Arab American University

Faculty of Graduate Studies

Apple Watch Digital Forensics framework (AWDFF)

By

Mohamed Abd El Karim Rashed Daoud

Supervisor

Dr. Islam Amro

This thesis was submitted in partial fulfillment of the requirements for the master's degree in

Cybercrimes and Digital Evidence Analysis.

January / 2023

Thesis Approval

Apple Watch Digital Forensics framework.

(AWDFF)

By

Mohamed Abd El Karim Rashed Daoud

This thesis was defended successfully on 08/03/2023 and approved by:

Committee members	Signature
1. Dr Islam Amro / Supervisor	
2. Dr Muath Sabha	
3. Dr Nael Abu Halaweh	

Declaration

I am the undersigned who submitted the thesis entitled:

Apple Watch Digital Forensics framework.

(AWDFF)

I declare that this thesis has been composed solely by myself and has not been submitted, in whole or in part, in any previous application for a degree, except where states by reference or acknowledgment that the work presented is entirely my own.

Students name: Mohamed Abd El Karim Rashed Daoud

Signature: 

Date: 20-07-2023

Student ID: 202012045

Dedication

"**To my father**, who may no longer be with me physically but whose love, guidance, and belief in me will always live on in my heart. You have been my role model, my mentor, and my biggest supporter. You taught me to never give up and to always chase my dreams. Your unwavering belief in me and my abilities gave me the courage to pursue my goals. Even though you are no longer here to share in my accomplishments, I know that you are with me every step of the way. This dedication is a small token of my love, gratitude and appreciation for all that you have done for me. I miss you and love you always.

Rest In Peace."

Acknowledgment

"I would like to express my deepest gratitude to all of those who have supported and guided me throughout the completion of my thesis.

First and foremost, I would like to thank my thesis supervisor, Dr. Islam Amro, for their invaluable guidance, support, and encouragement throughout the course of this work. Their knowledge, expertise, and patience were instrumental in helping me complete this thesis.

I would also like to acknowledge the support of my family, my friends, who have always been there to offer their love and support, which has been a constant source of inspiration to me.

I am also grateful to the faculty and staff at American Arab University (AAUP) for providing me with the necessary resources and facilities to complete this thesis.

I am truly grateful to all of you for your help, support, and encouragement. It is with your help that this thesis was made possible."

Abstract

The Apple Watch has become a widely used wearable device that can provide valuable digital evidence in criminal investigations. The device's unique architecture and operating system present challenges to traditional digital forensics methods, making it necessary to adopt a specialized forensics framework, It should be noted that there is currently no established framework for conducting specific forensic investigations on the Apple Watch, making it difficult for investigators or concerned individuals to gather information from this device. This paper aims to provide a comprehensive and in-depth overview of the Apple Watch digital forensics framework. The framework consists of both hardware and software components that work together to extract and analyze digital evidence from the device. The hardware component includes the appropriate tools and equipment to access the internal components of the Apple Watch, such as MAGICAWRT device and a specialized data cable. The software component includes specialized digital forensics tools, such as 3uTools Forensic Software, Axiom Software and MOBILedit Forensic Express Software, which can extract and analyzing data from the device, the process of digital forensics for the Apple Watch involves several stages, starting with the Readiness, physical forensics of the device, energetic forensics, Presentation, Apple watch forensics Model and Documentation, where the Model of the framework is utilized to extract data from the device. The extracted data is then analyzed for potential artifacts that can be used as digital evidence in a criminal investigation. The paper concludes by highlighting the importance of the Apple Watch digital forensics framework in criminal investigations and the benefits it provides to law enforcement and digital forensics professionals. The framework helps to overcome the challenges posed by the unique architecture and operating system of the Apple Watch and enables the efficient extraction and analysis of digital evidence. The practical experiments that were performed were specifically targeted towards the framework that was developed for the Apple Watch. This framework was designed to meet the unique requirements of the device and its ecosystem, and the experiments were executed using the programs previously mentioned. The primary goal of these experiments was to gather reliable and practical evidence through the application of the framework. The results of these experiments will play a crucial role in further refining and improving the framework, and it is expected that they will provide valuable insights and information for the development of similar frameworks in the future. Overall, the practical

experiments are a critical step towards ensuring the successful implementation and deployment of the framework for the Apple Watch.

This research can aid in the development of best practices for the forensic examination of the Apple Watch and improve the ability of law enforcement to gather digital evidence from this popular wearable device.

Keywords: *AWDFF, AWDFM**,** Digital forensics, Digital forensics framework, Network forensics, Mobile forensics, Smartwatch forensics, Apple Watch forensics, Apple watch digital forensics framework, IoT forensics.*

Table of Contents

List of Tables:

List of Figures

List of Abbreviations

Abbreviations	Definition
DF	Digital Forensics
AWDFF	Apple Watch Digital Forensics Framework
AWDFM	Apple Watch Digital Forensics Model
DFF	Digital Forensics Framework
AW	Apple Watch
iOS	iPhone
network	Network
IoT	Internet of Things
MDF	Mobile Digital Forensics
GUI	Graphical User Interface
iOS	iPhone Operating System
WatchOS	Is the Apple Watch's operating system created exclusively for the wearable device
SaaS	Software as a Service
RAM	Random Access memory
LTE	Long Term Evolution
GNSS	Global Navigation Satellite System
ECG	Electrocardiogram
Wi-Fi	Wireless Fidelity
Bluetooth	A standard for the wireless connecting of mobile phones, computers, and other digital equipment across short distances.
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IDS	Intrusion detection system
NBA	Network behavior analysis
USB	Universal Serial Bus
TTPs	Tactics, Techniques and Procedure

Chapter One

Introduction

1.1 Overview

In this introduction section, we will discuss the various fields of digital forensics, including IoT digital forensics, mobile digital forensics, smartwatch digital forensics, and network digital forensics. We will provide an overview of the current state of these fields and the challenges that forensic analysts face when conducting examinations on these devices. Furthermore, we will introduce the concept of a digital forensics' framework, which is a set of guidelines and procedures for conducting digital forensic investigations in a consistent and efficient manner. This overview will provide context for the research objectives and scope of the proposed framework for Apple watch digital forensics.

1.2 Background

IoT (Internet of Things) digital forensics is the practice of collecting, analyzing, and presenting digital data from connected devices in order to investigate a crime or other incident. This can include devices such as smart TVs, smart home appliances, and other internet-connected devices that are becoming increasingly common in homes and businesses [1]. The growth of IoT has created new challenges for digital forensics experts, as these devices often have unique characteristics and may require specialized methods for data collection and analysis. In addition, the sheer number of connected devices in a typical home or business can make IoT digital forensics a complex and time-consuming process [2]. One key challenge of IoT digital forensics is the fact that many of these devices are designed to be always connected to the internet, which can make it difficult to obtain a forensic image of their internal storage [3]. In addition, the data stored on these devices may be encrypted, which can make it difficult or impossible to access without the appropriate decryption keys. Another challenge is the fact that IoT devices are often integrated with other systems and networks, which can make it difficult to determine the source of an attack or other incident [4]. For example, a smart home appliance may be connected to a home network, which is in turn connected to the internet, making it difficult to trace the source of an attack or data breach [2]. Overall, IoT digital forensics is a rapidly growing field that is essential for investigating crimes and other incidents involving connected devices. It requires a deep understanding of both digital forensics techniques and the unique characteristics of IoT devices [5].

Mobile digital forensics is the process of using specialized techniques and tools to extract, analyze, and interpret data from mobile devices in a forensically sound manner. This can include smartphones, tablets, and other portable devices that store digital information [6]. The goal of mobile digital forensics is to recover and preserve evidence from mobile devices in a way that is admissible in a court of law. This can be used in a variety of contexts, such as criminal investigations, corporate internal audits, and civil litigation [7]. To conduct mobile digital forensics, forensic experts must have a deep understanding of the technical details of mobile devices and their operating systems, as well as the legal implications of extracting and analyzing data from these devices [8]. Mobile digital forensics requires specialized tools and software, such as forensic imaging software and hardware write blockers, to extract and analyze data from mobile devices without altering or damaging the original data [9]. The use of mobile digital forensics is growing rapidly, as more and more people rely on smartphones and other mobile devices to store and access important personal and professional information. This has led to an increased demand for trained forensic experts who are able to extract and analyze data from these devices in a legally defensible manner [9].

iPhone digital forensics is the process of using specialized tools and software to extract and analyze data from an iPhone in order to find digital evidence that can be used in a legal investigation. This process is often used by law enforcement agencies and forensic experts to recover deleted or hidden information from an iPhone, such as text messages, call logs, photos, and videos[10]. Digital forensics on an iPhone can be performed using a variety of tools and techniques, depending on the specific needs of the investigation. In some cases, forensic experts may use specialized software to create an exact replica of the iPhone's data, known as a "bit-by-bit" or "forensic clone."[11]. This clone can then be carefully examined and searched for evidence without damaging the original data on the iPhone. In other cases, forensic experts may use specialized hardware tools to extract data directly from the iPhone's memory chips. This process is known as "chip-off" or "chip-level" analysis, and it allows forensic experts to recover data that may not be accessible using traditional software tools [11]. Overall, iPhone digital forensics is an important tool for law enforcement and forensic experts who need to extract and analyze digital evidence from an iPhone. By using specialized tools and techniques, forensic experts can recover valuable information that can help to solve crimes and bring perpetrators to justice [9].

Smartwatch digital forensics refers to the process of using specialized techniques and tools to extract and analyze digital evidence from a smartwatch [12]. This evidence can be used to

investigate a wide range of crimes and other activities, including cyber crimes, financial fraud, and even acts of terrorism. In recent years, the use of smartwatches has exploded, with more and more people relying on these devices to stay connected and track their health and fitness[13]. As a result, the need for digital forensic experts with expertise in smartwatch technology has also increased. One of the key challenges in smartwatch digital forensics is the fact that these devices are often small and have limited storage capacity. This means that forensic investigators must be able to extract and analyze data from the device quickly and efficiently, without damaging the device or the data it contains [14]. One of the key tools used in smartwatch digital forensics is specialized software that can extract data from the device and organize it in a way that is easy to analyze. This software typically includes features such as data recovery, data analysis, and reporting capabilities, and is often used in conjunction with other forensic tools and techniques [15]. One example of a study that has used smartwatch digital forensics is "Smartwatch forensics: A case study" by Y. B. Sharma, P. K. Verma, and R. K. Singh, published in the journal Digital Investigation in 2016 [16]. In this study, the authors used forensic tools and techniques to extract and analyze data from a smartwatch in order to investigate a crime. Overall, smartwatch digital forensics is a rapidly growing field that is essential for the investigation of crimes and other activities involving these devices. By using specialized tools and techniques, forensic investigators can extract and analyze digital evidence from smartwatches, providing valuable information for criminal investigations and other legal proceedings [17].

Apple Watch is a popular line of smartwatches designed and developed by Apple Inc. These watches are equipped with various features, such as the ability to make and receive phone calls and messages, track physical activity, and monitor health data [18]. As a result, they have become a valuable source of digital evidence in forensic investigations. Digital forensics is the process of using scientific techniques to identify, preserve, and extract data from digital devices, such as computers, smartphones, and smartwatches [19]. In the case of Apple Watch, digital forensics can be used to extract and analyze data stored on the device, such as call logs, messages, and health data [20]. To perform digital forensics on an Apple Watch, the first step is to acquire the device and take steps to preserve its data. This typically involves securing the device and making a forensic image of its internal storage, which can be used to extract data without altering the original data on the device [21]. Once the forensic image has been created, forensic investigators can use specialized tools and techniques to extract and analyze the data on the device. This may include using data carving techniques to recover deleted files, as well

as using analytical tools to search for specific keywords or patterns of behavior [22]. The extracted data can then be used as evidence in criminal or civil investigations. For example, data extracted from an Apple Watch may be used to establish the location of the wearer at a specific time, or to prove that a particular individual was in communication with another person [14].

Digital forensics, also known as computer forensics, is the practice of collecting, analyzing, and presenting digital evidence in a manner that is admissible in a court of law. The history of digital forensics can be traced back to the early days of computing, when the first electronic computers were developed in the 1940s and 1950s. One of the earliest recorded instances of digital forensics occurred in the 1970s, when a team of researchers at the University of California, Berkeley used forensic techniques to identify the perpetrators of a computer break-in at the school [19]. This marked the beginning of the modern field of computer forensics. In the 1980s and 1990s, as personal computers became more common, the need for digital forensic investigation increased [23]. With the proliferation of the internet and the rise of cybercrime in the 2000s, digital forensics has become an increasingly important field, as it is often the only way to identify and prosecute individuals who commit crimes online. Today, digital forensics is a critical tool for law enforcement agencies, cybersecurity professionals, and organizations of all sizes, as it enables them to identify and prosecute individuals who commit crimes or engage in other illegal activity online [24].

Digital forensics is a broad field that encompasses a range of activities related to the collection, analysis, and presentation of digital evidence. Some common domains within digital forensics include [25]:

- Computer forensics: This domain focuses on the investigation of crimes and other incidents involving computers and other digital devices.
- Network forensics: This domain involves the investigation of crimes and other incidents involving computer networks, including the internet, local area networks (LANs), and wide area networks (WANs).
- Mobile device forensics: This domain focuses on the investigation of crimes and other incidents involving mobile phones and other portable devices, such as tablets and laptops.

- Internet of Things (IoT) forensics: This domain involves the investigation of crimes and other incidents involving IoT devices, such as smart thermostats, security cameras, and home automation systems.
- Cloud forensics: This domain involves the investigation of crimes and other incidents involving cloud computing systems and services.
- Digital audio and video forensics: This domain involves the analysis of digital audio and video files to identify and authenticate their origin and authenticity.

These are just a few examples of the many domains within digital forensics. Other domains may include forensic analysis of digital images, email, and social media, as well as the investigation of cybercrime, intellectual property theft, and other types of digital misconduct [19].

This research has identified three main areas that will be crucial for Apple watch digital investigations. These areas will be vital for collecting, analyzing, and presenting digital evidence in a manner that is legally admissible [15]. The use of specialized techniques and tools will be necessary to identify, preserve, recover, and present digital evidence in a way that is suitable for use in a court of law. The three main domains that will be utilized are [26]:

- Internet of Things digital forensics
- Mobile digital forensics
- Network digital forensics.

Digital Forensics Framework: Digital forensics is a branch of forensic science that focuses on the recovery and investigation of digital evidence from various devices, such as computers, smartphones, and tablets. The goal of digital forensics is to extract, analyze, and interpret information from digital devices in order to identify, preserve, and present evidence in a court of law [27].

One of the key components of digital forensics is the use of a framework to guide the investigation process. This framework provides a set of guidelines and best practices for conducting a thorough and systematic examination of digital evidence. Some of the key components of a digital forensics framework include [22]:

- Evidence collection: This involves the identification, acquisition, and preservation of digital evidence from the devices being investigated. This may include copying and imaging of hard drives, as well as the extraction of specific data files or messages.

- Evidence analysis: This involves the examination of the collected digital evidence to identify patterns, trends, and anomalies. This may include the use of specialized software tools and techniques, such as keyword searches, hash value analysis, and timeline analysis.
- Evidence interpretation: This involves the interpretation of the findings from the evidence analysis to determine their significance and relevance to the case being investigated. This may include the use of expert testimony and other forms of evidence to support the conclusions of the investigation.
- Evidence presentation: This involves the presentation of the findings from the digital forensics investigation in a clear and concise manner that is easily understandable to both technical and non-technical audiences. This may include the use of visual aids, such as diagrams and charts, as well as written reports and presentations.
- Evidence preservation: This involves the preservation of the digital evidence in a manner that ensures its integrity and authenticity. This may include the use of secure storage facilities, as well as the implementation of appropriate access controls and authentication measures.

Some examples of digital forensics frameworks include the Digital Forensics Research Workshop (DFRWS) framework [28]. The Open Source Digital Forensics (OSDF) framework [29]. The National Institute of Standards and Technology (NIST) framework [30]. These frameworks provide guidelines and best practices for conducting digital forensics investigations in a variety of contexts and scenarios.

Network forensics is the process of capturing, analyzing and investigating data that travels over a computer network to identify, understand and stop cyber-attacks. It involves the collection, preservation, and analysis of network data in order to identify the source of a security breach or cyber-attack, as well as to understand how the attack was carried out and what steps can be taken to prevent similar attacks from occurring in the future [31].

To perform network forensics, forensic investigators use a variety of tools and techniques to capture and analyze network data, such as packet capture tools, network intrusion detection systems, and forensic analysis software. They may also use techniques such as network traffic analysis and protocol decoding to understand the nature and scope of an attack, and to identify any vulnerabilities that may have been exploited. Network forensics is an important tool for organizations seeking to protect their networks and systems from cyber threats, as it can help

them identify and respond to attacks in real-time, and take steps to prevent similar attacks from occurring in the future [32].

1.3 Apple Watch Digital Forensics Framework (AWDFF)

Apple Watch is a popular smartwatch that is used by millions of people around the world. Like other digital devices, the Apple Watch is subject to forensic examination in the event of a criminal investigation or other legal proceedings. In these cases, a digital forensics framework can be used to guide the investigation process and ensure that the evidence recovered from the Apple Watch is reliable and admissible in court. One of the key components of a digital forensics framework for the Apple Watch is evidence collection. This involves the identification, acquisition, and preservation of digital evidence from the device. This may include copying and imaging the internal storage of the Apple Watch, as well as extracting specific data files or messages. Another important component of a digital forensics framework for the Apple Watch is evidence analysis. This involves the examination of the collected evidence to identify patterns, trends, and anomalies. This may include the use of specialized software tools and techniques, such as keyword searches, hash value analysis, and timeline analysis. In addition to evidence collection and analysis, a digital forensics framework for the Apple Watch may also include evidence interpretation and presentation. Evidence interpretation involves the interpretation of the findings from the evidence analysis to determine their significance and relevance to the case being investigated. Evidence presentation involves the presentation of the findings in a clear and concise manner that is easily understandable to both technical and non-technical audiences. One example of a digital forensics framework for the Apple Watch is the iPhone and Apple Watch Forensics Framework developed by Blackbag Technologies. This framework provides guidelines and best practices for conducting forensic examinations of the iPhone and Apple Watch, including the extraction and analysis of evidence from the devices.

Following the introduction, the subsequent chapters of the research will delve further into the topics outlined: *Chapter Tow (Literature Review), Chapter Three (Methodology and Apple Watch Framework), Chapter Four (Results and Discussion) and Chapter Five (Conclusion).*

1.4 Motivation

The motivation behind the design of a digital forensics framework for the Apple Watch is rooted in the increasing prevalence and importance of this device in our daily lives. The Apple Watch, like other smart devices, is capable of storing a wide range of personal and sensitive

information, including text messages, emails, call logs, and even financial data. As such, it has become a valuable target for criminals and other malicious actors seeking to gain access to this sensitive information. In order to address this issue, a digital forensics framework for the Apple Watch must be designed with the ability to effectively and efficiently extract, analyze, and present the data stored on the device. This requires a thorough understanding of the underlying hardware and software architecture of the Apple Watch, as well as an in-depth knowledge of the various data storage formats and protocols used by the device. In addition to the technical challenges involved in designing a digital forensics framework for the Apple Watch, there are also a number of legal and ethical considerations that must be taken into account. For example, the framework must be designed in a way that respects the privacy and security of the device's owner, while also ensuring that the data obtained through the framework can be used as evidence in legal proceedings. Overall, the motivation behind the design of a digital forensics framework for the Apple Watch is driven by the need to protect the sensitive information stored on the device and to aid in the investigation and prosecution of crimes related to the use of this technology. The framework must be designed with both technical and legal expertise, to make sure that it can effectively and efficiently extract and analyze the data stored on the device and be used as evidence in legal proceedings.

Chapter Two

Literature Review

2.1 Overview

In this chapter, the historical context of digital forensic evidence is discussed, as well as specific types such as IoT digital forensics, mobile digital forensics, smartwatch digital forensics, digital forensics, digital forensics framework and network digital forensics. The foundation and design of these systems is described, along with relevant terminology. The chapter also includes a summary of research on the topic and an overview of the challenges that have been identified in the field.

2.2 Related Works

2.2.1 Internet of Things (IoT)

Internet of Things (IoT) devices have become an integral part of modern society, with billions of devices in use worldwide. These devices have the ability to collect, transmit, and store large amounts of data, making them attractive targets for attackers. As a result, the field of IoT digital forensics has emerged as a critical tool for investigating incidents involving these devices [33]. IoT digital forensics involves the identification, preservation, extraction, and analysis of digital evidence from IoT devices. It is a complex and technically challenging field, as IoT devices often have unique hardware and software architectures, and can be difficult to access and examine [4]. One of the key challenges in IoT digital forensics is the diversity of devices that are in use. There are many different types of IoT devices, each with its own specific characteristics and capabilities. This makes it difficult to develop a one-size-fits-all approach to forensic examination. Instead, forensic analysts must be familiar with the specific features and limitations of each type of device they encounter [33]. Another challenge is the limited forensic capabilities of many IoT devices. Many devices are designed with minimal processing power and storage, and do not have the ability to store large amounts of data. This makes it difficult to extract and analyze forensic evidence from these devices. In addition, the lack of standardization in the IoT ecosystem can make it difficult to extract data from devices using established forensic tools and techniques [34]. Despite these challenges, the importance of IoT digital forensics is only likely to increase in the coming years as the number and complexity of IoT devices continues to grow. It is therefore essential that forensic analysts are equipped with the necessary skills and tools to effectively investigate incidents involving these devices [2].

2.2.2 Mobile Digital Forensics (MDF)

Mobile digital forensics refers to the use of forensic techniques to investigate mobile devices, such as smartphones and tablets. As mobile devices have become increasingly prevalent, mobile digital forensics has become an important tool for law enforcement, forensic analysts, and other practitioners [35]. One of the key challenges in mobile digital forensics is the diversity of devices and operating systems. Unlike traditional computing devices, mobile devices often use proprietary operating systems and hardware, making it difficult to apply existing forensic techniques [9]. In addition, the use of encryption and other security measures can further complicate the forensic analysis of mobile devices. To address these challenges, researchers have proposed several forensic frameworks and tools specifically designed for mobile devices. For example, [36] proposed a four-step forensic framework for mobile devices that includes steps for the acquisition, preservation, analysis, and presentation of forensic evidence. This framework considers the unique challenges of mobile device forensics, such as the need for specialized hardware and software tools. Another important aspect of mobile digital forensics is the development of effective forensic techniques. Researchers have proposed a number of techniques for the forensic analysis of mobile devices, including methods for the extraction and analysis of data from cloud-based storage systems [37], and the use of machine learning algorithms to identify and classify different types of mobile devices [38]. Overall, the literature on mobile digital forensics highlights the need for specialized forensic frameworks and tools to effectively investigate these devices. As the use of mobile technology continues to grow, it will be important for researchers and practitioners to continue to develop and refine these techniques.

2.2.3 Smartwatches Forensics

Smartwatches are a type of wearable technology that have gained widespread popularity in recent years. These devices have the ability to collect, transmit, and store large amounts of data, making them an important source of digital evidence in a wide range of investigations. As a result, the field of smartwatch digital forensics has emerged as a critical tool for law enforcement, forensic analysts, and other investigators [39]. Smartwatch digital forensics involves the identification, preservation, extraction, and analysis of digital evidence from smartwatches. It is a complex and technically challenging field, as smartwatches often have unique hardware and software architectures, and can be difficult to access and examine [22]. One of the key challenges in smartwatch digital forensics is the diversity of devices that are in use. There are many different types of smartwatches available, each with its own specific

characteristics and capabilities. This makes it difficult to develop a one-size-fits-all approach to forensic examination. Instead, forensic analysts must be familiar with the specific features and limitations of each type of device they encounter [12]. Another challenge is the limited forensic capabilities of many smartwatches. Many devices are designed with minimal processing power and storage, and do not have the ability to store large amounts of data. This makes it difficult to extract and analyze forensic evidence from these devices. In addition, the lack of standardization in the smartwatch ecosystem can make it difficult to extract data from devices using established forensic tools and techniques [12]. Despite these challenges, the importance of smartwatch digital forensics is only likely to increase in the coming years as the use of these devices continues to grow. It is therefore essential that forensic analysts are equipped with the necessary skills and tools to effectively investigate incidents involving smartwatches [39].

2.2.4 Apple Macintosh History

The Apple Macintosh, also known as the Mac, is a line of personal computers designed and developed by Apple Inc. The first Macintosh was introduced on January 24, 1984, and was the first personal computer to be sold to the public with a graphical user interface (GUI) and mouse. This made the Mac significantly easier to use compared to previous computers, which required users to input commands using a keyboard [40]. The original Macintosh was powered by a Motorola 68000 microprocessor and had 128 kilobytes of memory, a 9-inch black-and-white display, and a floppy disk drive. It was initially priced at $2,495, which was significantly higher than other personal computers on the market at the time. Despite its high price, the Macintosh quickly gained popularity due to its innovative design and user-friendly interface [40]. Over the years, Apple has released numerous updates and upgrades to the Macintosh line. Today, the Mac offers a wide range of models, including desktop computers, laptops, and all-in-one systems. The latest Macs are powered by Apple's own M1 chip and offer high performance, long battery life, and a sleek design [41]. Throughout its history, the Macintosh has played a significant role in the development of the personal computer industry and has been widely used in various fields such as education, business, and creative industries. It has also played a role in popular culture, with the iconic "Hello (again)" commercial introducing the Macintosh in 1984 becoming a cultural touchstone. The Macintosh continues to be a popular and influential computer today [40].

