LOCKED IOS DEVICE: DATA AVAILABILITY ON BEFORE FIRST UNLOCK (BFU) STATES EXTRACTION

Adly Gilang Kurnia

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia,
Depok, West Java, Indonesia
adly.gilang@ui.ac.id

Ruki Harwahyu*

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia,
Depok, West Java, Indonesia
ruki.h@ui.ac.id
*Corresponding author

Abstract

Globally, Apple iOS has 17.3% of smartphone market share, which aligns with the findings from Cellebrite in 2024. It highlights iOS devices as dominant digital evidence in digital forensics investigations. However, accessing the data in locked iOS devices remains a significant challenge due to limited data accessibility. This study evaluates the effectiveness of Before First Unlock (BFU) extraction in recovering user data from locked devices. We compare data availability and integrity between BFU and Full File System (FFS) extractions using mobile forensics tools and file hash comparison. The analysis revealed a 63.48% match rate (338,062 of 532,509 files) between BFU and FFS extractions, indicating some data loss in BFU. While some documents were recoverable, critical application data was inaccessible. This highlights the limitations of BFU extraction in retrieving complete datasets from locked iOS devices. However, the recovered data with verified integrity remains valuable for forensic investigations.

***Keywords*: Digital forensics; locked iOS device; Before First Unlock (BFU) extraction; data availability; data integrity**

1. Introduction

Digital forensics plays a critical role in law enforcement by providing methods for collecting, analyzing, and presenting digital evidence in court. However, the rise of mobile devices, particularly iOS devices with robust security features, has significantly increased the complexity of digital evidence acquisition. Studies as seen in the Fig. 1 , indicate that smartphone is the most common evidence. Fig. 2 showed locked iOS devices pose a major challenge, constituting up to 73% of the access difficulties encountered during investigations [1][2].

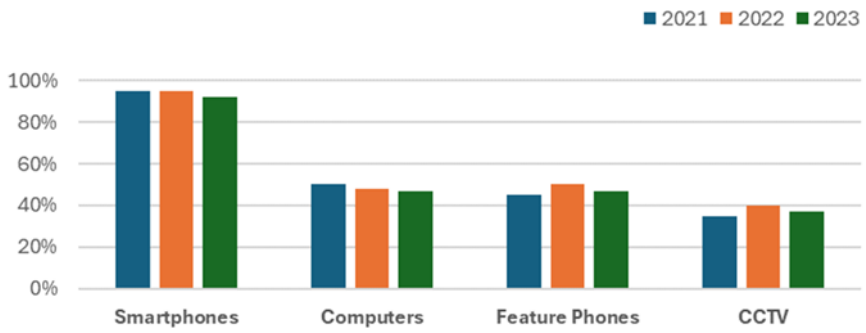


Fig. 1. Most Common Evidence Source (Cellebrite, 2024)

One of the biggest difficulties for forensic investigators is accessing data on locked iOS devices, especially those protected by fingerprint or facial recognition. Apple's strong security measures, including full-disk encryption and secure boot processes, make data acquisition particularly challenging on devices in the "Before

First Unlock" (BFU) state [3]. This complexity is further amplified by the potential use of counter-forensic techniques that impede data recovery efforts.

The state of a device at seizure significantly impacts recoverable data. Understanding the limitations of BFU data extraction is crucial for investigators to optimize their approach and maximize the potential for acquiring valuable evidence. In contrast, devices unlocked at the time of seizure (After First Unlock - AFU) offer greater accessibility to user data. BFU also presents a significant challenge due to data encryption, rendering traditional techniques ineffective. While AFU offers some level of decrypted data access, it might still have limitations. Understanding these lock state differences, and the resulting data accessibility variations is crucial for digital forensics professionals [4].

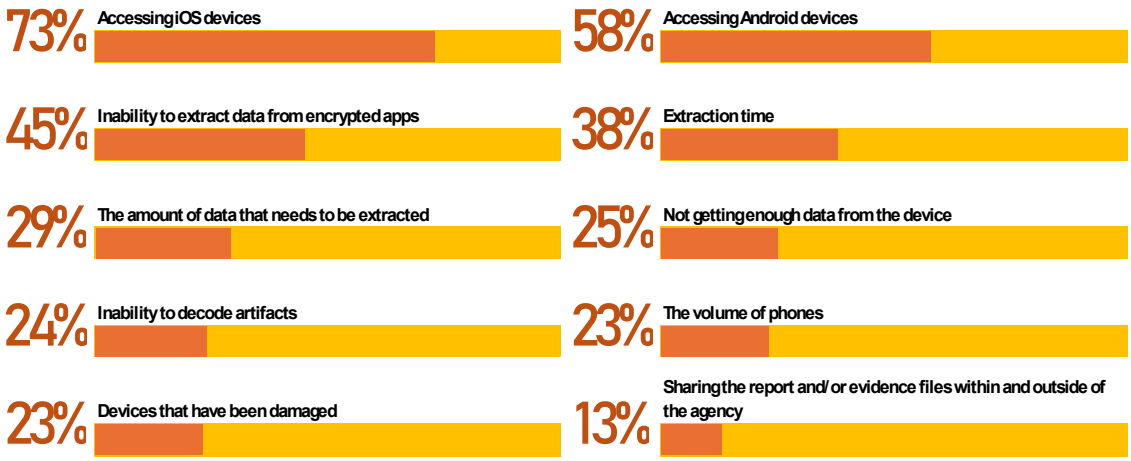


Fig. 2. Biggest Challenge in Digital Examinations (Cellebrite, 2024)

2. Related Works

Several studies have focused on discussing locked mobile devices that are related to this research and used as references. Herrera L. A. [5] discusses about shutting down an iOS device transitions it from AFU to BFU, which affects the amount of data that can be forensically retrieved from the device. This transition in device state highlights the importance of understanding the implications of AFU and BFU states on the forensic analysis process, as it directly influences the extent of data that can be accessed and examined by forensic specialists.

AL-Dowihi, L. W. et al [6] discuss about preserving evidence and acquiring data from locked iOS devices, particularly in the BFU state, underscores the importance of understanding and handling devices in this critical state for forensic analysis. The discussion emphasizes the significance of proper evidence preservation and data acquisition techniques for locked devices, which align with the challenges and opportunities presented by the BFU phase in mobile forensics.

Fukami, A. et al [7] discuss the importance of understanding the device state in relation to After First Unlock (AFU) and Before First Unlock (BFU) when dealing with biometric authentication methods on modern mobile devices. It explains that in most cases, biometric authentication only works when the target device is in the AFU state and not equipped with advanced security features like inactivity-time detection measures. They also mention the implications of the BFU state, where a password, passcode, or pattern-drawing is required to unlock the device and enable biometric authentication. Additionally, it highlights the presence of a "panic" password option in some smartphones that can execute hidden rules, potentially leading to data loss if used instead of the legitimate unlocking password prior to data extraction. The paper emphasizes the importance of considering the device's state and security features when conducting forensic examinations involving biometric authentication methods.

