp. 37–70.

[63] Z. Ma, "Apples and cars: A comparison of security," *arXiv preprint arXiv:2201.02601*, 2022.

[64] U. A. Umar and A. Wakili, "A comparative study of modern operating systems in terms of memory and security: A case study of windows, ios, and android," *SLU Journal of Science and Technology*, vol. 6, no. 1&2, pp. 131–138, 2023.

[65] M. Lanzing, E. Lievevrouw, and L. Siffels, "It takes two to techno-tango: An analysis of a close embrace between google/apple and the eu in fighting the pandemic through contact tracing apps," *Science as Culture*, vol. 31, no. 1, pp. 136–148, 2022.

[66] Apple, *Privacy - features*, https://www.apple.com/privacy/features/, (Accessed on 03/03/2023).

[67] A. Hoog and K. Strzempka, *iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices*. Elsevier, 2011.

[68] H. Mahalik, R. Tamma, and S. Bommisetty, *Practical mobile forensics*. Packt Publishing Ltd, 2016.

[69] D. Bennett, "The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations," *Information Security Journal: A Global Perspective*, vol. 21, no. 3, pp. 159–168, 2012.

[70] T. B. Tajuddin and A. Abd Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," in *2015 World Congress on Internet Security (WorldCIS)*, IEEE, 2015, pp. 132–138.

[71] Grayshift, *Graykey cell phone forensics tool*, https://www.grayshift.com/graykey/, (Accessed on 01/02/2023).

[72] *Magnet axiom - digital investigation platform*, https://www.magnetforensics.com/products/magnet-axiom/, note = (Accessed on 05/30/2021).

[73] J. Bays and U. Karabiyik, "Forensic analysis of third party location applications in android and ios," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2019, pp. 1–6.

[74] A. Gilbert and K. C. Seigfried-Spellar, "Forensic discoverability of ios vault applications," *Journal of Digital Forensics, Security and Law*, vol. 17, no. 1, p. 1, 2022.

[75] E. C. Cankaya and B. Kupka, "A survey of digital forensics tools for database extraction," in *2016 future technologies conference (ftc)*, IEEE, 2016, pp. 1014–1019.

[76] K. Oestreicher, "A forensically robust method for acquisition of icloud data," *Digital Investigation*, vol. 11, S106–S113, 2014.

[77] A. A. Ahmed and C. X. Li, "Locating and collecting cybercrime evidences on cloud storage," in *2016 International Conference on Information Science and Security (ICISS)*, IEEE, 2016, pp. 1–5.

[78] K. A. Alghafli, A. Jones, and T. A. Martin, "Forensics data acquisition methods for mobile phones," in *2012 International Conference for Internet Technology and Secured Transactions*, IEEE, 2012, pp. 265–269.

[79] P. C. Giannelli, "Chain of custody," 1996.

[80] J. C. Sremack, "The gap between theory and practice in digital forensics," 2007.

[81] NIST, *Sp 800-101 rev. 1, guidelines on mobile device forensics csrc*, https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final, (Accessed on 11/14/2021).

[82] thelma.allen@nist.gov, *Mobile devices*, May 2017. [Online]. Available: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/mobile.

[83] SWGDE, *Sswgde best practices for mobile device forensic analysis*, Accessed: 2021-11-13, 2020. [Online]. Available: https://www.swgde.org/documents/published.

[84] SWGDE, *Swgde best practices for mobile device evidence collection and preservation, handling, and acquisition*, Accessed: 2021-11-13, 2020. [Online]. Available: https://www.swgde.org/documents/published.

[85] SWGDE, *Swgde model standard operation procedures for computer forensics*, Accessed: 2021-11-13, 2012. [Online]. Available: https://www.swgde.org/documents/published.

[86] S. Rigby and M. K. Rogers, "The general digital forensics model," 2007.

[87] NEEDWORK, *Iso - iso/iec 27037:2012 - information technology security techniques guidelines for identification, collection, acquisition and preservation of digital evidence*, https://www.iso.org/standard/44381.html, (Accessed on 10/07/2021).

[88] *A review and comparative study of digital forensic investigation models springerlink*, https://link.springer.com/chapter/10.1007/978-3-642-39891-9_20, (Accessed on 10/07/2021).

[89] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," *Journal of Digital Forensics, Security and Law*, vol. 1, no. 2, p. 2, 2006.

[90] NEEDWORK, *Electronic crime scene investigation: A guide for first responders, second edition*, https://www.ojp.gov/pdffiles1/nij/219941.pdf, (Accessed on 10/07/2021).

[91] interpol, *Guidelines to digital forensics first responders v7*, https://www.interpol.int/content/download/16243/file/Guidelines20to0Digital20Forensics20First0ResponderesV7.pdf, (Accessed on 09/08/2021).

[92] B. S. G. W. William Newhouse Stephanie Keith, *Sp 800-181, nice framework csrc*, https://csrc.nist.gov/publications/detail/sp/800-181/archive/2017-08-07, (Accessed on 10/05/2021).

[93] NICE, *Sp 800-181 rev.1 workforce framework for cybersecurity (nice framework) csrc*, https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final, (Accessed on 10/05/2021).

[94] A. Mouhtaropoulos, C.-T. Li, and M. Grobler, "Digital forensic readiness: Are we there yet," *J. Int't Com. L. & Tech.*, vol. 9, p. 173, 2014.

[95] ACPO, *Acpo good practice guide for digital evidence*, https://athenaforensics.co.uk/wp-content/uploads/2019/01/National-Police-Chiefs-Council-ACPO-Good-Practice-Guide-for-Digital-Evidence-March-2012.pdf, (Accessed on 11/06/2021), 2012.

[96] A. Roder, K.-K. R. Choo, and N.-A. Le-Khac, "Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study," *arXiv preprint arXiv:1804.08649*, 2018.

[97] F. E. Salamh, M. M. Mirza, and U. Karabiyik, "Uav forensic analysis and software tools assessment: Dji phantom 4 and matrice 210 as case studies," *Electronics*, vol. 10, no. 6, p. 733, 2021.

[98] M. Stankovi, M. M. Mirza, and U. Karabiyik, "Uav forensics: Dji mini 2 case study," *Drones*, vol. 5, no. 2, p. 49, 2021.

[99] F. E. Salamh, U. Karabiyik, and M. K. Rogers, "Rpas forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon h," *Sensors*, vol. 19, no. 15, p. 3246, 2019.

[100] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *2017 IEEE Sensors Applications Symposium (SAS)*, IEEE, 2017, pp. 1–6.

[101] M. Herman, M. Iorga, A. M. Salim, *et al.*, "Nist cloud computing forensic science challenges," National Institute of Standards and Technology, Tech. Rep., 2020.

[102] NEEDWORK, *What is spatial temporal? definition and related faqs*, https://www.omnisci.com/technical-glossary/spatial-temporal, (Accessed on 11/14/2021).

[103] M. Li, Y. Sun, and H. Fan, "Contextualized relevance evaluation of geographic information for mobile users in location-based social networks," *ISPRS International Journal of Geo-Information*, vol. 4, no. 2, pp. 799–814, 2015.

[104] ISO, *Iso - iso/tc 211 - geographic information/geomatics*, https://www.iso.org/committee/54904.html, (Accessed on 11/06/2021).