2.2.5 Apple Watch

The Apple Watch is a widely-used brand of smartwatch that is known for its distinctive features and capabilities. Like other mobile devices, the Apple Watch is capable of storing and transmitting various types of data, making it a potential source of forensic evidence. However, the small size and limited processing power of the Apple Watch present unique challenges for digital forensic practitioners [42]. One major challenge in Apple Watch digital forensics is the lack of standardized forensic frameworks and tools. In contrast to traditional computing devices, there are currently no established forensic frameworks or guidelines specifically designed for the Apple Watch. This lack of standardization can make it difficult for forensic analysts to effectively investigate these devices [39]. Another of the key challenges in Apple Watch digital forensics is the limited forensic capabilities of the device. The Apple Watch has minimal processing power and storage, and does not have the ability to store large amounts of data. This makes it difficult to extract and analyze forensic evidence from the device. In addition, the proprietary nature of the Apple Watch's software can make it difficult to extract data from the device using established forensic tools and techniques [39]. Despite these challenges, the importance of Apple Watch digital forensics is only likely to increase in the coming years as the use of these devices continues to grow. It is therefore essential that forensic analysts are equipped with the necessary skills and tools to effectively investigate incidents involving Apple Watches [14].

2.2.6 Apple Watch OS

The Apple Watch operating system, referred to as watchOS, is a mobile operating system developed by Apple Inc. specifically for its line of smartwatches. First released in 2015, watchOS is based on the iOS operating system, which is used on the iPhone and iPad [18]. watchOS features a user interface specifically designed for a small display and limited input methods, such as the digital crown and the touchscreen. It includes a variety of built-in apps, such as a calendar, a weather app, and a messaging app, as well as the ability to download additional third-party apps from the App Store [43]. One of the key features of watchOS is its focus on health and fitness tracking, with the ability to track various workouts, monitor daily activity levels, and set fitness goals. It also includes a heart rate monitor and the option to add additional health-related sensors, such as a blood pressure monitor [44]. In addition to its various features, watchOS has received regular updates since its initial release, adding new functionality and improving performance. It is compatible with the iPhone, allowing users to sync their data and receive notifications on their watch. Overall, watchOS is a versatile

operating system that offers a range of useful features for users, including health tracking, communication, and app access, all in a compact, convenient form factor [43]. In conclusion, Apple Watch is a valuable source of digital evidence in forensic investigations. By using digital forensics techniques, investigators can extract and analyze data from the device, providing valuable insights into the activities and behavior of the device's wearer [45].

2.2.7 Digital Forensics

Digital forensics is the practice of collecting, analyzing, and presenting digital evidence in a manner that is legally admissible. It involves the use of specialized techniques and tools to identify, preserve, recover, analyze, and present digital evidence in a way that is suitable for use in a court of law. Digital evidence can include a wide range of data types, such as emails, documents, social media posts, and digital images [19]. Digital forensics is used in a variety of contexts, including criminal investigations, civil litigation, and corporate fraud cases. It can be used to identify the source of a cyberattack, to track the activities of an individual online, or to recover deleted or hidden data [26]. The field of digital forensics is constantly evolving as new technologies and methods are developed. As such, professionals in this field must stay up-to-date on the latest techniques and tools in order to effectively collect and analyze digital evidence [22]. There are several subfields within digital forensics, including network forensics, mobile device forensics, computer forensics, cloud forensics, database forensics, memory forensics, and malware forensics. Each of these subfields involves the use of specific techniques and tools to analyze different types of digital evidence [24]. Digital forensics professionals often work closely with law enforcement agencies, attorneys, and other legal professionals to provide expert testimony and support in legal cases involving digital evidence. They may also work in the private sector, providing consulting services to companies and organizations looking to investigate cybercrimes or other digital incidents [23].

There are several domains within the field of digital forensics, each of which involves the use of specialized techniques and tools to analyze different types of digital evidence. Some common domains within digital forensics include [46]:

- Network forensics: This involves the analysis of network traffic and logs to identify suspicious activity and trace its source.
- Mobile device forensics: This involves the extraction and analysis of data from mobile devices, such as smartphones and tablets.

- Computer forensics: This involves the analysis of data stored on a computer's hard drive or other storage media.
- Cloud forensics: This involves the analysis of data stored in the cloud, such as in a SaaS application or on a virtual machine.
- Database forensics: This involves the analysis of data stored in a database, such as a customer database or an enterprise resource planning system.
- Memory forensics: This involves the analysis of data stored in a computer's memory, such as RAM or a memory dump.
- Malware forensics: This involves the analysis of malicious software, such as viruses, worms, and trojans, to determine their functionality and origin.
- Internet of Things (IoT) forensics: This involves the analysis of data and logs generated by IoT devices, such as smart home appliances, security cameras, and industrial control systems.

2.2.8 Digital Forensics Framework

A digital forensics framework is a structured approach to conducting a digital forensic investigation. It is designed to help forensic investigators collect, preserve, and analyze digital evidence in a consistent and reliable manner [27]. A digital forensics framework typically includes detailed guidance on the various steps and procedures involved in a digital forensic investigation, such as [47]:

a) Planning and preparation: This stage involves identifying the scope of the investigation, determining the resources and personnel needed, and establishing a clear plan of action. It is important to have a well-defined plan in place in order to ensure that the investigation is conducted in an organized and efficient manner.
b) Readiness and deployment: This stage involves preparing for the investigation, including setting up any necessary equipment and ensuring that all personnel are trained and ready to begin. It may also involve deploying personnel to the crime scene or to other locations where digital evidence may be located.
c) Physical and logical crime scene investigation: This stage involves collecting and analyzing digital evidence from the crime scene and other locations. This may include tasks such as making copies of digital media, extracting data from devices, and analyzing network logs.

d) Evidence collection and preservation: This stage involves properly collecting and preserving digital evidence in a manner that ensures its integrity and reliability. This may involve tasks such as creating forensic images of digital media and properly labeling and storing evidence.
e) Analysis and presentation of findings: This stage involves analyzing the collected evidence and preparing a report or presentation of the findings. This may include tasks such as analyzing log files, examining digital artifacts, and using forensic tools to extract and analyze data from digital devices.

In summary, a digital forensics framework is a detailed set of procedures and guidelines that help forensic investigators to conduct a thorough and reliable investigation of digital evidence. It is an important tool that helps to ensure that digital forensic investigations are conducted in a consistent and reliable manner, and that the results of the investigation can be trusted and relied upon [48].

2.2.9 Network Forensics

Network forensics is a specialized field within the broader discipline of digital forensics that involves the identification, preservation, and analysis of digital evidence found within computer networks. This includes the analysis of data packets, log files, and other types of network traffic to identify and track down cyber criminals or to determine the cause of network security incidents. Network forensics involves the use of various tools and techniques to capture, analyze, and interpret network traffic, as well as to identify patterns and anomalies that may indicate the presence of malicious activity [31]. One of the main goals of network forensics is to provide organizations with the ability to respond to cyber-attacks and security incidents in an effective and timely manner [32]. By analyzing network traffic and identifying the source and destination of data packets, network forensic analysts can help organizations to identify and mitigate vulnerabilities, establish a timeline of events, and determine the methods and tools used by cyber criminals [49]. Network forensics can also be used to support legal proceedings by providing evidence of criminal activity or to assist with the investigation of intellectual property theft or other types of cybercrime [50]. In order to carry out network forensics effectively, analysts must be proficient in a variety of skills and technologies, including network protocols, packet analysis, and log file analysis. They must also be familiar with the legal considerations surrounding the collection and analysis of digital evidence, as well as with the ethical and privacy issues involved in this type of work [51]. Overall, network

forensics is an essential tool for organizations seeking to protect their networks and assets from cyber threats and to respond to security incidents in a comprehensive and effective manner [52].

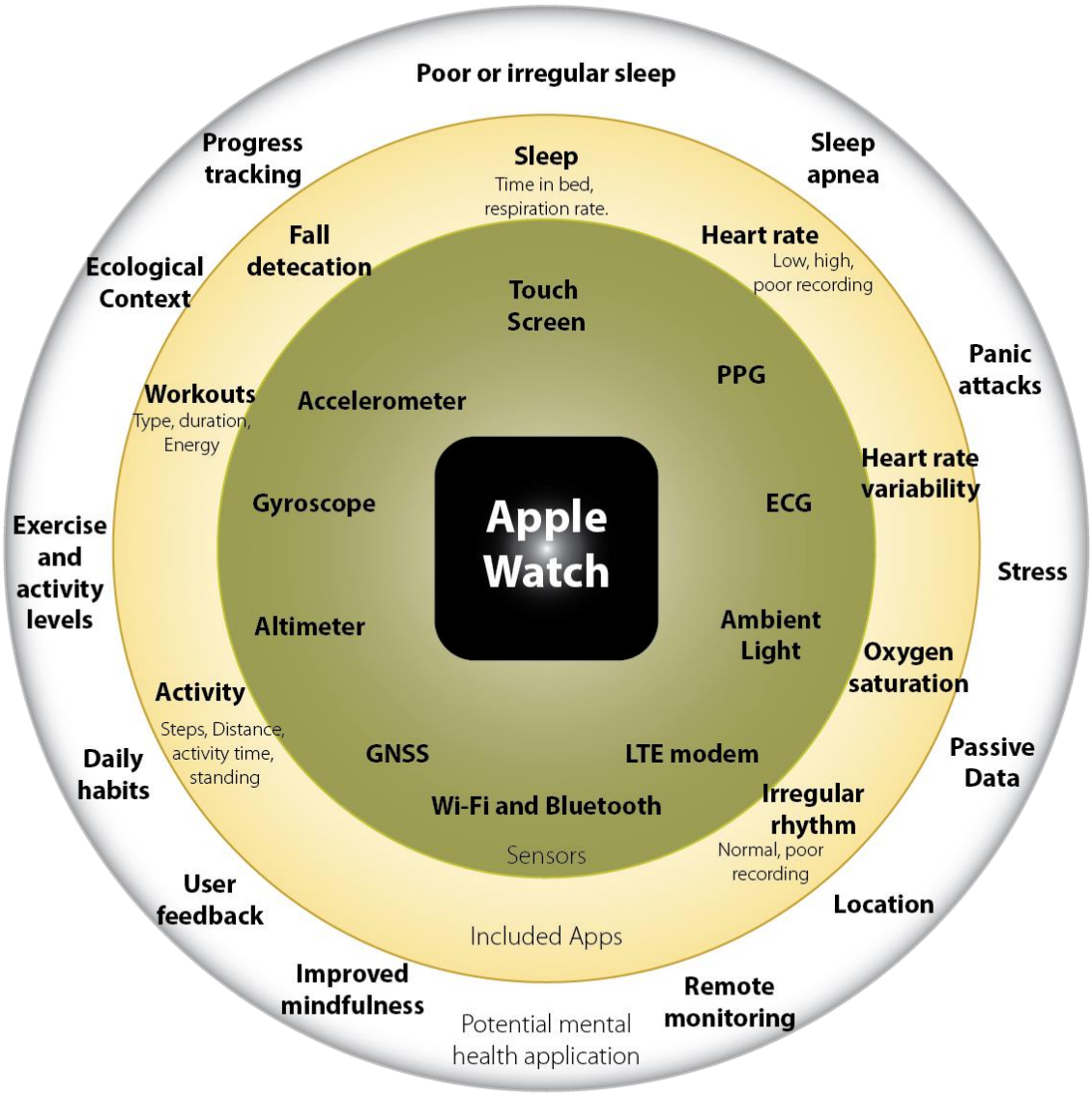


Figure 1: Summary of the sensors, apps, and possible mental health uses of the Apple Watch. PPG: photoplethysmography; ECG: electrocardiogram; GNSS: global navigation satellite system; LTE: Long-Term Evolution [38].

Figure 2: The development of Apple Watch Series functions. Upgrades to features (↑) and additions of new features (+) are mentioned. GNSS: global navigation satellite system; ECG: electrocardiogram; LTE: Long-Term Evolution; NFC: near-field communication; OLED [53].

2.5 Digital Investigation Process Models

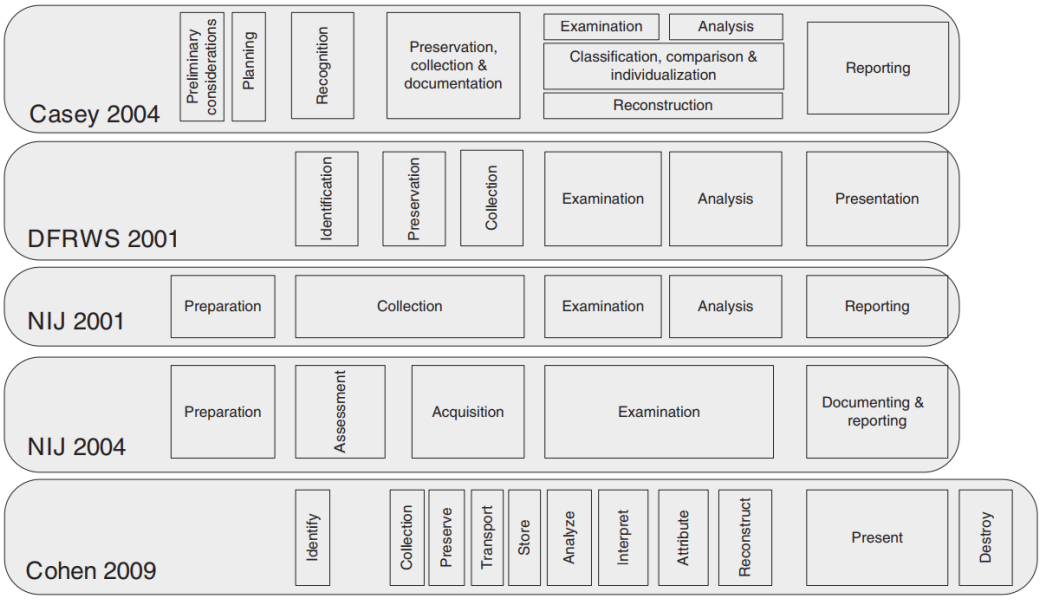


Figure 3: An examination of the comparative nomenclature concerning models of the digital investigation process [54].

In a formal and academic manner, when considering digital investigations, it is crucial to take into account the differences in terminology and level of detail across various process models. The comparison of terminology used for describing the linear process models is presented in Figure 3 [54]. The essential steps for conducting a comprehensive and proficient digital investigation are outlined as follows [54]:

- Preparation: Developing a plan of action to ensure an efficient investigation and obtaining necessary resources and materials.
- Survey/Identification: Locating potential sources of digital evidence, such as at a crime scene, within an organization, or on the Internet. For the purposes of clarity, the term "survey" is used throughout this chapter, as "identification" has a more specific meaning in forensic science related to evidence analysis.
- Preservation: Maintaining the integrity of in situ digital evidence by isolating the system, securing relevant log files, and collecting volatile data. This step encompasses subsequent collection and acquisition.
- Examination and Analysis: Locating and interpreting trace evidence. Some process models use these terms interchangeably.

  In this section, a clear differentiation is made between examination and analysis, where forensic examination involves extracting and viewing information from the evidence, making it available for analysis, and forensic analysis involves applying scientific

methods and critical thinking to answer fundamental questions related to the investigation, such as who, what, where, when, how, and why.

- Presentation: Presenting findings in a manner that is appropriate to the context of the investigation, whether it is legal, corporate, military, or otherwise.

2.6 Literature Review Summary

The Apple Watch has emerged as one of the most popular wearable devices in recent years, offering a range of features such as fitness tracking, communication, and entertainment. As a result, the device has become an important source of digital evidence in forensic investigations. This literature review aims to summarize the existing frameworks for Apple Watch digital forensics, with a focus on the extraction and analysis of data stored on the device. Several studies have been conducted in the area of Apple Watch digital forensics, and the majority of these studies have focused on the extraction of data from the device. The most commonly extracted data types include call logs, messages, GPS data, and fitness data such as heart rate and step count. The extraction of health-related data stored in the device's Health app has also been investigated. Most of the existing frameworks for Apple Watch digital forensics have been developed using commercial tools, such as the Elcomsoft iOS Forensic Toolkit and the Oxygen Forensic Detective. These tools allow forensic investigators to extract and analyze data stored on the device, including encrypted data, which is important in forensic investigations. In addition to the extraction of data, a few studies have also focused on the analysis of the extracted data. The analysis has primarily been performed using statistical and graphical methods, such as regression analysis and scatter plots. This allows forensic investigators to identify patterns and relationships in the data, which can provide valuable insights into the activities and behavior of the device's user. Despite the advances made in Apple Watch digital forensics, there is still a need for a comprehensive and systematic framework for the examination and analysis of digital evidence from the device. Currently, the existing frameworks have been effective in extracting and analyzing data from the device, but there is a need for a framework that integrates the various existing approaches and covers a wider range of data types and sources. In conclusion, this literature review highlights the growing importance of Apple Watch digital forensics in forensic investigations and the need for a comprehensive framework to support the examination and analysis of digital evidence from the device. The development of such a framework would greatly aid forensic investigators in their efforts to uncover important evidence from Apple Watches.

Chapter Three

Methodology and the proposed Framework

3.1 Overview

In this chapter, the most practical and effective techniques for obtaining information will be discussed. The strategies, steps, and experiments used in the research, as well as suggestions for improving the Apple watch model and framework, will be described in detail.

3.2 Research Problem Methodology: Apple Watch forensics framework

This study found that previous research on digital forensics often focused only on specific procedures and did not address broader aspects such as planning and preparation. Additionally, there was no research on potential outcomes of the presence of a smartwatch, such as the Apple Watch, at a crime scene.

Some studies did discuss the design of a digital forensic framework for smartwatches, but not specifically for the Apple Watch. These studies also did not cover readiness, deployment, physical and logical crime scene investigation, or evidence preservation. In this study, the author aim to address this gap in research by designing a comprehensive framework for digital forensics for the Apple Watch.

This framework covers readiness, physical and logical crime scene investigation, Energetic, presentation, Apple watch forensics model and documentation. The author also plans to develop a model to assist forensic investigators in conducting digital forensic investigations and making decisions. This model will cover all possible scenarios, both physical and digital, and will aim to provide the investigator with quick, accurate, and simple output from various fields to use as evidence. This research aims to address a problem that has not been previously addressed in scientific research and provide a decision aid.

Research Methodology: Apple Watch Forensics Framework

1. **Introduction**: The introduction presents the research objectives and identifies the research gap in existing literature regarding comprehensive frameworks for digital forensics on the Apple Watch. It highlights the need to address broader aspects such as planning, preparation, and potential outcomes of the presence of an Apple Watch at a crime scene.

2. **Research Questions:** The research questions aim to fill the identified research gap and develop a comprehensive framework for Apple Watch forensics. The specific research questions may include:

- What are the essential components of a comprehensive digital forensics' framework for the Apple Watch?
- How can readiness, physical and logical crime scene investigation, evidence preservation, and documentation be effectively integrated into the framework?
- How can a decision aid model be developed to assist forensic investigators in conducting digital forensic investigations and making informed decisions?
- What are the potential applications and benefits of the developed framework and decision aid in digital forensic investigations?

3. **Literature Review:** Conduct an extensive literature review to identify relevant studies related to digital forensics frameworks, smartwatches, and Apple Watch forensics. Analyze the existing research, identify gaps in the literature, and emphasize the lack of comprehensive frameworks covering all aspects of Apple Watch forensics.
4. **Methodology Design**: Design the methodology to develop the Apple Watch forensics framework. The methodology should include the following components:
    a. Framework Components: Identify and define the key components of the framework, such as readiness assessment, comprehensive physical and logical crime scene investigation procedures, evidence preservation protocols, energetic analysis techniques, effective presentation methods, and robust documentation practices.
    b. Decision Aid Model Development: Outline the process of developing a decision aid model that assists forensic investigators in conducting digital forensic investigations and making informed decisions. This involves considering various scenarios, both physical and digital, and developing an output system that provides efficient, accurate, and easily interpretable evidence from different fields.
    c. Integration and Validation: Describe how the developed framework and decision aid model will be integrated and validated. This may involve conducting experiments, utilizing real-world case studies, and engaging forensic investigators to gather feedback and ensure the effectiveness, efficiency, and usability of the framework.

5. **Framework Development:** Implement the designed methodology to develop the Apple Watch forensics framework. Document the development process, including any challenges encountered and modifications made to the methodology during the implementation phase. Provide detailed technical documentation and source code for the framework.
6. **Case Studies and Experiments:** Perform comprehensive case studies and experiments to evaluate the effectiveness, practicality, and reliability of the developed framework. Utilize real-world scenarios and Apple Watch devices to simulate forensic investigations. Document the results, observations, and lessons learned from each case study or experiment.
7. **Ethical Considerations:** Discuss the ethical considerations associated with Apple Watch forensics, including user privacy, data protection, and adherence to legal requirements. Address the potential impact of the research on user rights and ensure the use of anonymized or simulated data when conducting experiments.
8. **Conclusion:** Summarize the findings of the research, emphasizing the contributions of the developed Apple Watch forensics framework. Reflect on the limitations and potential future research directions. Discuss the practical applications, areas for improvement, and the broader impact of the framework on the field of digital forensics.
9. **References:** Provide a comprehensive list of all the references cited throughout the research methodology, following a consistent citation style (e.g., APA, MLA).

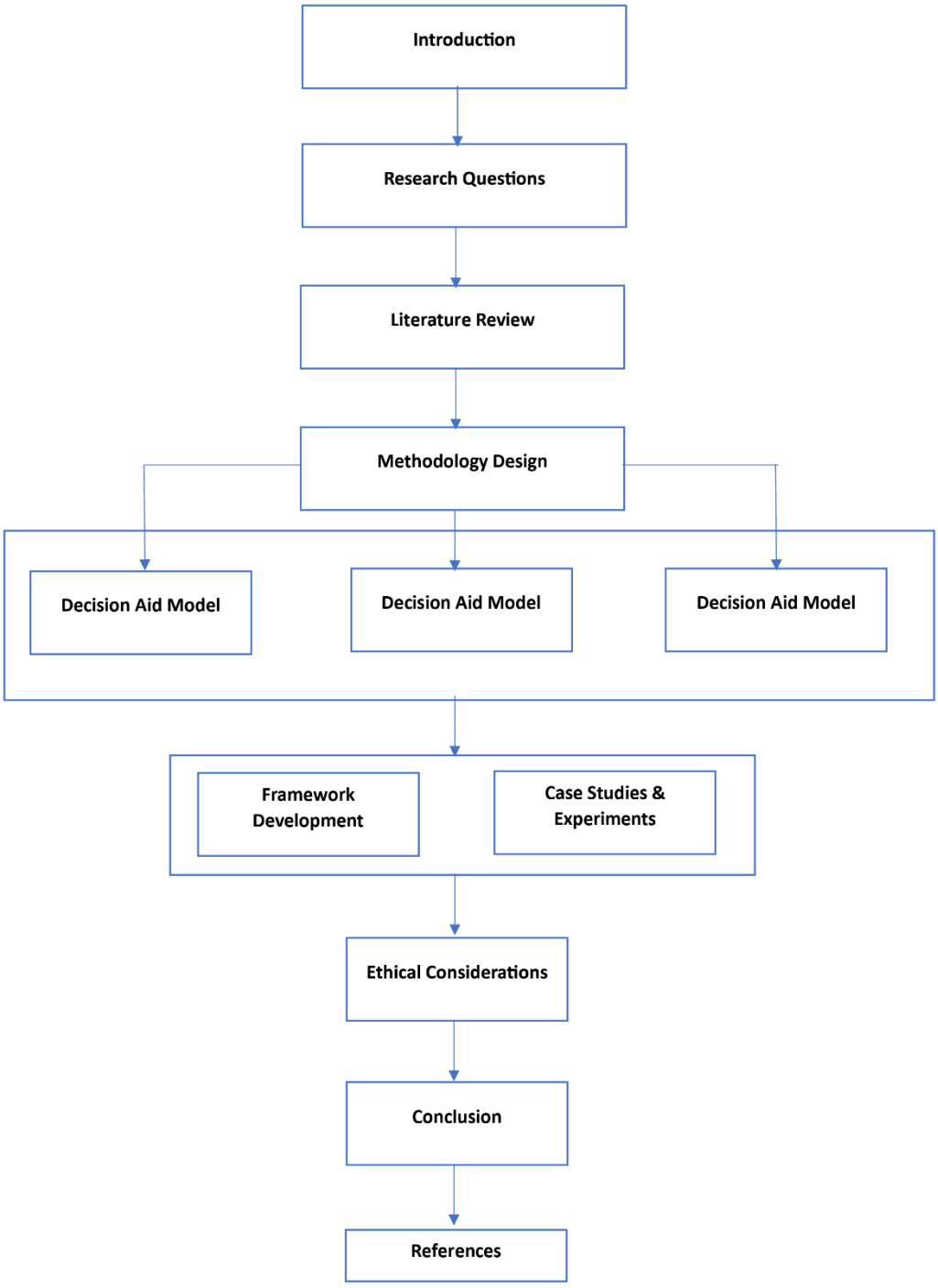


Figure 4: Research Methodology: Apple Watch Forensics Framework

3.3 Methodology and the Proposed Apple Watch Digital Forensics Framework (AWDFF)

This study's methodology is founded on the creation of realistic and applicable scenarios based on the proposed framework. After employing these scenarios, the workability of the proposed framework is validated, and then the extracted results are contrasted with any previously studied research. The field of digital forensics has not yet fully matured and lacks a comprehensive framework for addressing emerging technologies such as IoT, mobile, and network forensics. In addition, the knowledge and learning outcomes of digital forensics examiners have not been effectively shared for the benefit of future investigations. Although the first Digital Forensics Research Workshop (DFRWS) introduced a base framework for digital forensics research, there is a need for a more comprehensive framework to meet the demands of current investigations.

A framework is suggested for conducting forensic analysis on an Apple Watch, which consists of seven distinct stages. These stages are described and explained in detail to ensure a thorough and comprehensive forensic investigation.

In this thesis, a framework known as the *Apple Watch Digital Forensics Framework (AWDFF)* has been proposed and developed. The framework consists of seven distinct modules, which are illustrated in Figure 10. These modules include a series of procedures used to conduct digital forensics.

1) Digital Forensics Types

According to the research that has been conducted, it appears that there are five main categories of digital forensics:

1. Computer forensics involves the examination of computer systems and devices for evidence related to a crime or investigation. This can include analyzing hard drives, storage media, and other components of a computer system to uncover information such as deleted files, user activity, and system logs.
2. Network forensics involves the analysis of network traffic and communication data for the purpose of identifying and investigating cyber-crimes or security breaches. This can include analyzing packets of data transmitted over a network, as well as examining logs and other data sources to track the movements and activities of users or devices on the network.