Katalov, V. [8] discusses the accessibility attributes related to keychain items based on the device's unlock status, including After First Unlock (AFU) and Before First Unlock (BFU) states. It explains that keychain items marked with the kSecAttrAccessibleAlways attribute are always accessible, even if the device is locked or in the BFU state and are extractable during the BFU extraction process. Additionally, it mentions that keychain records protected with the kSecAttrAccessibleAlways attribute do not require the user's screen lock password to decrypt, making them accessible even before the device is unlocked for the first time. These details highlight the importance of understanding the different accessibility states of keychain items in locked or unlocked devices for forensic analysis and data extraction purposes.

Alendal, G. et al [9] researched specifically mentions the "before-first-unlock (BFU) state" in the context of their attack. The attack demonstrated in the study works on powered off devices, known as the BFU state, without requiring knowledge of user credentials. This highlights the significance of the attack being able to bypass the

security of the eSE in the BFU state, emphasizing the vulnerability of the system even before it is unlocked for the first time.

Alendal, G. [10] doctoral thesis explores the challenges and techniques related to accessing data on mobile phones in different states such as Before First Unlock (BFU) and After First Unlock (AFU). The research focuses on bypassing encryption, security measures, and exploiting vulnerabilities to acquire forensically valuable data from locked devices, especially in the BFU state where the device does not need to be powered on or unlocked. By analyzing security vulnerabilities and attack paths, the thesis provides insights into the complexities and strategies involved in accessing user data on mobile phones under various security states.

Fikri, A. et al [11] discuss about the performance differences between Dalvik and ART, this can be crucial for forensic analysts when dealing with locked devices. By knowing how these runtime environments handle data processing and memory management, analysts can potentially develop more effective methods to access and extract data from locked Android devices. The insights gained from the study can help optimize data recovery processes, leading to quicker and more successful extraction of data from locked devices in forensic investigations.

Mobile forensics involves the collection, preservation, analysis, and presentation of digital evidence from mobile devices. However, iOS devices present unique challenges due to their inherent security features. Apple utilizes a combination of full-disk encryption, secure boot processes, and sandboxing to safeguard user data [3]. Additionally, biometric authentication further complicates data access, as unlocking often requires fingerprints or facial recognition which investigators may not possess.

The locked state of a device plays a critical role in iOS forensics. The BFU state, where the device remains locked since its last power cycle, presents the most significant challenge for data extraction. When you turn off your iPhone, it enters BFU mode and remains there until you unlock it. In locked iOS devices, content is securely encrypted until the user enters their screen lock passcode. This is required in order to generate the encryption key which is needed to decrypt the iOS device's file system. Almost all the content of an iOS device is encrypted until the point when the user unlocks it to enable the phone to start up [12]. This difficulty arises from two key factors: first, data encryption. In this scenario, most user data reside in an encrypted state, rendering traditional forensic techniques used for unencrypted devices largely ineffective. Second, the potential risks associated with unauthorized data extraction from locked devices necessitate the implementation of robust countermeasures to prevent data breaches and unauthorized access [13].

This research aims to bridge the knowledge gap regarding data availability and integrity of extractability data on BFU iOS devices. By analysing the user data, the challenges associated with data extraction, and potential mitigation strategies, this research seeks to provide valuable insights for law enforcement agencies and digital forensic practitioners when dealing with locked iOS devices in the BFU state.

3. Methodology and Tools

This research employs a qualitative approach by using mobile forensics tools to extract the data from the device. By using Apple iPhone X with iOS 15.6.1 and some mobile forensics tools Cellebrite UFED Premium v7.68.602 and Oxygen Forensics Detective v16.1.0.200 to extract and analyze the image. To ensure the extracted image data can be used in court, we follow NIST Guidelines on Mobile Devices Forensics [14][15]. This guideline consists of four stages: collection, examination, analysis, and reporting as shown in Fig. 3 [16].

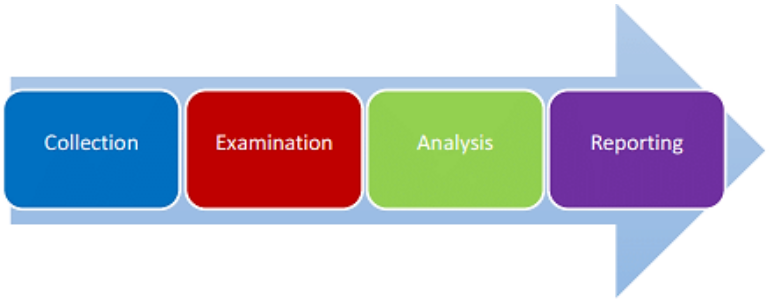


Fig. 3. Forensic Mobile Stages by NIST

The forensic process involves four main steps: collection, examination, analysis, and reporting [16].

- Collection: Gathering data from various sources while following guidelines to preserve its integrity [16].
- Examination: Using tools to examine the collected data in detail, looking for evidence related to the incident [16].
- Analysis: Using methods to draw conclusions from the examined data and determine its significance [16].
- Reporting: Documenting the findings, actions taken, tools used, and providing recommendations for improvement [16].

This process helps investigators systematically analyse digital evidence in a way that is reliable and can be used in legal proceedings.

3.1. *Data Extraction Scenario*

This research focuses on data extraction from iOS devices in their original state, without rooting or jailbreaking. Two extraction conditions were evaluated: a locked state (Before First Unlock - BFU) and an unlocked state (Full Filesystem access). The BFU extraction was using Cellebrite UFED Premium capability and did not utilize the checkm8 exploit, which using physical extraction method from DFU mode.

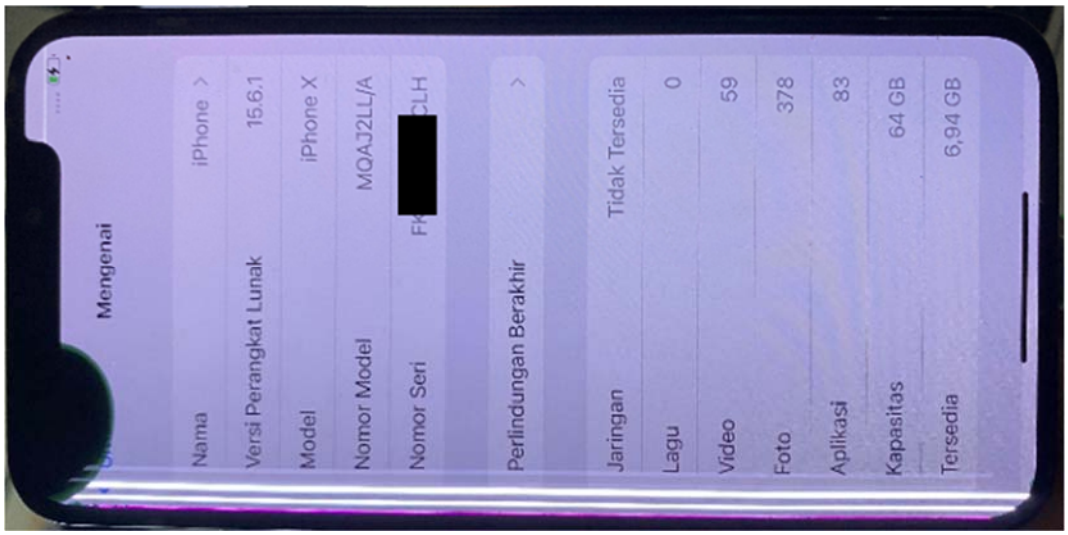


Fig. 4. Target Device for Extraction

While the checkm8 could be combined with tools like checkra1n and libmobiledevice, forensic investigator can gain access to semi-encrypted data on certain iPhone models through jailbreak, even when the device is locked [17]. However, checkm8 method has limitations in device and iOS version compatibility, we aimed to explore the potential of BFU data extraction capabilities for future forensic applications. In the unlocked state, data will be extracted using the Full File System method.

