

DOI: https://doi.org/10.48009/3_iis_2024_108

Foundations of mobile forensics: an academic approach

Jason E James, *Indiana State University*, jason.james@indstate.edu

Abstract

The rapid proliferation of mobile devices in contemporary society has revolutionized communication, commerce, and social interaction. With this widespread adoption of mobile technology comes the need for robust digital forensic methodologies to investigate criminal activities, security breaches, and civil disputes involving these devices. The following research presents a scholarly examination of the fundamental principles and methodologies for understanding and conducting mobile forensic investigations. In addition, it provides an overview of key topics, including mobile device architecture, data acquisition methods, mobile device security, and mobile device tools. The following content review analysis explores the basics of mobile forensics and its relevance in contemporary society and demonstrates the academic rigor and real-world applicability of mobile forensic principles and serves as a valuable resource for educators, researchers, and practitioners seeking to advance their knowledge and skills in the field of mobile forensics, fostering a deeper understanding of digital investigations in an increasingly mobile-centric world.

Keywords: mobile forensics, digital forensics, academics, faraday bags, afu, bfu

Background

The National Institute of Standards and Technology (NIST) defines **mobile forensics**, or cell phone forensics, as "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods." It is one of the specialties under **digital forensics**, a branch of forensic science focused on identifying, acquiring, processing, analyzing, and reporting data stored electronically and can be presented in court. Mobile forensics solely focuses on obtaining data from mobile devices (e.g., mobile phones, smartphones, tablets, and wearable GPS units) that can be identified as evidence (Ayers, et al, 2014).

In the early days, with the growing popularity of personal computers, it was known as "computer forensics" and recognized early on by law enforcement as a source of evidence in crimes. Prior to the digital age, data was stored differently. Boxes and filing cabinets of paper and letters became bytes and files on floppy disks, hard drives and servers. Computer forensics became digital forensics to encompass all the different ways data could be stored or transmitted. Although the first known computer crimes were in the 1970s, the origins of the relatively new field of digital forensics can be traced to the mid-1980s and early 1990s. Forensics teams usually consisted of members of law enforcement officers who were computer hobbyists or had some type of computer background. Those officers tasked with investigating crimes had limited training and no official framework to follow to ensure repeatability in their investigations. (Kulm, 2023).

In today's modern era, digital evidence is associated with approximately 90 percent of crimes committed. Cell phones are everywhere, and they often contain information law enforcement professionals need to

solve crimes. People don't do anything without their smartphones, not even criminals (Lamb, 2019).

Introduction

The history of mobile forensics can be traced back to the advent of mobile phones and the increasing integration of digital technology into these devices. In the 1990s during the early days of mobile phones, forensic analysis primarily focused on call records and text messages. However, the limited storage capacity and functionality of these early devices restricted the amount of data that could be retrieved. In the 2000s, the emergence of smartphones, such as the BlackBerry and the early Windows Mobile devices, marked a significant shift in mobile forensics. These devices offered more advanced features, including email, web browsing, and third-party applications, expanding the scope of forensic analysis.

In 2007, everything changed, the release of the iPhone, and the subsequent proliferation of Android devices revolutionized the mobile landscape. These smartphones introduced touchscreens, advanced operating systems, and a wide range of applications. Mobile forensics had to adapt to the increased complexity of these devices. As smartphones became more complex and secure, specialized forensic tools started to emerge in the early 2000s. Companies like Cellebrite developed tools capable of extracting and analyzing data from a variety of mobile devices. These tools played a crucial role in forensic investigations.

In the 2010s, the increasing focus on user privacy and security, mobile operating systems started implementing stronger encryption measures. This posed a challenge for mobile forensic experts, as accessing encrypted data required advanced techniques and sometimes cooperation from device manufacturers. In cases where traditional logical extraction methods were not successful, forensic experts began using more advanced techniques like chip-off and JTAG (Joint Test Action Group). These methods allowed direct access to the memory chips of the devices, bypassing the operating system's security (Oxygen Forensics, 2023). However, in December 2015 the game changed for mobile forensics.

Literature Review

Digital forensics is one of the fastest growing fields in cybersecurity and digital forensics graduates have an extremely high placement rate. With the use of technology constantly rising and criminals becoming even more active online, careers within digital forensics are growing rapidly and will continue for the foreseeable future. Both privately owned businesses as well as government entities such as the FBI, CIA, NSA as well as law enforcement agencies across the country and worldwide all need well-trained digital forensics investigators and analysts. According to the Bureau of Labor Statistics, the field of digital forensics is expected to grow by about 10 percent by the year 2032 (Liddle, 2024).

The number of Universities in the United States teaching digital forensics continues to grow. One of the most common courses included in these programs is mobile forensics. With mobile phones now the primary evidence source in 96% of investigations, developing ways to lawfully access data from mobile devices has become critical in accelerating justice (Nurick, 2021). Yet, there is very little literature and only a couple books that cover the foundations of mobile forensics and many of those books are outdated. The only book that continues to be published every couple of years is Practical Mobile Forensics published by Packt and authored by Rohit Tamma, Oleg Skulkin, and Heather Mahalik. However, that book is more technical in nature and not really for learning the foundations of mobile forensics, especially for students with little to know background. In fact, after a review of scholarly journal articles for mobile forensics, very few existed, and most were technical in nature or outdated and none of them laid the foundations of mobile forensics.