3. Mobile forensics involves the examination of mobile devices such as smartphones and tablets for evidence related to a crime or investigation. This can include analyzing call logs, text messages, app data, and other types of information stored on the device.
4. Cloud forensics involves the analysis of data and information stored in cloud-based systems for the purpose of identifying and investigating cyber-crimes or security breaches. This can include examining logs and other data sources to track the movements and activities of users or devices within the cloud environment.
5. Internet of things (IoT) forensics involves the examination of connected devices and systems that make up the IoT for evidence related to a crime or investigation. This can include analyzing the data and communication streams of IoT devices such as smart thermostats, security cameras, and home automation systems to uncover information about their usage and activities.

Following the studies, the species suitable for use in the Apple Watch digital forensics framework were identified and depicted in Figure 4.

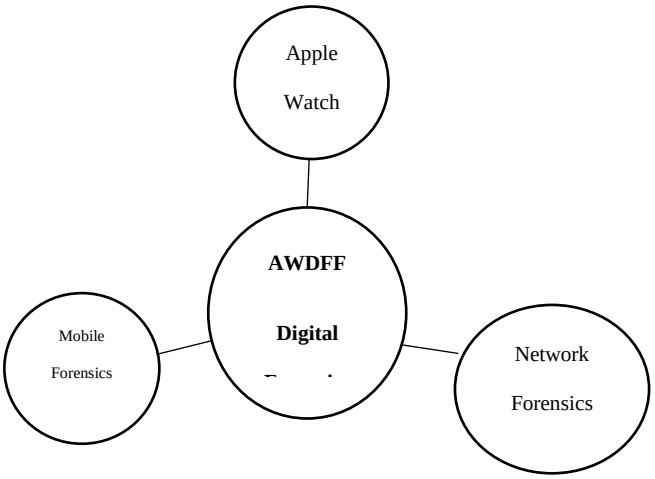


Figure 5: AWDFF- Digital Forensics Types

2) Readiness

The proposed framework recommends starting the process with the planning phase of the preparation module once the necessary type of digital forensics has been determined. In addition to the previously mentioned procedures, the readiness phase (Figure 4) also considers two crucial procedures: technical and legal considerations.

a) The planning procedure initiates the readiness module, which involves creating a detailed strategy in advance of the detection or identification of an incident. This strategy should take into account all relevant factors, including the scope of the

investigation, the resources required, the expected timeline, and any potential risks or challenges. It will serve as a roadmap for conducting the investigation in a systematic and organized manner.

b) The technical considerations involve taking into account various technological aspects during the forensic investigation. These factors include the infrastructure of the forensics environment, such as the hardware, software, and network configurations. The architecture of the environment, including the logical and physical design, should also be considered. The availability and suitability of forensics technology, such as tools and methods, must be evaluated, as well as any security concerns that may arise during the investigation.

c) The legal considerations encompass regulatory concerns of law and law enforcement authorities, as well as contracts between the user and the service provider for conducting a forensics investigation. The chain of custody of digital evidence and its admissibility in court should be carefully considered to ensure that the evidence can be used in legal proceedings. Questions about jurisdiction must also be evaluated, whether the crime in question is domestic or international. This may involve determining the applicable laws and regulatory frameworks, as well as any legal or ethical obligations related to the investigation.

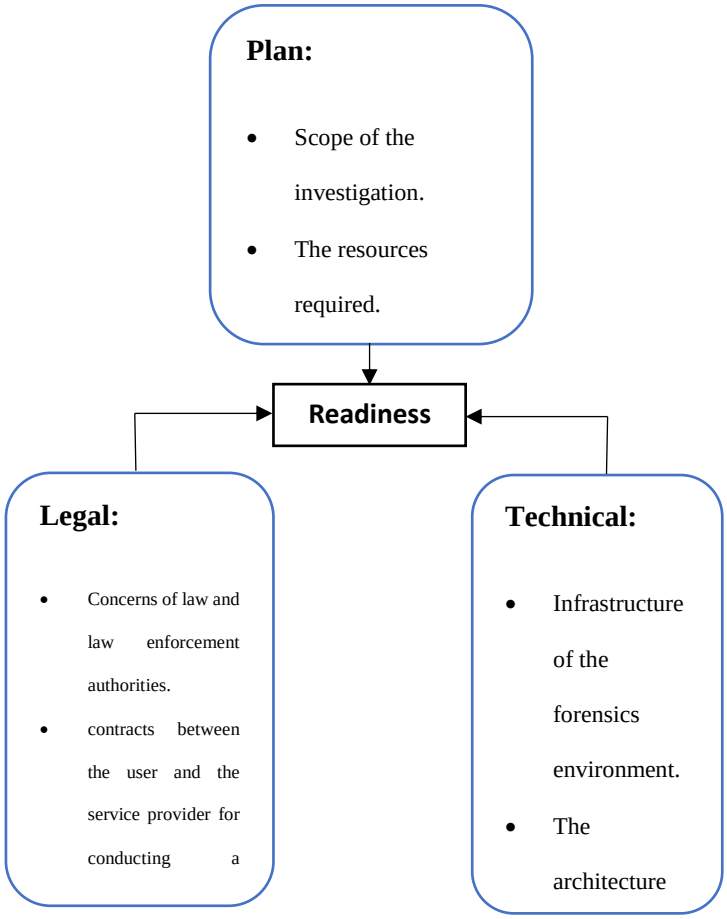


Figure 6: Readiness phase

3) Physical Forensics

Proactive forensics refers to actions taken to protect and secure evidence during a live investigation or after a crime has been identified. Physical forensics involves collecting and preserving physical evidence, such as DNA or fingerprints, to support digital forensics and legal prosecution. This process includes securing the scene, preserving the physical scene, and detecting the incident or crime.

1. Securing the scene: involves protecting the crime scene and potential evidence from contamination and unauthorized access or modification. First responders at the crime scene will follow organizational policies to secure the scene and digital evidence. This helps to maintain the integrity of the crime scene.
2. Preservation of Physical Scene: Proactive preservation involves preserving the integrity of physical evidence. This may involve providing a portable power supply to keep digital evidence alive and taking measures to protect and back up the data.
3. Detect Incident/Crime: Detection of an incident or crime is an essential step in starting a digital forensics investigation. It involves informing the appropriate authority.

Figure 7: Physical Forensics

4) Energetic Forensics

Energetic digital forensics (DF) (Figure 7) is the most critical part of the DF module and is carried out after a digital crime has been discovered to provide support for legal prosecution. The Energetic digital forensic investigation is divided into five distinct phases, each of which must be completed in order to thoroughly investigate the crime. In addition, there is a capability for conditional iteration, allowing for further DF to be conducted if necessary. These five phases are:

1. *Identification:* During this stage of the investigation, the investigator must identify all relevant evidence and determine its location, whether it is within the crime scene internal network or on the cloud. The investigator should also be able to recognize necessary instruments and methods before proceeding with further steps. This may involve reviewing logs, analyzing network traffic, or examining devices for signs of tampering or unusual activity.

2. *Acquisition:* The digital forensics evidence captures, or imaging process is carried out to ensure that the evidence can be used and is admissible in court. It is important to preserve the authenticity of the primary evidence and maintain the chain of custody to prevent contamination or tampering. This may involve creating copies of digital evidence, such as documents, emails, or images, or creating forensic images of physical devices, such as computers or mobile phones.
3. *Preservation:* Preservation is the process of separating and protecting the original evidence in a secure manner to prevent contamination. This may involve sealing physical evidence in tamper-evident bags, creating encrypted copies of digital evidence, or storing evidence in secure locations. The first responder is typically responsible for preserving evidence at the crime scene or immediately after the crime has been discovered.
4. *Examination:* The examination phase is the primary step used to find information with the help of forensics equipment and methods through the application of a systematic and methodical strategy. This may involve analyzing digital evidence using specialized software, examining physical devices for signs of tampering or damage, or reconstructing events based on the available evidence. The investigator should use a systematic approach and document all findings in a comprehensive and reliable manner.
5. *Analysis:* The analysis phase involves reviewing, evaluating, categorizing, and drawing conclusions from the examination's results in order to assist in the development and presentation of the digital forensics report. This may involve comparing the results to established patterns or trends, identifying any anomalies or inconsistencies, and assessing the relevance and reliability of the evidence. The findings should be clearly documented and communicated to relevant parties, such as law enforcement or the organization's management.

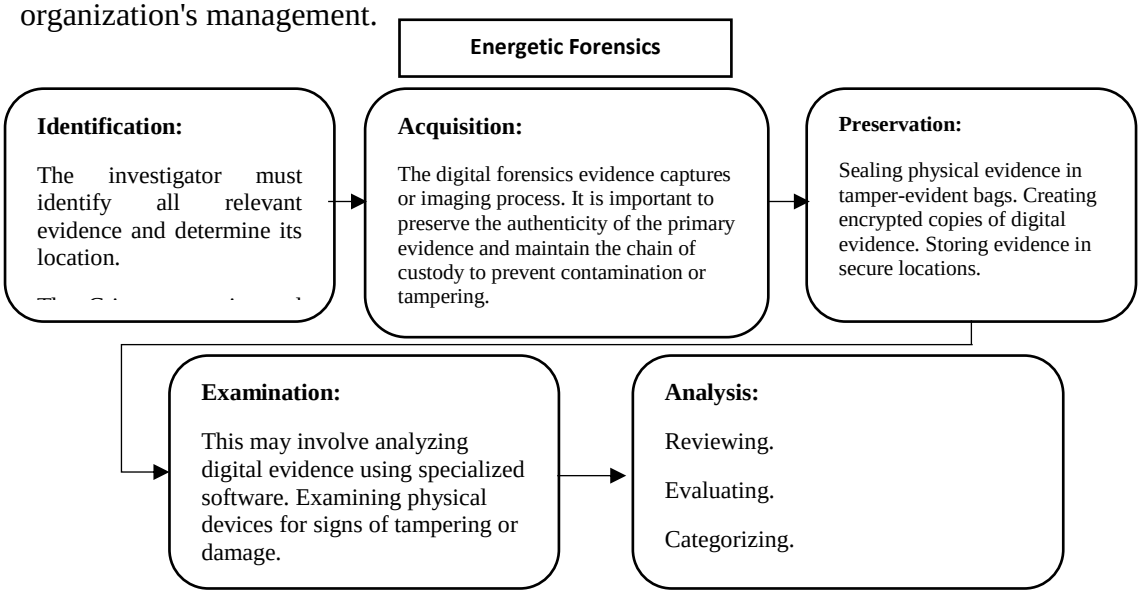


Figure 8: Energetic Forensics

5) Presentation

The presenting module (Figure 8) serves as the final output of the DF processes, including the end-result, facts, and results. The decision on whether or not a crime has occurred is made by a court of law or the organization's management based on the facts and discoveries uncovered by the investigator. The presenting module consists of four phases: report, reconstruction, dissemination, and return of evidence.

1. *Report:* The report includes in-depth explanations of the start of the forensics investigation, the readiness of the evidence to be examined, and the identification of the investigator. It should provide a clear and comprehensive overview of the entire process, including the methods used, the findings, and any conclusions drawn.
2. *Reconstruction:* Reconstruction refers to the process of analyzing and evaluating the results of the DF examination. This may be necessary to validate the process by which a particular result was achieved for various reasons, such as to confirm the authenticity or reliability of the evidence.
3. *Dissemination:* It is important to share the results of the completed DF with other investigators who may conduct similar investigations in the future. This can help to promote best practices and improve the overall effectiveness of forensic investigations.
4. *Return of evidence:* The final step for the investigator is to return any evidence found to its rightful owner. This may involve returning physical evidence to its owner or deleting copies of digital evidence once it is no longer needed for the investigation.

Figure 9: The presenting module

6) Apple Watch Forensics Model

In this study, the author developed a forensic model for the Apple Watch to be used in a scenario where the device may have witnessed a crime (for example, data stored on the Apple Watch may implicate a suspect), see figure 8. To test this model, the author conducted a series of controlled experiments involving different activities (such as running or going to the gym) during which typical user activity was recorded. These activities allowed the author to generate data for testing the Apple Watch device (when it is isolated or paired with an unavailable smartphone), the companion app (when the smartphone paired with the smartwatch is available), and the associated network (when the smartphone paired with the smartwatch is available). The details of this investigation scenario will be described further in the study.

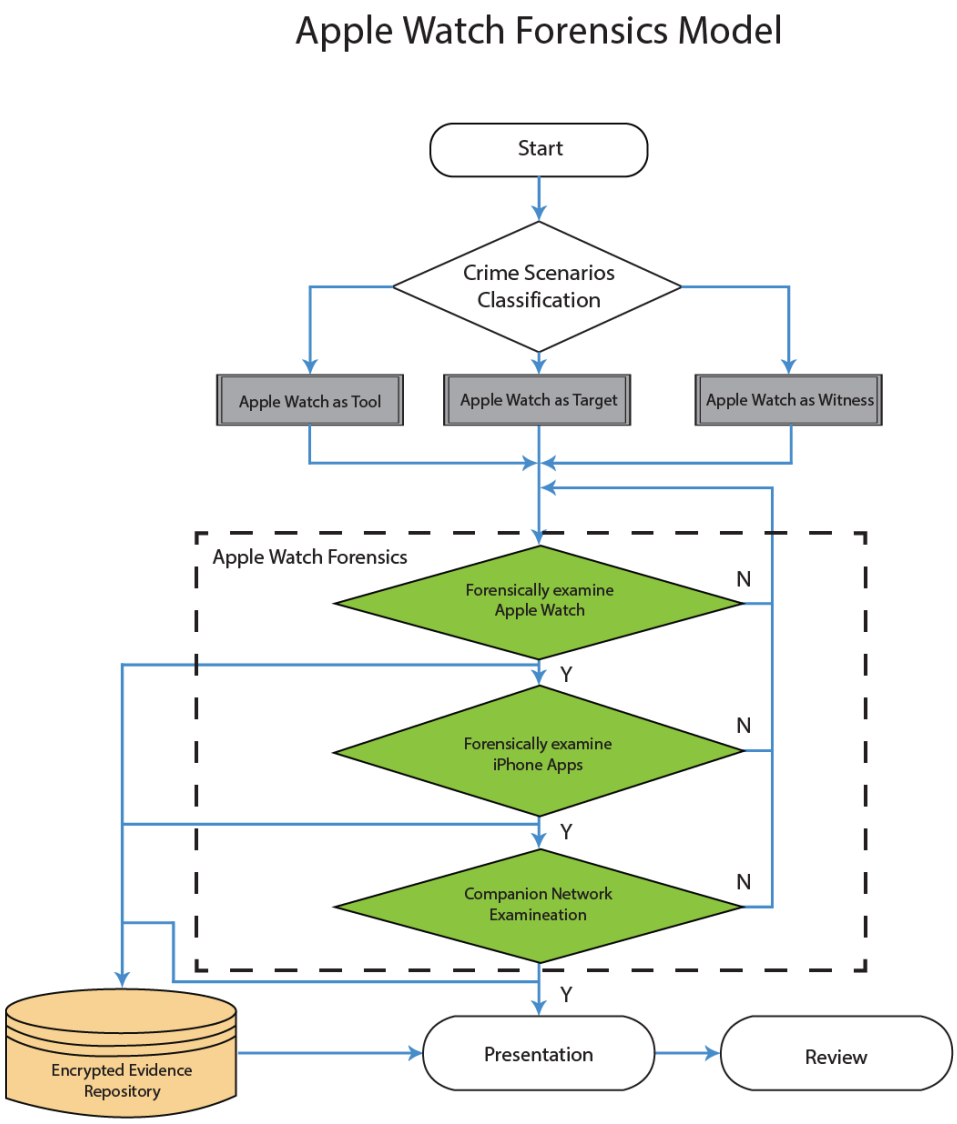


Figure 10: Proposed Apple Watch Forensics Model

7) Documentation

The documentation of a forensics investigation is a crucial aspect of the proposed framework for handling such cases. This process begins with the preparation of all relevant information and ends with the presentation of that information in a clear and organized manner. The documentation is then used to create a forensics report, which serves as a key resource for the organization or court involved in the case. The forensics report helps to provide a comprehensive overview of the investigation and is used to assist in determining the outcome of the case, whether it be a conviction or acquittal.

In addition to being an important tool for reaching a conclusion in the case, the forensics report is also stored in the AWFM (Apple Watch Forensics Model) for future reference. This module serves as a centralized repository for all of the documentation related to the investigation and can be accessed and utilized in the event that additional investigations need to be conducted. Overall, the documentation and creation of a forensics report is a vital part of the proposed framework for handling forensic cases and plays a crucial role in the pursuit of justice.

Summary: The proposed Apple Watch Digital Forensics Framework (AWDFF)

After designing the Digital Forensics Framework (DFF) for the Apple Watch, the researchers realized that the nature of the crime scene and the status of the Apple Watch may require a more responsive approach. In some cases, the speed of access to the Apple Watch is important, and the DFF may take longer to access important directories because it follows all the processes and stages in the framework. To increase effectiveness, the researchers developed an advanced version of the DFF called the Apple Watch Digital Forensics Framework (AWDFF).

The AWDFF is based on the DFF, but some elements may be modified or deleted depending on the nature of the incident. For example, if the evidence is only digital, the physical crime scene investigation may be skipped in the AWDFF. However, if the crime scene is both physical and digital, the AWDFF includes both physical and logical crime scene investigations.

The AWDFF takes into account two factors that are important in determining the nature of the crime scene: the forensics domain (which determines the initial goals of the incident, such as reducing the performance of the device or stealing data) and the type of crime (which determines whether the crime is only digital or physical, or both). These factors help to determine how the crime scene should be dealt with in the AWDFF.

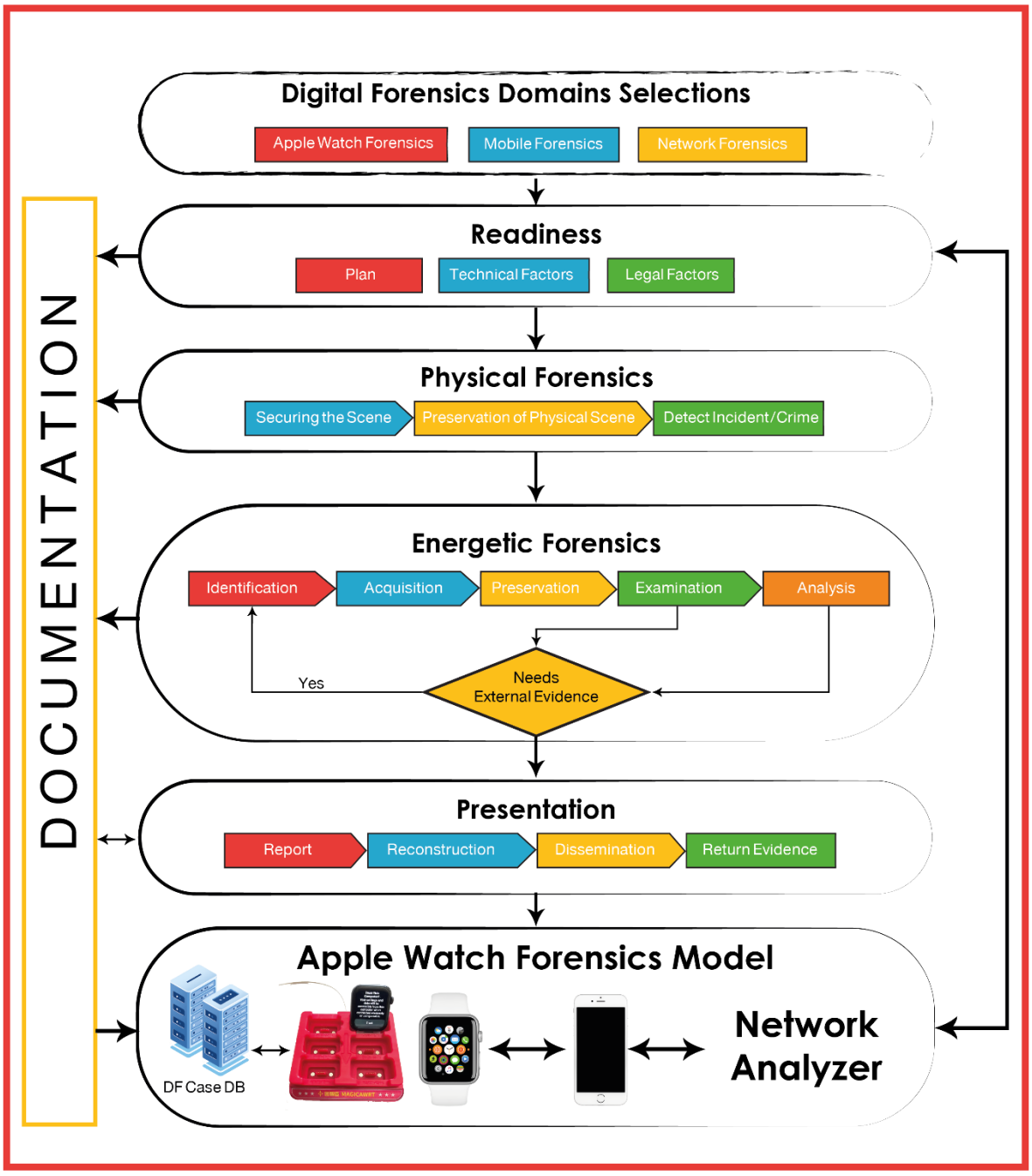


Figure 11: Proposed Apple Watch Digital Forensics Framework (AWDFF)

Chapter Four

Scenarios and Experiment Design

4.1 Overview

In this chapter, we will delve into a simulated crime scene scenario that involves the discovery of an Apple Watch and an iPhone. The purpose of this scenario is to apply and test a proposed framework that has been developed to analyze and evaluate such incidents. We will go through the steps of implementing this scenario according to the framework and assess its effectiveness in providing relevant information about the crime scene. This will provide us with an opportunity to not only evaluate the framework, but also gain insights into the potential applications and limitations of the technology involved.

4.2 The Scenario

In a forensic investigation scenario involving an Apple Watch, the type of digital forensics adopted will depend on the specific investigation process and framework being used. There are several possible scenarios that investigators may encounter when trying to gather evidence from an Apple Watch.

1. Only Apple Watch: If investigators only find the Apple Watch at the crime scene, they will need to use specialized techniques to extract evidence from the device. This may include using forensic tools to create a physical or logical image of the device's storage, and then analyzing the image to uncover evidence such as deleted files or communications.
2. iPhone only: If investigators only find an iPhone at the crime scene, they may still be able to gather evidence related to the Apple Watch. For example, if the iPhone is associated with an Apple Watch, investigators can use forensic tools to extract data from the iPhone's health-related apps that may be related to the Apple Watch.
3. Network only: If investigators do not find either the Apple Watch or the iPhone at the crime scene, they may still be able to gather evidence related to the Apple Watch if a network is present. This may include extracting artifacts from network logs or other network-based evidence that may be related to the Apple Watch.
4. Apple Watch and iPhone: If investigators find both the Apple Watch and the iPhone at the crime scene, they will be able to extract evidence from both devices, which can then be cross-referenced to uncover additional information.

5. Apple Watch and Network: If investigators find the Apple Watch and a network at the crime scene, they can extract evidence from the device and network to gather more information about the Apple Watch's usage and activity.
6. iPhone and Network: If investigators find the iPhone and a network at the crime scene, they can extract evidence from the phone and network to gather more information about the associated Apple Watch's usage and activity.

Overall the type of digital forensics adopted for an Apple Watch system in a forensic investigation will depend on the specific scenario and what the investigator has at his disposal, but all of the above scenarios have the potential to yield valuable evidence.

These possibilities can be organized and represented in a 3x3 matrix, where ***AW*** stands for Apple Watch, ***iOS*** represents iPhone, and ***network*** represents Network as shown in Table 2.

Table 1: Forensics Domains Matrix

Domain	*aw*	*i*	*n*
aw	**1**	**4**	**5**
iOS	**4**	**2**	**6**
network	**5**	**6**	**3**

Before beginning the investigation process, the criminal investigator must construct the AWDFF, as it clearly outlines all the procedures and helps to pinpoint key elements to focus on. It is important to keep in mind that the criminal investigation process should be heavily reliant on documentation for each step.

4.3 AWDFF - Digital Forensics Domains Selections

The Forensics Domains determine the type of forensics that will be used in the Apple Watch Digital Forensics Framework (AWDFF) and, therefore, influence the digital forensic investigation process, see Figure 10. The nature of the attack on the system can fall into a number of limited possibilities, such as:

1. Apple Watch Domain

   In certain circumstances, the Apple Watch may be found at the crime scene in a damaged or disconnected state, making it relevant as evidence in the digital or physical forensic

investigation. As a result, the Apple Watch may be examined as part of the Internet of Things domain, but it is also considered a special domain in and of itself.

2. Mobile Domain

In certain circumstances, the Apple Watch and its associated iPhone may be found at a crime scene, making them relevant as evidence in a digital or physical forensic investigation. However, it is possible that only the iPhone is found at the crime scene. In this case, the mobile phone will be examined as part of the Internet of Things (IoT) domain, but it is also considered a special domain.

3. Network Domain

In some cases, the network can be considered a special domain for investigation in a digital forensic case. This is because it may be possible to access certain protocols and communication or messages that occurred on the network at the crime scene in order to obtain concrete and conclusive evidence.