Full File System extraction will include the file structure of the device, collecting the folders, sub-folders, and their data. This generates more data than the Logical extraction and can be used for further examination—the deep dive [18]. The target device for this research was an Apple iPhone X with iOS 15.6.1 and 64 GB of storage as seen in Fig. 4. After the extractions are completed, the image of the devices will be imported to Oxygen Forensics Detective to be analyzed further.

3.2. *Data Analysis: Extracted Content Comparison*

The analysis of the extracted data employed the following methods and procedures:

- Forensic image parsing: the extracted data was imported into Oxygen Forensic Detective (OFD) to explore the recoverable files and applications. This initial examination provided a broad overview of the data types and potential applications that could be further analyzed.
- Manual file system exploration: a manual exploration of the extracted forensic image, this exploration aimed to locate specific data types and observe their file paths, providing insights into the organization of the data on the BFU device.
- Hash list comparison: the hash list of the files from the BFU and FFS extractions were generated. Identify the file system by matching to the hash set from the National Software Reference Library (NSRL) RDS, a collection of digital signatures of known, traceable software applications [19] or from the database that already included in OFD. Generated hash list from BFU and FFS will be compared and analyzed in terms of file name, path, and size.

Document availability and readiness: explore the recovered documents in BFU extraction. This procedure is to ensure the document can be open, read and can be used in investigations.

4. Analysis Results

This chapter presents the results obtained from the data extraction processes outlined in the materials and method section. The analysis focuses on comparing the effectiveness of data extraction between the Before First Unlock (BFU) and Full Filesystem (FFS) methods. Additionally, a file hash comparison analysis was conducted to assess data integrity.

4.1. *Before First Unlock (BFU) Extraction Result*

The BFU extraction, conducted using Cellebrite UFED Premium, aimed to evaluate the range of data recoverable from a locked iOS device. The extraction process and result of extracted data can be seen in Fig. 5 and Fig. 6.

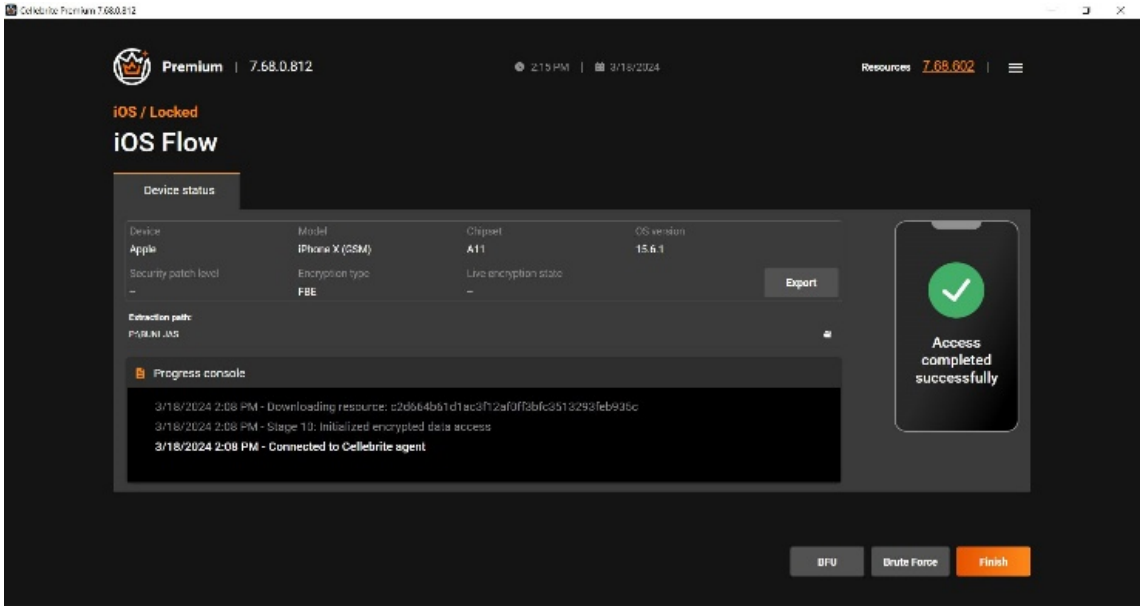


Fig. 5. BFU Extraction Process

Name	Date modified	Type	Size
EXTRACTION_BFU.zip	18/03/2024 14.48	Compressed (zipped) Folder	27.624.091 KB
SummaryReport.pdf	18/03/2024 14.48	Foxit PDF Reader Document	664 KB
EXTRACTION_BFU.ufd	18/03/2024 14.48	UFED Dump	2 KB

Fig. 6. BFU Extraction Data

The size of the extracted image is around 27.6 GB of 64GB device capacity. By comparing the size, we could see just around 40% of the media obtained in BFU locked device extraction. The extracted data was imported into Oxygen Forensic Detective (OFD) to gain a preliminary understanding of the recoverable files and applications. Fig. 7 and Fig. 8data that could be recovered by OFD at this stage, this doesn't necessarily imply limitations in recoverable data. Other applications might require deeper analysis with additional forensic tools.