Methodology

The author used the knowledge gained as a digital forensics' unit director, attendance at numerous training events and conferences as well as many years of experience in the digital forensics field. In addition, content analysis was utilized by other experts in the field to lay the foundation for foundations of mobile forensics for academic teaching. Topics covered will include the following:

1. Introduction to mobile forensics
2. Mobile device architecture
3. Mobile device seizure
4. Data acquisition methods
5. Mobile Device Security
6. Extracting and Analyzing Data

However, before we delve into the topics, lets lay a foundation of how mobile forensics has evolved since December 2015.

Discussion

In the early part of 2016, Apple and the FBI were engaged in a massive fight over encryption, following the December 2015 mass shooting in San Bernardino where a husband and wife shot and killed more than a dozen people. They left behind an iPhone 5C running iOS 9, the latest operating system available for iPhone at the time. The government wanted to gain access to the phone to see if it could determine any links between the two shooters and the Islamic State, but they could not break the encryption. The FBI attempted to have a court force Apple to create a backdoor in iOS that would allow them to retrieve whatever data sat behind the screen's password. Apple fiercely opposed that order, explaining that it doesn't have a backdoor into iOS, and creating one would be a massive security risk for all iPhone users (Smith, 2021).

The FBI ended up unlocking the iPhone used by one of the San Bernardino shooters in 2015 thanks to the help of an Australian cybersecurity company. Azimuth Security, a small infosec company based in Sydney, Australia, came up with the hacking solution for the FBI (Reichert, 2021). After that event, two companies, Cellebrite and Grayshift (now Magnet Forensics) developed software that could bypass the security, and even brute force the passcode, and break into iPhones. In 2019, law enforcement could send devices into the company's lab where the company then uses whatever secret exploits it must to crack the lock and either send it back to investigators so they can take data from the device or have Cellebrite do it for them. In 2021, Cellebrite launched Cellebrite Premium ES for law enforcement to disable the PIN, pattern, password screen locks or passcodes on the Apple iOS and Google Android devices. The combination of hardware and software was designed to maintain lawful access for law enforcement agencies while protecting privacy (Brewster, 2018b).

After Cellebrite reported that it could unlock the latest Apple iPhone models, another digital forensics service company emerged promising it could unlock iPhones as well. The American startup company was named Grayshift and was run by long-time U.S. intelligence agency contractors and an ex-Apple security engineer. The device, known as Graykey (now Magnet Forensics Graykey), can disabled iPhone security and can extract the full file system from the Apple device. The tool could also make repeated guesses at passcodes, a technique known as brute forcing, to first get into the device and provide law enforcement with the passcode for the device (Brewster, 2018a).

Cellebrite and Grayshift (now Magnet Forensics) changed the game of mobile forensics as we know it. They not only provided the ability to break into iOS devices and Android devices but provide something

law enforcement could never obtain, full file system extractions (which we will cover more later and the importance of what is known as FFS). So why is all this important, well it's because students in academics need to learn not only the technical information but the foundations of mobile forensics as well, since mobile forensics foundations have changed in just 5 years and continue to change each year.

Results

Since the introduction of the smartphone, the device has played an increasingly important role in people's life, to the point that today, we could not imagine a day without it. The smartphone market in the United States is one of the world's largest, with over 310 million smartphone users as of 2023. In line with the overall growth of the smartphone market worldwide, the smartphone penetration rate in the United States has continuously risen over the past several years, reaching around 92 percent in 2023 (Laricchia, 2024).

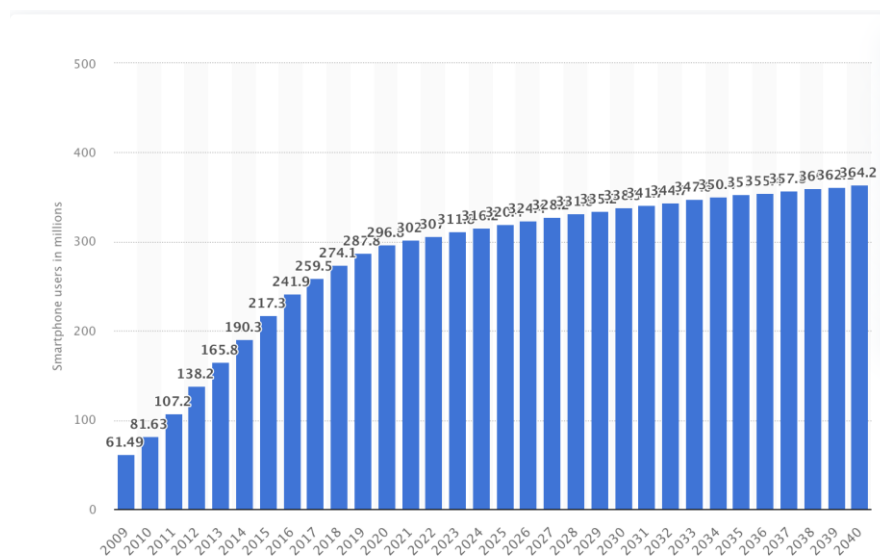


Figure 1: Number of smartphone users in the United States from 2009 to 2040 (Statista, 2022)

Since 2015, cell phone ownership has increased 20%. About 97% of Americans owned a smartphone in 2022, compared to 81% in 2015. Today, nine out of 10 of all cell phone owners have a smartphone. Future trends predict that the number of American smartphone users will increase to more than 364 million people by 2040 (Bazen, 2023).