[105] G. M. Djuknic and R. E. Richton, "Geolocation and assisted gps," *Computer*, vol. 34, no. 2, pp. 123–125, 2001.

[106] C. Gentile, N. Alsindi, R. Raulefs, and C. Teolis, *Geolocation techniques: principles and applications*. Springer Science & Business Media, 2012.

[107] E. Van Buskirk and V. T. Liu, "Digital evidence: Challenging the presumption of reliability," *Journal of Digital Forensic Practice*, vol. 1, no. 1, pp. 19–26, 2006.

[108] R. Koen and M. S. Olivier, "The use of file timestamps in digital forensics.," in *ISSA*, Citeseer, 2008, pp. 1–16.

[109] B. Schatz, G. Mohay, and A. Clark, "A correlation method for establishing provenance of timestamps in digital evidence," *digital investigation*, vol. 3, pp. 98–107, 2006.

[110] *Https://www.magnetforensics.com/docs/axiom/release_notes.html*, https://www.magnetforensics.com/docs/axiom/release_notes.html, (Accessed on 11/06/2021).

[111] S. Krishnan, B. Zhou, and M. K. An, "Smartphone forensic challenges," *International Journal of Computer Science and Security (IJCSS)*, vol. 13, no. 5, p. 183, 2019.

[112] N. R. Council, *Learning to Think Spatially*. Washington, DC: The National Academies Press, 2006, ISBN: 978-0-309-09208-1. DOI: 10.17226/11019. [Online]. Available: https://www.nap.edu/catalog/11019/learning-to-think-spatially.

[113] J. Hightower and G. Borriello, "Location sensing techniques," *IEEE Computer*, vol. 34, no. 8, pp. 57–66, 2001.

[114] P. A. Zandbergen, "Accuracy of iphone locations: A comparison of assisted gps, wifi and cellular positioning," *Transactions in GIS*, vol. 13, pp. 5–25, 2009.

[115] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in *9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing*, IEEE, 2013, pp. 608–615.

[116] M. Omer, Y. Ran, and G. Y. Tian, "Indoor localization systems for passive uhf rfid tag based on rssi radio map database," *Progress In Electromagnetics Research M*, vol. 77, pp. 51–60, 2019.

[117] K. Ashton *et al.*, "That internet of things thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[118] M. A. M. Vieira, C. N. Coelho, D. j. da Silva, and J. M. da Mata, "Survey on wireless sensor network devices," in *EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696)*, IEEE, vol. 1, 2003, pp. 537–544.

[119] K. Karimi and G. Atkinson, "What the internet of things (iot) needs to become a reality," *White Paper, FreeScale and ARM*, pp. 1–16, 2013.

[120] M. M. Mirza and U. Karabiyik, "2021 international symposium on networks, computers and communications (isncc): Trust, security and privacy (isncc-2021 tsp)," Dubai, United Arab Emirates, May 2021.

[121] B. Eissfeller, G. Ameres, V. Kropp, and D. Sanroma, "Performance of gps, glonass and galileo," in *Photogrammetric Week*, vol. 7, 2007, pp. 185–199.

[122] Garmin, *What is gps? garmin*, https://www.garmin.com/en-US/aboutGPS/, (Accessed on 11/15/2021).

[123] W. Navidi, W. S. Murphy Jr, and W. Hereman, "Statistical methods in surveying by trilateration," *Computational statistics & data analysis*, vol. 27, no. 2, pp. 209–227, 1998.

[124] N. Vallina-Rodriguez, J. Crowcroft, A. Finamore, Y. Grunenberger, and K. Papagiannaki, "When assistance becomes dependence: Characterizing the costs and inefficiencies of a-gps," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 17, no. 4, pp. 3–14, 2013.

[125] P. A. Zandbergen and S. J. Barbeau, "Positional accuracy of assisted gps data from high-sensitivity gps-enabled mobile phones," *The Journal of Navigation*, vol. 64, no. 3, pp. 381–399, 2011.

[126] K. Merry and P. Bettinger, "Smartphone gps accuracy study in an urban environment," *PloS one*, vol. 14, no. 7, e0219890, 2019.

[127] T. Kim Geok, K. Zar Aung, M. Sandar Aung, *et al.*, "Review of indoor positioning: Radio wave technology," *Applied Sciences*, vol. 11, no. 1, p. 279, 2021.

[128] P. Pascacio, S. Casteleyn, J. Torres-Sospedra, E. S. Lohan, and J. Nurmi, "Collaborative indoor positioning systems: A systematic review," *Sensors*, vol. 21, no. 3, p. 1002, 2021.

[129] B. Bellalta, L. Bononi, R. Bruno, and A. Kassler, "Next generation ieee 802.11 wireless local area networks: Current status, future directions and open challenges," *Computer Communications*, vol. 75, pp. 1–25, 2016.

[130] K. Chintalapudi, A. Padmanabha Iyer, and V. N. Padmanabhan, "Indoor localization without the pain," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, 2010, pp. 173–184.

[131] Y. Liu, Z. Yang, X. Wang, and L. Jian, "Location, localization, and localizability," *Journal of computer science and technology*, vol. 25, no. 2, pp. 274–297, 2010.

[132] C. Yang and H.-R. Shao, "Wifi-based indoor positioning," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 150–157, 2015.

[133] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067–1080, 2007.

[134] M. H. Sarshar, "Analyzing large scale wi-fi data using supervised and unsupervised learning techniques," Ph.D. dissertation, 2017.

[135] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 2016, pp. 165–178.

[136] M. Naveed, X. Wang, and C. Gunter, "Poster: Privacy implications of bssid based location services,"

[137] M. Chernyshev, C. Valli, and P. Hannay, "On 802.11 access point locatability and named entity recognition in service set identifiers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 584–593, 2015.

[138] M. Chernyshev, C. Valli, and P. Hannay, "802.11 tracking and surveillance-a forensic perspective," in *Proceedings of the International Conference on Security and Management (SAM)*, The Steering Committee of The World Congress in Computer Science, Computer , 2015, p. 349.

[139] WiGLE, *Wigle: Wireless network mapping*, https://wigle.net/, (Accessed on 11/19/2021).

[140] A. LaMarca, J. Hightower, I. Smith, and S. Consolvo, "Self-mapping in 802.11 location systems," in *International Conference on Ubiquitous Computing*, Springer, 2005, pp. 87–104.

[141] WiGLE, *Wigle.net/graph-large.html*, https://wigle.net/graph-large.html, (Accessed on 07/10/2023).

[142] WiGLE, *Wigle.net/stats*, https://wigle.net/stats, (Accessed on 07/10/2023).

[143] M. Chernyshev, C. Valli, and P. Hannay, "Service set identifier geolocation for forensic purposes: Opportunities and challenges," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, 2016, pp. 5487–5496.

[144] P. ONeill, "Bluetooth contact tracing needs bigger, better data," *MIT Technology Review*, 2020.

[145] Q. Zhao, H. Wen, Z. Lin, D. Xuan, and N. Shroff, "On the accuracy of measured proximity of bluetooth-based contact tracing apps," in *International Conference on Security and Privacy in Communication Systems*, Springer, 2020, pp. 49–60.