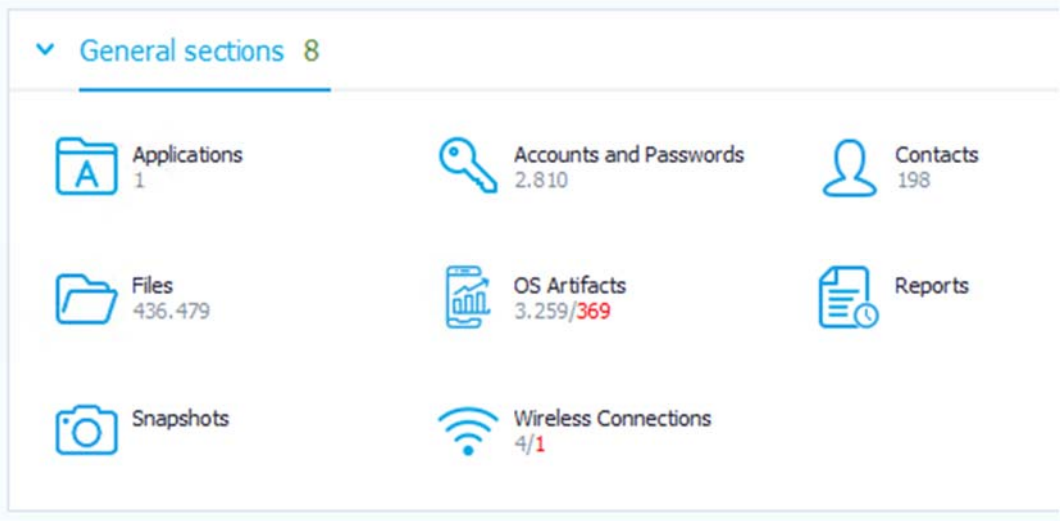


Fig. 7. BFU General Data Extracted Result

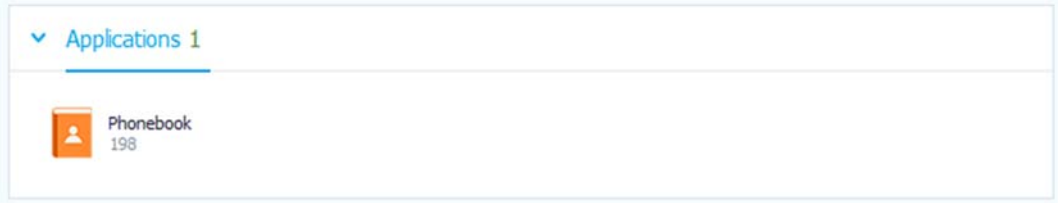


Fig. 8. BFU Application Extraction Result

4.2. *Full File System Extraction Result*

The FFS extraction serves as a benchmark for data recovery and conducted using the Full Filesystem access method, the extraction result can be seen in Fig. 9.

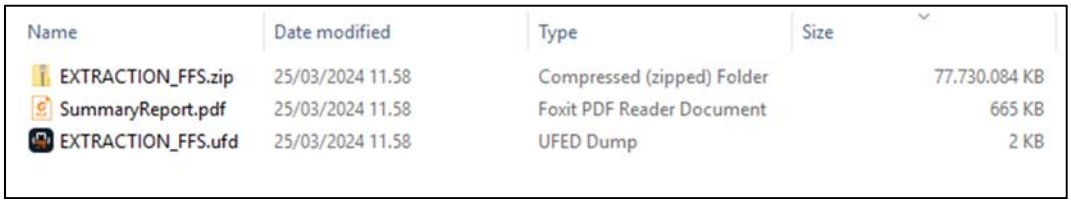


Fig. 9. FFS Extraction Data

Similar to the BFU extraction, the data from the FFS extraction was imported into OFD for a preliminary overview. As seen in the Fig. 10 and Fig. 11, the import process identified numerous installed applications on the device. While OFD may not be able to fully parse the data from all applications, this initial exploration suggests a rich potential for further analysis that could support the investigation.