So how does all this relate to mobile forensics? Your phone, between all your apps, knows almost everything about you—where you go and when, who you talk to, when you're using your phone, and more. So, for criminals, anonymity is key (which isn't to say that anonymity is only for criminals). Asynchronous messengers and end-to-end encrypted apps are popular for criminal communication (think WhatsApp, Facebook Messenger, GroupMe, Signal, Telegram, and others), with different messaging apps popping up every day, even though data from "encrypted" apps can still be accessed through digital forensics software—and that even includes "deleted" messages.

Any type of crime can involve digital evidence: crimes against children, drugs, homicides, harassment, etc. Even civil wrongdoings can be perpetrated with a mobile device. In fact, Digital evidence is included in 90% of crimes committed, making mobile forensics even more valuable than ever before (Reiber, 2019).

Mobile Device Architecture

Mobile device architecture refers to the structural design and organization of the components within a mobile device. This architecture includes both hardware and software elements that work together to provide the functionality and performance expected from modern smartphones, tablets, and other portable devices. Understanding mobile device architecture is crucial in the field of mobile forensics as it influences how data can be extracted and analyzed. iOS and Android are not the same and although many things' components are the same, one thing is completely different and that is the software within each.

Hardware Components

System on Chip (SoC) includes the Central Processing Unit (CPU), Graphics Processing Unit (GPU), and Random Access Memory (RAM). The CPU the brain of the device, executing instructions and managing tasks just like the CPU in a computer. The GPU handles rendering of images, videos, and animations. RAM is used for temporary storage and quick data access.

Storage includes both Internal and External Storage. Internal storage includes flash memory (NAND) that stores the operating system, applications, and user data and external storage (only in Android) support external storage through SD cards or similar media. Input/Output (I/O) interfaces include the touchscreen (primary interface for user input, physical buttons (home button, volume controls, power button), camera, microphone, speakers, and sensors (accelerometers, gyroscopes, proximity sensors, ambient light sensors, and fingerprint scanners).

Communication modules include the cellular modem (facilitates communication over mobile networks), Wi-Fi (enables wireless network connections), Bluetooth (allows for short-range wireless communication such as wireless headphones) and GPS (provides location tracking and navigation services). Power management includes the battery which provides power to the device and power management IC which manages power distribution and charging (Indiana Cyber Security, 2024).

Software Components

The Operating System (OS) is the core software that manages hardware resources and provides services for application software. The two mobile operating systems in use today include iOS (proprietary used in Apple devices) and Android (open source used in devices from various manufacturers like Samsung, Google, Motorola, and LG).

Firmware is low-level software programmed into the device's hardware. It includes the bootloader, which initializes the system and loads the OS. The kernel is the core part of the OS that manages system resources, including memory, processes, and hardware interfaces. System Services provided by the OS to support application functionality, such as network connectivity, location services, and multimedia playback. Last are applications which include both Pre-installed Applications (Apps that come with the device) and User-installed Applications (Apps installed by the user from app stores) (Fingas, 2021).

Mobile Device Seizure

Conducting a proper initial investigation is a vital part of any forensic examination. How the evidence is prepared, seized, and then packaged after the proper seizure can be just as important. Data can be easily destroyed by improperly preparing and packaging a device.

The small things are extremely important to the overall success of every investigation. “Bagging and tagging” the device using the proper procedures is not the only concern. The the state of the device at the time of seizure and during property transportation and storage is also important. You must also understand the ways in which a mobile device communicates, and the types of security used with mobile devices so that you can determine the most appropriate ways to protect the device before and after it is seized.

Data from a collected device can be suppressed during a trial, even after a proper seizure, if it was improperly documented regarding the chain of custody. The way in which a device is transported from the scene to a lab or storage facility is also important.

