UNIVERSITY OF ÉVORA

Mobile Digital Forensics: Report

Javier Lamar Leon , Paulo Quaresma, Vitor Nogueira

jlamarleon@uevora.pt, pq@uevora.pt, vbn@uevora.pt

July 2024

Introduction

In today's digital age, mobile devices have become an integral part of our daily lives. With millions of people worldwide owning a smartphone, these devices have become a primary means of communication, information storage, and data exchange. The widespread use of mobile devices has also led to an exponential increase in the number of cybercrimes and digital forensic investigations. As a result, the need for effective tools and techniques to extract, analyze, and present evidence from these devices has become a critical component of digital forensics.

Mobile device forensic tools play a vital role in extracting valuable information from mobile devices, including text messages, emails, social media chats, location data, photographs, videos, and other digital artifacts. These tools are used by law enforcement agencies, digital forensic investigators, and corporate security professionals to investigate various types of crimes, including fraud, theft, child exploitation, and terrorism.

The rapid evolution of mobile technology has made it increasingly challenging for investigators to keep pace with the ever-changing landscape of mobile devices and their associated data. With the increasing complexity of smartphones, tablets, and other mobile devices, traditional forensic techniques are no longer sufficient to effectively extract and analyze evidence from these devices. This is where specialized mobile device forensic tools come into play. The next list shows the main forensic digital tools.

1. Magnet Forensics (Closed-source) - `https://www.magnetforensics.com/`
2. Cellebrite UFED Physical Analyzer (Closed-source) - `https://cellebrite.com/`
3. Nuix (Closed-source) - `https://www.nuix.com/`
4. OpenText (Closed-source) - `https://www.opentext.com/`
5. Paraben (Closed-source) - `https://paraben.com/`

6. Binalyze (Mixed) - `https://www.binalyze.com/`
7. Compelson (Closed-source) - `https://www.mobiledit.com/`
8. Detego Global (Mixed) - `http://www.detegoglobal.com/`
9. Exterro (Closed-source) - `https://www.exterro.com/`
10. GMDSOFT (Mixed) - `https://www.gmdsoft.com/`
11. MSAB (Closed-source) - `https://www.msab.com/`
12. Oxygen Forensics (Closed-source) - `https://www.oxygen-forensic.com/`
13. ADF (Closed-source) - `https://www.adfsolutions.com/`
14. Kali NetHunter (Open-source) - `https://www.kali.org/docs/nethunter/`

From the previous list, we notice that only one tool is open source. However, the Kali application is a suite that brings together different tools for the task of digital forensics. In this report, a section is dedicated to this application.

On the other hand, closed-source mobile forensic tools are generally more developed in terms of functionalities. They offer extensive device support, advanced data acquisition methods, comprehensive data analysis, and sophisticated reporting capabilities. Additionally, they often have strong security features to ensure data integrity and maintain a proper chain of custody, which is crucial for legal proceedings.

Open-source tools, while valuable for certain use cases and budgets, typically lag in device support, advanced features, and user-friendly interfaces. They may be sufficient for less complex investigations or for educational purposes, but they lack the comprehensive capabilities and professional support found in their closed-source counterparts.

For most professional forensic investigations, especially those requiring extensive device support and advanced features, closed-source tools are the preferred choice. However, open-source tools play an important role in making forensic capabilities accessible and providing cost-effective solutions for less demanding tasks.

Digital forensics tools provide a range of functionalities to assist investigators in collecting, analyzing, and preserving evidence from smartphones and tablets. Some of the main functionalities of these tools include:

- **Mobile Device Acquisition**

  Extracts data from mobile devices, even in cases where the device is experiencing issues such as a "boot loop". This includes retrieving information from internal storage, SD cards, SIM cards

- **Deleted File Recovery**

  Recovers data from devices that are locked, physically damaged, or have corrupted files. This is crucial for accessing information that is not readily available due to protection mechanisms or physical damage.

- **Decryption**

  Decrypts data that is protected by encryption technologies, enabling access to information on devices where data encryption is implemented either by default or by user settings.

- **Smartphone Biometrics**

  Provides the ability to access mobile devices equipped with advanced biometric features that utilize unique characteristics for user authentication. These include fingerprint scanning, facial recognition, iris scanning, and even voice recognition.

- **iPhone Devices Access**

  Access to iPhone devices and iOS versions with improved security measures

- **Operating System Compatibility**

  Supports a wide range of operating systems and models, including different versions of Android and iOS. This ensures that the tool can handle the diverse array of mobile devices encountered in forensic investigations.

- **Software and Security Updates**

  Provides the ability to upgrade and handle the latest updates and security patches on mobile devices, ensuring the tool remains effective as devices are updated.

- **Forensic Process Optimization**

  Reduces the time required to analyze a device, which typically takes 5 to 7 days, thereby significantly improving the efficiency of forensic investigations.

- **Data Analysis**

  Analyzes the extracted data objects and elements from the JTAG (Joint Test Action

Group) and Chip-Off images of mobile devices. This can involve comparing, contrasting, and investigating data in conjunction with other data sources.

- **Compliance with Regulations and Privacy Laws**

  Ensures that the tools and processes comply with relevant regulations and privacy laws, which is crucial for maintaining the integrity and legality of forensic investigations.