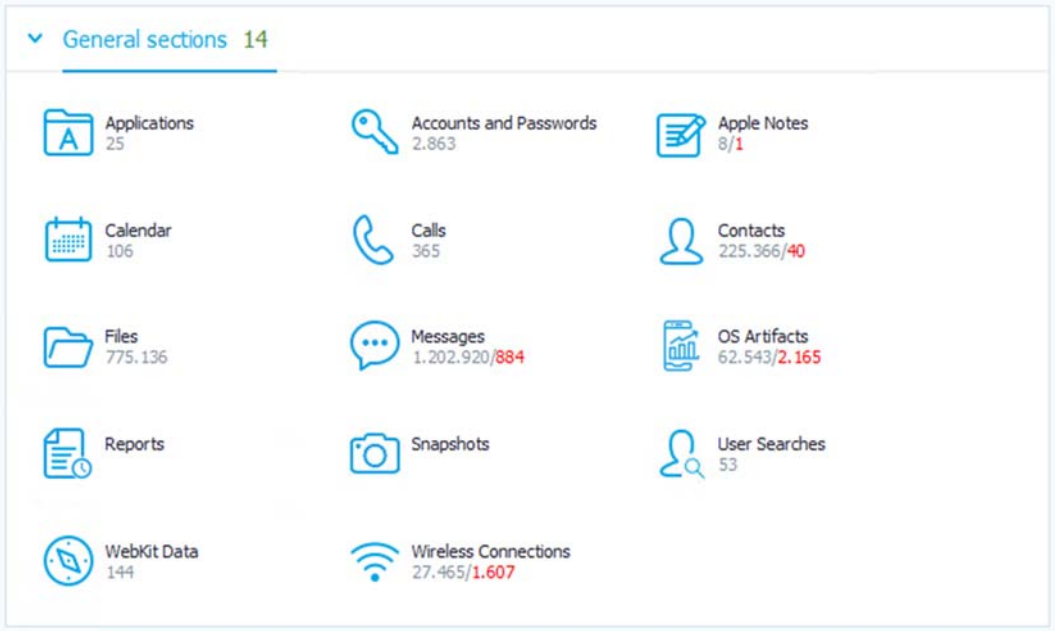


Fig. 10. FFS General Data Extraction Result

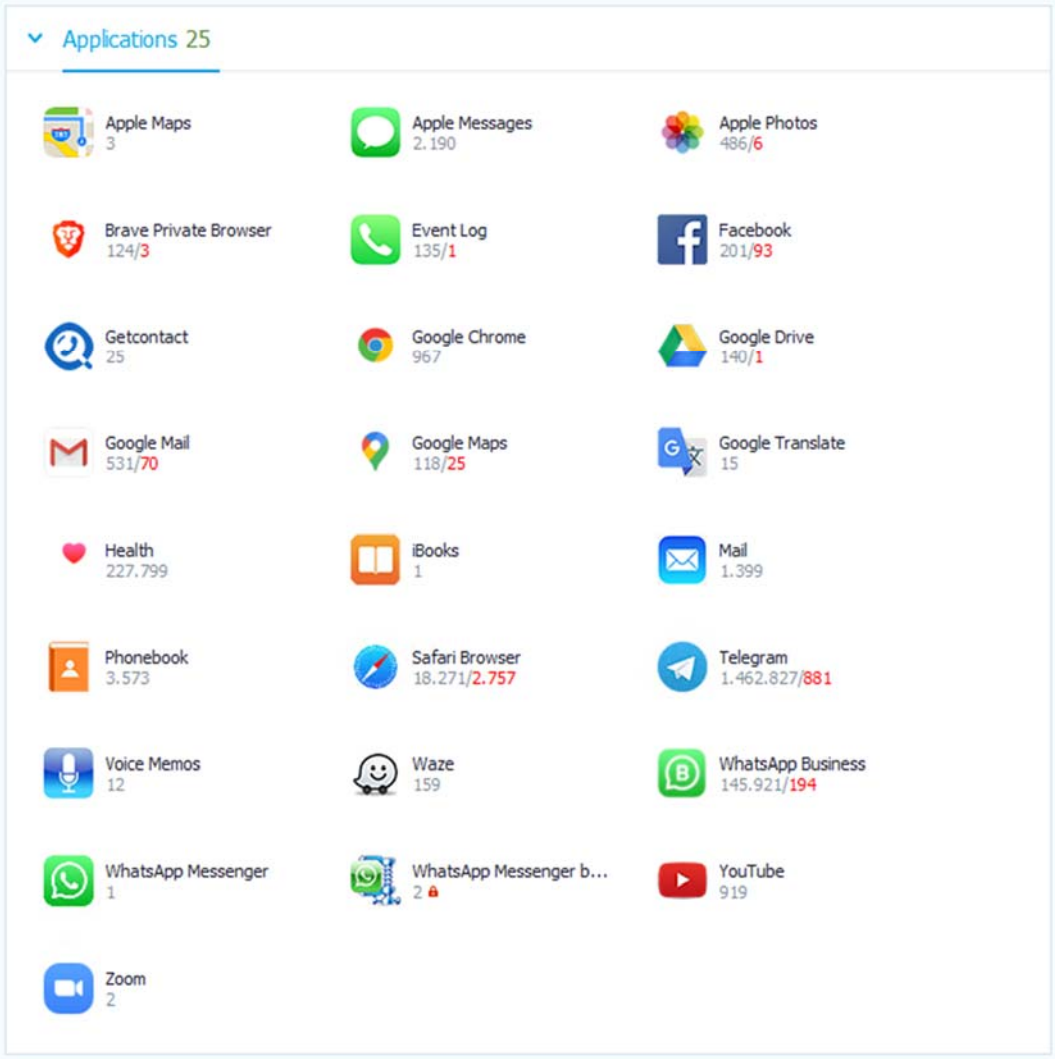


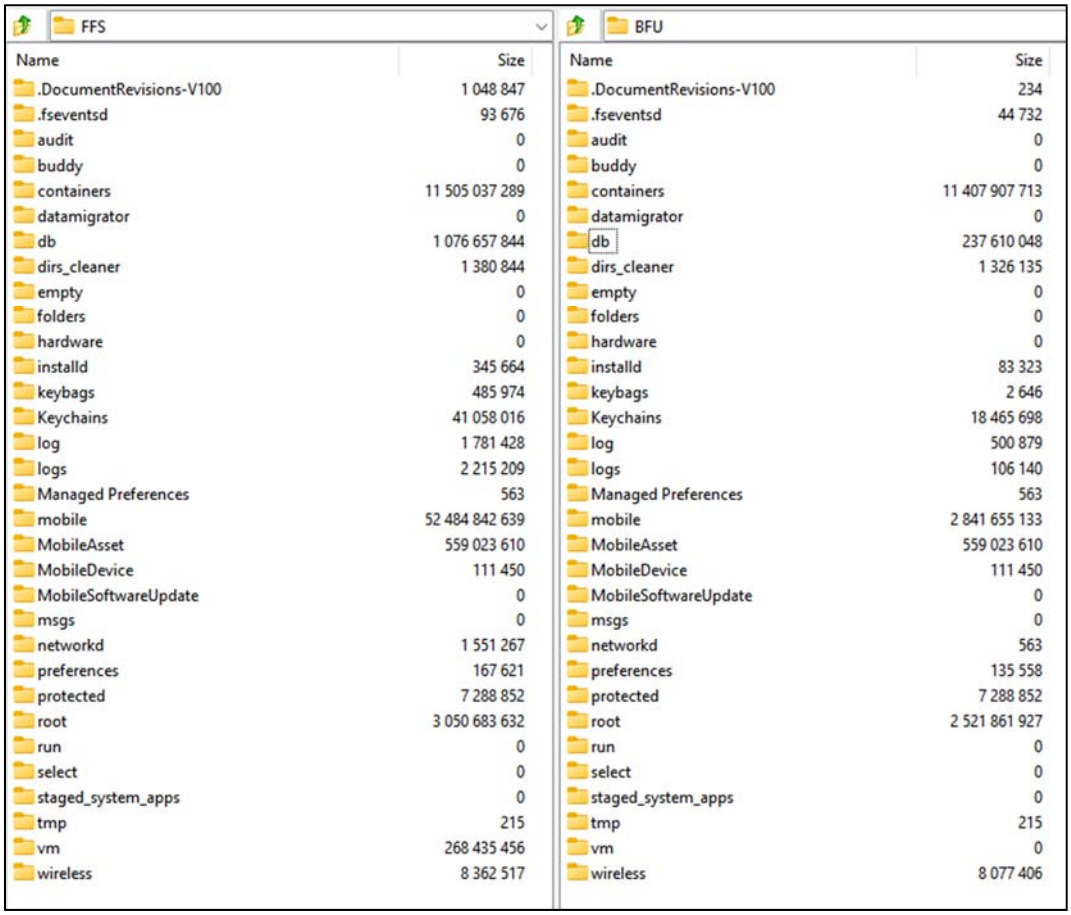
Fig. 11. FFS Application Extraction Result

4.3. *Extraction Comparison Analysis*

By comparing extraction images manually using 7zip file manager and Oxygen Forensic Detective file explorer, revealed significant size differences for folders within the /private/var/ directory, suggesting missing data. In the Fig. 12 shown that the files folder structure and the folder name are same, but the contents were different in folder size. The size of the folder in line with the number of files that contained in the /Private/var folder as seen in Fig. 13 , the number of files in BFU extraction is only 33.64% of the FFS extraction.

In another example, as seen in the Fig. 14, WhatsApp Business application folder located at /private/var/mobile/Containers/Shared/AppGroup/0865B859-617B-4053-9E12-AA348E4CBD0C/, lacked the ChatStorage.sqlite database, hindering investigation into communication data.

However, some documents within the Message/Media/ folder were recoverable and readable, although with encrypted filenames by WhatsApp and the system. These documents could still undergo OCR (Optical Character Recognition) processing to index the text content and identify document types. Documents in the WhatsApp folder is stored within folders named based on WhatsApp account IDs or group IDs. BFU extraction is a limited data collection that does contain mostly system data, but also contains some good user data mixed in as well [20].



FFS

Name	Size
.DocumentRevisions-V100	1 048 847
.fseventsd	93 676
audit	0
buddy	0
containers	11 505 037 289
datamigrator	0
db	1 076 657 844
dirs_cleaner	1 380 844
empty	0
folders	0
hardware	0
installd	345 664
keybags	485 974
Keychains	41 058 016
log	1 781 428
logs	2 215 209
Managed Preferences	563
mobile	52 484 842 639
MobileAsset	559 023 610
MobileDevice	111 450
MobileSoftwareUpdate	0
msgs	0
networkd	1 551 267
preferences	167 621
protected	7 288 852
root	3 050 683 632
run	0
select	0
staged_system_apps	0
tmp	215
vm	268 435 456
wireless	8 362 517

BFU

Name	Size
.DocumentRevisions-V100	234
.fseventsd	44 732
audit	0
buddy	0
containers	11 407 907 713
datamigrator	0
db	237 610 048
dirs_cleaner	1 326 135
empty	0
folders	0
hardware	0
installd	83 323
keybags	2 646
Keychains	18 465 698
log	500 879
logs	106 140
Managed Preferences	563
mobile	2 841 655 133
MobileAsset	559 023 610
MobileDevice	111 450
MobileSoftwareUpdate	0
msgs	0
networkd	563
preferences	135 558
protected	7 288 852
root	2 521 861 927
run	0
select	0
staged_system_apps	0
tmp	215
vm	0
wireless	8 077 406