How you deal with an active device can determine the success of the evidence collection. The physical collection of the actual mobile device and any accessories can also determine the validity of the introduced evidence if used in a legal proceeding. A mobile device can be connected to a cellular network, a Wi-Fi network, Bluetooth, or a near field communication (NFC) device and eliminating the risk of contamination of important digital data is critical. Isolating cellular devices from any type of communication is extremely important for preserving the digital evidence and preventing wiping of the device so the following procedures should be followed to when seizing a device and eliminating the risk of contamination of data,

- If the device is on, keep power on (if powered off, leave off)
- Put device in Airplane mode
- Turn off Wi-fi and Bluetooth
- Place in a Faraday Bag

Faraday bags are specialized pouches made of materials that block electromagnetic signals. Faraday bags work by creating a shield around electronic devices, preventing incoming or outgoing electromagnetic signals. This shield blocks radio frequencies, Wi-Fi, Bluetooth, cellular, and other wireless communications. By encapsulating devices within a Faraday bag, users can effectively isolate them from external interference, making it nearly impossible for unauthorized parties to access or tamper with sensitive information. In an era defined by digital connectivity and constant technological advancement, protecting electronic devices from unauthorized access and remote wiping is imperative. Depending on the state of the device, it might not be possible to put the device in airplane mode or turn off Wi-fi and Bluetooth, therefore the way to eliminate the risk of unauthorized access or remote wiping is to place in a Faraday bag until proper extraction of digital evidence.



Figure 2: Mission Darkness Faraday Bag (Mission Darkness, 2024)

The seizure of mobile devices is a fundamental aspect of digital forensics, pivotal for preserving the integrity and availability of digital evidence. By ensuring legal compliance, preventing tampering, and enabling comprehensive forensic analysis, proper seizure practices lay the groundwork for successful investigations and the effective use of digital evidence in legal proceedings. As mobile devices continue to play an integral role in daily life, their importance in forensic investigations will only grow, making the proper seizure of these devices ever more critical.

Data Acquisition Methods

In mobile forensics, the acquisition of data from mobile devices is a critical step. This process involves creating a forensic copy of the data stored on a mobile device while maintaining its integrity for further analysis. There are several methods of data acquisition in mobile forensics, each suited to different scenarios and types of devices. The main acquisition methods are manual, physical, logical, and full file system.

Manual acquisition involves manually browsing through the device and recording information by taking notes and screenshots. The method is only useful when automated tools are unavailable or when dealing with very old or uncommon devices because it is highly time-consuming and prone to human error. Manual acquisition is generally not recommended due to the risk of altering the device's data and should only be used as a last resort.

Logical acquisition extracts data from the device using the device's operating system and communication protocols. Logical acquisition accesses and copies files and directories that are visible to the user, including contacts, messages, call logs, photos, and installed apps. Logical acquisition is generally faster and less invasive than physical acquisition but is limited to data that is not encrypted or restricted by the operating system and does not include deleted data and limits third party application data.

Physical Acquisition involves creating a bit-by-bit copy of the entire physical storage, including unallocated space, deleted files, and hidden data. The method captures all data on the device, providing a more comprehensive dataset for analysis but is more complex and time-consuming than logical acquisition. Physical acquisition requires specialized tools and hardware, such as JTAG (Joint Test Action Group) or chip-off techniques. With advancement in technology, physical acquisition is very rarely used because access to the inside of a device is required and connection to the chipset (Salvation Data, 2022).

JTAG acquisition (type of physical acquisition) uses the JTAG interface to extract data directly from the device's memory chips and involves connecting to the test access ports on the device's motherboard. JTAG requires specialized knowledge, training and equipment and is only used when other methods are not feasible and on older devices where access to the interface is possible. Chip-off Acquisition involves physically removing memory chips from the device's motherboard and reading them with specialized tools and provides access to all data on the memory chip. However, Chip-off is highly invasive and requires significant technical expertise and only used as a last resort due to the potential for damaging the device. Chip-off can only be used on older devices where access to the chips is possible (Salvation Data, 2022).

Full File System Acquisition (Before First Unlock and After First Unlock)

The last and most highly used method used today is full file system (FFS). FFS provides a middle ground between logical and physical acquisition and captures the entire file system, including directory structures and file metadata, unallocated space and deleted files. FFS is useful for devices where physical acquisition is impractical but more detailed data than logical acquisition is needed. FFS relies on gaining root access or exploiting vulnerabilities to access protected areas of the file system. When a phone is collected as

evidence, it is important to consider various procedures to ensure that the maximum amount of information can be extracted from the device. When it comes to iOS and Android devices, the lock state is one of the most important attributes to consider. Phones can be in what is called a Before First Unlock (BFU) or After First Unlock (AFU) state. Depending on which lock state the device is in, the extraction of the device will only be able to collect certain information. This is because iPhones, as well as newer versions of Android, utilize a form of encryption known as file-based encryption which makes files inaccessible while the device is locked after a reboot (Campbell, 2023).

One of the two possible lock states a mobile device is in is known as Before First Unlock, or BFU. The BFU state refers to a phone that has been powered off or reset and has not been signed back into using the screen lock passcode. For iPhones that are in a BFU state, certain features such as the notification center, control center, camera, Wi-Fi, Face ID, Touch ID, screenshots, and lock screen widgets are unavailable to the user until the correct lock screen passcode is entered. Also, upon entering the passcode for the locked iPhone, the message “Your passcode is required when iPhone restarts” will appear.