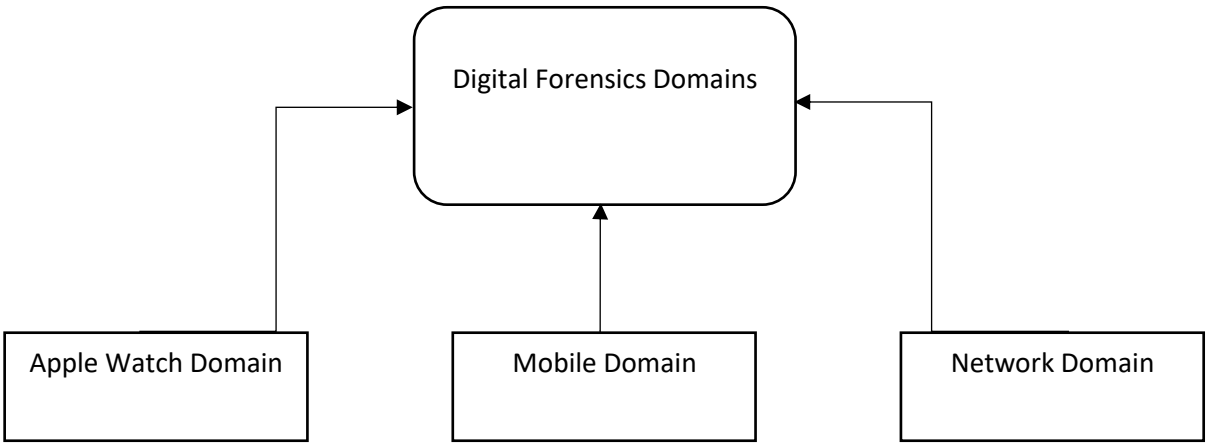


Figure 12: Digital Forensics Domains Selections

4.4 Investigative Scenario

It's a late night and a group of teenagers are out partying at a local club. As they make their way home, they notice a strange figure lurking in the shadows. As they get closer, they realize that it's a man who appears to be unconscious.

The teenagers approach the man and find that he has an iPhone and an Apple Watch on his wrist. They quickly call the police and wait for them to arrive. When the officers arrive, they begin to investigate the scene. They notice that the man has a large gash on his head and that his wallet and keys are missing.

The officers collect the iPhone and Apple Watch as evidence and begin to examine them for any clues. They find that the phone has a number of calls and messages from a person named "Sara." They also notice that the Apple Watch has a fitness tracking app that shows the man's movements from earlier in the night.

Using this information, the officers are able to track down Sara and bring her in for questioning. During the interrogation, Sara admits that she was with the man earlier in the night and that they got into a fight. She claims that she tried to take his phone and wallet to stop him from calling her, but he grabbed her and tried to take them back. She says that she panicked and hit him with a nearby object, causing the gash on his head.

The officers are able to verify Sara's story using the location data from the Apple Watch and the calls and messages on the iPhone. In the end, they charge Sara with assault and theft, and the case goes to trial.

The iPhone and Apple Watch of the suspect have been confiscated, and authorities are eager to answer the following questions using our forensic analysis:

1. The Apple Watch stores information on its internal memory chips. If so, is it recoverable and analyzable?
2. Is it possible to restore user activity data from the Apple Watch application installed on an iPhone? If so, is it possible to rebuild the data to reveal prior user activities?
3. Can deleted user behavior data from the Apple Watch application installed on an iPhone be recovered?

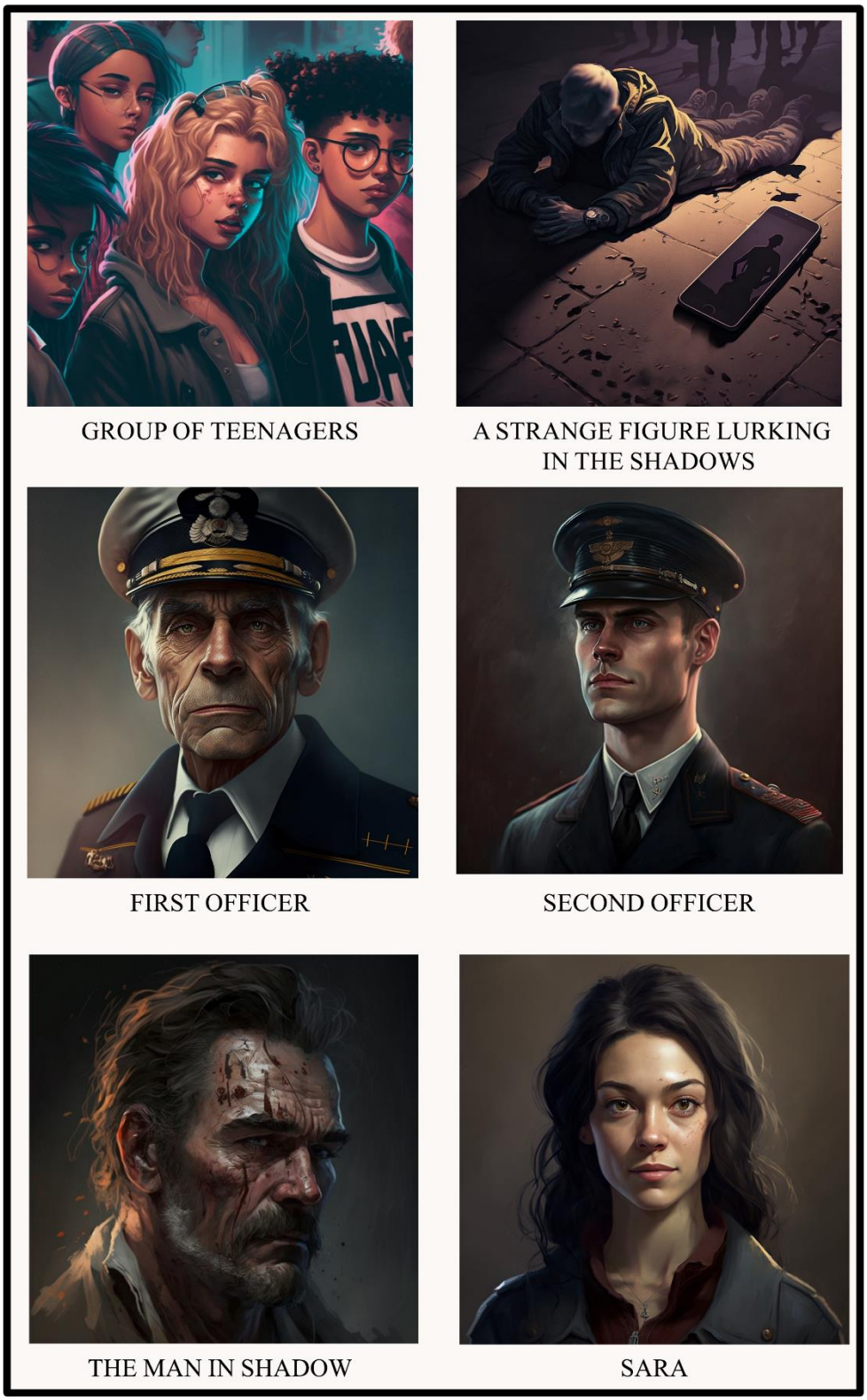


Figure 13: Physical Scenario Story board

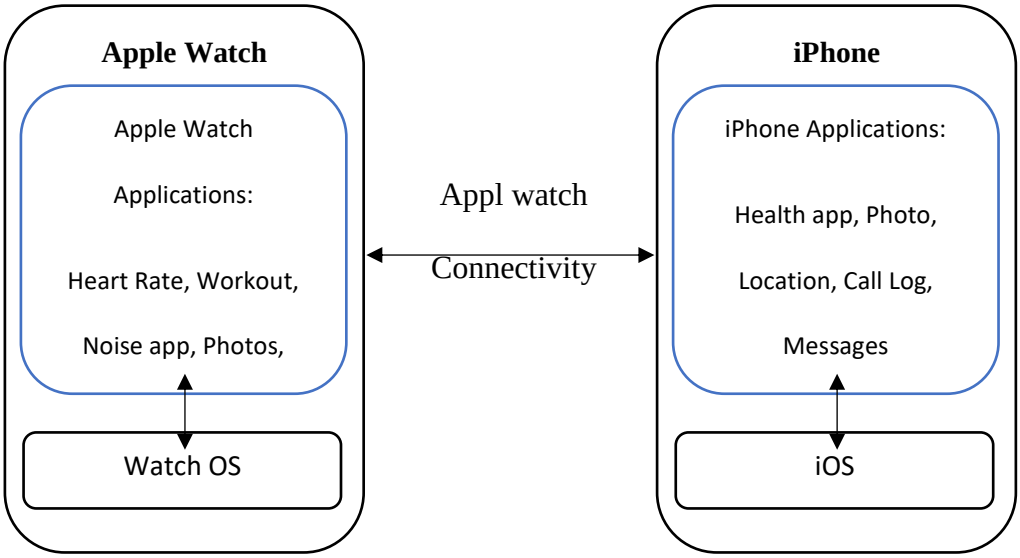


Figure 14: Digital Scenario

We shall proceed to employ the framework that we have meticulously constructed and developed previously, in order to analyze and examine the specific criminal case that has occurred. By utilizing the scenario that was previously outlined and described, we will gain a deeper understanding and insight into the events and circumstances surrounding the case in question.

4.5 Digital Forensics Domains

From this scenario, we can infer that technology can play a significant role in solving crimes. The phone and Apple Watch were crucial evidence in identifying the perpetrator, and the location data and calls and messages helped to confirm the perpetrator story and establish a chain of events of the criminal case. Additionally, it highlights the importance of quick response and proper evidence collection.

The Apple Watch is a popular wearable device that can be used for fitness tracking, communication, and other functions. As with other digital devices, the data stored on an Apple Watch can be forensically analyzed to extract information for use in legal or investigatory contexts. There are several frameworks available for performing digital forensics on Apple Watch devices. These frameworks typically include tools for acquiring and analyzing data from the device, as well as techniques for interpreting the results of the analysis. One popular framework for Apple Watch digital forensics is the Elcomsoft Phone Breaker. This tool allows forensic examiners to acquire data from the device, including call logs, messages, and location data. It also includes a feature for decrypting the device's backup, allowing for the analysis of more data. Another framework for Apple Watch digital forensics is the Oxygen Forensics

Detective. This software includes a variety of tools for data acquisition and analysis, including the ability to extract data from the device's firmware and analyze the data stored on the device's internal storage.

In addition to these specialized frameworks, there are also general purpose digital forensics tools, such as MOBILedit Forensic Express, that can be used to acquire and analyze data from Apple Watch devices. It is important to note that digital forensics analysis of Apple Watch and other ios based devices require special knowledge, technical skill and use of specific tools as the data is encrypted and access to the device is protected by various security measures. Overall, the use of a specialized digital forensics framework is necessary to properly acquire and analyze data from an Apple Watch device. These frameworks typically include a variety of tools and techniques for extracting and interpreting data, and can provide valuable information for legal or investigatory purposes.

4.5.1 Apple Watch Digital Forensics Domain

In this scenario, the Apple Watch were used as digital evidence to help investigate a crime scene. The fitness tracking app on the Apple Watch was able to provide location data that helped verify the suspect's story, while the calls and messages on the iPhone provided additional information that helped identify and locate the suspect. The digital forensic analysis of the devices played a crucial role in solving the case and led to the suspect being charged with assault and theft.

a. Readiness

Apple Watch digital forensics is the process of extracting and analyzing data from an Apple Watch for the purpose of investigating a crime or other incident. In order to perform digital forensics on an Apple Watch, the device must be in a "ready" state, meaning that it is powered on and unlocked. If the device is locked or powered off, it will not be possible to access the data stored on it.

- **Plan:** From an Apple Watch digital forensics readiness perspective, a plan would involve several key steps to ensure that the data on the device can be properly collected, preserved, and analyzed.

1. Identification and preservation of the device: The first step would be to identify and preserve the device in question. This would involve labeling and packaging the device

to prevent any damage or contamination, and ensuring that the device is not powered off or tampered with in any way.

2. Data acquisition: The next step would be to acquire the data from the device. This would involve using specialized software and hardware to create a forensic image of the device, which would capture all of the data on the device, including deleted files and information stored in the device's memory.
3. Data analysis: Once the data has been acquired, it can be analyzed using specialized software and techniques. This would involve searching for specific data points, such as call logs, messages, and location data, that may be relevant to the investigation.
4. Reporting and documentation: The final step would be to document and report the findings of the digital forensic analysis. This would involve creating a detailed report of the findings, including any relevant information that was discovered, and providing this information to the relevant authorities.

Overall, this plan would ensure that all the necessary steps are taken to properly collect, preserve, and analyze the data from the Apple Watch and to support the investigation.

- **Technical Factors:** From an Apple Watch digital forensics readiness perspective, there are several technical factors to consider in order to ensure that the data on the device can be properly collected, preserved, and analyzed.

1. Device connectivity: The Apple Watch must be connected to the iPhone to synchronize the data. The digital forensic examiner must consider the possibility of the iPhone being locked, turned off or destroyed. If the device is not connected to the iPhone, the data may not be available for examination.
2. Data storage: The Apple Watch stores data in a proprietary format, and specialized software and hardware is required to access the data. The examiner must ensure that they have the necessary tools and equipment to perform the examination.
3. Encryption: Data stored on the Apple Watch may be encrypted, which can make it difficult to access. The examiner must be familiar with the encryption methods used by the device and have the appropriate tools to decrypt the data.
4. Battery level: Apple Watch's battery must be charged to a certain level to perform a forensic acquisition. If the battery is low or dead, the device may not power on, and the data may not be accessible.

5. Firmware version: The examiner should be aware of the firmware version of the Apple Watch. Different firmware versions may store data in different locations, which can affect the examination process.
6. Data Synchronization: Data on the Apple watch is synchronized with the paired iPhone, which means that some data may be stored on the iPhone. The examiner should also consider examining the paired iPhone for additional data.

Overall, considering these technical factors and taking necessary steps can ensure that the data from the Apple watch can be properly collected, preserved, and analyzed to support the investigation.

- **Legal Factors:** From an Apple Watch digital forensics readiness perspective, there are several legal factors to consider in order to ensure that the data on the device can be properly collected, preserved, and analyzed in compliance with the law.

1. Search Warrant: In most jurisdictions, a search warrant is required to seize and examine digital evidence, including an Apple Watch. The warrant must be specific in describing the place to be searched and the items to be seized.
2. Chain of custody: The chain of custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. The examiner must maintain a proper chain of custody of the device, including a detailed record of who had possession of the device at all times.
3. Privacy: The data stored on the device may be considered personal and private information. The examiner must be aware of the privacy laws and regulations that apply to the data and must ensure that the examination is conducted in compliance with these laws.
4. Admissibility: The examiner must be aware of the rules of evidence and the standards for admissibility of digital evidence in the jurisdiction where the case will be tried. The examiner must ensure that the examination is conducted in a manner that will allow the evidence to be admitted in court.
5. Data Preservation: The examiner must ensure that the data is preserved in a manner that will not alter or destroy the original data. The examiner must also be aware of the time limits for preservation of the data.

Overall, considering these legal factors and taking necessary steps can ensure that the data from the Apple watch can be properly collected, preserved, and analyzed in compliance with the law and that the evidence can be admissible in court.

b. Physical forensics

Physical digital forensics on an Apple Watch involves the examination of the physical hardware and components of the device to uncover evidence of a crime or incident. This can include analyzing the device's memory, storage, and other internal components for signs of tampering or damage.

- **Securing the scene** for Apple Watch digital forensics from a physical forensics' perspective involves several steps.

First, the device should be turned off and the battery should be removed if possible. This will prevent the device from being powered on and potentially wiping or altering any data.

Second, the device should be placed in a Faraday bag or other shielding material to prevent any external signals from interacting with the device.

Third, the device should be handled with gloves or other protective materials to prevent any fingerprints or other physical evidence from being left on the device.

Fourth, the device should be properly packaged and labeled to ensure it is not damaged during transport and to maintain the chain of custody.

Finally, the device should be stored in a secure location until it can be examined by a forensic examiner.

- **Preserving the physical scene** for Apple Watch digital forensics from a physical forensics' perspective is an important step in the process of collecting and analyzing evidence from the device.

The first step in preserving the physical scene is to document and photograph the location where the device was found. This includes taking pictures of the device itself, as well as any surrounding areas that may be relevant to the investigation.

Next, it is important to secure the area and prevent any unauthorized individuals from accessing the scene. This may involve setting up barriers or using security personnel to keep people away from the area.

It is also important to take steps to protect the device from damage or tampering. This may include placing the device in a protective case or container, or covering it with an anti-static bag.

Finally, it is important to document all actions taken at the scene, including any items that were collected and the names of individuals who were present. This information should be recorded in a detailed report that can be used as evidence in court.

It is important to remember that the preservation of physical scene is a critical step in digital forensics, as it can help to ensure that the integrity of the evidence is maintained and that the device can be successfully analyzed for digital evidence.

- **Detecting an incident or crime** for Apple Watch digital forensics from a physical forensics' perspective involves several steps.

The first step is to identify the potential evidence that may be present on the device. This may include identifying the device's serial number, model, and any other relevant information that can help to link it to a specific crime or incident.

Next, it is important to examine the device for any physical signs of damage or tampering. This may include looking for scratches, dents, or other indicators that the device may have been tampered with.

It is also important to review any relevant logs or other data that may be stored on the device. This may include looking for recently-opened apps, call history, or other information that can help to identify the device's owner or user.

Finally, it is important to work with other investigators or experts to identify any other evidence that may be present at the scene. This may include DNA or other physical evidence that can help to link the device to a specific individual or crime.

It is important to remember that the detection of an incident or crime is a critical step in digital forensics, as it can help to ensure that the evidence is properly collected and analyzed and that the perpetrator can be held accountable for their actions.

c. Energetic Forensics

Energetic forensics from an Apple Watch digital forensics perspective refers to the analysis of the device's power consumption and energy usage patterns in order to uncover evidence of a

crime or incident. This can include analyzing the device's battery usage, power logs, and other related data to determine when and how the device was used.

- **Identification** for Apple Watch digital forensics from an energetic forensics' perspective involves analyzing the energy usage of the device to identify patterns or anomalies that may be related to a specific crime or incident.

The first step in identification is to gather data on the device's energy usage, this can be done by using specialized software or tools that allow you to monitor the device's battery level, charging patterns, and other energy-related information. This data can be analyzed to identify any unusual usage patterns or events that may be related to a specific crime or incident.

It's also important to examine the device's power source, such as the charging cable and adapter, to look for any signs of tampering or damage that may indicate that the device has been tampered with.

Another important aspect of identification is to analyze the device's firmware and software for any indications of malware or other malicious activity. This can include looking for signs of jailbreaking or rooting, which can indicate that the device has been compromised.

Finally, it is important to work with other investigators or experts to identify any other evidence that may be present on the device, such as images, videos or other files that may be relevant to the investigation.

It is important to remember that identification is a critical step in digital forensics, as it helps to ensure that the evidence is properly collected and analyzed and that the perpetrator can be held accountable for their actions. An energetic forensics perspective can help to identify patterns or anomalies that may be related to a specific crime or incident.

- **Acquisition** in energetic forensics from an Apple Watch digital forensics perspective involves the process of collecting and preserving the device's energy state at the time of acquisition in order to maintain the integrity of the data stored on it. The energy state of an Apple Watch refers to the device's current power level and status, including the battery status and the device's power source.

Acquisition of the energy state of an Apple Watch can be done by using specialized software that can extract the information about the device's battery level, power source, and other

energy-related data. Additionally, it is important to take a screenshot of the battery status and power source to ensure that the information can be verified later on.

It is also important to take note of the time of acquisition and the time zone, as this can affect the timestamps of the data stored on the device. This is also important for the purpose of correlation with other data sources and not to misinterpret the time of events.

Before the acquisition, it is important to keep the device powered on and connected to a power source during the process, this will prevent the device from entering a low power mode, which can cause data to be lost or altered. Additionally, it is important to avoid interacting with the device during the acquisition process as this can also affect the energy state and the integrity of the data.

In summary, acquisition in energetic forensics from an Apple Watch digital forensics perspective involves using specialized software to extract information about the device's battery level, power source, and other energy-related data, taking a screenshot of the battery status and power source, noting the time of acquisition and time zone, keeping the device powered on and connected to a power source, and avoiding interaction with the device during the acquisition process to maintain the integrity of the data stored on the device.

- **Preservation** in energetic forensics from an Apple Watch digital forensics perspective involves taking steps to ensure that the device's energy state at the time of acquisition is captured and preserved in order to maintain the integrity of the data stored on it. The energy state of an Apple Watch refers to the device's current power level and status, including the battery status and the device's power source.

To preserve the energy state of an Apple Watch, it is important to keep the device powered on and connected to a power source during the acquisition process. This will prevent the device from entering a low power mode, which can cause data to be lost or altered. Additionally, it is important to avoid interacting with the device during the acquisition process as this can also affect the energy state and the integrity of the data.

Another important aspect of preservation in energetic forensics is to preserve the battery status, as the battery status information can be used to determine the device’s usage and power state at the time of acquisition. This can be done by taking a screenshot of the battery status or by using specialized software that can extract this information.

It is also important to take note of the time of acquisition and the time zone, as this can affect the timestamps of the data stored on the device. This is also important for the purpose of correlation with other data sources and not to misinterpret the time of events.

In summary, preservation in energetic forensics from an Apple Watch digital forensics perspective involves keeping the device powered on and connected to a power source during the acquisition process, preserving the battery status, and noting the time of acquisition and time zone to maintain the integrity of the data stored on the device.

- **Examination** in energetic forensics from an Apple Watch digital forensics perspective involves analyzing the energy-related data collected from the device during the acquisition process in order to understand the device's power state and usage at the time of acquisition. The energy-related data includes the device's battery level, power source, and other energy-related information that can be used to determine the device's usage and power state at the time of acquisition.

During the examination, the energy-related data collected during acquisition is analyzed to understand the device's power state and usage at the time of acquisition. This information can be used to determine if the device was running on battery power or if it was connected to a power source, as well as the battery level at the time of acquisition. This information can also be used to determine the device's usage patterns and to identify any anomalies or unusual activity.

It is also important to compare the examination results with the time of acquisition and the time zone to ensure that the timestamps of the data stored on the device are accurate. This can be used to correlate the examination results with other data sources and to understand the context of the data.

Examination in energetic forensics can also be done by using specialized software that can analyze the energy-related data and extract meaningful information,

In summary, examination in energetic forensics from an Apple Watch digital forensics perspective involves analyzing the energy-related data collected from the device during the acquisition process to understand the device's power state and usage at the time of acquisition, comparing the examination results with the time of acquisition and the time zone, and using specialized software to analyze the energy-related data and extract meaningful information.

- **Analysis** for energetic forensics from an Apple Watch digital forensics perspective involves evaluating the energy-related data collected from the device during the acquisition process in order to understand the device's power state and usage at the time of acquisition. The energy-related data includes the device's battery level, power source, and other energy-related information that can be used to determine the device's usage patterns and identify any anomalies or unusual activity.

The analysis process can involve several techniques, such as data visualization, statistical analysis and correlation with other data sources. Through these techniques, it is possible to understand the device's power state and usage patterns over time, identifying patterns or anomalies that could indicate a suspicious activity or data of interest.

It is also important to consider the time of acquisition and time zone during the analysis process, as this can affect the timestamps of the data stored on the device. This can be used to correlate the analysis results with other data sources and to understand the context of the data.

Specialized software can also be used to automate the analysis process and extract meaningful information from the energy-related data.

In summary, Analysis for energetic forensics from an Apple Watch digital forensics perspective involves evaluating the energy-related data collected from the device during the acquisition process to understand the device's power state and usage at the time of acquisition, applying techniques such as data visualization, statistical analysis and correlation with other data sources, considering the time of acquisition and time zone, and using specialized software to automate the analysis process and extract meaningful information.

d. Apple watch forensics Model:

According to the model proposed and developed by the author for Apple Watch digital forensics framework, which was developed to be used in cases of cybercrimes and to investigate them,

The Apple Watch could be an important and definitive witness in this crime, or it could indicate the involvement of a suspect.

In this model, the necessary results were reached as follows:

1. Classification of crime scenarios: One or all of the following questions must be answered here, or some of them:

- Was the watch used as a tool of crime?
- Was the watch targeted and attacked?
- Is the watch a witness to the suspect?

After answering these questions, work begins on the proposed model as follows:

2. A forensics examination of the Apple Watch, and in the event that the required information and evidence are extracted from inside the watch and the encrypted evidence is sent to the encrypted evidence repository to be decrypted with special programs, In the event of failure to check the watch, we repeat the process again to make sure and to find other solutions to extract the required information.
3. Examination of the iPhone and its applications, if it is associated with the watch or otherwise, as long as it was found at the crime scene, and in the event that there is encrypted data, it is also transferred to the encrypted evidence repository to be decrypted with special programs. In the event that nothing is found, we return once to choose another option to complete the criminal examination process.
4. examining the associated network at the scene of the crime, and in the event that there is evidence and encrypted data, it is also transferred to the encrypted evidence repository in order to decrypt it and extract the required information. In the absence of information, we can choose another option or complete the process.
5. In the end, after extracting the evidence and examining the encrypted data and decoding it, a presentation and an overview of all that was extracted are made before the competent authorities.