[146] U. Karabiyik and K. Akkaya, "Digital forensics for iot and wsns," in *Mission-Oriented Sensor Networks and Systems: Art and Science*, Springer, 2019, pp. 171–207.

[147] L. Li, M. F. Goodchild, and B. Xu, "Spatial, temporal, and socioeconomic patterns in the use of twitter and flickr," *Cartography and geographic information science*, vol. 40, no. 2, pp. 61–77, 2013.

[148] D. Komosny, M. Voznak, and S. U. Rehman, "Location accuracy of commercial ip address geolocation databases," *Information technology and control*, vol. 46, no. 3, pp. 333–344, 2017.

[149] P. Sokol, L. Rózenfeldová, K. Luivjanská, and J. Harata, "Ip addresses in the context of digital evidence in the criminal and civil case law of the slovak republic," *Forensic Science International: Digital Investigation*, vol. 32, p. 300 918, 2020, ISSN: 2666-2817. DOI: https://doi.org/10.1016/j.fsidi.2020.300918. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281720300135.

[150] P. Winter, R. Padmanabhan, A. King, and A. Dainotti, "Geo-locating bgp prefixes," eng, IFIP, 2019, pp. 9–16, ISBN: 3903176176.

[151] E. Katz-Bassett, J. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards ip geolocation using delay and topology measurements," eng, ser. IMC '06, ACM, 2006, pp. 71–84, ISBN: 1595935614.

[152] A. Mylonas, V. Meletiadis, L. Mitrou, and D. Gritzalis, "Smartphone sensor data as digital evidence," *Computers & Security*, vol. 38, pp. 51–75, 2013.

[153] M. Giardino, D. Giordan, and S. Ambrogio, "Gis technologies for data collection, management and visualization of large slope instabilities: Two applications in the western italian alps," *Natural Hazards and Earth System Sciences*, vol. 4, no. 2, pp. 197–211, 2004.

[154] Esri, *What is gis? geographic information system mapping technology*, https://www.esri.com/en-us/what-is-gis/overview, (Accessed on 11/11/2021).

[155] G. Andrienko, N. Andrienko, U. Demsar, *et al.*, "Space, time and visual analytics," *International journal of geographical information science*, vol. 24, no. 10, pp. 1577–1600, 2010.

[156] P. A. Burrough, R. A. McDonnell, and C. D. Lloyd, *Principles of geographical information systems*. Oxford university press, 2015.

[157] F. G. Michael, "Geographical information science," *International Journal Geographical Information System*, vol. 6, no. 1, pp. 31–45, 1992.

[158] T. Blaschke, H. Merschdorf, P. Cabrera-Barona, S. Gao, E. Papadakis, and A. Kovacs-Györi, "Place versus space: From points, lines and polygons in gis to place-based representations reflecting language and culture," *ISPRS International Journal of Geo-Information*, vol. 7, no. 11, p. 452, 2018.

[159] T. Blaschke, K. Donert, F. Gossette, *et al.*, "Virtual globes: Serving science and society," *Information*, vol. 3, no. 3, pp. 372–390, 2012.

[160] Google, *Google earth*, https://www.google.com/earth/index.html, (Accessed on 09/06/2021).

[161] J. Dangermond, *What is a Geographic Information System (GIS)?* ASTM International, 1992.

[162] F. Escobar, G. Hunter, I. Bishop, and A. Zerger, "Introduction to gis," *Department of Geomatics, The University of Melbourne, Available online at: http://www. sli. unimelb. edu. au/gisweb/(Accessed 02 April 2008)*, 2008.

[163] M. F. Goodchild, "Scale in gis: An overview," *Geomorphology*, vol. 130, no. 1-2, pp. 5–9, 2011.

[164] S. E. Piovan and S. E. Piovan, "Principles and techniques of cartography," *The Geohistorical Approach: Methods and Applications*, pp. 39–88, 2020.

[165] D. M. Theobald, "Topology revisited: Representing spatial relations," *International Journal of Geographical Information Science*, vol. 15, no. 8, pp. 689–705, 2001.

[166] T.-H. Nguyen, A. A. Oloufa, and K. Nassar, "Algorithms for automated deduction of topological information," *Automation in construction*, vol. 14, no. 1, pp. 59–70, 2005.

[167] C. A. Davis and F. T. Fonseca, "Assessing the certainty of locations produced by an address geocoding system," *Geoinformatica*, vol. 11, pp. 103–129, 2007.

[168] O. Kounadi, T. J. Lampoltshammer, M. Leitner, and T. Heistracher, "Accuracy and privacy aspects in free online reverse geocoding services," *Cartography and Geographic Information Science*, vol. 40, no. 2, pp. 140–153, 2013.

[169] ESRI, *What is geoprocessing?* https://pro.arcgis.com/en/pro-app/latest/help/analysis/geoprocessing/basics/what-is-geoprocessing-.htm, (Accessed on 04/01/2023).

[170] S. Johnson, *The ghost map: The story of London's most terrifying epidemic–and how it changed science, cities, and the modern world*. Penguin, 2006.

[171] G. A. Elmes, G. Roedl, and J. Conley, *Forensic GIS: The role of geospatial technologies for investigating crime and providing evidence*. Springer, 2014, vol. 11.

[172] M. A. Umar, A. A. Machina, M. Ibrahim, *et al.*, "Fighting crime and insecurity in nigeria: An intelligent approach," *International of Computer Engineering in Research Trend. Vol*, vol. 8, pp. 6–14, 2021.

[173] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Current and future trends in mobile device forensics: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, pp. 1–31, 2018.

[174] I. Vasiliev, S. Freundschuh, D. M. Mark, G. Theisen, and J. McAvoy, "What is a map?" *The Cartographic Journal*, vol. 27, no. 2, pp. 119–123, 1990.

[175] M. Harrington and M. Cross, *Google Earth Forensics: Using Google Earth Geo-Location in Digital Forensic Investigations*, eng. Rockland, MA: Elsevier Science & Technology Books, 2014, ISBN: 9780128002162.

[176] A. Tillekens, N.-A. Le-Khac, and T. T. P. Thi, "A bespoke forensics gis tool," in *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2016, pp. 987–992.

[177] N. A. Hassan and R. Hijazi, "The evolution of open source intelligence," in *Open Source Intelligence Methods and Tools*, Springer, 2018, pp. 1–20.

[178] D. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and open source intelligence (dfint+ osint): A timely and cohesive mix," *Future Generation Computer Systems*, vol. 78, pp. 558–567, 2018.

[179] S. Gibson, "Open source intelligence: An intelligence lifeline," *The RUSI Journal*, vol. 149, no. 1, pp. 16–22, 2004.

[180] C. Best, "Open source intelligence," *F. Fogelman-Soulié, Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security*, pp. 331–343, 2008.

[181] NEEDWORK, *Homepage - maltego*, https://www.maltego.com/, (Accessed on 10/07/2021).

[182] A. Dhein, "Securing the analytical interpretation of geolocation data in cellular forensics," 2019.

[183] J. Moore, I. Baggili, and F. Breitinger, "Find me if you can: Mobile gps mapping applications forensic analysis & snavp the open source, modular, extensible parser," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 1, p. 7, 2017.