Figure 2: iPhone 14 that is in the BFU lock state (Notice the camera button, lock screen widgets, and Wi-Fi features are disabled, as well as the unique passcode message)

The experience with Android is similar, as many features within the Quick Settings drop-down menu are locked behind the passcode by default as well as the lock screen phone and camera features. Android devices also may display limited push notifications in this state, along with a custom “Phone restarted” notification that will appear on the lock screen. On the passcode screen, there is a message that says “Use PIN after restart” that is displayed as well.

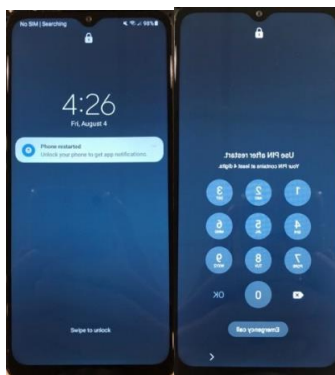


Figure 3. An Android phone (Samsung Galaxy A32 5G) in the BFU lock state (Notice the “Phone restarted” notification, as well as the unique passcode message).

When these devices are in a BFU state, information located on the device is securely encrypted and inaccessible. Upon entering the correct passcode of a device in the BFU state, an encryption key is generated to unlock the filesystem and the contents contained within it. This changes a device's lock state from BFU to After First Unlock, or AFU (Campbell, 2023). The second of two possible unlocks is once the user successfully logs onto the phone after the device was powered off, the phone enters the AFU state. A phone that is in the AFU state is that of any phone that has been unlocked at least once since the device has been reset or completely powered off. A phone that is in the AFU state stays in the state until the device loses power or is rebooted. While a device is in the AFU state, more information can be extracted from the phone, as the filesystem is no longer fully encrypted. When looking for iOS or Android devices that are in the AFU state, features that are normally unavailable for the device when it is in BFU mode, will appear. For iOS, this includes many of the previously mentioned features working properly, such as notification center, control center, camera, Wi-Fi, Face ID, Touch ID, screenshots, and lock screen widgets (Campbell, 2023).



Figure 4: The same iPhone 14 that was shown in BFU section is now in the AFU lock state. Notice the camera, lock screen widgets, and Wi-Fi features are now enabled. The passcode message no longer specifies the device is in BFU mode. A screenshot was able to be taken of both the lock screen and passcode screen.

Android devices that are in the AFU state will have access to all notifications as well, as well as the phone and camera app buttons enabled on the lock screen. The custom BFU passcode messages will not be displayed, and Android devices will not have the “Phone restarted” notification.



Figure 5: The same Samsung Galaxy A32 5G that was shown in BFU section is now in the AFU lock state. Notice the lack of the “Phone restarted” notification, as well the phone and camera buttons now enabled. The passcode message no longer specifies the device is in BFU mode.

Mobile Device Security

Mobile devices have two states: AFU and BFU. AFU devices have been unlocked at least once, while BFU devices have not been unlocked via passcode after restart.

BFU devices have typically been restarted or turned off and require a passcode. They still have their data encrypted and secured and a brute force would be required to obtain a passcode for access. AFU devices have been kept on and have been unlocked at least once. The passcode could potentially be bypassed, and you can proceed to gain access data under the hood. Beyond understanding these two different states, it is just as important as understanding the different types of encryptions (Lorentz, 2023).

Security mechanisms include encryption, secure boot, hardware security modules, and biometric authentication. Mobile devices use encryption to protect data at rest and includes either file-based encryption (FBE) and/or full-disk encryption (FDE). FDE is encryption of an entire disk drive. In the case of full-disk encryption, every piece of data in the disk is encrypted using a single encryption key. When an FDE-enabled device is locked, all the data in it is encrypted and it can be accessed only by entering a valid encryption key. Once the device is unlocked all the data in it gets decrypted and can be accessed by the user. FDE is only available only on dying breeds of Androids prior to Android operating system (OS) version 10. Since OS 10, Android has been using FBE. In FDE, the user must enter the password before the device will even start (Baxter, 2022).

File-Based Encryption is the standard used today by both iOS and Android devices. FBE has no secure startup and each file has its own encryption key, unlike Full Disk Encryption. FBE is the common security mechanism on modern mobile operating systems, iOS and Android, and used to protect sensitive user data. Unlike FDE, which covers an entire storage volume, FBE selectively encrypts individual files or directories for extra protection. This approach enhances security without sacrificing flexibility and performance. FBE operates by associating each file with a unique encryption key. When a user unlocks their device, the system decrypts the specific keys related to their profile, granting access to the files. This granular encryption allows for seamless data sharing between different applications while maintaining high security (Maverick, 2024).

While Apple is known for using hardware encryption, they should be just as well known for using a technology called Data Protection that relies around file-based encryption. Each file is controlled on a per-file basis by assigning it to a specific class that determines when the data becomes available to an end user. Data Protection classes are how Apple decides when files are accessible to the user by decrypting that piece of information. There are four main policies that control the data:

- Complete Protection (Class A)
- Protected Unless Open (Class B)
- Protected Until First User Authentication (Class C)
- No Protection (Class D)

The highest level of protection is considered the Complete Protection class (or Class A). This means that the information is only available when the device is unlocked. This class key is protected using a key derived from the user's handset lock code. Shortly (around 10 seconds in most cases) after the device is locked, this key is discarded from the memory rendering the data inaccessible until the device is unlocked again with either the passcode or biometrics. Information protected at this level will only be able to be extracted from a device when a passcode or key is known (Full File System): HELP – Health, Email, Location, and Safari passwords.