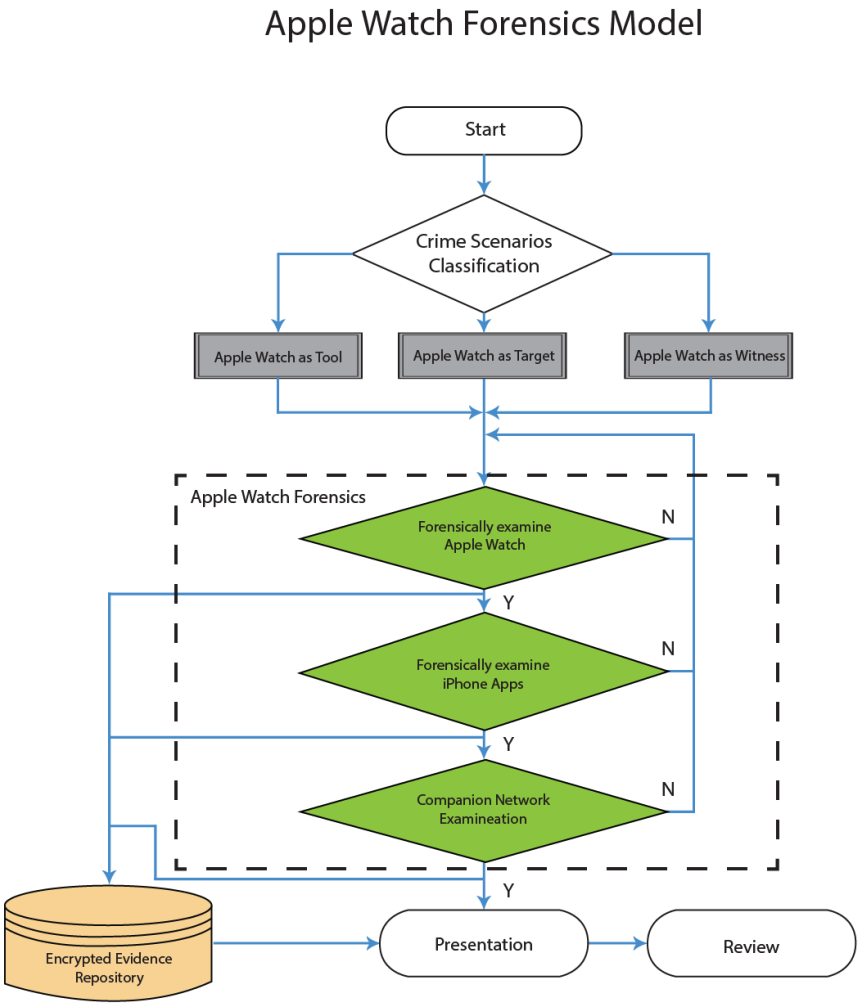


Figure 15: Proposed Apple watch forensics Model

e. Presentation

- **A report** on Apple watch digital forensics should include an overview of the case, details of the reconstruction and analysis process, dissemination of the evidence, and a plan for returning the evidence to the appropriate parties.
- **The reconstruction** process should involve the collection and preservation of all relevant data from the Apple watch, including system files, user data, and any associated cloud data. This data should then be analyzed to determine any relevant information for the case.
- **Dissemination** of the evidence should be done in a secure and controlled manner to ensure the integrity of the evidence is maintained. This may involve providing copies of the evidence to authorized parties, such as law enforcement or legal counsel, or presenting the evidence in a court of law.
- **The return of the evidence** should be done in a timely manner, and the chain of custody should be carefully documented to ensure the integrity of the evidence is maintained. The return process should also include the destruction of any copies of the evidence that are no longer needed.

In summary, a comprehensive report on Apple watch digital forensics should include details on the reconstruction, dissemination, and return of the evidence, as well as a plan for maintaining the integrity of the evidence throughout the process.

f. Documentation

Documentation is an essential component of any Apple watch digital forensics framework. It is important to document all aspects of the process, including the initial seizure of the device, the steps taken during the examination, and the results of the analysis. This documentation serves as evidence in court and is used to demonstrate the integrity and authenticity of the findings.

The initial documentation should include information such as the date and time of seizure, the location where the device was found, and the names of the individuals involved in the seizure. It is also important to document the condition of the device at the time of seizure, including any physical damage or tampering.

During the examination, it is important to document each step taken, including the tools and techniques used, and the findings. This documentation should also include any observations or notes made during the examination.

The final documentation should include a summary of the findings, including any relevant information that was discovered, and any conclusions that can be drawn from the examination. It is also important to include any limitations or issues that were encountered during the examination, and any recommendations for further action.

In summary, documentation is a vital component of an Apple watch digital forensics framework. It is important to document all aspects of the process, including the initial seizure, examination, and findings to ensure that the integrity and authenticity of the evidence is maintained, and the findings are admissible in court.

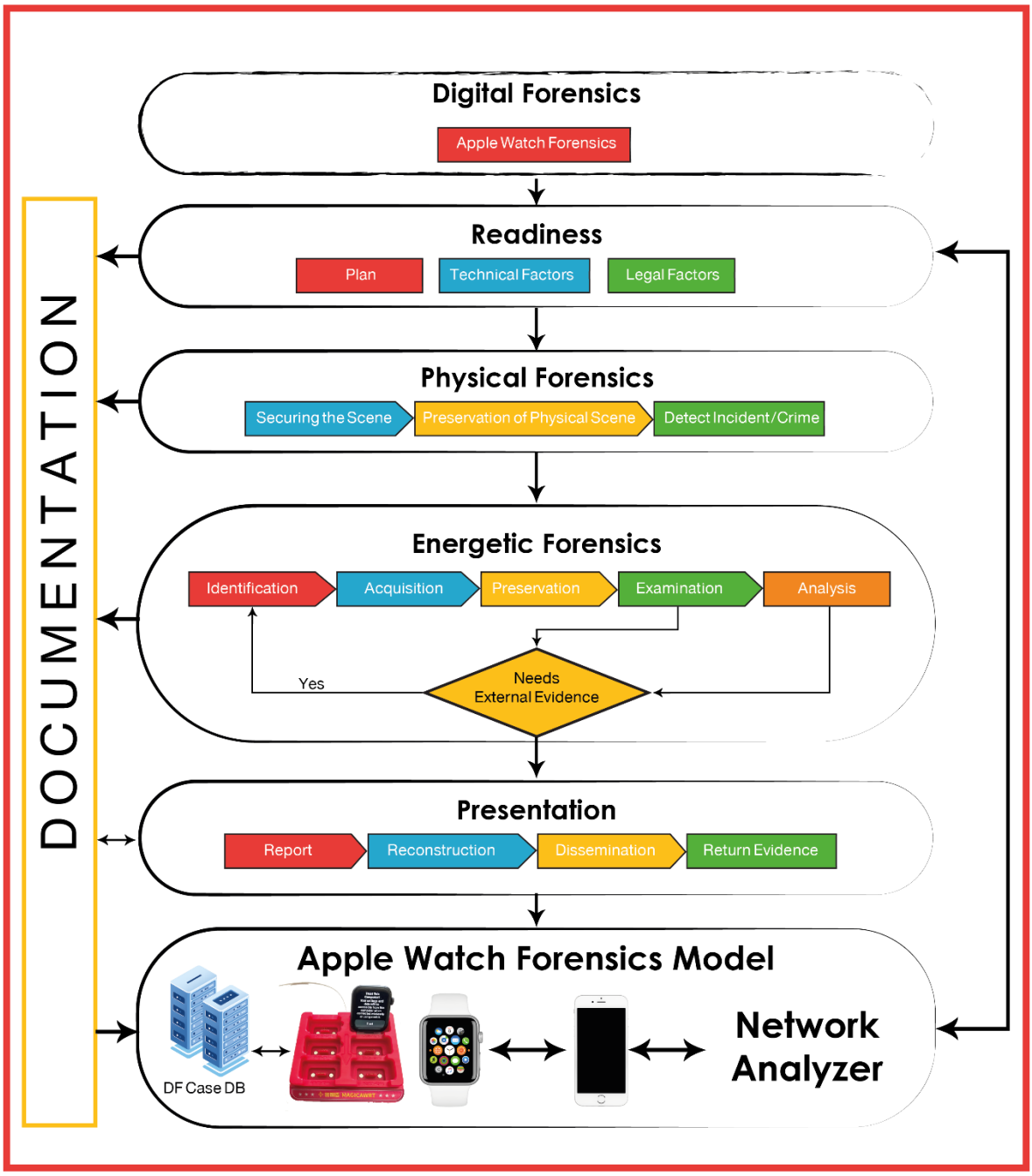


Figure 16:Proposed AWDFF for Apple Watch digital forensics Scenario Case

4.5.2 Mobile Digital Forensics Domain

Mobile digital forensics is the process of extracting, analyzing, and preserving digital evidence from mobile devices. The process typically involves the following steps:

a. Readiness:

Readiness from a mobile digital forensics perspective refers to the state of being prepared to properly extract, analyze, and interpret digital evidence from mobile devices. It involves having the necessary knowledge, tools, and procedures in place to conduct a thorough and effective digital forensic investigation.

- **Plan:** Proper protocols and procedures should be in place to ensure that the digital evidence is collected and handled in a manner that preserves its integrity and authenticity. It's important to follow strict protocols and standards to ensure that the evidence is admissible and maintain the chain of custody of the digital evidence.
- **Technical Factors:** One of the most important aspects of readiness is having the necessary knowledge and skills to properly extract and analyze digital evidence from mobile devices. This includes understanding the various types of mobile devices and operating systems, as well as being familiar with the tools and techniques used to extract data from them. This knowledge is critical to be able to identify the most relevant data and to know how to properly process it. Another key aspect of readiness is having the necessary tools and equipment for extracting and analyzing digital evidence. This includes hardware and software for imaging and analyzing mobile devices, as well as specialized tools for analyzing network traffic and other data. It's also important to ensure that these tools are kept up-to-date with the latest versions and updates to ensure that they are compatible with current devices.
- **Legal Factors:** Finally, readiness also includes having a clear understanding of the legal aspects of digital forensics, including the laws and regulations that govern the collection and use of digital evidence. It is important that the digital forensic team is aware of their legal obligations to maintain the evidence integrity and its admissibility in court.

In summary, readiness from a mobile digital forensics perspective requires having the necessary knowledge, tools, and procedures in place to conduct a thorough and effective digital forensic investigation. This includes having a clear understanding of mobile devices, the tools

and techniques used to extract data, and the legal aspects of digital forensics, as well as maintaining protocols and procedures to ensure the integrity of the evidence.

b. Physical Forensics

- **Securing the Scene:** Securing the scene from a mobile digital forensics perspective involves taking the necessary steps to preserve the integrity of the evidence and prevent contamination or damage to the devices and data. This is important to ensure that the digital evidence is admissible in court and to be able to retrieve as much useful information as possible.

The first step in securing the scene is to identify and isolate the iPhone devices that may contain relevant digital evidence. This includes not just the device of the suspect, but also any other devices that may have been in the vicinity of the incident, such as security cameras or other mobile phones. Once identified, the devices should be secured and protected to prevent tampering or damage.

The next step is to collect the devices and their accessories and document the condition of them. This includes taking photographs of the devices and any damage or markings, as well as noting the make and model, the firmware version, and any other relevant details.

The devices should be placed in a Faraday bag to prevent any data from being deleted or changed due to incoming or outgoing signals. This bag is a specialized bag that blocks all wireless signals, including cellular, WiFi, and Bluetooth. This is important to maintain the integrity of the data on the device, and to prevent any further contamination or alteration of the evidence.

Once the devices are secured, a forensic image of the device's memory should be made. This image will serve as an exact copy of the device's memory, and it will be used to analyze the data. This process is usually done using specialized hardware and software.

It's important to maintain a chain of custody for the devices and the images. This means that the devices and the images should be secured, and their movements tracked, and the person responsible for their care should be documented.

Securing the scene and collecting the mobile digital evidence is crucial step in mobile digital forensics. It plays an important role in preserving the evidence and prevents any contamination that may prevent the evidence from being admissible in court. Proper procedures and protocols should be followed to ensure that the integrity and authenticity of the evidence is maintained.

- **Preservation of Physical scene:** Preservation of the physical scene from a mobile digital forensics perspective is the process of securing and protecting the location where a mobile device is found in order to prevent contamination or damage to the device and its surrounding environment. This is important to ensure that the digital evidence is admissible in court and to be able to retrieve as much useful information as possible from the device and its surroundings.

The first step in preserving the physical scene is to identify and secure the area where the mobile device was found. This includes not just the device itself, but also any other items or locations that may have been involved in the incident or may have been in contact with the device. This could include other mobile devices, computers, storage media, or other electronic equipment.

Once the area has been secured, the scene should be documented with photographs and videos, detailing the location of the device and any other relevant items. It is important to note the condition of the device, any signs of damage, and any other relevant information. Additionally, it's important to note the position of the device, and its immediate environment.

Next, it's important to secure and preserve the device by placing it in a Faraday bag, which blocks all incoming and outgoing signals. This is important to maintain the integrity of the data on the device, and to prevent any further contamination or alteration of the evidence.

It's important to maintain a chain of custody for the devices and the images. This means that the devices and the images should be secured, and their movements tracked, and the person responsible for their care should be documented.

Preserving the physical scene is critical step in mobile digital forensics. It plays an important role in preserving the evidence and prevents any contamination that may prevent the evidence from being admissible in court. Proper procedures and protocols should be followed to ensure that the integrity and authenticity of the evidence is maintained and a clear understanding of the incident or crime can be inferred.

- **Detect incident/crime:** From a digital forensics perspective, detecting an incident or crime involves extracting, analyzing, and interpreting digital evidence to uncover relevant information. The process typically begins with the identification and preservation of digital evidence, such as computer systems, mobile devices, and storage media.

Once the evidence has been collected, it is analyzed using specialized software tools and techniques. This analysis can include examining file systems, network traffic, and deleted or hidden files. The goal is to uncover relevant information, such as the date and time of the incident, the individuals involved, and the actions that were taken.

One of the important aspects of Digital Forensics is the ability to identify and recover data from digital devices that has been manipulated or erased by the perpetrator. this is useful in incidents where the perpetrator tries to hide their tracks by deleting files or formatting storage devices.

After the analysis is complete, the digital forensics investigator will document their findings in a report. The report includes an overview of the digital evidence collected and the analysis performed, as well as any conclusions or recommendations.

The collected digital evidence, along with the report, can be used in court to help prove or disprove the incident or crime. It's considered an important piece of evidence in many criminal cases as it can provide an objective, technical and scientific evidence.

It's worth noting that Digital Forensics investigators should be aware of the legal aspects of their work and the legal procedures to maintain the authenticity and integrity of the evidence in the court of law. They must follow strict protocols and standards to ensure that the evidence is admissible and maintain the chain of custody of the digital evidence.

c. Energetic Forensics

- **Identification:** Identification from Energetic forensics perspective refers to the process of determining the identity of a suspect or perpetrator in a criminal case. This process is typically triggered by an incident or crime that has occurred, and it involves the collection, analysis, and interpretation of digital evidence to identify the individual(s) responsible.

In reactive forensics, digital evidence is collected from the devices and environment that is suspected to have been used or been in contact with the perpetrator. This evidence can include, but not limited to computers, mobile devices, storage media, cloud accounts, and any other devices that store digital data. The collected evidence is analyzed using specialized tools and techniques to extract relevant information such as user account, IP address, timestamps, and others.

- **Acquisition:** Next, the data on the iPhone device is acquired using specialized tools and techniques (MOBILedit Forensic Express). This can include physical acquisition,

in which a complete copy of the device's memory is made, or logical acquisition, in which specific data of interest is extracted.

- **Preservation:** In mobile forensics, preservation refers to the process of collecting and maintaining evidence from mobile devices in a manner that preserves its integrity and authenticity. In energetic forensics scenario, preservation typically occurs after an incident has been detected and is focused on capturing evidence that may be relevant to an investigation.

The first step in preservation is to secure the device and ensure that no further changes are made to the evidence. This can include shutting down or disconnecting the mobile device, or physically securing the location where the incident occurred.

Next, an image of the relevant storage devices (such as the internal storage or SD card of a mobile device) is created using specialized software. This image is an exact duplicate of the original storage device and can be used for analysis without risking damage to the original evidence.

Once the image has been created, it can then be processed using various forensic tools to extract any relevant data. These tools are specialized for mobile devices and can be used to extract data such as call logs, text messages, contacts, and other information.

It's important to note that during the preservation process, it's crucial to properly handle the device and maintain its power state, for example if the device is off, it should remain off during the process. Additionally, if the device is locked, the password or PIN should not be entered as that would alter the evidence.

It's also important to document all actions and tools used in the process to maintain the integrity of the evidence and to be able to use it as proof in court. The preservation process in mobile forensics is critical since it determines the authenticity of the evidence, and to prevent the loss or modification of information during the investigation process.

- **Examination** in mobile forensics refers to the process of analyzing and extracting relevant data from a mobile device using specialized tools and techniques. In energetic forensics scenario, examination typically occurs after an incident has been detected and preserved and is focused on identifying and extracting evidence that may be relevant to an investigation.

The first step in examination is to analyze the image of the mobile device that was created during the preservation process. This image is then processed using various forensic tools to extract data such as call logs, text messages, contacts, and other information.

Forensic tools used in mobile forensics are specialized software that are designed to extract data from mobile devices and can handle a wide range of different file types and operating systems. Tools can be used to extract data from a variety of sources such as the device's internal storage and even cloud accounts linked to the device.

The examination process can also include the analysis of specific areas of the device such as the file system, applications and their data, and the device's memory to identify any hidden or deleted data that may be relevant to the investigation.

It's important to document all actions and tools used during the examination process to maintain the integrity of the evidence and to be able to use it as proof in court. Additionally, the examination process should be done in a controlled environment, to prevent any accidental changes or accidental contamination of the evidence.

The examination process in mobile forensics is critical in order to identify and extract relevant data from the mobile device and to present it as evidence in court. This can be especially important in legal cases as it can be the key evidence that helps establish facts and identify suspects.

- **Analysis:** Energetic mobile forensics is a method of analyzing mobile devices in response to a specific event or incident, such as a criminal investigation or security breach. The goal of energetic mobile forensics is to extract, preserve, and analyze digital evidence from mobile devices in a forensically sound manner.

The first step in energetic mobile forensic analysis is the seizure and preservation of the mobile device. This involves properly powering off the device and taking steps to prevent any further changes to the data stored on the device. The device is then imaged to create a forensic copy of the data, which can be analyzed without modifying the original data.

Next, the forensic analyst will use specialized software and tools to extract and analyze data from the device. This can include extracting call logs, text messages, contacts, GPS data, and other types of information that may be relevant to the investigation. The analyst may also look for deleted data, which can be recovered using specialized software.

The extracted data is analyzed to identify relevant information and potential leads. This can include identifying patterns in phone usage, tracking the movements of a suspect, or identifying potential suspects through call or text message logs. The information collected and analyzed can be used to build a case, provide leads for further investigation, or to serve as evidence in court.

Additionally, in recent times with increase of mobile application usage, Application data and application based activities also need to be extracted and analyze from mobile device during investigation.

It's important to note that the process of mobile forensics can be complex, and it's important to have a clear understanding of the legal implications of the investigation and to ensure that the process adheres to laws and regulations regarding the search and seizure of electronic evidence.

d. Presentation:

The report and the digital evidence collected is presented to the court in trial to help the judge or jury to make a decision.

It's worth noting that for successful digital forensics in mobile devices, it's important that the investigator follows strict protocols and standards, proper chain of custody and admissibility of the evidence in court.

- **Reporting:** Reporting from a presentation perspective in mobile forensics refers to the process of documenting the results of a mobile device analysis in a clear, concise, and comprehensive manner that can be presented to a court, law enforcement agencies, or other relevant parties.

A mobile forensic report should include detailed information about the analysis process, including the type of device analyzed, the tools and methods used, and any limitations of the analysis. It should also include information about the device itself, such as the make, model, and operating system version.

The report should include a summary of the findings, highlighting the most important information and evidence. It should also include detailed information about the data extracted from the device, such as call logs, text messages, contacts, GPS data, and any other relevant information.

The report should be written in a professional and unbiased manner, and it should be reviewed and validated by a qualified expert in the field of mobile forensics.

The report should be easy to understand for non-technical audience and should be presented in logical and clear manner with the help of visual aids such as images and diagrams. The report should also include any relevant screenshots or images from the device that can help to support the findings.

Additionally, any information that is not relevant to the case should be marked as such and should not be included in the report.

It's important to keep in mind that mobile forensic reports are considered as legal document and should be reliable and admissible as evidence in court and should follow all the legal and ethical guidelines.

- **Reconstruction:** Reconstruction from a presentation perspective in mobile forensics refers to the process of creating a comprehensive report of the findings from the analysis of a mobile device, along with visual aids such as images and diagrams, that can be presented to a court or other relevant parties. The report should clearly explain the methodology used, the evidence collected and analyzed, and the conclusions drawn from the analysis.

The reconstruction process starts with reviewing and analyzing all the data obtained from the mobile device, the analyst will then carefully select only the most relevant and significant data for the presentation. This data is then organized in a logical and easy-to-understand manner, which can include timelines, charts, and other types of visual aids.

The report should be accurate and thorough, yet easy to understand for non-technical audience. The report should provide information on the tools and methods used during the analysis, as well as any limitations of the analysis.

It should be also including information about the device such as model, operating system version and specific details about the device history if relevant to the case.

In addition to the technical report, the presentation should also include a summary of the findings, highlighting the most important information and evidence. A visual representation of the data, such as a chart or map, can help to simplify complex information and make it easier to understand for the audience.

It's important to note that the reconstruction and presentation of findings from mobile forensics analysis should adhere to legal and ethical guidelines, and the report must be reliable and admissible as evidence in court.

- **Dissemination** from a presentation perspective in mobile forensics refers to the process of sharing the results of a mobile device analysis with relevant parties, such as law enforcement agencies, legal teams, or other stakeholders. The goal of dissemination is to ensure that the findings of the analysis are communicated in a clear and efficient manner, so that they can be used to support investigations or legal proceedings.

The dissemination process typically begins with the creation of a mobile forensic report, which is a comprehensive document that summarizes the analysis process, the evidence collected, and the conclusions drawn from the analysis. This report is then shared with the relevant parties, such as law enforcement agencies, legal teams, or other stakeholders.

When disseminating the report, it is important to ensure that the information is presented in a clear, concise, and easy-to-understand manner, so that it can be used effectively by the recipients. Visual aids such as images, charts and diagrams are also important to simplify the complex information.

It's also important to note that not all parties will have the same level of technical knowledge and may not understand certain technical terms or methods used, so the report should be written in a manner that is easy to understand for non-technical audience.

In addition to the written report, the forensic analyst may also be asked to present the findings in person, such as in court or at a meeting with law enforcement. In these situations, the analyst should be prepared to explain the analysis process and the evidence collected in a clear and concise manner.

It's also important to keep in mind that dissemination should be done only with the permission of all the relevant parties and it should be done in a way that adheres to legal and ethical guidelines. Also, it's important to ensure that sensitive information is kept confidential and not shared with parties who are not authorized to receive it.

- **Returning evidence** from a presentation perspective in mobile forensics refers to the process of returning the original device or data to the original owner after the completion of a mobile device analysis. This process is an important step in the overall

mobile forensics process as it ensures that the original device or data is returned to the rightful owner and that the integrity of the evidence is maintained.

The first step in returning evidence is to create a detailed inventory of the device or data that is being returned. This inventory should include information such as the make, model, and serial number of the device, as well as a detailed description of the data that was collected and analyzed.

After the inventory is complete, the device or data should be securely packaged and labeled with identifying information such as the owner's name, case number, and the date of return. It is important that the package is properly sealed and secure to prevent damage to the device or data and to maintain the integrity of the evidence.

It's also important to make sure that the device or data is returned to the correct person or organization. This can be done by confirming the identity of the person or organization who is receiving the device or data, and by obtaining a signature or other proof of receipt.

The forensic analyst should also provide a written statement about the process of analysis and any findings, this can help the owner or relevant parties in understanding how the device or data was handled and analyzed.

It's important to keep in mind that return of evidence should be done in accordance with legal and ethical guidelines, and the integrity of the evidence should be maintained at all times. Also, it's important to keep in mind that the device or data returned is not altered in any way and it should be in the same state as it was before the analysis.

e. Documentation

from a mobile forensics' perspective refers to the process of creating and maintaining records of the steps taken during the analysis of a mobile device, including the methods used, the evidence collected, and the conclusions drawn. This documentation is important for maintaining the integrity of the evidence and for demonstrating the validity of the analysis in a court of law.

The first step in documentation is to create a detailed log of the analysis process, which should include information such as the date and time of the analysis, the make and model of the device, and the tools and methods used during the analysis. It should also include a record of any

actions taken on the device, such as powering off the device or making a forensic image of the data.

Next, the forensic analyst should create detailed notes and records of the evidence collected and analyzed, including any relevant images, files, or data extracted from the device. These records should be organized in a logical and easy-to-understand manner and should be clearly labeled with information such as the date and time the evidence was collected, the source of the evidence, and the analyst's observations and conclusions.

As part of documentation, the analyst should also create a detailed timeline of the events, this can be helpful in understanding the activities and events leading to the investigation and during the course of investigation.

It's also important to document any issues or limitations encountered during the analysis, such as hardware or software failures or challenges in extracting or analyzing certain types of data.

It's important to keep in mind that the documentation process should be thorough, accurate and unbiased. The documentation should be reviewed and validated by a qualified expert in the field of mobile forensics and should be stored securely to maintain its integrity.

It's also important to ensure that all documentation is admissible as evidence in court and follows the legal and ethical guidelines.