[184] N. Shantaram, "Forensic analysis of navigation applications on android and ios platforms," Ph.D. dissertation, Purdue University Graduate School, 2021.

[185] P. Aagaard, B. Dinyarian, O. Abduljabbar, and K.-K. R. Choo, "Family locating sharing app forensics: Life360 as a case study," *Forensic Science International: Digital Investigation*, vol. 44, p. 301 478, 2023.

[186] J. Sablatura and U. Karabiyik, "Pokémon go forensics: An android application analysis," *Information*, vol. 8, no. 3, p. 71, 2017.

[187] D. R. Hayes, C. Snow, and S. Altuwayjiri, "Geolocation tracking and privacy issues associated with the uber mobile application," in *Proceedings of the Conference on Information Systems Applied Research ISSN*, vol. 2167, 2017, p. 1508.

[188] N. Matulis and U. Karabiyik, "Digital forensics for mobility as a service platform: Analysis of uber application on iphone and cloud," 2022.

[189] Y. H. Yoon and U. Karabiyik, "Forensic analysis of fitbit versa 2 data on android," *Electronics*, vol. 9, no. 9, 2020, ISSN: 2079-9292. DOI: 10.3390/electronics9091431. [Online]. Available: https://www.mdpi.com/2079-9292/9/9/1431.

[190] J. Williams, Á. MacDermott, K. Stamp, and F. Iqbal, "Forensic analysis of fitbit versa: Android vs ios," in *2021 IEEE Security and Privacy Workshops (SPW)*, IEEE, 2021, pp. 318–326.

[191] A. Almogbil, A. Alghofaili, C. Deane, and T. Leschke, "Digital forensic analysis of fitbit wearable technology: An investigators guide," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, 2020, pp. 44–49.

[192] A. Almogbil, A. Alghofaili, C. Deane, and T. Leschke, "The accuracy of gps-enabled fitbit activities as evidence: A digital forensics study," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, 2020, pp. 186–189.

[193] S. Kang, S. Kim, and J. Kim, "Forensic analysis for iot fitness trackers and its application," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 564–573, 2020.

[194] S. Hutchinson, M. M. Mirza, N. West, *et al.*, "Investigating wearable fitness applications: Data privacy and digital forensics analysis on android," *Applied Sciences*, vol. 12, no. 19, p. 9747, 2022.

[195] F. E. Salamh, "A forensic analysis of home automation devices (fahad) model: Kasa smart light bulb and eufy floodlight camera as case studies," *International Journal of Cyber Forensics and Advanced Threat Investigations*, pp. 1–1, 2020.

[196] S. E. Prastya, I. Riadi, and A. Luthfi, "Forensic analysis of unmanned aerial vehicle to obtain gps log data as digital evidence," *IJCSIS*, vol. 15, no. 3, 2017.

[197] T. E. A. Barton and M. H. B. Azhar, "Forensic analysis of popular uav systems," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, IEEE, 2017, pp. 91–96.

[198] M. Yousef and F. Iqbal, "Drone forensics: A case study on a dji mavic air," in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, IEEE, 2019, pp. 1–3.

[199] S. H. Mekala and Z. Baig, "Digital forensics for drone data–intelligent clustering using self organising maps," in *International Conference on Future Network Systems and Security*, Springer, 2019, pp. 172–189.

[200] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4i-digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, p. 100 015, 2020.

[201] B. Gokaraju, R. Agrawal, D. A. Doss, and S. Bhattacharya, "Identification of spatio-temporal patterns in cyber security for detecting the signature identity of hacker," in *SoutheastCon 2018*, 2018, pp. 1–5.

[202] K.-K. Choo and A. Dehghantanha, "Contemporary digital forensics investigations of cloud and mobile applications," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Elsevier, 2017, pp. 1–6.

[203] W. R. Parkhurst, *Routing first-step*. Cisco Press, 2004.

[204] W. Stallings, "Ipv6: The new internet protocol," *IEEE Communications Magazine*, vol. 34, no. 7, pp. 96–108, 1996.

[205] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," in *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, IEEE, 2013, pp. 544–550.

[206] S. Hong and K.-H. Rhee, "An approach for the similar file detection with gps information," in *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, IEEE, 2011, pp. 320–324.

[207] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: Challenges and new insights," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2018, pp. 1–6.

[208] . GÜLATA and S. BAKTIR, "Unmanned aerial vehicle digital forensic investigation framework," *Journal of Naval Sciences and Engineering*, vol. 14, no. 1, pp. 32–53, 2018.

[209] P. Harvey, *Exiftool by phil harvey*, https://exiftool.org/, (Accessed on 11/07/2021).

[210] R. Montasari and R. Hill, "Next-generation digital forensics: Challenges and future paradigms," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, IEEE, 2019, pp. 205–212.

[211] J. S. Ward and A. Barker, "Undefined by data: A survey of big data definitions," *arXiv preprint arXiv:1309.5821*, 2013.

[212] A. Gandomi and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics," *International journal of information management*, vol. 35, no. 2, pp. 137–144, 2015.

[213] S. L. Garfinkel, "Digital forensics research: The next 10 years," *digital investigation*, vol. 7, S64–S73, 2010.

[214] N. C. C. O. APPEALS, *State of north carolina vs. bradley graham cooper*, https://wwwcache.wral.com/asset/specialreports/nancycooper/2013/02/28/12166096/4128-sccoa.pdf, (Accessed on 11/09/2021).

[215] F. M. Granja and G. D. R. Rafael, "The preservation of digital evidence and its admissibility in the court," *International Journal of Electronic Security and Digital Forensics*, vol. 9, no. 1, pp. 1–18, 2017.

[216] P. McCarthy and J. Slay, "Mobile phones: Admissibility of current forensic procedures for acquiring data," in *the Second IFIP WG*, vol. 11, 2006.

[217] V. Wadhwa, "Laws and ethics cant keep pace with technology," *Massachusetts Institute of Technology: Technology Review*, vol. 15, 2014.

[218] J. M. Balkin, "The path of robotics law," *Calif. L. Rev. Circuit*, vol. 6, p. 45, 2015.

[219] B. Endicott-Popovsky and D. J. Horowitz, "Unintended consequences: Digital evidence in our legal system," *IEEE Security & Privacy*, vol. 10, no. 2, pp. 80–83, 2012.

[220] A. Alva and B. Endicott-Popovsky, "Digital evidence education in schools of law," 2012.

[221] S. Raghav and A. K. Saxena, "Mobile forensics: Guidelines and challenges in data preservation and acquisition," in *2009 IEEE Student Conference on Research and Development (SCOReD)*, IEEE, 2009, pp. 5–8.

[222] L. M. Aouad, T. M. Kechadi, and R. Di Russo, "Ants road: A new tool for sqlite data recovery on android devices," in *International Conference on Digital Forensics and Cyber Crime*, Springer, 2012, pp. 253–263.

[223] SWGDE, *Swgde technical notes on internet of things devices - google drive*, https://drive.google.com/file/d/1zcDxCLSrwTbwFlTAtjwB6UxMgMHOj3GY/view, (Accessed on 11/12/2021), Sep. 2020.