Fig. 12. Comparison of /Private/var/ Folder

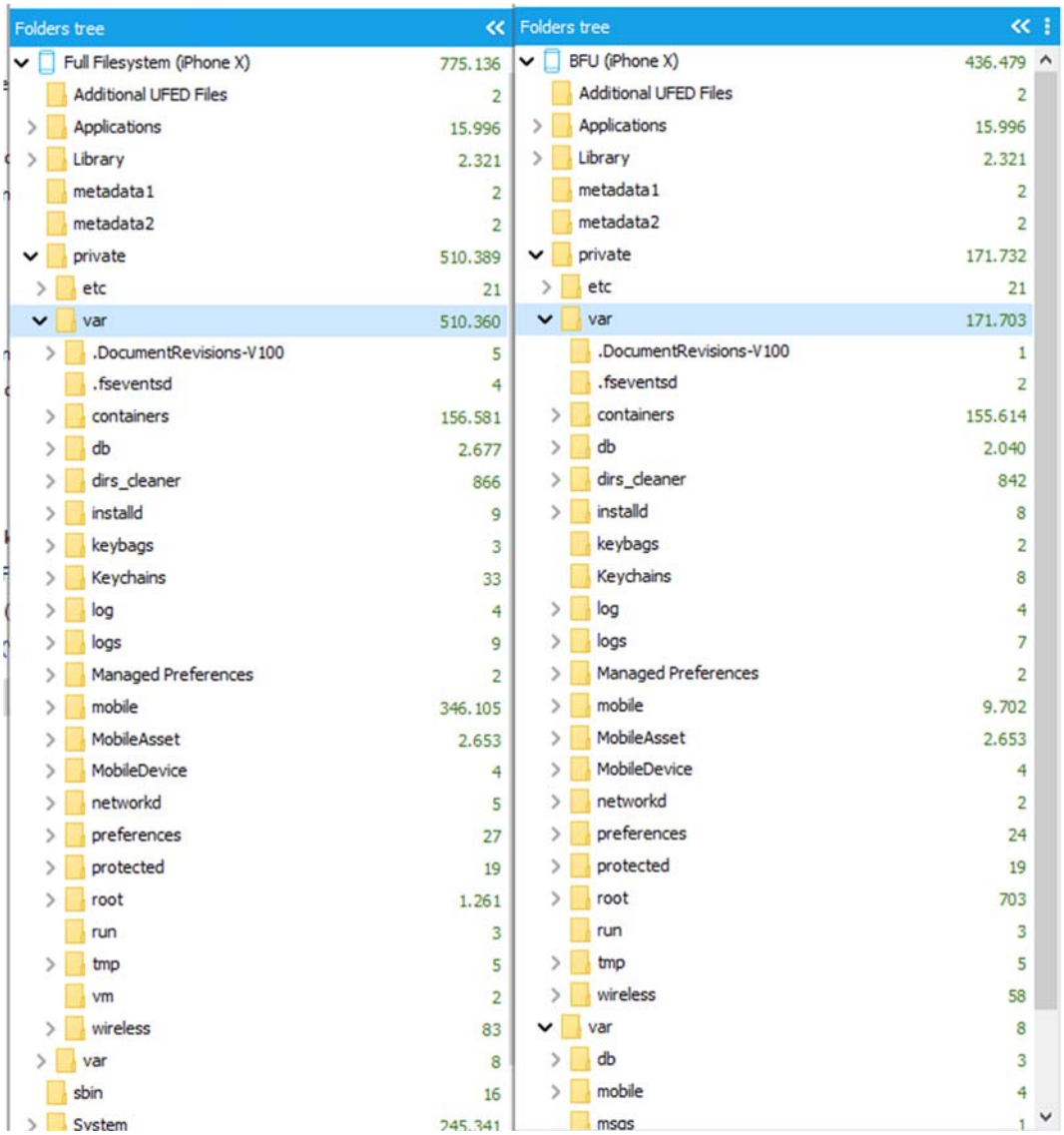


Fig. 13. Comparison Number of Files in /Private/var Folder

A file hash comparison analysis was conducted by using the SHA-1 hashing algorithm to ensure data integrity and identify discrepancies between the BFU and FFS extractions. This analysis compared unique hash values for each file extracted from both methods, verifying if the corresponding files remained unaltered during the extraction processes. The results of the comparison are summarized as follows:

- Total Files Analyzed: 436.479 files were obtained from the BFU extraction, 78.877 files identified as known files as seen in Fig. 15. The hash list was generated and 338.203 unique SHA-1 hash were listed including the system files.
- Matched Files in FFS Extraction: from 338.203 hash listed from the BFU extraction exhibited, matched hash values in the FFS extraction data. This indicates a high degree of consistency between two extraction methods for most of the recovered files as seen in Table 1.