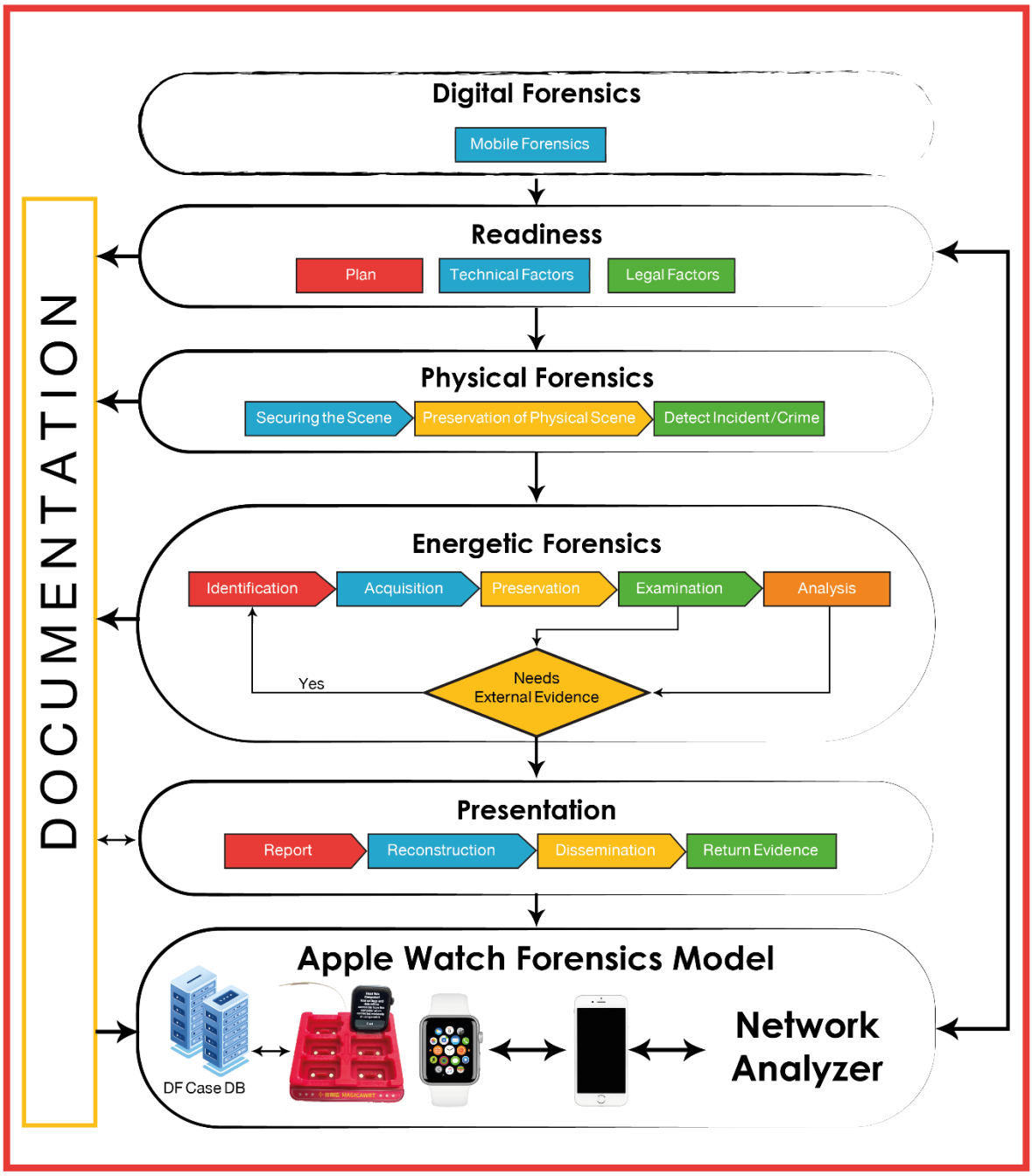


Figure 17:Proposed AWDFF for mobile digital forensics Scenario Case

4.5.3 Network Forensics Domain

Network forensics is the process of collecting, analyzing, and preserving evidence from network-based incidents. This evidence is used to investigate network security breaches, troubleshoot network issues, and identify malicious activity. Network forensics involves capturing network traffic, analyzing logs, and using specialized tools to extract information from the data. It is an important aspect of incident response and cybersecurity.

a. Readiness

Network digital forensics readiness refers to the preparedness of an investigation organization to detect, respond to, and investigate network security incidents. This includes having the necessary tools, processes, and personnel in place to effectively collect, preserve, and analyze digital evidence.

- **Plan:** A readiness plan for network digital forensics is a comprehensive document that outlines the steps an organization will take to prepare for, respond to, and investigate network security incidents. The plan should be tailored to the specific needs of the organization and should be reviewed and updated regularly to ensure it remains effective.

A readiness plan for network digital forensics should include the following components:

- Incident response plan: This outlines the procedures that will be followed in the event of a network security incident. It should include steps for preserving evidence, communicating with relevant parties, and reporting the incident.
- Network monitoring: The plan should include details on the network monitoring tools that will be used to detect and alert on suspicious activity.
- Digital forensics team: The plan should identify the personnel who will be responsible for performing network forensic investigations and outline their roles and responsibilities.
- Evidence collection: The plan should include procedures for capturing and preserving network traffic and other digital evidence in a forensically sound manner.
- Evidence analysis: The plan should include procedures for analyzing network traffic and other digital evidence to identify the cause of an incident and determine the scope of the damage.
- Reporting and communication: The plan should include procedures for reporting and communicating the findings of an investigation to relevant parties.

- Training and drills: The plan should include regular training and drills to ensure that the incident response team and other personnel are prepared to respond to network security incidents.

Having a readiness plan in place can ensure that an organization is prepared to detect, respond to, and investigate network security incidents and minimize the damage caused by an incident.

- **Technical Factors:** When it comes to network digital forensics readiness, there are several technical factors that organizations should consider in order to effectively detect, respond to, and investigate network security incidents.
- Network monitoring: Implementing tools such as intrusion detection systems (IDS) and network behavior analysis (NBA) systems to monitor network activity and detect suspicious activity is critical. These tools can also provide detailed information that can be used in forensic investigations.
- Evidence collection: It is important to have the capability to capture and preserve network traffic and other digital evidence in a forensically sound manner. This may include using network taps, packet capture appliances, or other tools to collect network traffic, as well as procedures for preserving the integrity of the evidence.
- Evidence analysis: Having tools and processes in place for analyzing network traffic and other digital evidence to identify the cause of an incident and determine the scope of the damage is crucial. This may include using network forensics analysis tools, incident response platforms, or other specialized software to analyze the evidence.
- Incident response platform: Having an incident response platform that integrates with the organization's security stack and provides a centralized view of security incidents and alerts can help to improve the incident response process and make it more efficient.
- Data backup and archiving: Organizations should have a backup and archiving strategy in place to ensure that data can be recovered in the event of an incident. This is important for both incident response and forensic investigations.
- Personnel training: Having personnel trained in network digital forensics, incident response, and incident handling is key for readiness. This includes not only the incident response team, but also other personnel who may be involved in incident response or forensic investigations.
- Regular testing and updating: Regularly testing and updating incident response plans, procedures and tools, can help to ensure that they remain effective and that the organization is prepared to respond to the latest threats.

Having these technical factors in place can ensure that an organization is equipped to effectively detect, respond to, and investigate network security incidents, and minimize the damage caused by an incident.

- **Legal Factors:** When it comes to network digital forensics readiness, there are several legal factors that organizations should consider in order to ensure that their incident response and forensic investigations are conducted in a manner that is compliant with relevant laws and regulations.
- Data privacy and protection laws: Organizations need to be aware of data privacy and protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) and ensure that their incident response and forensic investigation activities are compliant with these laws.
- Admissibility of digital evidence: Organizations should be aware of the rules of evidence and the procedures for preserving and collecting digital evidence that will be admissible in court. This includes understanding the chain of custody and the best practices for preserving the integrity of digital evidence.
- Cybercrime laws: Organizations should be familiar with the laws related to cybercrime and ensure that their incident response and forensic investigations are conducted in compliance with these laws.
- Compliance with industry regulations: Organizations may be subject to specific industry regulations such as the Payment Card Industry Data Security Standard (PCI-DSS) and should ensure that their incident response and forensic investigations are compliant with these regulations.
- Legal requirements for incident reporting: Organizations should be familiar with the legal requirements for incident reporting and ensure that they are compliant with these requirements. This may include reporting incidents to law enforcement, regulatory bodies, or other relevant parties.
- Legal representation: Organizations should have a legal representative or a team of legal representatives that can provide legal guidance and support during incident response and forensic investigations.
- Insurance policies: Organizations should be familiar with their insurance policies and understand what is covered in the case of a security incident, and how to make a claim if necessary.

Having these legal factors in place can ensure that an organization is prepared to handle legal issues that may arise during incident response and forensic investigations, and minimize the risk of legal repercussions.

b. Physical Forensics:

- **Securing the scene** is an important step in physical forensics from a network digital forensics perspective, as it ensures that the integrity of the evidence is preserved and that the investigation can proceed in a manner that will yield accurate and reliable results. From a network digital forensics perspective, securing the scene may involve the following steps:
- Isolation: The scene should be isolated to prevent contamination and to ensure that the integrity of the evidence is preserved. This may involve physically securing the area and limiting access to authorized personnel only.
- Documenting the scene: The scene should be thoroughly documented, including taking photographs and videos of the area, and noting the location of any relevant evidence. This documentation can be used as reference during the investigation and can also be used to support any legal proceedings that may occur.
- Evidence collection: Evidence should be collected in a manner that preserves its integrity. This may involve using specialized equipment such as evidence bags, gloves, and other protective gear to handle the evidence.
- Chain of custody: A chain of custody should be established for all evidence collected. This includes documenting who has had access to the evidence, when it was collected, and how it has been stored.
- Secure storage: The evidence should be securely stored to prevent any tampering or damage. This may involve using specialized storage containers and keeping the evidence in a secure location.

By following these steps, organizations can ensure that the scene is properly secured and that the integrity of the evidence is preserved. This will allow them to conduct a thorough and effective investigation and to produce accurate and reliable results.

- **Preservation of the physical scene** is crucial in physical forensics from a network digital forensics perspective, as it ensures that the integrity of the evidence is maintained and that the investigation can proceed in a manner that will yield accurate

and reliable results. From a network digital forensics perspective, preservation of the physical scene may involve the following steps:

- Securing the scene: The scene should be secured to prevent contamination and to ensure that the integrity of the evidence is preserved. This may involve physically securing the area and limiting access to authorized personnel only.
- Documenting the scene: The scene should be thoroughly documented, including taking photographs and videos of the area, and noting the location of any relevant evidence. This documentation can be used as reference during the investigation and can also be used to support any legal proceedings that may occur.
- Evidence collection: Evidence should be collected in a manner that preserves its integrity. This may involve using specialized equipment such as evidence bags, gloves, and other protective gear to handle the evidence.
- Chain of custody: A chain of custody should be established for all evidence collected. This includes documenting who has had access to the evidence, when it was collected, and how it has been stored.
- Secure storage: The evidence should be securely stored to prevent any tampering or damage. This may involve using specialized storage containers and keeping the evidence in a secure location.
- Temperature and humidity control: The physical scene should be preserved in a controlled environment with a stable temperature and humidity to prevent damage to the evidence.
- Timely collection: Evidence should be collected as soon as possible after the incident to prevent any damage or alteration of the scene.

By following these steps, organizations can ensure that the physical scene is properly preserved and that the integrity of the evidence is maintained. This will allow them to conduct a thorough and effective investigation and to produce accurate and reliable results.

- **Detection of an incident or crime** from a physical forensics perspective for network digital forensics involves identifying and locating the physical evidence that is related to the incident or crime, and then using that evidence to determine the cause of the incident or crime, and the scope of any damage. From a network digital forensics perspective, detection of an incident or crime may involve the following steps:
- Network monitoring: Use of network monitoring tools such as intrusion detection systems (IDS) and network behavior analysis (NBA) systems can detect suspicious

activity on the network and provide valuable information that can be used to identify the cause of an incident or crime.

- Log analysis: Analyzing system and security logs can also provide valuable information about the incident or crime. This may include reviewing system and application logs, firewall logs, and other security logs to identify suspicious activity.
- Physical examination of devices: Examining the physical devices that were involved in the incident or crime can provide valuable information. This may include conducting a physical examination of servers, routers, switches, and other network devices to identify signs of tampering or damage.
- Analysis of storage media: Analysis of storage media such as hard drives and USB drives can provide valuable information about the incident or crime. This may include conducting file system analysis, data carving, and other techniques to extract information from the storage media.
- Interviews: Interviews with relevant personnel, such as system administrators and network operators, can also provide valuable information about the incident or crime.
- Correlating data: Correlating the data obtained from these various sources can help to paint a comprehensive picture of the incident or crime, and to identify the cause and scope of the damage.

By following these steps, organizations can effectively detect an incident or crime and gather the necessary information to investigate and resolve the issue.

c. Energetic Forensics:

- **Identification** in energetic forensics from a network digital forensics perspective refers to the process of identifying the source and cause of a network security incident, such as a cyber-attack or data breach. From a network digital forensics perspective, identification in energetic forensics may involve the following steps:
- Network monitoring: Use of network monitoring tools such as intrusion detection systems (IDS) and network behavior analysis (NBA) systems can detect suspicious activity on the network and provide valuable information that can be used to identify the source of an incident.
- Log analysis: Analyzing system and security logs can also provide valuable information about the incident. This may include reviewing system and application logs, firewall logs, and other security logs to identify suspicious activity.

- Packet capture and analysis: Capturing and analyzing network traffic can provide valuable information about the incident, such as IP addresses, ports, and protocols used by the attacker.
- Malware analysis: Analysis of any malware that may have been used in the incident can provide valuable information about the source of the attack.
- Correlation of data: Correlating the data obtained from these various sources can help to paint a comprehensive picture of the incident, and to identify the source of the attack.
- Identifying the attackers: Identifying the attackers' infrastructure, tactics, techniques, and procedures (TTPs) and possibly the group or individual behind the attack.

By following these steps, organizations can effectively identify the source and cause of a network security incident, and gather the necessary information to investigate and resolve the issue.

- **Acquisition** in energetic forensics from a network digital forensics perspective refers to the process of collecting, preserving, and analyzing data related to a network security incident, such as a cyber-attack or data breach. From a network digital forensics perspective, acquisition in energetic forensics may involve the following steps:
- Network traffic capture: Capturing network traffic using tools such as network taps, packet capture appliances, or other tools to collect network traffic, and preserving the integrity of the evidence.
- Memory and hard drive imaging: Creating bit-by-bit copies of the memory and hard drive of the affected systems, which can be used for offline analysis and to preserve the integrity of the evidence.
- Log collection: Collecting system and security logs from the affected systems, which can provide valuable information about the incident.
- Evidence collection: Collecting any other relevant physical evidence such as hard drives, USB drives, and other storage devices that have been used to store digital evidence.
- Evidence preservation: Preserving the integrity of the evidence by following best practices such as maintaining the chain of custody, storing the evidence in a secure location, and ensuring that the evidence is not tampered with or modified.
- Evidence analysis: Analyzing the evidence using specialized tools and techniques such as network forensics analysis tools, incident response platforms, or other

specialized software to analyze the evidence and identify the cause of the incident and the scope of the damage

By following these steps, organizations can effectively acquire the data related to a network security incident, preserve its integrity, and analyze it to identify the cause of the incident and the scope of the damage.

- **Preservation** in energetic forensics from a network digital forensics perspective refers to the process of maintaining the integrity of the evidence related to a network security incident, such as a cyber-attack or data breach. This includes ensuring that the evidence is not tampered with or modified, and that it can be used in legal proceedings if necessary. From a network digital forensics perspective, preservation in energetic forensics may involve the following steps:
- Evidence labeling and documentation: Properly labeling and documenting the evidence, including the date, time, and location of where the evidence was collected and the person who collected it.
- Chain of custody: Establishing a chain of custody for all evidence collected, which includes documenting who has had access to the evidence, when it was collected, and how it has been stored.
- Secure storage: Storing the evidence in a secure location to prevent any tampering or damage, and using specialized storage containers if necessary.
- Temperature and humidity control: Storing the evidence in a controlled environment with a stable temperature and humidity to prevent damage to the evidence.
- Imaging: Creating bit-by-bit copies of the digital evidence to preserve the integrity of the original data and to provide an unaltered copy for analysis.
- Timely preservation: Preservation should be done as soon as possible after the incident to prevent any damage or alteration of the evidence.

By following these steps, organizations can ensure that the integrity of the evidence is maintained, and that the evidence can be used in legal proceedings if necessary.

- **Examination** in energetic forensics from a network digital forensics perspective refers to the process of analyzing the data and evidence related to a network security incident, such as a cyber-attack or data breach. This includes using specialized tools and techniques to extract information from the evidence and to identify the cause of the

incident and the scope of the damage. From a network digital forensics perspective, examination in energetic forensics may involve the following steps:

- Evidence analysis: Analyzing the evidence using specialized tools and techniques such as network forensics analysis tools, incident response platforms, or other specialized software to extract information from the evidence.
- File system analysis: Analyzing the file system of the affected systems to extract information such as deleted files, hidden files, and timestamps.
- Data carving: Extracting deleted or hidden files from the affected systems.
- Memory analysis: Analyzing the memory of the affected systems to extract information such as running processes, network connections, and open files.
- Malware analysis: Analyzing any malware that may have been used in the incident to extract information about the attack.
- Correlation of data: Correlating the data obtained from various sources, such as network traffic, system logs, and other evidence, to paint a comprehensive picture of the incident and identify the cause of the attack.

By following these steps, organizations can effectively examine the data and evidence related to a network security incident, and extract the necessary information to identify the cause of the incident and the scope of the damage

- **Analysis** in energetic forensics from a network digital forensics perspective refers to the process of interpreting the data and evidence related to a network security incident, such as a cyber-attack or data breach, in order to determine the cause of the incident and the scope of the damage From a network digital forensics perspective, analysis in energetic forensics may involve the following steps:
- Evidence analysis: Analyzing the evidence using specialized tools and techniques such as network forensics analysis tools, incident response platforms, or other specialized software to extract information from the evidence.
- File system analysis: Analyzing the file system of the affected systems to extract information such as deleted files, hidden files, and timestamps.
- Data carving: Extracting deleted or hidden files from the affected systems.
- Memory analysis: Analyzing the memory of the affected systems to extract information such as running processes, network connections, and open files.
- Malware analysis: Analyzing any malware that may have been used in the incident to extract information about the attack.

- Correlation of data: Correlating the data obtained from various sources, such as network traffic, system logs, and other evidence, to paint a comprehensive picture of the incident and identify the cause of the attack.
- Identifying the attackers: Identifying the attackers' infrastructure, tactics, techniques, and procedures (TTPs) and possibly the group or individual behind the attack.
- Determining the scope of the damage: Determining the scope of the damage caused by the incident, including the systems, data, and resources that were affected.
- Developing a response plan: Developing a plan to respond to the incident, including steps to contain the incident, eradicate the threat, recover from the incident, and implement measures to prevent future incidents.

By following these steps, organizations can effectively analyze the data and evidence related to a network security incident, and determine the cause of the incident and the scope of the damage, to respond and prevent further incidents.

d. Presentation

Presentation in network digital forensics refers to the process of communicating the findings of a digital forensic investigation to relevant parties in a clear and concise manner. This includes creating detailed reports, visual aids, and other forms of documentation that can be used to present the findings of the investigation

- **Reporting** for presentation from a network digital forensics perspective refers to the process of creating a detailed, accurate, and comprehensive report that documents the findings of a digital forensic investigation. This report is used to communicate the findings of the investigation to relevant parties, such as management, legal counsel, and other stakeholders. From a network digital forensics perspective, reporting for presentation may involve the following steps:
- Defining the scope of the investigation: Clearly defining the scope of the investigation and the objectives of the report.
- Evidence documentation: Detailing the evidence collected, including the location, type, condition, the methods used to collect it, and the persons who collected it.
- Analysis documentation: Documenting the analysis of the evidence, including the methods and tools used, the findings, and the conclusions reached.

- Correlation of data: Correlating the data obtained from various sources, such as network traffic, system logs, and other evidence, to paint a comprehensive picture of the incident and identify the cause of the attack.
- Identifying the attackers: Identifying the attackers' infrastructure, tactics, techniques, and procedures (TTPs) and possibly the group or individual behind the attack.
- Determining the scope of the damage: Determining the scope of the damage caused by the incident, including the systems, data, and resources that were affected.
- Developing a response plan: Developing a plan to respond to the incident, including steps to contain the incident, eradicate the threat, recover from the incident, and implement measures to prevent future incidents.
- Organizing and writing the report: Organizing the information and writing the report in a professional manner, making sure it is clear, concise, and easy to understand.
- Reviewing and editing: Reviewing and editing the report to ensure that it is accurate, complete, and free of errors.
- Formatting the report: Formatting the report in a professional and visually appealing manner, including the use of tables, charts, and images to supplement the text and make it more engaging to read.
- Reviewing and getting feedback: Reviewing the report with the relevant parties and getting feedback on the report to make any necessary revisions.

By following these steps, organizations can create a comprehensive, accurate, and easy to understand report that effectively communicates the findings of a network digital forensic investigation to relevant parties.

- **Reconstruction:** From a network digital forensics perspective, reconstruction refers to the process of analyzing and piecing together information from various sources to reconstruct an event or series of events that occurred on a network. This process involves collecting, preserving, and analyzing data from various sources such as servers, routers, switches, and other network devices, as well as endpoints such as computers and mobile devices.

Reconstruction can be used to identify and track down the source of a network intrusion, reconstruct a cyber attack, and identify the scope of an incident. This can be done by analyzing log files, packet captures, and other data to identify patterns and anomalies that may indicate

suspicious activity. Once suspicious activity is identified, the data can be further analyzed to reconstruct the event and determine the actions taken by the attacker.

Reconstruction can also be used to identify and track down the source of data breaches and other types of network incidents. This can be done by analyzing data from various sources, such as network traffic and endpoint data, to identify patterns and anomalies that may indicate suspicious activity. Once the source of the incident is identified, the data can be further analyzed to reconstruct the event and determine the scope of the incident

Overall, reconstruction plays a vital role in network digital forensics, as it allows investigators to identify the source and scope of network incidents, and can aid in the identification and prosecution of cybercriminals.

- **Dissemination** in the context of network digital forensics refers to the process of sharing information and evidence gathered during an investigation with relevant parties. This can include law enforcement agencies, legal teams, and other organizations involved in the case. From a network digital forensics perspective, dissemination is important for several reasons. First, it allows for the proper legal handling of any evidence collected during the investigation. This includes ensuring that the chain of custody is maintained and that the evidence is admissible in court. Second, dissemination allows for collaboration and information sharing between different organizations and agencies involved in the case. This can help to speed up the investigation and lead to a more efficient resolution.

Finally, dissemination can also help to build awareness and understanding of the issue at hand. This can include educating the public about the dangers of cybercrime, or providing information to organizations on how to better protect themselves from similar attacks in the future.

Overall, dissemination plays a critical role in network digital forensics by ensuring that evidence is handled properly, that collaboration and information sharing occurs, and that broader understanding and awareness is built around the issue at hand.

- **Returning evidence** in the context of network digital forensics refers to the process of returning physical or digital evidence to its rightful owner after it has been used in an investigation. This can include items such as computers, servers, or other digital devices that have been seized as part of an investigation.

From a network digital forensics perspective, returning evidence is important for several reasons. First, it ensures that the evidence is properly returned to its rightful owner, and that their rights and property are protected. This is particularly important in cases where the evidence is needed for ongoing business operations or other important functions.

Second, returning evidence can help to maintain the chain of custody and ensure that the evidence is still admissible in court. This is particularly important if the evidence is needed for future legal proceedings.

Finally, returning evidence can also help to maintain good relations with the organization or individual from whom the evidence was seized. This can be important in cases where ongoing cooperation is needed for the investigation or for future cases.

Overall, returning evidence plays a critical role in network digital forensics by ensuring that the evidence is properly returned to its rightful owner, that the chain of custody is maintained, and that good relations are built and maintained with the organization or individual from whom the evidence was seized.

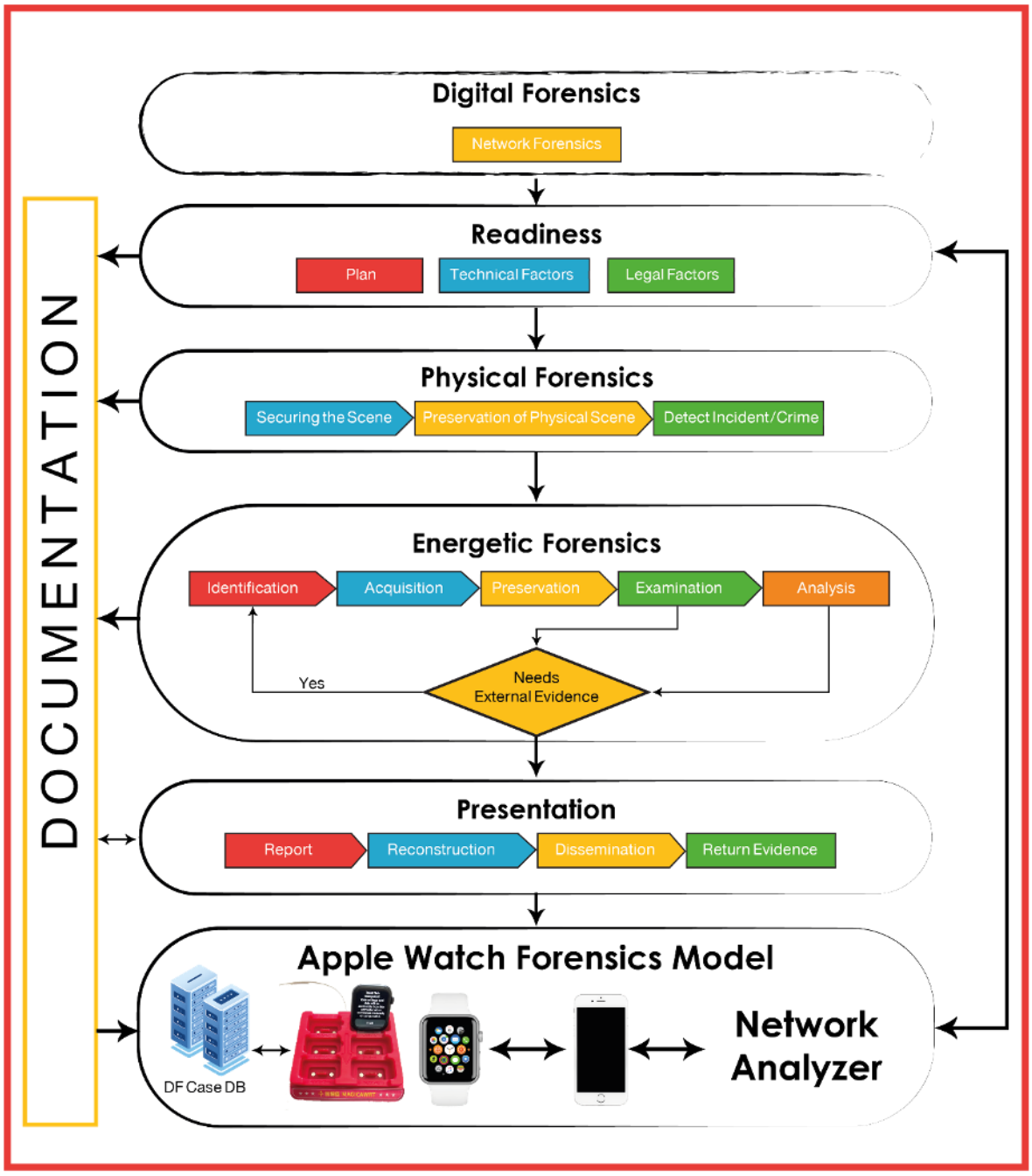


Figure 18: Proposed AWDFF for Network digital forensics Scenario Case

Table 2: The Expected Artifacts

The Expected Artifacts for Apple Watch	**The Expected Artifacts for iPhone Mobile**	**The Expected Artifacts for Network traffics of Apple Watch**
When analyzing an Apple Watch using digital forensics tools, some of the artifacts that may be found include: • Call history and contacts. • Text messages and iMessages. • Emails. • Calendar events and reminders. • GPS location data. • Photos and videos. • Music and audio files. • Application data, such as from third-party apps. • Health and fitness data, such as from the built-in Heart Rate sensor and Activity Tracker. • Passcode or passcode attempts. • Siri interactions. • iCloud backup data. It should be noted that the specific artifacts that can be found will depend on the device's configuration, usage, and whether it was previously synced to another device or iCloud account.	When analyzing an iPhone using digital forensics tools, some of the artifacts that may be found include: • Call history and contacts. • Text messages and iMessages. • Emails. • Calendar events and reminders. • GPS location data. • Photos and videos. • Music and audio files. • Application data, such as from third-party apps and app usage history. • Browsing history and bookmarks. • Health and fitness data, such as from the built-in Health app. • Passcode or passcode attempts. • Siri interactions. • iCloud backup data. • Application specific data, such as WhatsApp chats, social media, etc. • Keychain data and saved passwords. • Device settings and configuration information. It should be noted that the specific artifacts that can be found will depend on the device's configuration, usage, and whether it was previously synced to another device or iCloud account.	When analyzing network traffic related to an Apple Watch using digital forensics tools, some of the artifacts that may be found include: • Network connections made by the watch, such as to synchronize data with the paired iPhone or iCloud account. • Data transmitted and received by the watch, such as text messages, emails, and calendar events. • GPS location data transmitted by the watch. • Health and fitness data transmitted by the watch. • Remote commands sent to the watch, such as through Siri or the Remote app. • iCloud backup data transmitted to and from the watch. • Information about the watch's firmware and software updates. • Information about paired devices and connections. It should also be noted that the specific artifacts that can be found will depend on the network environment, the device's configuration, usage and the data retention policy of the network.