[224] M. M. Mirza and U. Karabiyik, *Evaluation of gps exif data reporting for digital forensics tools*, https://www.cerias.purdue.edu/assets/symposium/2020-posters/9BB-E39.pdf, (Accessed on 11/12/2021).

[225] O. Güngör, W. Honekamp, and H. S. IACS, "Forensic determination of movement and usage profiles using smartphone apps," *Mobility in a Globalised World 2020*, vol. 25, p. 137, 2021.

[226] NEEDWORK, *Mobile os market share 2021 statista*, https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/, (Accessed on 11/09/2021).

[227] M. Marjani, F. Nasaruddin, A. Gani, *et al.*, "Big iot data analytics: Architecture, opportunities, and open research challenges," *ieee access*, vol. 5, pp. 5247–5261, 2017.

[228] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, "Cloudme forensics: A case of big data forensic investigation," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 5, e4277, 2018.

[229] S. Maus, H. Höfken, and M. Schuba, "Forensic analysis of geodata in android smartphones," in *International Conference on Cybercrime, Security and Digital Forensics, http://www. schuba. fh-aachen. de/papers/11-cyberforensics. pdf*, 2011.

[230] J. Ajayakumar and K. Ghazinour, "I am at home: Spatial privacy concerns with social media check-ins," eng, *Procedia Computer Science*, vol. 113, pp. 551–558, 2017, ISSN: 1877-0509.

[231] N. Scrivens and X. Lin, "Android digital forensics: Data, extraction and analysis," eng, in *Proceedings of the ACM Turing 50th Celebration Conference - China*, ser. ACM TUR-C '17, vol. 127754, ACM, 2017, pp. 1–10, ISBN: 9781450348737.

[232] D. Kasiaras, T. Zafeiropoulos, N. Clarke, and G. Kambourakis, "Android forensics: Correlation analysis," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, IEEE, 2014, pp. 157–162.

[233] D. Kim, Y. Lee, and S. Lee, "Mobile forensic reference set (mfres) and mobile forensic investigation for android devices," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6618–6632, 2018.

[234] W. Lawless, R. Mittu, D. Sofge, I. S. Moskowitz, and S. Russell, *Artificial intelligence for the internet of everything*. Academic Press, 2019.

[235] B. M. Horowitz, "Policy issues regarding implementations of cyber attack resilience solutions for cyber physical systems," in *2018 AAAI Spring Symposium Series*, 2018.

[236] DCC, *Dcc curation lifecycle model*, https://www.dcc.ac.uk/sites/default/files/documents/publications/DCCLifecycle.pdf, (Accessed on 11/26/2021).

[237] NEEDWORK, *Device information can be too much of a good thing for law enforcement investigation - purdue university news*, https://www.purdue.edu/newsroom/releases/2021/Q4/device-information-can-be-too-much-of-a-good-thing-for-law-enforcement-investigation.html?inproceedingsga=2.168847656.822209326.1637886744-1998020861.1604240360, (Accessed on 11/25/2021).

[238] E. Curry, A. Freitas, and S. ORiáin, "The role of community-driven data curation for enterprises," in *Linking enterprise data*, Springer, 2010, pp. 25–47.

[239] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *digital investigation*, vol. 3, pp. 44–49, 2006.

[240] S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," in *2nd International Conference on i-Warfare and Security*, vol. 20087, 2007, pp. 77–84.

[241] M. Rogers, "Anti-forensics: The coming wave in digital forensics," *Retrieved September*, vol. 7, p. 2008, 2006.

[242] K. Dahbur and B. Mohammad, "Toward understanding the challenges and countermeasures in computer anti-forensics," in *Cloud Computing Advancements in Design, Implementation, and Technologies*, IGI Global, 2013, pp. 176–189.

[243] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, "Research trends in digital forensic science: An empirical analysis of published research," in *International Conference on Digital Forensics and Cyber Crime*, Springer, 2012, pp. 144–157.

[244] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The proactive and reactive digital forensics investigation process: A systematic literature review," in *International Conference on Information Security and Assurance*, Springer, 2011, pp. 87–100.

[245] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," *Digital investigation*, vol. 18, S66–S75, 2016.

[246] R. Wang, M. Xue, K. Liu, and H. Qian, "Data-driven privacy analytics: A wechat case study in location-based social networks," in *International Conference on Wireless Algorithms, Systems, and Applications*, Springer, 2015, pp. 561–570.

[247] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, and C. Stracquodaine, "Unmanned aerial vehicle security using behavioral profiling," in *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, 2015, pp. 1310–1319.

[248] Z. Birnbaum, A. Dolgikh, V. Skormin, E. OBrien, D. Muller, and C. Stracquodaine, "Unmanned aerial vehicle security using recursive parameter estimation," *Journal of Intelligent & Robotic Systems*, vol. 84, no. 1, pp. 107–120, 2016.

[249] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "Unmanned aerial vehicle kill chain: Purple teaming tactics," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2021, pp. 1081–1087.

[250] F. Salamh, "A 3-dimensional uas forensic intelligence-led taxonomy (u-fit)," Ph.D. dissertation, Purdue University Graduate School, 2021.

[251] S. Middleton, G. Kordopatis-Zilos, S. Papadopoulos, and Y. Kompatsiaris, "Location extraction from social media: Geoparsing, location disambiguation, and geotagging," eng, *ACM Transactions on Information Systems (TOIS)*, vol. 36, no. 4, pp. 1–27, 2018, ISSN: 1046-8188.

[252] H. Deng, M. Lee, A. Hakeem, *et al.*, "Fast forensic video event retrieval using geospatial computing," eng, ser. COM.Geo '10, ACM, 2010, pp. 1–8, ISBN: 9781450300315.

[253] census. "Tiger/line shapefiles." Accessed: 2020-10-5. (2020), [Online]. Available: https://www.census.gov/geographies/mapping-files/time-series/geo/tiger-line-file.html.

[254] L. Vincent, "Taking online maps down to street level," *Computer*, vol. 40, no. 12, pp. 118–120, 2007.

[255] U. Karabiyik, M. Canbaz, A. Aksoy, *et al.*, "A survey of social network forensics," eng, *The journal of digital forensics, security and law*, vol. 11, no. 4, pp. 55–128, 2016, ISSN: 1558-7223.

[256] G. Xu, S. Gao, M. Daneshmand, C. Wang, and Y. Liu, "A survey for mobility big data analytics for geolocation prediction," eng, *IEEE Wireless Communications*, vol. 24, no. 1, pp. 111–119, 2017, ISSN: 1536-1284.

[257] J. E. R. McMillan, W. B. Glisson, and M. Bromby, "Investigating the increase in mobile phone evidence in criminal activities," in *2013 46th Hawaii International Conference on System Sciences*, IEEE, 2013, pp. 4900–4909.

[258] K. J. Berman, W. B. Glisson, and L. M. Glisson, "Investigating the impact of global positioning system evidence," in *2015 48th Hawaii International Conference on System Sciences*, IEEE, 2015, pp. 5234–5243.

[259] K. A. Cole, S. Gupta, D. Gurugubelli, and M. K. Rogers, "A review of recent case law related to digital forensics: The current issues," *ADFSL Conference on Digital Forensics, Security and Law*, 2015.