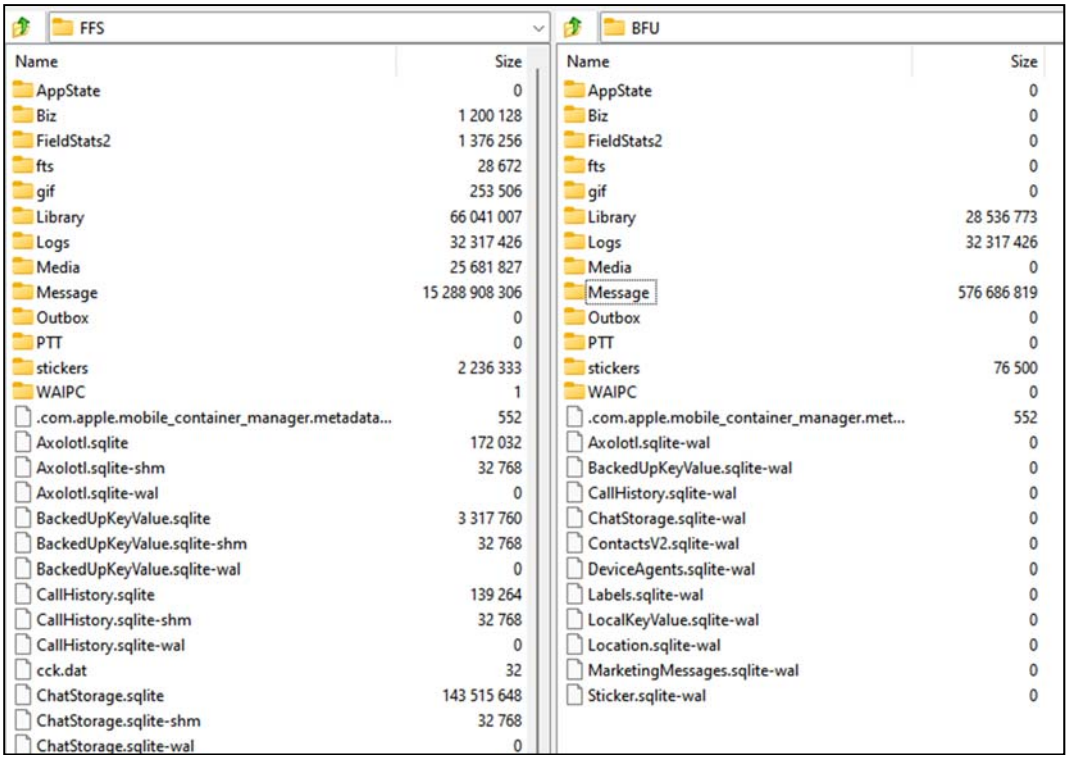


Fig. 14. File System Obtained in WhatsApp Business Folder

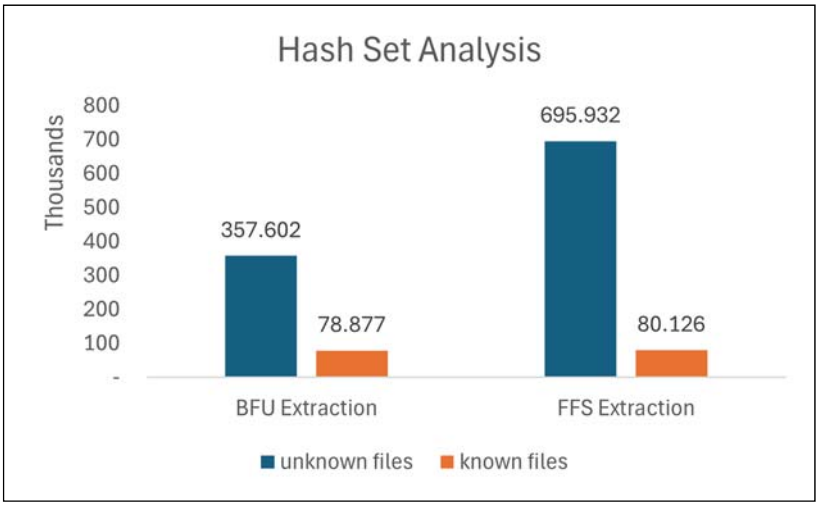


Fig. 15. Hash Set Comparison

Unmatched Files: A total of 141 hash displayed discrepancies in their hash values between the BFU and FFS extractions. These discrepancies shown in Table 1 likely represent system-generated files prone to frequent updates (logs, cache, metadata, etc.).

File Category	Hash Matched	Hash Not Matched
Archive	55472	1
Audio	1758	0
Database	368	25
Document	7606	3
File	63625	45
Image	29833	0
JSON	3718	0
Plist	175394	67
VCF	30	0
Video	258	0
Total Hash	**338062 (99.96%)**	**141 (0.04%)**

Table 1. BFU Hash Comparison Result

Table 2 showcases the types of data recoverable from both extractions. While the variety of recoverable data may be comparable to the FFS extraction, not all files and folders were recovered due to encryption and restricted access to system data.

Further analysis from the device identification, both BFU and FFS extraction successfully obtain the information like OS version, phone name, serial number, IMEI, MSISDN, until the Apple ID that registered in the device. Even the allocated storage information is obtained with some detail category like application size, book, logs, user data, music, photo and camera roll. The different in is only advertising ID that obtained in FFS extraction.

File Category	BFU	FFS
Application	0	9
Archive	55473	55968
Audio	1758	2470
Database	393	3572
Document	7609	11526
File	63670	125665
Image	29833	142728
JSON	3718	8633
Plist	175461	178677
VCF	30	30
Video	258	3231
Total Files	**338203**	**532509**

Table 2. File Category Obtained

In the BFU extraction, the keychain information was not obtained this might be due to different protection levels such as "Complete Protection (kSecAttrAccessibleWhenUnlocked)" and "Protected Until First User Authentication (kSecAttrAccessibleAfterFirstUnlock)". These protection classes determine when the keychain items are accessible, either when the device is unlocked or after the first user authentication [21][22].

Keychain protection classes determine when the class is accessible. Below are current data protection classes from the Apple Security Guide [3]:

- Complete Protection (kSecAttrAccessibleWhenUnlocked): The default value for keychain items added without explicitly setting an accessibility constant. Developers use this protection level when the application needs access to the keychain data only when the application is in the foreground. When used, the keychain item data can be accessible only when the device is unlocked. Keychain data items with this attribute migrate to a new device when using encrypted backup.
- Protected Until First User Authentication (kSecAttrAccessibleAfterFirstUnlock): similar to Complete Protection but keychain items are available to the users after they first unlock the device. The keychain items are stored in an encrypted format on a disk and cannot be accessed until after the device has booted and until the first device unlocks.
- Protected when passcode enabled (kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly): Developers use this protection level when the application needs access to the keychain data only when the application is in the foreground and needs additional security. When used, the keychain item data can be accessible only when the device is unlocked and a passcode is enabled on the device. Data cannot be stored on the device keychain when the pin code is not set on the device. The keychain data items with this attribute never migrate to a new device. If the pin code is disabled, the keychain item data gets deleted.
- No Protection (kSecAttrAccessibleAlways): When this protection level is used, the data in the keychain item is always accessible even when the device is locked.

5. Discussion

The research on extracting data from locked iOS devices in Before First Unlock (BFU) states has provided valuable insights into the challenges and opportunities associated with digital forensics in iOS environments. The comparison between the Before First Unlock (BFU) and Full Filesystem (FFS) extraction methods has shed light on the effectiveness of data recovery and integrity assessment. The analysis results indicate that while the BFU extraction may have limitations in extracting the encrypted applications, it still holds potential for further investigation. On the other hand, the Full Filesystem extraction revealed a rich array of installed applications, suggesting a wealth of forensic evidence for analysis.

The file hash comparison analysis conducted to ensure data integrity between the BFU and FFS extractions is a crucial step in validating the extracted data. By employing the SHA-1 hashing algorithm, the research has

demonstrated a systematic approach to verifying the integrity of extracted files, which is essential for maintaining the admissibility of evidence in legal proceedings.

Some other techniques that done for locked devices is physical data extraction methods, such as chip-off analysis, where the memory chip is physically removed from the device to extract and reconstruct human-readable data [23]. But even the low-level data extraction techniques like Chip-Off have become more challenging in recent years due to manufacturers' focus on enhancing user security [23][24].

Another way to extract data from iOS devices is from the iCloud backup. Some tools like the iPhone Backup Extractor as another tool designed for iOS devices, enabling the extraction of files from iPhone backups and iCloud for various data types, including contacts, messages, multimedia, calendars, notes, and more [25][26]. But this method requires investigators to confiscate the iCloud account and restore the data to the spare iOS device to decrypt the data.

For another reference, in Android operating system, bypassing pattern locks could be done with rooting Android devices, extracting the gesture.key file, and using rainbow tables to crack pattern locks. This could be importance of forensic analysis in accessing data on locked Android devices and provides a methodology for forensic investigators to analyze and bypass pattern locks effectively [27]. This reference could be used to learn and try to bruteforce the passcode in iOS.