The next level is the Protected Unless Open or Class B. This information is protected with the user's handset lock code but may need to remain available for writing while the device is locked. This includes things like the email attachments which may need to download while the device is still locked. A separate per-file key is generated and used until the file is closed. Once closed, this key is wiped from the memory.

The predominant default level of protection is Class C or Protected Until First User Authentication (AFU state). This is the level of protection that most of the information in iOS falls under such as iMessages/SMS, Call Logs, Contacts, Camera Roll, and is the default class for all third-party application data. The keys responsible for decrypting the data lives in memory while the device is powered on and will remain until the device is rebooted. It is not removed from the memory when the device is locked like Class A protection. AFU images are used to describe information that can be acquired from a device that has been powered on and unlocked at least once. This means that data acquired from an AFU device is data that is under Class C or Class D protection.

Class D or No Protection classes is a class key protected with only the device's UID value. This is always available even before the passcode of the device is ever entered. Even if a file is not specifically assigned a Data Protection class, it is still assigned a Class D protection (i.e. Life 360). Data protected under Class D means that information will be available as soon as the device is booted and available in BFU images.

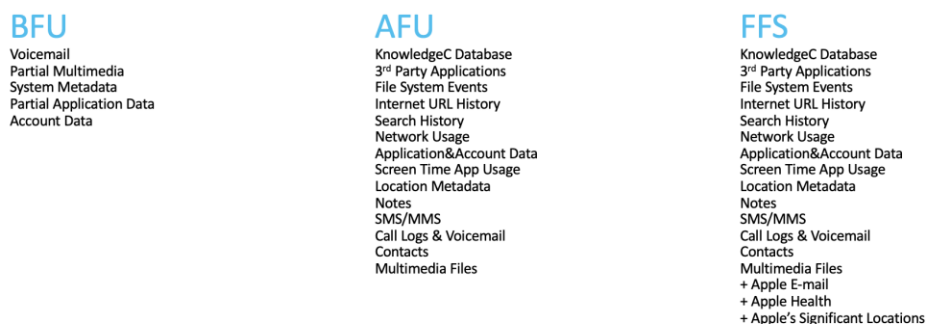


Figure 6: iOS device states and application data that is available for extraction

As far as Android devices, devices that used full-disk encryption along with a user-set password (secure startup) would sit in a “limbo” state where the device would not fully boot up or allow the user to receive phone calls, messages, or alarms. File-based encryption enabled a feature called Direct Boot in Android which allows the user's device to power on without unlocking all of the files in the file system.

Unlike iOS devices, on FBE-enabled Android devices, the data is stored under one of two different categories: Device Encrypted (DE) – Decrypted during Boot (BFU) or Credential Encrypted (CE) – AFU. The order of operations for a device using file-based encryption to boot would be similar to the following:

- Device Powered On -> Device Encrypted data unlocked -> Password Prompt -> User's Credential Encrypted data unlocked

Data which falls into the device encrypted (DE) category will be available as soon as the device has booted and before the user has entered their passcode. Applications which utilize this function can also have a way to store data and make it accessible before the user's passcode is entered.

BFU

- Account Information
- Partial Multimedia
- Wi-Fi Profiles
- Installed Applications
- Android Keystore
- Android Usage History
- Bluetooth Profiles

AFU/FFS

- 3rd Party Applications
- Application&Account Data
- Wi-Fi Profiles
- Installed Applications
- Android Keystore
- Android Usage History
- Bluetooth Profiles
- Internet URL History
- Calendar Events (Android/Google)
- Web Search History
- Application History and Screenshots
- Location Metadata
- Notes
- SMS/MMS
- Call Logs & Voicemail
- Contacts and Email
- Multimedia Files

Figure 7: Android device states and application data that is available for extraction

The stronger protection is when files fall into the credential encrypted (CE) category. This data is protected (encrypted) until the user who owns the container has entered their passcode at least once. This makes multi-user devices more secure as each separate profile can control the access of their own data. In FBE Android devices, a BFU (before first unlock) device would contain anything that is available at the DE level. A device in the “AFU” state would extract everything at the CE level for the primary user. The difference between this and iOS is that an AFU in Android is equal to a full file system in iOS.

Extracting and analyzing data

In digital forensics, extracting data from digital devices is a critical process that requires specialized tools and procedures to ensure the integrity and admissibility of the evidence. This section outlines the commonly used digital forensics software tools and the standard procedures for data acquisition. Magnet Forensics and Cellebrite provide the most popular digital forensics software used by industry professionals around the world. Although both offer several products used in the digital forensics’ world, each of them has two products that are considered the gold standard in the community.