4.6 Explanation of the scenario practically

In this section, we will examine the process and strategies for creating multiple backups of the Apple Watch, including the types of system files and data that it contains, as well as any challenges encountered during the backup creation process. Additionally, given the relevance of the subject matter and the need to address the existing files and potential information recovered from the Apple Watch, we will also examine the various file types that were retrieved from the device. To accomplish this, we will utilize two specific software programs to obtain the necessary files and subsequently compare the results of both programs.

MAGICAWRT (Figure 17) is a device that allows for forensic examination of Apple devices such as the Apple Watch. It is designed to provide access to the internal file system of these devices, enabling the creation of backups and extraction of data for analysis. One of its key features is its ability to bypass the standard security measures implemented on Apple devices, allowing for a deeper level of examination. Additionally, MAGICAWRT is equipped with the necessary hardware and software to interface with the Apple Watch and make a backup of the device. It is a widely used tool among forensic investigators and researchers due to its effectiveness and reliability.

Figure 19: MAGICAWRT

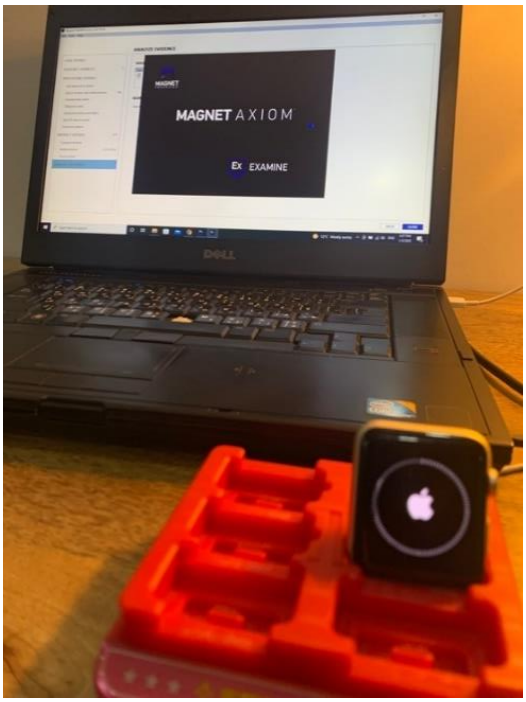


Figure 20: Apple Watch Backup using MAGICAWRT Device and Axiom Software

First Apple Watch Software Forensics:

The Axiom program is the initial program utilized in this study. As depicted in Figure 18, it was able to successfully detect and access the Apple Watch after multiple unsuccessful attempts by other programs. We used the device MAGICAWRT to get inside the apple watch and make the backup. Given that this program not only creates a backup of the Apple Watch, but also provides a detailed analysis of the extracted data, we will begin our examination by discussing the various artifact categories of files that have been extracted.

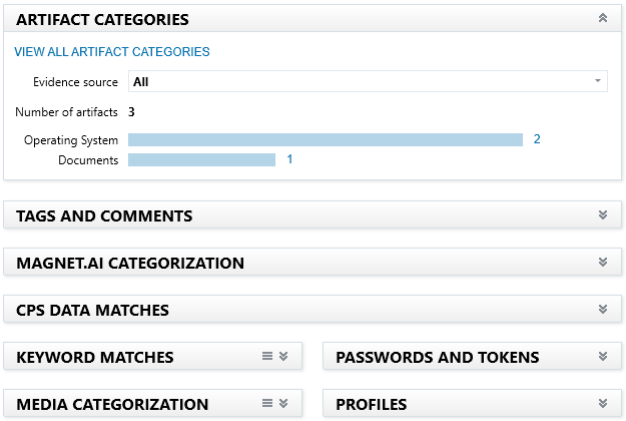


Figure 21: Axiom Examine interface

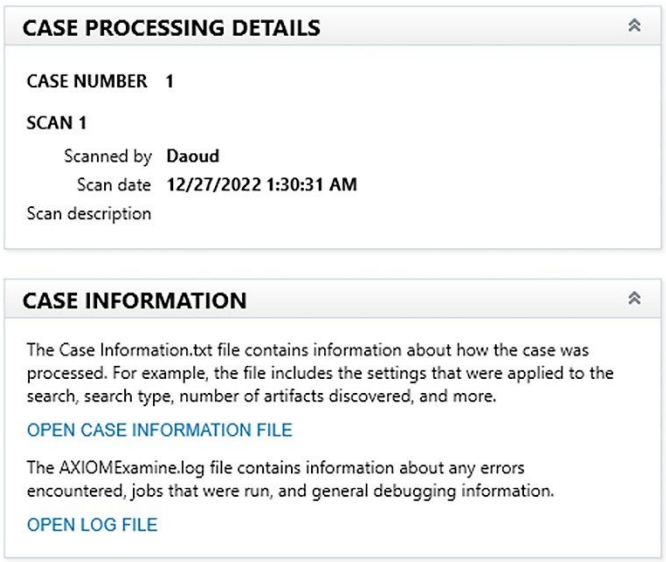


Figure 22: AXIOM Case Details and information

When we opened the case information, we found many information about the apple watch like:

Summary:

========

Start Time: Dec 27, 2021 01:30:25

End Time: Dec 27, 2021 01:30:42

Search Duration: 00:00:02

Indexing Duration: 00:00:00

Search Outcome: Success

Final results of search:

========================

File System Information: 1 items

iOS Device Information: 1 items

Text Documents: 1 items

Subsequently, we aimed to locate the specific file system information that was necessary for our examination, and were able to do so utilizing the program depicted in the accompanying figure 21.

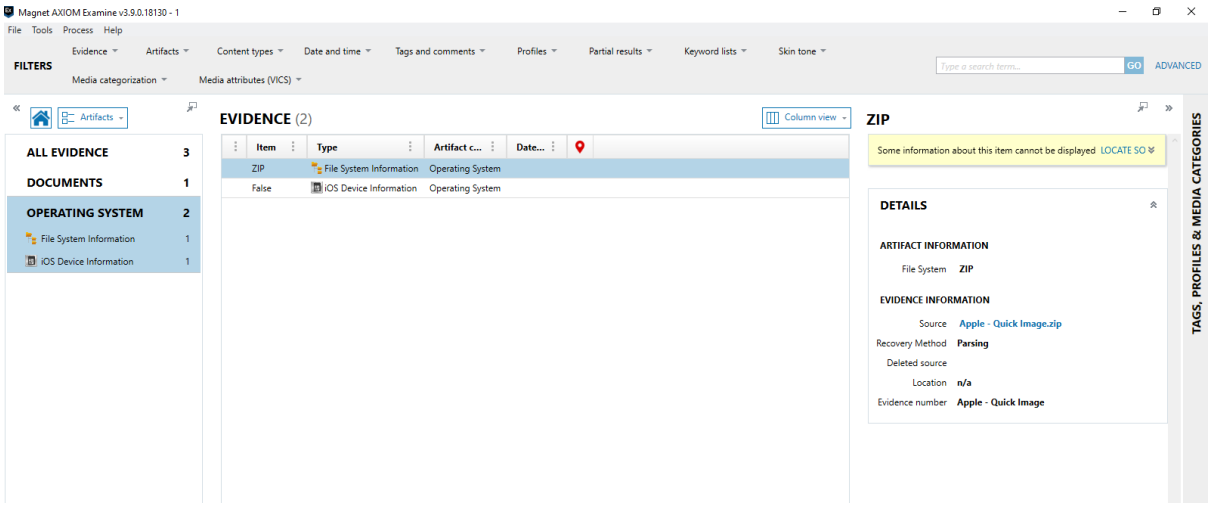


Figure 23: File System information

The file system information category encompasses all relevant data pertaining to it, and the specific details of this file are outlined in figure 22.

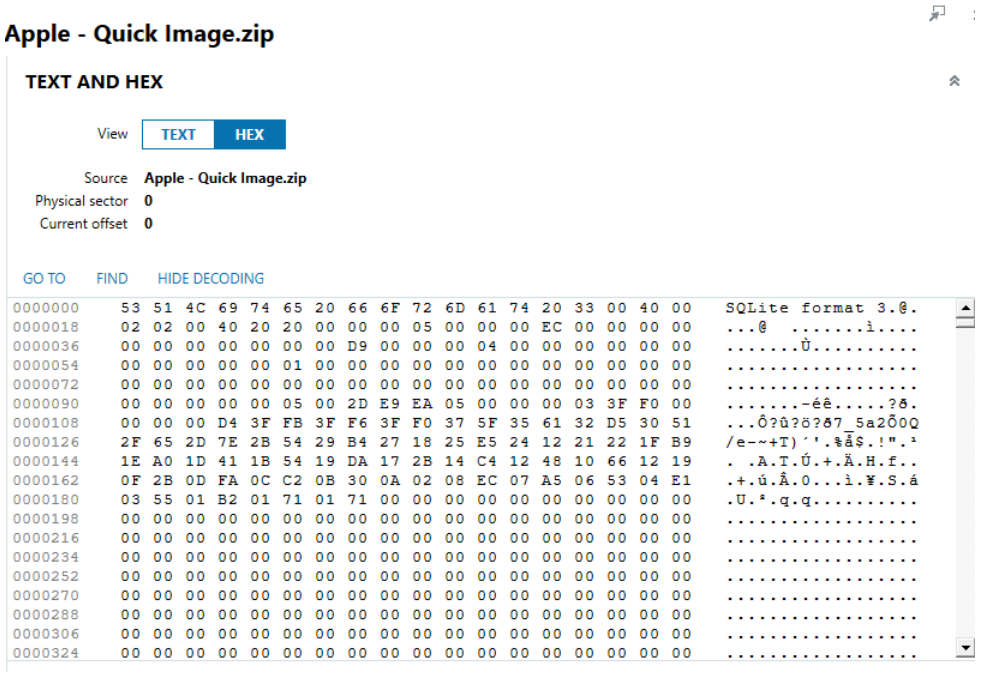


Figure 24: Apple Watch OS File System HEX

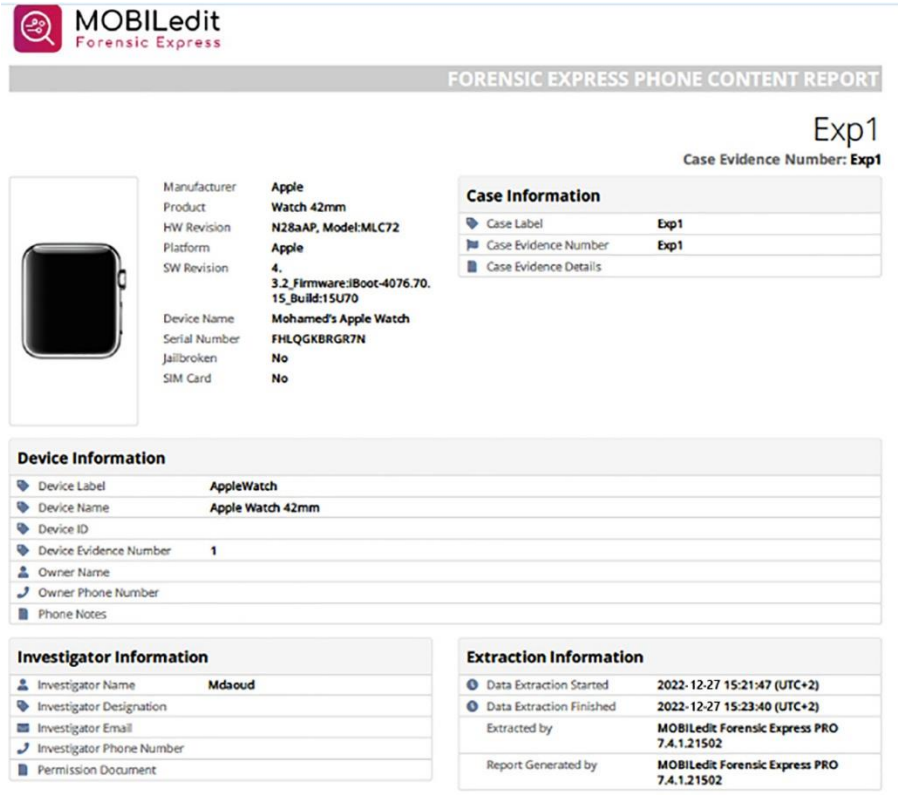
In summary, our examination demonstrates that the Apple Watch contains its own distinct system files and serves as a storage medium for valuable information that necessitates precise analysis to access. While we were able to access and read certain files and directories, our program was unable to retrieve all of the necessary files such as calls, messages, photos, and other evidentiary material. While there may exist other programs that are capable of retrieving these files, the program currently at our disposal enabled us to create an image and access the system files of the Apple Watch.

Second Apple Watch Software Forensics:

Mobiledit is the second program utilized in this study. As depicted in Figure 23, it was able to successfully detect and access the Apple Watch after multiple unsuccessful attempts by other programs. Given that this program not only creates a backup of the Apple Watch but also provides a detailed report of the extracted data and artifacts, we will begin our examination by showcasing the Mobiledit Forensic Express Phone Content.

Figure 25: Apple Watch Backup using MAGICAWRT device and Mobiledit Software

In this study, we utilized a previously used Apple Watch and created a backup of the device. Upon examination of the backup, we discovered a range of information related to the device, including its usage history from its initial activation until the present time, as well as the name of the owner, the Apple Watch series or model, and other relevant details. This information is depicted in Figure 24.


MOBILedit
Forensic Express

FORENSIC EXPRESS PHONE CONTENT REPORT

Exp1

Case Evidence Number: Exp1

Manufacturer	Apple
Product	Watch 42mm
HW Revision	N28aAP, Model:MLC72
Platform	Apple
SW Revision	4.3.2_Firmware:iBoot-4076.70.15_Build:15U70
Device Name	Mohamed's Apple Watch
Serial Number	FHLQGKBRGR7N
Jailbroken	No
SIM Card	No

Case Information

Case Label	Exp1
Case Evidence Number	Exp1
Case Evidence Details	

Device Information

Device Label	AppleWatch
Device Name	Apple Watch 42mm
Device ID	
Device Evidence Number	1
Owner Name	
Owner Phone Number	
Phone Notes	

Investigator Information

Investigator Name	Mdaoud
Investigator Designation	
Investigator Email	
Investigator Phone Number	
Permission Document	

Extraction Information

Data Extraction Started	2022-12-27 15:21:47 (UTC+2)
Data Extraction Finished	2022-12-27 15:23:40 (UTC+2)
Extracted by	MOBILedit Forensic Express PRO 7.4.1.21502
Report Generated by	MOBILedit Forensic Express PRO 7.4.1.21502

Figure 26: Apple Watch Device properties

Additionally, we identified the list of applications present on the device as a crucial aspect of our examination. The list of applications provides insight into the usage of the device and can aid in identifying any relevant information or activity that may have occurred on the device. Furthermore, it can also indicate the potential presence of any third-party apps that may have been installed on the device and can be used to extract additional information related to the device usage.

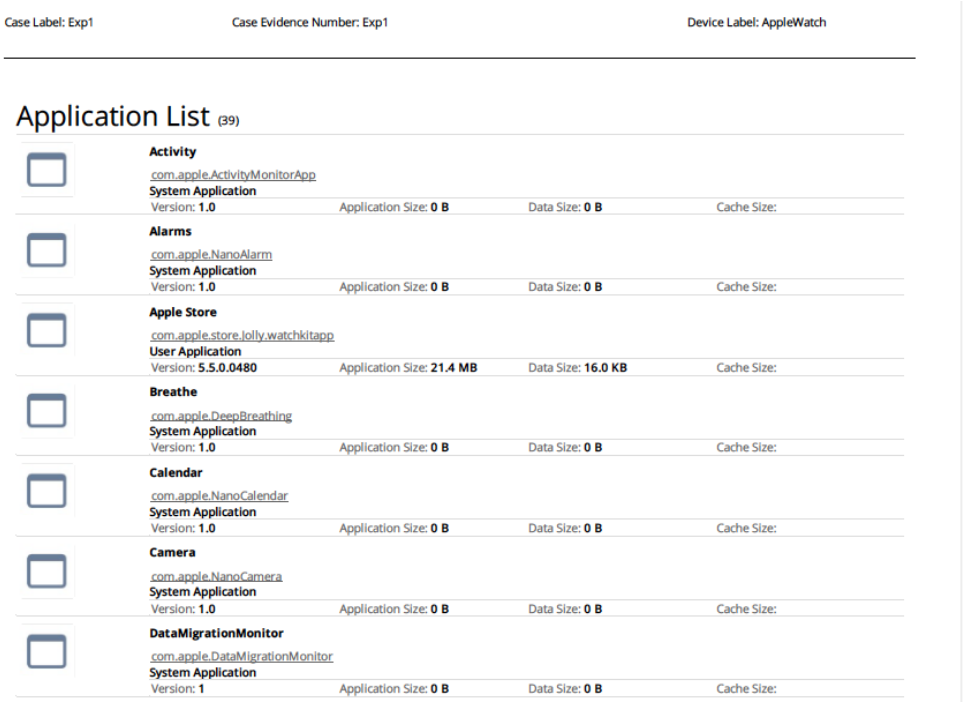


Figure 27: Applications List on the Apple Watch

Subsequently, the program presents a variety of topics, with the most notable being the types of files present on the device and their respective quantities. This information is essential in understanding the nature and scope of the data stored on the device, and in identifying any potential evidentiary material that may be present. Additionally, it can provide insight into the types of activities that have been conducted on the device and aid in identifying any anomalies or inconsistencies within the data.

Files

Internal Files (344 files)

Filename	Size	Created	Modified	Accessed
/				
/DCIM/				
/DCIM/100APPLE/		2020-06-22 18:51:52	2021-09-05 13:58:03	
IMG_0712.JPG SHA-256 hash: F406370CBDD4014986FA0F01E59E8823779F5D93CF853F828964A45E505C540A MD5 hash: AB1707913188EC76D94709D760D52386E	116 KB	2021-03-05 13:01:57	2021-03-05 13:01:57	
IMG_0712.MOV SHA-256 hash: BAC3E5F553FDB8F54EE12A77916305962155B90727590C4022DDD61EEF86DFC7 MD5 hash: A01A5C46AED5D3691E81711045F80E736	364 KB	2021-03-05 13:01:57	2021-03-05 13:01:57	
IMG_0718.JPG SHA-256 hash: 9E139D15884A04873D3003932037 6DCBFF7D116BB62121CE85EE9CF624D6A067 MD5 hash: 971266 4C9FC66663B7137D530A44EDFC	72.6 KB	2021-03-05 13:12:56	2021-03-05 13:12:57	
IMG_0719.JPG SHA-256 hash: 77DED80C6013F98FBF4B1B4896516016 1C59B7A0D8B4B11D70ADA5236A1412CA MD5 hash: 54B1001127A5BEA545E4FF2287B53C05	62.4 KB	2021-03-05 13:12:57	2021-03-05 13:12:57	
IMG_0720.JPG SHA-256 hash: 25266E01BF1A9CBCE4AE9EEB4082951 1EF1BF241DAD6ECDBFDB1824666B212F0 MD5 hash: 2ECCA69BC5398B621747 0E0487355C7	126 KB	2021-03-05 13:13:02	2021-03-05 13:13:02	
IMG_0720.MOV SHA-256 hash: 9C0BED45852A6DDEE86FCE743DD87DD25A549D452112C2923F112612A9AB4F73 MD5 hash: 59820 4EBDACB860BC798D01FCBBE8496	339 KB	2021-03-05 13:13:02	2021-03-05 13:13:02	
IMG_0721.JPG SHA-256 hash: 7435CBC5659B2EA84FA7A9D876D92E0EBC3501530200D2D9EE7E250E9B41E330 MD5 hash: 57A973D8F5A91BB62EB851A1C1689522	140 KB	2021-03-05 13:13:07	2021-03-05 13:13:07	
IMG_0721.MOV SHA-256 hash: B64DCC827 65FC379DECDB0D4AF41E4106A55A1004CDFED0013C9002CBB3C788E MD5 hash: 7E3D55C9DCB8A277E25DD2569A126C3F	394 KB	2021-03-05 13:13:07	2021-03-05 13:13:07	
IMG_0723.JPG SHA-256 hash: 01873497D82AE2A518A570BF495CC9DED9EC2178B66B59025072119006351ECA MD5 hash: 5458SCFDD9F5EFC0612BE5D90BAFAB9F	101 KB	2021-03-05 13:16:36	2021-03-05 13:16:37	
IMG_0724.JPG SHA-256 hash: 402882C3730E10DE59C6E7B9E435FB256FDFEFD35704D3C2F0270F3B734D12D MD5 hash: 806337A937204BA4A2DD3783755A1380	104 KB	2021-03-05 13:24:06	2021-03-05 13:24:23	
IMG_0735.JPG SHA-256 hash: F4083C780687307F3B87EF6F609F4EE88D827968210 9FE3AF288557EFA4E450A MD5 hash: D6AA1A493440SE4DF68CD516D8326C8E	76.3 KB	2021-03-05 15:58:08	2021-03-05 15:58:09	
IMG_0735.MOV SHA-256 hash: 9AC3220B9FD4EBF09E381D E9E839020112DBD6E963 17D3CC2A4E2304B0866676 MD5 hash: A7ABB0D017C4A5C976FDE2DA61BDBA6D	349 KB	2021-03-05 15:58:09	2021-03-05 15:58:09	
IMG_0762.JPG SHA-256 hash: 6FCE5E7F67928 26F2A6A3A185400DA47B46375D815D58C0DFFFABF529ACDD4A2 MD5 hash: FFE2DE134053A848BA870CEB602DE494	125 KB	2021-03-22 22:37:23	2021-03-22 22:37:23	
IMG_0762.MOV SHA-256 hash: FF719FD1DE74C65A7D65F942FFAAA488BAE958D0F743368339 1A383ACC8EADCB MD5 hash: 048E78934SBC215D569D8D875EB227F3	276 KB	2021-03-22 22:37:23	2021-03-22 22:37:24	

Figure 28: Files Types

As outlined in Appendix 1, Upon examination of the case information, we discovered a wealth of information pertaining to the Apple Watch. This included details such as the device's serial number, firmware version, and storage capacity. Additionally, we were able to gather information about the watch's usage, including the number of times it had been powered on, the amount of time it had been in use, and the number of times certain apps had been launched. We also discovered information about the watch's owner, including their name, contact information, and any associated iCloud account information. Furthermore, we were able to retrieve data such as message conversations, call logs, and calendar events, as well as other types of files such as photographs and videos that were stored on the device. Overall, our examination of the case information provided a comprehensive understanding of the Apple Watch and its usage. This information is demonstrated in the final report.