[260] R. F. Erbacher, "Validation for digital forensics," in *2010 Seventh International Conference on Information Technology: New Generations*, IEEE, 2010, pp. 756–761.

[261] M. Meyers and M. Rogers, "Computer forensics: The need for standardization and certification," *International Journal of Digital Evidence*, vol. 3, no. 2, pp. 1–11, 2004.

[262] J. Williams, "Acpo good practice guide for digital evidence," *Metropolitan Police Service, Association of chief police officers, GB*, pp. 1556–6013, 2012.

[263] S. Satpathy and S. N. Mohanty, *Big data analytics and computing for digital forensic investigations*. CRC Press, 2020.

[264] s. UK intelligence and cyber agency, *Gchq/cyberchef: The cyber swiss army knife - a web app for encryption, encoding, compression and data analysis*, https://github.com/gchq/CyberChef, (Accessed on 01/15/2023).

[265] Mac4n6, *Mac4n6/apollo: Apple pattern of life lazy output'er*, https://github.com/mac4n6/APOLLO, (Accessed on 01/15/2023).

[266] *Log2timeline/plaso: Super timeline all the things*, https://github.com/log2timeline/plaso, (Accessed on 02/12/2023).

[267] T. P. (log2timeline), *Welcome to the plaso documentation plaso (log2timeline) 20230630 documentation*, https://plaso.readthedocs.io/en/latest, (Accessed on 02/12/2023).

[268] A. Brignoni, *Abrignoni/ileapp: Ios logs, events, and plist parser*, https://github.com/abrignoni/iLEAPP, (Accessed on 01/15/2023).

[269] Microsoft, *Meet windows 11: The newest windows version*, https://www.microsoft.com/en-us/windows/windows-11, (Accessed on 04/10/2023).

[270] M. L. Contributors, *Install wsl*, https://learn.microsoft.com/en-us/windows/wsl/install, (Accessed on 01/15/2023).

[271] P. Singh and P. Singh, "Linux development on wsl," *Learn Windows Subsystem for Linux: A Practical Guide for Developers and IT Professionals*, pp. 131–168, 2020.

[272] M. Mobile, *Wireless that's easy, online, $15 bucks a month*, (Accessed on 07/10/2023).

[273] T. B. Hick, *Public images*, https://thebinaryhick.blog/public_images/, (Accessed on 01/15/2023).

[274] J. K. Magnet Forensics, D. Navarro, H. Froio, A. Cash, and J. Hyde, *Cfreds portal*, https://cfreds.nist.gov/all/MagnetForensics/2022iOS15FullFileSystemMagnetCTF, (Accessed on 02/02/2023).

[275] D. Corpora, *Digital corpora: Corpora/scenarios/magnet/*, https://downloads.digitalcorpora.org/corpora/scenarios/magnet/, (Accessed on 05/02/2023).

[276] C. .-. NIST, *Cfreds portal*, https://cfreds.nist.gov/, (Accessed on 02/07/2023).

[277] T. B. Hick, *Ios 13 images.imagesnow available!* https://thebinaryhick.blog/2020/04/16/ios-13-images-images-now-available/, (Accessed on 04/20/2022).

[278] D. Corpora, *Digital corpora sponsored by the aws open data sponsorship program*, https://digitalcorpora.org/, (Accessed on 04/15/2023).

[279] T. B. Hick, *Ios 14 + macos big sur = lots of images*, https://thebinaryhick.blog/2021/02/20/ios-14-macos-big-sur-lots-of-images/, (Accessed on 11/28/2021).

[280] M. Forensics, J. Hyde, D. Navarro, *et al.*, *Magnet virtual summit 2023 ctf - ios 16 iphone*, https://go.magnetforensics.com/e/52162/41A1130001E-files-full-001-zip/lhmdf2/1324249432?h=iUPlnWlPjHpMjEkwU1o-llEAtRJSy8xNuSYq5byHzx4, (Accessed on 02/25/2023).

[281] stark4n6, *Magnet virtual summit 2023 ctf - ios 16 iphone*, https://www.stark4n6.com/2023/03/magnet-virtual-summit-2023-ctf-ios-16.html, (Accessed on 03/15/2023).

[282] R. Ayers, B. Livelsberger, and B. Guttman, "Quick start guide for populating mobile test devices," National Institute of Standards and Technology, Tech. Rep., 2018.

[283] NEEDWORK, *What is geoprocessing*, http://www.geography.hunter.cuny.edu/~jochen/gtech361/lectures/lecture12/concepts/01%20What%20is%20geoprocessing.htm, (Accessed on 11/28/2021).

[284] A. D. Documentation, *Core location*, https://developer.apple.com/documentation/corelocation, (Accessed on 01/20/2023).

[285] *Regex for ip address (ipv4) - ihateregex*, https://ihateregex.io/expr/ip, (Accessed on 05/01/2023).

[286] G. George, *Geongeorge/i-hate-regex: The code for ihateregex.io - the regex cheat sheet*, https://github.com/geongeorge/i-hate-regex, (Accessed on 05/01/2023).

[287] F. team, *Cell phone privacy and warrant requirements*, https://www.findlaw.com/criminal/criminal-rights/cell-phone-privacy-and-warrant-requirements.html, (Accessed on 04/10/2023).

[288] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[289] A. A. Torres-Garca, O. Mendoza-Montoya, M. Molinas, J. M. Antelis, L. A. Moctezuma, and T. Hernández-Del-Toro, "Pre-processing and feature extraction," in *Biosignal Processing and Classification Using Computational Learning and Intelligence*, Elsevier, 2022, pp. 59–91.

[290] dcode.fr, *Geohash coordinates converter - online latitude longitude calculator*, https://www.dcode.fr/geohash-coordinates, (Accessed on 04/02/2023).

[291] C. Veness, *Chrisveness/latlon-geohash: Gustavo niemeyers geocoding system*, https://github.com/chrisveness/latlon-geohash/tree/master, (Accessed on 04/02/2023).

[292] Google, *Plus codes*, https://plus.codes/map, (Accessed on 04/02/2023).

[293] Dcode.fr, *Open location converter - plus code to/from gps (lat/long) - online*, https://www.dcode.fr/open-location-code, (Accessed on 04/02/2023).

[294] Airdata, *Drone data management and flight analysis*, https://airdata.com/, (Accessed on 09/19/2022).

[295] B. Lovejoy, *Rittenhouse lawyer claims ipad pinch-to-zoom fakes video - 9to5mac*, https://9to5mac.com/2021/11/11/rittenhouse-lawyer-pinch-to-zoom/, (Accessed on 11/29/2021).

[296] C. TV, *Kenosha protest shooting (wi v. kyle rittenhouse 2021) court tv archives*, https://www.courttv.com/trials/wi-v-rittenhouse-2021/, (Accessed on 07/10/2023).

[297] S. B. A. Press, *Attorneys allege kyle rittenhouse evading being served for civil lawsuit by man he shot*, https://madison.com/news/state-and-regional/crime-and-courts/attorneys-allege-kyle-rittenhouse-evading-being-served-for-civil-lawsuit-by-man-he-shot/article_0aa12b3e-f73b-5c61-ba7b-c3c4aada4dc2.html, (Accessed on 07/10/2023).