Magnet Forensics

In the rapidly evolving landscape of digital forensics, a field where technology meets investigative work to uncover digital evidence, Magnet Forensics stands out as a pivotal player. This realm, essential for solving crimes in our increasingly digital world, relies on cutting-edge tools and methodologies to analyze data from various digital devices. Magnet Forensics has carved a niche for itself by offering comprehensive solutions that address the complex needs of today’s digital investigations. Magnet Forensics has established itself as a leader in the digital forensics’ domain through its suite of tools designed to streamline investigations and enhance the analytical capabilities of forensic professionals. Each tool in their arsenal addresses specific challenges in the field, making the process of digital investigation more efficient and thorough (Salvation Data, 2024).

Magnet Forensics’ flagship product that leads the way in digital investigations is Axiom. It is a complete platform that provides in-depth forensic examination of mobile and computer devices, not simply a tool. Digital evidence from a variety of sources may be recovered, examined, and reported on with great efficiency using Axiom. Its adaptability, which allows it to sort through data from operating systems, cloud storage, and even encrypted files, contributes to its resilience by giving investigators a comprehensive picture of the evidence. Advanced analytics integration makes complicated cases combining digital and mobile forensics much more useful by revealing illuminating trends.

Magnet Forensics' other flagship product is a state-of-the-art mobile forensics tool for accessing data on mobile devices, known as Graykey. Access is the cornerstone of digital forensics and Graykey is used to unlock leading iOS and Android devices to get the evidence needed. Graykey can access and extract evidence from mobile devices irrespective of device state including credential stores like Keychain (iOS) and Keystore (Android) to decrypt content. Graykey can perform same day extractions from locked iOS and modern Android devices including deleted data. In addition, Graykey can extract the full contents from iOS and modern Android devices (FFS) and uncover more pictures, videos, chat histories, location data, and Internet evidence than a logical acquisition (Magnet Forensics, 2024).

Cellebrite

Digital forensics plays a critical role in modern investigations, where digital devices hold a wealth of information that can provide valuable evidence. The other gold standard used by digital forensics professionals for extracting and analyzing data from mobile devices are Cellebrite's powerful suite of tools known as Universal Forensic Extraction Device (UFED), Physical Analyzer (PA), and Premium. Cellebrite UFED and PA are a suite of leading digital forensics tools used for the extraction, decoding, analysis, and reporting of data from mobile devices which is widely used by law enforcement, military, and corporate investigators for mobile device forensics. The UFED suite includes hardware and software components designed to facilitate comprehensive data extraction and forensic analysis and allows forensic examiners to conduct in-depth analysis of full file system, physical and logical extractions from various mobile devices.

Cellebrite Premium is an advanced digital forensics solution developed by Cellebrite for law enforcement and intelligence agencies. It is designed to perform in-depth extraction and decoding of data from locked and encrypted mobile devices, including the latest smartphones and tablets. Cellebrite Premium offers capabilities beyond those of standard tools, enabling access to data that is typically protected by robust security measures. Cellebrite Premium provides digital investigators the ability to recover legally valid passwords, unlock devices, gain After First Unlock (AFU) access, and perform full file system extractions from iOS devices on site. In addition, Cellebrite Premium allows investigators to bypass locks and perform physical extractions on a wide range of popular Android devices such as Samsung, LG, Motorola and other devices. Unlike UFED and PA, Premium gives digital investigators access to the following: third-party applications, social media apps, saved passwords and tokens, chat conversations, location data, e-mail attachments, deleted content, system logs, etc.

Magnet Forensics and Cellebrite suite of tools represent the pinnacle of mobile forensic capabilities, offering unparalleled access to data on locked and encrypted devices and advanced unlocking, extraction, and analysis features which make them essential tools for law enforcement and intelligence agencies facing increasingly sophisticated digital security measures.

Conclusion

In conclusion, the foundations of mobile forensics are built on a deep understanding of mobile technologies, advanced data acquisition and analysis techniques and a commitment to ongoing education and research. By embracing these principles, we can enhance the capabilities of forensic practitioners and contribute to the pursuit of justice in the digital age. The academic study of mobile forensics provides a solid foundation for understanding the principles, techniques, and challenges associated with the field. By fostering a rigorous academic approach, we can ensure that forensic practitioners are well-equipped to handle the dynamic landscape of mobile technology and effectiveness of forensic investigations.