System Logs

Diagnostic logs (sysdiagnose)

Ethernet Address	**38:c9:86:d7:01:da**
Wi-Fi MAC Address	**38:c9:86:d7:01:d8**
Bluetooth Address	**38:c9:86:d7:01:d9**
Hardware Model	**N28aAP**
Platform	**s7002**
Firmware	**iBoot-4076.70.15**
User Name	**Mohamed's Apple Watch**
Device Name	**Apple Watch**
Product	**Watch OS**
Type	**Watch1,2**
Version	**4.3.2**
Device Build Version	**15U70**
Country Code	**AE**
Serial Number	**FHLQGKBRGR7N**
Device Unique ID	**20eb846910538f90e853d68a8465f18c84531f4a**
Total Data Available	**4.7 GB**
Total Data Capacity	**5.5 GB**
Total Disk Capacity	**7.5 GB**
Total System Available	**0 B**
Total System Capacity	**1.9 GB**

Figure 29: Apple Watch System Logs

4.7 Report Generation

Table 3: Automatic Generation Digital Forensics Report

Automatic Generation
Digital Forensics Report

Case Details

Investigator Name:Mdaoud	*Case Evidence No.:* Exp1 *Report Date:* 03/01/2023 *Report Time:* 15:23 PM (Albireh)
Device Information: Device Labe: Apple Watch Device Name: Apple Watch 42mm Device Owner: Mohamed	*Name of Suspect(s)/Type of Case:* Adam and Sara/ assault

Devices Properties

Manufacturer	**Apple**
Product	**Watch 42mm**
HW Revision	**N28aAP, Model:MLC72**
Platform	**Apple**
SW Revision	**4.3.2_Firmware:iBoot-4076.70.15_Build:15U70**
Device Name	**Mohamed's Apple Watch**
Serial Number	**FHLQGKBRGR7N**
Device Unique ID	**20eb846910538f90e853d68a8465f18c84531f4a**
Device Time	**2023-01-03 15:23:10 (UTC+2)**
Time Zone Wi-Fi MAC Address Bluetooth Address	**Asia/Hebron** **38:C9:86:D7:01:D8** **38:C9:86:D7:01:D9**
Ethernet Address	**38:C9:86:D7:01:DA**
Jailbroken	**No**
Communication Type	**Apple Mobile Device Service**
SIM Card	**No**
Total Storage	**7.5 GB**
Used Storage	**3.0 GB**

Framework processes

Selected Domains: Apple Watch Domain	*Type of crime:* Assault Crime scene only
Readiness: A comprehensive plan for the investigative procedure has been established. The relevant organizational factors have been thoroughly evaluated. The evidence obtained has been confirmed to adhere to the legally accepted methods of collection and analysis.	*Physical Forensics:* The Apple Watch device was secured to ensure its protection. The physical location where the device was found was preserved to prevent any potential contamination or alteration of the scene. The incident was identified and detected during the examination process.

The necessary software for investigating each domain has been employed as deemed appropriate.	
Logical Crime Scene Investigation: The process involved identifying the digital directories from each domain, conducting a thorough evaluation of these directories, and creating backups, imaging, and dumping as necessary. This was done to ensure the preservation of the digital evidence and to facilitate its analysis and examination.	*Other media:* Not found
Findings: *Phone Recent*: Sends and Received. Contacts: Phone Numbers. *Messages:* Text and Multimedia Messages. *Gallery:* Photos and Videos. *Mails:* Emails.	
Comments: The systems were returned to their respective owners through their personal participation in the retrieval process.	

Chapter Five

Discussion and Conclusion

5.1 Overview

Chapter 5 is the final chapter and includes the research conclusion, in which the implications of the research are discussed and ideas for future work are presented. The chapter also includes a summary of the overall research findings and a conclusion to the thesis.

5.2 Discussion

Upon the completion of the practical experiments that were undertaken in accordance with the methodology outlined in the previous section of this thesis, and in accordance with the theoretical framework proposed in the present study, several notable artifacts were discovered. These artifacts, which were uncovered through the diligent and thorough execution of the aforementioned experiments, are of particular significance in relation to the central research question and overall aims of the study. The discovery of these artifacts represents a significant step forward in our understanding of the subject matter being investigated, and will undoubtedly be of great value to future research in this field.

Table 4: Apple Watch experiment Artifacts

Data Category	***Content***	***Figure #***
1. Phone Recent	Sends or received,	Figure 29.
2. Contacts	Phone Numbers	Figure 30.
3. Messages	Text Messages	Figure 31.
4. Gallery	Photos	Figure 32.
5. Mails	Emails	Figure 33.

Figure 30: Phone Recent (sends or received)

Figure 31: Contacts

Figure 32: Text Messages

Figure 33: Photos

Figure 34: Mails

Also, upon completion of the extraction of relevant evidence, it can be concluded that the implementation of the proposed Apple Watch Digital Forensics Framework (AWDFF) will yield impressive results. The framework's effectiveness is further enhanced by the utilization of the proposed Apple Watch Forensics Model (AWFM) within it. The framework and its model will prove to be highly valuable when presented in court and to relevant authorities.

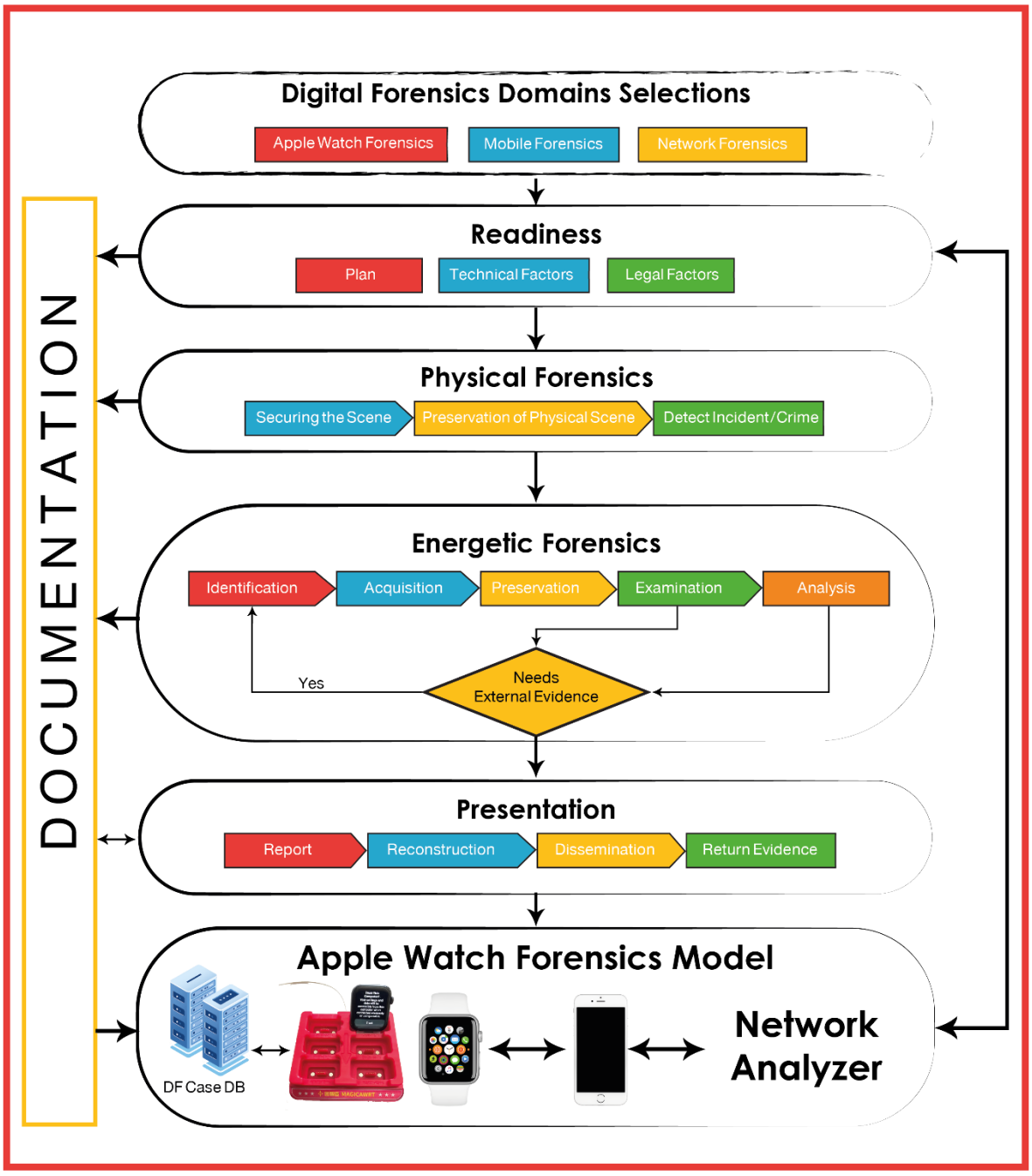


Figure 35: : Apple Watch Digital Forensics Framework (AWDFF)

5.3 Conclusion

The Internet of Things (IoT) has become an integral part of our daily lives and has changed the way we interact with technology. However, the increasing use of these devices has also raised numerous challenges in the field of digital forensics, particularly in the case of the Apple Watch. This small yet powerful device has a unique set of features and a complex architecture that make it difficult to extract and analyze data through traditional forensics methods.

One of the biggest challenges faced in Apple Watch forensics is the lack of specialized tools and standardized frameworks. The device's complex architecture and proprietary software make it challenging to extract and analyze data, making it difficult to produce comprehensive and accurate reports. The lack of proper tools and frameworks also makes it difficult to conduct forensic investigations in a timely and efficient manner, which can have serious implications in criminal investigations and other legal proceedings.

The importance of Apple Watch digital forensics cannot be overstated. As the device is constantly collecting and storing data, it can provide valuable insights into an individual's activities and habits. This information can play a crucial role in criminal investigations and other legal proceedings, making it essential to have reliable and accurate evidence. The development of effective and efficient forensics tools and frameworks is essential in helping to tackle the challenges posed by the IoT and provide reliable evidence in court.

Finally, the growth of IoT devices has presented numerous challenges in the field of digital forensics, particularly in the case of the Apple Watch. The need for specialized forensics tools and frameworks is crucial in overcoming these challenges and producing comprehensive and accurate reports. The importance of Apple Watch digital forensics cannot be overstated, as it plays a crucial role in criminal investigations and other legal proceedings. Therefore, it is essential to continue the development of effective and efficient forensics tools and frameworks to ensure that we can make the most of the insights and evidence provided by these devices.

This paper addresses the growing trend of crimes and incidents involving information and communication technology in the Middle East, where there is a lack of standardized digital forensics frameworks. To address this need, a common standard framework called the Apple Watch Digital Forensics Framework (AWDFF) is proposed. The framework is designed to be more structured than existing frameworks, utilizing a modularized approach with five modules:

Readiness, Physical Forensics, Energitic Forensics, Presentation and Apple Watch Forensics Model (AWFM). Through extensive literature review, survey findings and analysis, the proposed framework includes all essential phases while eliminating redundant or unnecessary phases found in existing frameworks. Additionally, the framework is comprehensive in nature, guiding investigators from readiness to dissemination. It is noted that while the proposed Apple Watch Forensics Model (AWFM) of the framework is expected to increase digital forensics efficiency, it still needs to be developed and evaluated by experts. The framework is developed with the specific aim of targeting investigators working in the field of cyber-crimes.

References:

[1] G. Kumar, R. Saha, C. Lal, and M. Conti, “Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications,” *Futur. Gener. Comput. Syst.*, vol. 120, pp. 13–25, 2021, doi: 10.1016/j.future.2021.02.016.

[2] T. Zia, P. Liu, and W. Han, “Application-specific digital forensics investigative model in internet of things (IoT),” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, 2017, doi: 10.1145/3098954.3104052.

[3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[4] D. Rani, D. Rani, and N. S. Gill, “Internet of Things (IoT) Characteristics, Applications, and Digital Forensics Investigation Process: A Review,” *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 9, pp. 6512–6519, 2020, doi: 10.30534/ijeter/2020/254892020.

[5] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, “IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers,” *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 300926, 2020, doi: 10.1016/j.fsidi.2020.300926.

[6] S. Dogan and E. Akbal, “Analysis of mobile phones in digital forensics,” *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1241–1244, 2017, doi: 10.23919/MIPRO.2017.7973613.

[7] E. Gentry and M. Soltys, “SEAKER: A mobile digital forensics triage device,” *Procedia Comput. Sci.*, vol. 159, pp. 1652–1661, 2019, doi: 10.1016/j.procs.2019.09.335.

[8] M. M. Cruz-Cunha, N. R. Mateus-Coelho, and IGI Global, *Handbook of research on cyber crime and information privacy*, vol. I. 2020.

[9] Ş. Şentürk, T. Apaydin, and H. Yaşar, “Image and File System Support Framework for a Digital Mobile Forensics Software,” *2020 Turkish Natl. Softw. Eng. Symp. UYMS 2020 - Proc.*, pp. 2020–2022, 2020, doi: 10.1109/UYMS50627.2020.9247055.

[10] G. H. Carlton and G. C. Kessler, “Disconnects of Specialized Mobile Digital Forensics within the Generalized Field of Digital Forensic Science,” *Int. J. Interdiscip. Telecommun. Netw.*, vol. 10, no. 3, pp. 62–65, 2018, doi: 10.4018/ijitn.2018070106.

[11] S. C. Sathe and N. M. Dongre, “Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018,” *Proc. 2nd Int. Conf. Inven. Syst. Control. ICISC 2018*, no. Icisc, pp. 280–286, 2018.

[12] Kehinde Omotola Adebayo, “Digital Forensic Analysis of Smart Watches,” p. 25, 2020, [Online]. Available: https://digikogu.taltech.ee/et/Download/94fd963c-ec1d-4d41-85f2-d27ecea7b1cf

[13] S. Sunardi, I. Riadi, and J. Triyanto, “Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice,” *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 6, no. 2, p. 63, 2021, doi: 10.31328/jointecs.v6i2.2315.

[14] L. Dawson and A. Akinbi, “Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study,” *Forensic Sci. Int. Reports*, vol. 3, no. October 2020, p. 100198, 2021, doi: 10.1016/j.fsir.2021.100198.

[15] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le-Khac, “Internet of things forensics – Challenges and a case study,” in *IFIP Advances in Information and Communication Technology*, 2018, vol. 532, pp. 35–48. doi: 10.1007/978-3-319-99277-8_3.

[16] B. K. Sharma, M. A. Joseph, B. Jacob, and B. Miranda, “Emerging trends in Digital Forensic and Cyber security-An Overview,” *ITT 2019 - Inf. Technol. Trends Emerg. Technol. Blockchain IoT*, pp. 309–313, 2019, doi: 10.1109/ITT48889.2019.9075101.

[17] A. Almogbil, A. Alghofaili, C. Deane, T. Leschke, A. Almogbil, and A. Alghofaili, “The Accuracy of GPS-Enabled Fitbit Activities as Evidence: A Digital Forensics Study,” *Proc. - 2020 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. 2020 6th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud-EdgeCom 2020*, pp. 186–189, 2020, doi: 10.1109/CSCloud-EdgeCom49738.2020.00040.

[18] A. Freeman, “Creating the Project,” *Essent. Angular ASP.NET Core MVC 3*, pp. 15–40, 2019, doi: 10.1007/978-1-4842-5284-0_3.

[19] J. Kävrestad, “What Is Digital Forensics?,” *SpringerBriefs Comput. Sci.*, vol. 0, no.

9783319674490, pp. 3–7, 2017, doi: 10.1007/978-3-319-67450-6_1.

[20] G. Cho, “Design and Implementation of APFS Object Identification Tool for Digital Forensics,” vol. 14, no. 1, pp. 10–18, 2022.

[21] S. S. Dhruva *et al.*, “Heart Watch Study: Protocol for a pragmatic randomised controlled trial,” *BMJ Open*, vol. 11, no. 12, 2021, doi: 10.1136/bmjopen-2021-054550.

[22] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, “IoTDots: A Digital Forensics Framework for Smart Environments,” Sep. 2018, [Online]. Available: http://arxiv.org/abs/1809.00745

[23] A. B. J. Humaira Arshad, “journal_jips_JIPS-2018-14-2-346.pdf.”

[24] M. Pourvahab and G. Ekbatanifard, “Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology,” *IEEE Access*, vol. 7, pp. 153349–153364, 2019, doi: 10.1109/ACCESS.2019.2946978.

[25] S. Costantini, G. de Gasperis, and R. Olivieri, *Digital forensics and investigations meet artificial intelligence*, vol. 306. Annals of Mathematics and Artificial Intelligence, 2019.

[26] H. M. Ammari, *Mission-Oriented Sensor Networks and Systems: Art and Science*, vol. 2. 2019.

[27] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, “D4I - Digital forensics framework for reviewing and investigating cyber attacks,” *Array*, vol. 5, p. 100015, Mar. 2020, doi: 10.1016/j.array.2019.100015.

[28] U. T. Nasional, “Yunus Yusoff , Roslan Ismail and Zainuddin Hassan,” vol. 3, no. 3, pp. 17–31, 2011.

[29] D. Comer and A. Rastegatnia, “OSDF: An Intent-based Software Defined Network Programming Framework,” *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2018-Octob, pp. 527–535, 2019, doi: 10.1109/LCN.2018.8638149.

[30] B. Krumay, E. W. N. Bernroider, and R. Walser, *Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review*

Considering the NIST Cybersecurity Framework, vol. 11252 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-030-03638-6_23.

[31] H. Alazzam, O. Abualghanam, Q. M. Al-Zoubi, A. Alsmady, and E. Alhenawi, "A New Network Digital Forensics Approach for Internet of Things Environment Based on Binary Owl Optimizer," *Cybern. Inf. Technol.*, vol. 22, no. 3, pp. 146–160, 2022, doi: 10.2478/cait-2022-0033.

[32] F. M. Ghabban, I. M. Alfadli, O. Ameerbakhsh, A. N. Abuali, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Comparative analysis of network forensic tools and network forensics processes," *2021 2nd Int. Conf. Smart Comput. Electron. Enterp. Ubiquitous, Adapt. Sustain. Comput. Solut. New Norm. ICSCEE 2021*, pp. 78–83, 2021, doi: 10.1109/ICSCEE50312.2021.9498226.

[33] G. Maria Jones, S. Godfrey Winster, and S. V. N. Santhosh Kumar, *Analysis of mobile environment for ensuring cyber-security in IoT-based digital forensics*, vol. 900. Springer Singapore, 2019. doi: 10.1007/978-981-13-3600-3_14.

[34] A. K. S. Lin, L. Z. Eds, and G. Goos, *Edge Computing – EDGE 2020*. 2020. doi: 10.1007/978-3-030-59824-2.

[35] K. K. R. Choo and A. Dehghantanha, *Contemporary Digital Forensics Investigations of Cloud and Mobile Applications*. Elsevier Inc., 2017. doi: 10.1016/B978-0-12-805303-4.00001-0.

[36] E. Casey, "Standardization of forming and expressing preliminary evaluative opinions on digital evidence," *Forensic Sci. Int. Digit. Investig.*, vol. 32, no. xxxx, p. 200888, 2020, doi: 10.1016/j.fsidi.2019.200888.

[37] U. R. Acharya, S. L. Oh, Y. Hagiwara, J. H. Tan, and H. Adeli, "Deep convolutional neural network for the automated detection and diagnosis of seizure using EEG signals," *Comput. Biol. Med.*, vol. 100, pp. 270–278, 2018, doi: 10.1016/j.compbiomed.2017.09.017.

[38] G. Dhiman and A. Kaur, "STOA: A bio-inspired based optimization algorithm for industrial engineering problems," *Eng. Appl. Artif. Intell.*, vol. 82, no. March, pp. 148–174, 2019, doi: 10.1016/j.engappai.2019.03.021.

[39] *2018 International Conference on Computing Sciences and Engineering (ICCSE).*

IEEE, 2018.

[40] D. A. Ofori *et al.*, “No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title,” *Molecules*, vol. 2, no. 1, pp. 1–12, 2020, [Online]. Available: http://clik.dva.gov.au/rehabilitation-library/1-introduction-rehabilitation%0Ahttp://www.scirp.org/journal/doi.aspx?DOI=10.4236/as.2017.81005%0Ahttp://www.scirp.org/journal/PaperDownload.aspx?DOI=10.4236/as.2012.34066%0Ahttp://dx.doi.org/10.1016/j.pbi.201

[41] F. Guterl, “Design case history: Apple’s Macintosh: A small team of little-known designers, challenged to produce a low-cost, exceptionally easy-to-use personal computer, turns out a technical milestone,” *IEEE Spectr.*, vol. 21, no. 12, pp. 34–43, 2013, doi: 10.1109/mspec.1984.6370374.

[42] S. Francisco *et al.*, “U ndergoing C ardioversion (AWE STRUCk): A Pragmatic Randomized Controlled Trial,” pp. 1–31, 2021.

[43] O. Gusg, “Application development for the Apple Watch,” no. May, 2018.

[44] G. Riches, R. Martinez, J. Maison, M. Klosterman, and M. Griffin, *Apple Watch for Developers*. 2015. doi: 10.1007/978-1-4842-1338-4.

[45] C. Hinds and P. Fenton, “ESeizure: A Mobile App for Digital Forensics First Responders,” *Proc. - 2017 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2017*, pp. 86–90, 2018, doi: 10.1109/CSCI.2017.14.

[46] G. Horsman, “Tool testing and reliability issues in the field of digital forensics,” *Digit. Investig.*, vol. 28, pp. 163–175, 2019, doi: 10.1016/j.diin.2019.01.009.

[47] M. M. Haque and S. A. Hossain, “National digital forensics framework for Bangladesh,” *3rd Int. Conf. Electr. Inf. Commun. Technol. EICT 2017*, vol. 2018-Janua, no. December, pp. 1–6, 2018, doi: 10.1109/EICT.2017.8275133.

[48] L. Peng, “2021 4th International Conference on Artificial Intelligence and Big Data, ICAIBD 2021,” *2021 4th Int. Conf. Artif. Intell. Big Data, ICAIBD 2021*, pp. 279–283, 2021.

[49] D. Paul Joseph and J. Norman, *An analysis of digital forensics in cyber security*, vol. 815. Springer Singapore, 2019. doi: 10.1007/978-981-13-1580-0_67.

[50] R. M. Mohammad, “A Neural Network based Digital Forensics Classification,” *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2018-Novem, pp. 1–7, 2019, doi: 10.1109/AICCSA.2018.8612868.

[51] A. Shalaginov and K. Franke, “Automated generation of fuzzy rules from large-scale network traffic analysis in digital forensics investigations,” *Proc. 2015 7th Int. Conf. Soft Comput. Pattern Recognition, SoCPaR 2015*, vol. 0, no. 1, pp. 31–36, 2016, doi: 10.1109/SOCPAR.2015.7492778.

[52] M. Khanafseh, M. Qatawneh, and W. Almobaideen, “A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 610–629, 2019, doi: 10.14569/ijacsa.2019.0100880.

[53] G. Y. Lui, D. Loughnane, C. Polley, T. Jayarathna, and P. P. Breen, “The Apple Watch for Monitoring Mental Health–Related Physiological Symptoms: Literature Review,” *JMIR Ment. Heal.*, vol. 9, no. 9, 2022, doi: 10.2196/37354.

[54] J. Kizza and F. Migga Kizza, *Digital Evidence and Computer Crime*. 2011. doi: 10.4018/978-1-59904-379-1.ch015.

الملخص

أصبحت Apple Watch جهازًا يمكن ارتداؤه، يستخدم على نطاق واسع ويمكن أن يوفر أدلة رقمية قيمة في التحقيقات الجنائية. تشكل البنية الفريدة للجهاز ونظام التشغيل تحديات أمام أساليب الطب الشرعي الرقمي التقليدية، مما يجعل من الضروري اعتماد إطار عمل متخصص في الطب الشرعي، وتجدر الإشارة إلى أنه لا يوجد حاليًا إطار عمل محدد لإجراء تحقيقات جنائية محددة على Apple Watch ، مما يجعل من الصعب على المحققين أو الأفراد المعنيين لجمع المعلومات من هذا الجهاز. تهدف هذه الورقة إلى تقديم نظرة عامة شاملة ومتعمقة عن إطار عمل الطب الشرعي الرقمي لـ Apple Watch. يتكون إطار العمل من مكونات الأجهزة والبرامج التي تعمل معًا لاستخراج وتحليل الأدلة الرقمية من الجهاز. يشتمل مكون الأجهزة على الأدوات والمعدات المناسبة للوصول إلى المكونات الداخلية لـ Apple Watch، مثل جهاز MAGICAWRT وكابل بيانات متخصص. يشتمل مكون البرنامج على أدوات جنائية رقمية متخصصة، مثل 3uTools Forensic Software و Axiom Software و MOBILedit Forensic Express Software ، والتي يمكنها استخراج البيانات وتحليلها من الجهاز ، وتتضمن عملية الطب الشرعي الرقمي لـ Apple Watch عدة مراحل ، بدءًا من الجاهزية ، الطب الشرعي المادي للجهاز ، الطب الشرعي النشط ، العرض التقديمي ، نموذج الأدلة الجنائية لساعة Apple والتوثيق ، حيث يتم استخدام نموذج الإطار لاستخراج البيانات من الجهاز. ثم يتم تحليل البيانات المستخرجة بحثًا عن القطع الأثرية المحتملة التي يمكن استخدامها كدليل رقمي في تحقيق جنائي. تختتم الورقة بإلقاء الضوء على أهمية إطار عمل الطب الشرعي الرقمي لـ Apple Watch في التحقيقات الجنائية والفوائد التي يوفرها لمتخصصي إنفاذ القانون والطب الشرعي الرقمي. يساعد إطار العمل في التغلب على التحديات التي تفرضها البنية الفريدة ونظام التشغيل لساعة Apple Watch ويتيح استخراج الأدلة الرقمية وتحليلها بكفاءة. كانت التجارب العملية التي تم إجراؤها موجهة تحديدًا نحو الإطار الذي تم تطويره لـ Apple Watch. تم تصميم هذا الإطار لتلبية المتطلبات الفريدة للجهاز ونظامه البيئي ، وتم تنفيذ التجارب باستخدام البرامج المذكورة سابقًا. كان الهدف الأساسي من هذه التجارب هو جمع أدلة موثوقة وعملية من خلال تطبيق إطار العمل. ستلعب نتائج هذه التجارب دورًا حاسمًا في زيادة صقل وتحسين إطار العمل، ومن المتوقع أن توفر رؤى ومعلومات قيمة لتطوير أطر عمل مماثلة في المستقبل. بشكل عام، تعد التجارب العملية خطوة حاسمة نحو ضمان التنفيذ الناجح ونشر إطار عمل Apple Watch. يمكن أن يساعد هذا البحث في تطوير أفضل الممارسات لفحص الطب الشرعي لـ Apple Watch وتحسين قدرة تطبيق القانون على جمع الأدلة الرقمية من هذا الجهاز القابل للارتداء الشهير.