[298] E. Casey, *Handbook of digital forensics and investigation*. Academic Press, 2009.

[299] M. Forensics, *Bringing it back with biome data*, https://www.magnetforensics.com/blog/bringing-it-back-with-biome-data, (Accessed on 04/11/2023).

[300] L. J. Donnelly, "The role of geoforensics in policing and law enforcement," *Emergency Global Barclay media Limited*, pp. 19–22, 2010.

[301] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Special Publication*, vol. 10, no. 14, pp. 800–86, 2006.

[302] R. McKemmish, "When is digital evidence forensically sound?" In *IFIP international conference on digital forensics*, Springer, 2008, pp. 3–15.

[303] *Daubert v. merrell dow pharmaceuticals, inc. :: 509 u.s. 579 (1993) :: Justia us supreme court center*, https://supreme.justia.com/cases/federal/us/509/579/, (Accessed on 01/22/2023).

[304] D. B. Garrie, "Digital forensic evidence in the courtroom: Understanding content and quality," *Nw. J. Tech. & Intell. Prop.*, vol. 12, p. i, 2014.

[305] R. Bose and F. Reitsma, "Advancing geospatial data curation," 2006.

[306] G. Vert, M. Stock, P. Jankowski, and P. Gessler, "An architecture for the management of gis data files," *Transactions in GIS*, vol. 6, no. 3, pp. 259–275, 2002.

[307] ESRI, *Arcgis storymaps*, https://storymaps.arcgis.com/, (Accessed on 04/10/2023).

[308] ESRI, *Experience builder system*, https://experience.arcgis.com/page/landing, (Accessed on 4/11/2023).

[309] C. S. Fish, "Elements of vivid cartography," *The Cartographic Journal*, vol. 58, no. 2, pp. 150–166, 2021.

[310] G. N. Peterson, *GIS cartography: a guide to effective map design*. CRC Press, 2020.

[311] ESRI Inc., *Arcgis pro*, version 2.9.0, 2021. [Online]. Available: https://www.esri.com/en-us/arcgis/products/arcgis-pro/overview.

[312] F. Dib, *Regex101: Build, test, and debug regex*, https://regex101.com/, (Accessed on 03/25/2023).

[313] USGS, *Tnm download*, https://apps.nationalmap.gov/downloader/, (Accessed on 01/27/2022), 2019.

[314] C. f. G. I. North Carolina Department of Information Technology Government Data Analytics Center and Analysis., *Contours: 2' interval nc onemap*, https://www.nconemap.gov/datasets/be8005c9ca8e4bfe92246e2a8c2bc03a_0/about, (Accessed on 11/29/2021).

[315] USGS, *Apps*, https://apps.nationalmap.gov/, (Accessed on 04/27/2023).

[316] USGS, *Usgs 3dep viewer*, https://apps.nationalmap.gov/3depdem/, (Accessed on 04/27/2023).

[317] N. F. M. Program, *North carolina spatial data download*, https://sdd.nc.gov/, (Accessed on 04/27/2023).

[318] IPinfo.io, *Dashboard - bulk upload*, https://ipinfo.io/account/bulk-upload, (Accessed on 11/28/2022).

[319] p. NumFOCUS Inc., *Pandas - python data analysis library*, https://pandas.pydata.org/, (Accessed on 03/10/2023).

[320] M. F. Goodchild and L. Li, "Assuring the quality of volunteered geographic information," *Spatial statistics*, vol. 1, pp. 110–120, 2012.

[321] M. F. Goodchild, "The quality of big (geo) data," *Dialogues in Human Geography*, vol. 3, no. 3, pp. 280–284, 2013.

[322] S. K. Wong and S.-M. Yiu, "Location spoofing attack detection with pre-installed sensors in mobile devices.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 11, no. 4, pp. 16–30, 2020.

[323] M. Rogers, "Cyber security & social media: How big is your digital footprint and why should you care," 2016.

[324] B. Stahl, M. Carroll-Mayer, D. Elizondo, K. Wakunuma, and Y. Zheng, "Intelligence techniques in computer security and forensics: At the boundaries of ethics and law," in *Computational Intelligence for Privacy and Security*, Springer, 2012, pp. 237–258.

[325] B. S. Passione and S. A. Robila, "Digital piracy, technology, the legal system and computing education," in *2018 IEEE Integrated STEM Education Conference (ISEC)*, IEEE, 2018, pp. 133–136.

[326] A. Jarrett and K.-K. R. Choo, "The impact of automation and artificial intelligence on digital forensics," *Wiley Interdisciplinary Reviews: Forensic Science*, vol. 3, no. 6, e1418, 2021.

[327] M. Al Fahdi, N. Clarke, and S. Furnell, "Towards an automated forensic examiner (afe) based upon criminal profiling & artificial intelligence," 2013.

[328] T. N. I. for Cybersecurity Careers and S. (NICCS), *Workforce framework for cybersecurity (nice framework)*, https://niccs.cisa.gov/workforce-development/nice-framework?category=Investigate, (Accessed on 05/05/2023).

VITA

Mohammad Meraj Mirza

TECHNICAL SKILLS

Interdisciplinary scientist/researcher with research and development skills and experience in the following areas:

- **Digital Forensics & Incident Response (DFIR):** Arkime, Autopsy - The Sleuth Kit, Belkasoft Evidence Center X, BlackBag, Bulk Extractor, Cellebrite, EnCase, Forensic Toolkit (FTK)®, Ghidra, Kali Linux, Magnet Forensics, Nmap, SANS Workstation - Investigative Forensics Toolkit (SIFT), Security Onion, Snort, Splunk, Tsurugi Linux, Velociraptor, and Volatility.
- **Geographic Information System (GIS):** Data Ops, Database and Operation Management, Digitization, Geographic Profiling, Geoprocessing, Machine Learning (ML), Model Curation & Validation & Deployment, Real-Time Data, Spatial Analysis, 2D & 3D Visualization, and Python.
- **Intelligence:** Criminal Intelligence (CRIMINT), Digital forensic intelligence (DFINT), Geospatial Intelligence (GEOINT), Forensic Intelligence (FROINT), Image Intelligence (IMINT), Intelligence-Led Investigations, Intelligence-Led Policing (ILP), Location Intelligence (LI), Threat Intelligence, Open-Source Intelligence (OSINT).