6. Conclusion and Future Work

This research presented a comparative analysis of data extraction methods: Before First Unlock (BFU) and Full Filesystem (FFS). The analysis aimed to evaluate the effectiveness of BFU extraction for recovering user data from locked iOS devices. Manual file exploration and file hash comparison analysis was conducted to ensure the data organization and integrity of the extracted data.

The results revealed that BFU extraction offers a valuable approach for forensic investigations, even with limitations in extracting encrypted application data through forensic tools. File hash comparison demonstrated a high degree of consistency between BFU and FFS extractions for most recovered files. However, discrepancies in BFU extraction were observed in system-generated files and folders due to encryption and restricted access to certain data areas.

The analysis in this research revealed several key points:

- BFU extraction offers a valuable approach for extracting user data from locked iOS devices, even with limitations in extracting encrypted application data using forensic tools like Cellebrite UFED Premium.
- File hash comparison analysis demonstrates the integrity of the extracted data for most files. However, discrepancies in system-generated files highlight the dynamic nature of such data.
- While the types of recoverable data might be similar between BFU and FFS extractions, limitations exist in BFU extraction due to encryption and restricted access. Missing data can be shown in discrepancies between folder sizes and number of files that are contained in the folder.
- Encrypted file names and missing databases (like WhatsApp's ChatStorage.sqlite) pose additional challenges in BFU extraction. However, techniques like OCR can be applied to extract information from documents without opening each of them.

Overall, BFU extraction results are still valuable information for forensic investigations, offering the potential to uncover crucial evidence even when full filesystem access is unavailable.

Acknowledgements

This research is fully funded by Ministry of Communication and Information Technology, Indonesia – Domestic Master Scholarship Program.

Conflict of Interests

The authors do not have conflicts of interest to declare. We certify that the submission is original work and is not under review at any other publication.

References

[1] Cellebrite. (2024). Industry Trends Survey 2024. Cellebrite. Retrieved from: https://cellebrite.com/en/industry-trends-survey-2024/

[2] Krishnan, S., Zhou, B., & An, M. K. (2019). Smartphone forensic challenges.

[3] Apple Inc. (2021). Apple Platform Security Guide. Retrieved from https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

[4] Campbell, W. (2023, August 23). BFU and AFU Lock States. DigiForce Lab.

[5] Herrera, L. A. (2020, June). Challenges of acquiring mobile devices while minimizing the loss of usable forensics data. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

[6] Alomari, Mariam & Alogaiel, Razan & Alghulayqah, Hana & Alsadah, Sharifa & Al-Dowihi, Lulwah & Alahmadi, Resal & Alattas, Hussain. (2023). Mobile investigation; Forensics analysis of iOS devices. 10.13140/RG.2.2.16584.60169.

[7] Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, 38, 301169.

[8] Katalov, V. (2021). Extracting and Decrypting iOS Keychain: Physical, Logical and Cloud Options Explored. DFIR Review.

[9] Alendal, G., Axelsson, S., & Dyrkolbotn, G. O. (2021). Chip chop—smashing the mobile phone secure chip for fun and digital forensics. Forensic Science International: Digital Investigation, 37, 301191.

[10] Alendal, G. (2022). Digital Forensic Acquisition of mobile phones in the Era of Mandatory Security: Offensive Techniques, Security Vulnerabilities and Exploitation.

[11] Fikri, A., Presekal, A., Harwahyu, R., & Sari, R. F. (2018, November). Performance comparison of dalvik and ART on different android-based mobile devices. In 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) (pp. 439-442). IEEE.

[12] Cellebrite Digital Intelligence Glossary. BFU iPhone - Mobile Device Forensics. Available: https://cellebrite.com/en/glossary/bfu-iphone-mobile-device-forensics/

[13] Junttila, A. (2023). Countermeasures against digital forensics of handheld devices, computers and services.

[14] Grance, T. , Chevalier, S. , Scarfone, K. and Dang, H. (2006), Guide to Integrating Forensic Techniques into Incident Response, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50875 (Accessed March 29, 2024)

[15] Ayers, R., Brothers, S., & Jansen, W. (2014). NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. U.S. Department of Commerce. National Institute of Standards and Technology.

[16] Umar, R., Riadi, I., & Muthohirin, B. F. (2019). Live forensics of tools on android devices for email forensics. TELKOMNIKA (Telecommunication Computing Electronics and Control), 17(4), 1803-1809.

[17] Wu, J., Chen, G., Xu, Y., Li, G., & Liu, Q. (2021, December). A research of digital forensic method based on the Checkm8 heap vulnerability. In 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA) (Vol. 2, pp. 164-168). IEEE.

[18] Ogden, D. (2017). Mobile Device Forensics: Beyond Call Logs and Text Messages. US Att'ys Bull., 65, 11.

[19] Current RDS hash sets. NIST. (2024, March 1). https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/current-rds

[20] Cellebrite. What Can Be Recovered From BFU Data Collection. Available: https://cellebrite.com/en/what-can-be-recovered-from-bfu-data-collection/

[21] Shetty, D. (2017). Hacking iOS Applications: a detailed testing guide [PDF]. Retrieved from https://web.securityinnovation.com/hubfs/iOS%20Hacking%20Guide.pdf

[22] V. Katalov, "BFU Extraction: Forensic Analysis of Locked and Disabled iPhones," ElcomSoft blog, 26-Dec-2019. [Online]. Available: https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/.

[23] Karjagi, A. J., & Quadri, S. (2023). Design Of A Framework For Data Extraction And Analysis From Android-Embedded Smartphones. Russian Law Journal, 11(3).

[24] MacLeod, M. (Year). Discussing How Manufacturers' Focus on Device Security Can Hinder Mobile Forensic Investigations. Retrieved from https://supermairio.github.io/assets/pdfs/Mobile_Forensics_Essay.pdf

[25] Dodevska, Marina & Dımıtrova, Vesna & Dobreva, Jovana & Mollakuqe, Elissa. (2023). Android vs iOS phone forensics: tools and techniques.

[26] Zinkus, M., Jois, T. M., & Green, M. (2021). Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions. arXiv preprint arXiv:2105.12613.

[27] Rao, V. V., & Chakravarthy, A. S. N. (2016, December). Analysis and bypassing of pattern lock in android smartphone. In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-3). IEEE.

Authors Profile

Adly Gilang Kurnia, postgraduate student at Universitas Indonesia who is pursuing master's degree from Department of Electrical Engineering at Universitas Indonesia. His currently research is in Computer Science, focused on Cyber Forensics including computer, mobile and network forensics.

Ruki Harwahyu, received the B.E. degree in computer engineering from Universitas Indonesia (UI), Jakarta, Indonesia, in 2011, the M.E. degree in computer and electronic engineering from UI and the National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan, in 2013, and the Ph.D. degree in electronic and computer engineering from NTUST in 2018. He is currently an Assistant Professor with the Department of Electrical Engineering, Faculty of Engineering, UI. He serves as an IT Adviser with the Faculty of Engineering, UI; a Lead System Developer with UI Greenmetric World University Ranking; and a member of the Learning Technology Enhancement Team, Faculty of Engineering, UI. His current research interests include computer and communication networks and Internet of Things.