References

- Ayers, R., Brothers, S., and Jensen, W. (2014, May). *Guidelines on Mobile Device Forensics*. Retrieved April 1, 2024 from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>
- Baxter, B. (2022, January 24). *File-based encryption vs full-disk encryption*. Retrieved April 22, 2024 from <https://www.hexnode.com/blogs/file-based-encryption-vs-full-disk-encryption/>
- Bazen, A. (2023, December 12). *Cell phone statistics 2024*. Retrieved April 15, 2024 from https://www.consumeraffairs.com/cell_phones/cell-phone-statistics.html
- Brewster, T. (2018a, March 5). *Mysterious \$15,000 'GrayKey' Promises To Unlock iPhone X For The Feds*. Retrieved April 15, 2024 from <https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/?sh=7e85201e2950>
- Brewster, T. (2018b, February 26). *The Feds Can Now (Probably) Unlock Every iPhone Model In Existence – UPDATED*. Retrieved April 15, 2024 from <https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/?sh=5e3690b9667a>
- Campbell, W. (2023, August 23). *BFU and AFU Lock States*. Retrieved April 25, 2024 from <https://madlabs.dsu.edu/digforce/blog/2023/08/23/bfu-and-afu-lock-states/>
- Indiana Cyber Security. (2024). *Understanding mobile device architecture and operating systems*. Retrieved April 20, 2024 from <https://www.indianacybersecurity.com/Understanding-mobile-device-architecture-and-operating-systems.php>
- Fingas, J. (2021). *The Anatomy of a Smartphone – Things for Designers to Consider for Mobile Development*. Retrieved April 21, 2024 from <https://www.interaction-design.org/literature/article/the-anatomy-of-a-smartphone-things-for-designers-to-consider-for-mobile-development>
- Kulm, A. (2023, March 11). *Solving Crime Through Digital Evidence*. Retrieved April 1, 2024 from <https://dda.ndus.edu/ddreview/solving-crime-through-digital-evidence/>
- Lamb, D. (2019, April 21). *10 Ways Mobile Forensics Can Benefit Your Law Enforcement Agency*. Retrieved April 1, 2024 from <https://erintechnology.com/10-ways-mobile-forensics-can-benefit-your-law-enforcement-agency/>
- Larrichia, F. (2024, February 23). *Smartphones in the U.S. - statistics & facts*. Retrieved April 13, 2024 from <https://www.statista.com/topics/2711/us-smartphone-market/#topicOverview>
- Liddle, A. (2024, April 11). *Computer forensics degree: The key to a thriving career*. Retrieved April 15, 2024 from <https://cybersecurityguide.org/careers/computer-forensics/>
- Lorentz, P. (2023, August 7). *Episode 23: I BEG TO DFIR – Data Extractions Explained: FFS, AFU, BFU, Advanced Logical – Digital Forensics Webinar*. Retrieved April 22, 2024 from <https://callebrite.com/en/episode-23-i-beg-to-dfir-data-extractions-explained-ffs-afu-bfu-advanced-logical-digital-forensics-webinar/>

Issues in Information Systems

Volume 25, Issue 3 pp. 94-108, 2024

- Magnet Forensics. (2024, April 25). *Magnet Graykey: Accelerate your mobile investigations*. Retrieved April 25, 2024 from <https://www.magnetforensics.com/products/magnet-graykey/>
- Maverick. (2024, February 3). *Understanding File-Based Encryption (FBE) and Its Role in Android*. Retrieved April 22, 2024 from <https://www.airdroid.com/mdm/file-based-encryption/>
- Mission Darkness. (2024, May 5). *Mission Darkness™ Non-Window Faraday Bag for Phones*. Retrieved May 5, 2024 from <https://mosequipment.com/collections/keyfob-and-phone-faraday-bags/products/mission-darkness-non-window-faraday-bag-for-phones>
- Nurick, O. (2021, August 4). *The Solution That Changed Modern Digital Investigations Forever*. Retrieved April 15, 2024 from <https://celebrite.com/en/the-solution-that-changed-modern-digital-investigations-forever/>
- Oxygen Forensics (2023, November 27). *What is Mobile Forensics?* Retrieved April 4, 2024 from <https://oxygenforensics.com/en/resources/mobile-device-forensics/>
- Reiber, L. (2019, June 4). *How Are Criminals Using Smart Devices To Commit Crimes?* Retrieved April 16, 2024 from <https://www.forbes.com/sites/quora/2019/06/04/how-are-criminals-using-smart-devices-to-commit-crimes/?sh=2049950827b8>
- Reichert, C. (2021, April 16). *iPhone from 2015 San Bernardino shooting was unlocked for FBI by Australian security firm, report says*. Retrieved April 15, 2024 from <https://www.cnet.com/tech/mobile/iphone-from-2015-san-bernardino-shooting-was-unlocked-for-fbi-by-australian-security-firm-report-says/>
- Salvation Data. (2022, January 28). *Data Acquisition in Mobile Forensics: The Critical Process to Collect Mobile Evidence*. Retrieved April 23, 2024 from <https://www.salvationdata.com/knowledge/data-acquisition-in-mobile-forensics/>
- Salvation Data. (2024, February 19). *Is Magnet Forensics the Ultimate Forensic Solution? Insights Revealed*. Retrieved April 25, 2024 from <https://www.salvationdata.com/knowledge/magnet-forensics/>
- Smith, C. (2021, April 14). *The true story of how the FBI cracked the San Bernardino shooter's iPhone*. Retrieved April 16, 2024 from <https://bgr.com/tech/san-bernardino-iphone-hack-how-azimuth-broke-encryption/>
- Statista. (2022, August). *Number of smartphone users in the United States from 2009 to 2040*. Retrieved April 15, 2024 from <https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/>