HONOR SOCIETIES:

- Phi Kappa Phi [2023 - Present]
- Sigma Xi [2023 - Present]

IDENTIFIERS:

- Web of Science ResearcherID: AAV-2793-2021 https://www.webofscience.com/wos/author/rid/AAV-2793-2021

- ORCiD: 0000-0002-1143-3237 https://orcid.org/0000-0002-1143-3237

ACADEMIC MEMBERSHIP AND SERVICES:

- The American Academy of Forensic Science (AAFS) Associate Member Affiliate [2023 - Present]
- CompTIA Community Member [2023 - Present]
- $(ISC)^2$ Candidate [2023 - Present]
- Information Systems Audit and Control Association (ISACA) Member [2023 - Present]
- RSA Conference 2022 Security Scholar
- The American Academy of Forensic Science (AAFS) Student Affiliate [2020 - 2023]
- Institute of Electrical and Electronics Engineers (IEEE) Student Member [2020 - Present]
- Association for Computing Machinery (ACM) Student Member [2020 - Ongoing]
- The Center for Education and Research in Information Assurance and Security (CERIAS) Student Affiliate [2020 - Present]
- Technical Program Committee (TPC) - Association of Digital Forensics, Security and Law (ADFSL) [2022 - Present]
- TPC - of The International Symposium on Digital Forensics and Security (ISDFS) [2021- Present]
- TPC - of International Symposium on Networks, Computers, and Communications (ISNCC) [2021 - Present]
- Reviewer and Editorial & Production Associate - Journal of Digital Forensics, Security and Law (JDFSL) [2021 - Present]

RESEARCH AWARDS AND FUNDING:

- Purdue University - Recipient of Travel Funding for Scholarly Activities - Computer and Information Technology [2022 & 2023]
- Taif University - Researchers Supporting Project number (TURSP-2020/329)

PUBLICATIONS:

- **M. M. Mirza**, A. Ozer, and U. Karabiyik, "Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS," Applied Sciences, vol. 12, no. 21, p. 11180, Nov. 2022, doi: 10.3390/app122111180. [Online]. Available: https://dx.doi.org/10.3390/app122111180
- Hutchinson, S., **Mirza, M. M.**, West, N., Karabiyik, U., Rogers, M., Mukherjee, T., Aggarwal, S., Haeyong, C., and Pettus-Davis, C. "Investigating Wearable Fitness Applications: Data Privacy and Digital Forensics Analysis on Android." Applied Sciences. 2022; 12(19):9747. [Online]. Available: https://doi.org/10.3390/app12199747
- H. Zhu, Y. Peng, H. Xu, F. Tong, X. -Q. Jiang and **M. M. Mirza**, "Secrecy Enhancement for SSK-Based Communications in Wireless Sensing Systems," in IEEE Sensors Journal, vol. 22, no. 18, pp. 18192-18201, 15 Sept.15, 2022, doi: 10.1109/JSEN.2022.3193638. [Online]. Available: https://dx.doi.org/10.1109/JSEN.2022.3193638
- W. Xie, B. Li, Y. Peng, H. Zhu, F. AL-Hazemi, and **M. M. Mirza**, "Secrecy Enhancement for SSK-Based Visible Light Communication Systems," Electronics, vol. 11, no. 7, p. 1150, Apr. 2022, doi: 10.3390/electronics11071150. [Online]. Available: https://dx.doi.org/10.3390/electronics11071150
- Y. Zang, Y. Peng, S. Park, H. Hai, F. AL-Hazemi, and **M. M. Mirza**, "A Novel Cooperative Transmission Scheme in UAV-Assisted Wireless Sensor Networks," Electronics, vol. 11, no. 4, p. 600, Feb. 2022, doi: 10.3390/electronics11040600. [Online]. Available: https://dx.doi.org/10.3390/electronics11040600
- F. E. Salamh, **M. M. Mirza**, S. Hutchinson, Y. H. Yoon and U. Karabiyik, "Whats on the Horizon? An In-Depth Forensic Analysis of Android and iOS Applications,"

in IEEE Access, vol. 9, pp. 99421-99454, 2021, doi: 10.1109/ACCESS.2021.3095562. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3095562

- M. Stankovi, **M. M. Mirza**, and U. Karabiyik, "UAV Forensics: DJI Mini 2 Case Study," Drones, vol. 5, no. 2, p. 49, Jun. 2021, doi: 10.3390/drones5020049. [Online]. Available: https://dx.doi.org/10.3390/drones5020049

- F. E. Salamh, **M. M. Mirza**, and U. Karabiyik, "UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies," Electronics, vol. 10, no. 6, p. 733, Mar. 2021, doi: 10.3390/electronics10060733. [Online]. Available: https://dx.doi.org/10.3390/electronics10060733

- **M. M. Mirza** and U. Karabiyik, "Enhancing IP Address Geocoding, Geolocating and Visualization for Digital Forensics," 2021 International Symposium on Networks, Computers, and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-7, doi: 10.1109/ISNCC52172.2021.9615668. [Online]. Available: https://doi.org/10.1109/ISNCC52172.2021.9615668

- **M. M. Mirza**, F. E. Salamh and U. Karabiyik, "An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116192. [Online]. Available: https://doi.org/10.1109/ISDFS49300.2020.9116192

EXTENDED ABSTRACT PUBLICATIONS:

- **Mohammad Meraj Mirza**; Rwitam Bandyopadhyay; Akif Ozer; Bharath Vemula; Umit Karabiyik; and Marcus Rogers, "Escaping the Monolithic Architecture for Digital Forensics and Incident Response Systems Using a Microservices Approach" Digital & Multimedia Sciences at the 2023 AAFS Annual Meeting.

- **Mohammad Meraj Mirza**, Akif Ozer, and Umit Karabiyik "Cyber Forensic Investigations of Web3 Cryptocurrency Wallets on iOS and Android" Digital & Multimedia Sciences at the 2023 AAFS Annual Meeting.

- **Mohammad Meraj Mirza** and Umit Karabiyik, "Skills for Success: Advancing Pattern of Life Analysis in Cyber Forensics Using a Multidimensional Approach" Abstract in the Digital & Multimedia Sciences at the 2022 AAFS Annual Meeting.

- **Mohammad Meraj Mirza** and Umit Karabiyik, "A Holistic Framework for Investigating Geospatial Data in Cyber Forensics" Abstract in the Digital & Multimedia Sciences at the 2021 AAFS Annual Meeting.

POSTERS:

- Akif Ozer, **Mohammad Meraj Mirza**, and Umit Karabiyik "Cyber Forensics Investigation of Web3 Wallets" at the 24th annual CERIAS Security Symposium [March 2023]. Available https://www.cerias.purdue.edu/symposium/index.php/posters/year/2023/678-1DF

- Shinelle Hutchinson, **Mohammad Meraj Mirza**, and Umit Karabiyik, "The Health of Wearables Investigations" at Purdue Polytechnic Student Poster Symposium 2022.

- **Mohammad Meraj Mirza** and Umit Karabiyik, "Integrating Cybersecurity, Cyber Forensics, Cyber Threat Intelligence, and Geospatial Technologies and Techniques into a multidisciplinary approach allowed us to better understand the present gaps and limitations of defense systems against emerging air-breathing threats" at RSAC Security Scholar Poster Boards [June 2022]

- **Mohammad Meraj Mirza** and Umit Karabiyik, "Using Red & Blue Team Exercises to Highlight Challenges, Gaps, and Deficiencies in Defense Systems Capabilities Against Emerging Air Threats [845-371]" at the 23rd annual CERIAS Security Symposium [March 2022]. Available https://www.cerias.purdue.edu/symposium/index.php/posters/year/2022/845-371

- **Mohammad Meraj Mirza** and Umit Karabiyik, "Evaluation of GPS EXIF Data Reporting for Digital Forensics Tools" at the 21st annual CERIAS Security Symposium [September 2020]. Available https://www.cerias.purdue.edu/assets/symposium/2020-posters/9BB-E39.pdf