- **Integration with Machine Learning and AI**

  Incorporates machine learning and AI capabilities to enhance data analysis, automate repetitive tasks, and improve the overall efficiency and accuracy of forensic investigations.

- **Intuitive and User-Friendly Interface**

  Features an intuitive and user-friendly interface, making the tools accessible and easier to use for a wide range of entities and professionals, regardless of their technical expertise.

- **Chain of Custody Management**

  Maintains a documented history of evidence handling, ensuring the integrity of the evidence from collection to court presentation.

- **Reporting and Documentation**

  Generates comprehensive reports and documentation of the forensic process and findings, which can be used in legal proceedings.

- **Metadata Extraction**

  Extracts metadata from files and applications, providing additional context and information about the data, such as timestamps, geolocation, and author details.

- **Cloud Data Acquisition**

  Acquires data stored in cloud services associated with the mobile device, such as backups, emails, and social media accounts.

- **Password Bypass and Brute Force Tools**

  Includes tools to bypass or crack passwords and security locks on mobile devices, enabling access to otherwise inaccessible data.

- **Device to field forensics work**

  Offers field mobile forensics as a front-line solution for police, sheriffs, school resource officers, field agents, and investigators.

- **SQLite Data Recovery**

  Ability to report recovered SQLite database information.

Among the leading closed-source digital forensics tools, **Cellebrite**, **Magnet**, and **OpenText Forensic** software stand out as top contenders[1]. These tools have gained significant recognition due to their extensive use by law enforcement agencies and widespread acceptance as evidence in court proceedings. Their robust features, reliability, and ability to produce comprehensive forensic reports have solidified their position as preferred choices for digital forensic investigations.

Next, we present a comparison [2] of the primary forensic tools according to some functionalities:

Functionality	**Cellebrite**	**Magnet**	**OpenText**	**Kali Linux**
Decoding and Analysis	✓	✓	✓	✓
Cloud Data Extraction	✓	✓	✗	✗
Deleted File Recovery	✓	✓	✓	✓
Mobile Device Acquisition	✓	✓	✓	✓
SQLite Data Recovery	✓	✓	✗	✗
String Search	✓	✓	✓	✓
iPhone Devices Access	✓	✓	✓	✗
Smartphone Biometrics	✓	✓	✓	✗
Chain of Custody Management	✓	✓	✓	✗
Integration with Machine Learning and AI	✓	✓	✓	✗
Device to field forensics work	✓	✗	✗	✗

On the other hand, certifications play a vital role in bolstering a digital forensics career, serving as tangible proof of a professional's skills and adherence to industry best practices. They demonstrate an individual's ability to handle complex cases confidently and signal a commitment to staying current with technological advancements and investigative methods. Certifications from organizations (like OffSec Certified Professional [3] or Cellebrite[4]) reduce the likelihood of costly errors, ensuring digital evidence remains intact and admissible in court. Staying updated with certifications showcases a dedication to the profession and an ongoing pursuit of excellence.

[1] https://www.elabforensics.com/advanced-digital-forensics-criminal-defense/
[2] https://www.dhs.gov/science-and-technology/nist-cftt-reports
[3] https://www.offsec.com/courses/pen-200/
[4] https://cellebrite.com/en/training/

In this report, we will review two mobile device forensic tools: Kali Linux and Cellebrite. Kali Liux was chosen for its open-source nature, offering accessibility and community support. Cellebrite, on the other hand, was selected for its comprehensive range of capabilities as a leading commercial tool.

Kali Linux

Kali Linux[5] (see logo Fig. 1), a Debian-based Linux distribution, is developed and maintained by Offensive Security for digital forensics and penetration testing. Initially a rewrite of BackTrack, Kali Linux was created by Mati Aharoni and Devon Kearns. The platform comes with over 600 pre-installed penetration testing programs, making it a comprehensive tool for various information security tasks.

The following are the main features of Kali Linux:

1. **ARMEL and ARMHF Support**

   As ARM-based single-board systems like the Raspberry Pi and BeagleBone Black become more prevalent and affordable, we recognize the need for robust ARM support in Kali. Kali Linux provides fully functional installations for both ARMEL and ARMHF systems. It supports a wide range of ARM devices and integrates ARM repositories with the mainline version, allowing ARM tools to be updated alongside the rest of the distribution.

2. **Multi-Language Support**

   While penetration tools are primarily written in English, we have ensured that Kali offers true multilingual support. This allows more users to work in their local language and easily find the necessary tools.

3. **Full Customization of Kali ISOs**

   Creating a customized version of Kali for specific needs is straightforward using metapackages tailored to security professionals' requirements and a highly accessible ISO customization process. Kali Linux is heavily integrated with live-build, providing great flexibility in customizing and modifying Kali Linux ISO images.

4. **Live USB Boot**

[5] https://www.kali.org/

Figure 1: kali Linux logo

This feature allows us to install Kali on a USB device and boot it without modifying the host operating system, making it ideal for forensic work. With optional persistence volumes, we can choose which file system Kali will use at startup, enabling files to be saved across sessions and multiple profiles to be created. Each persistent volume can be encrypted, a crucial functionality for our industry. Additionally, the LUKS nuke option allows for quick data destruction.

5. **Kali NetHunter**

   Kali NetHunter allows us to run Kali on our Android phones. This includes a ROM overlay for many devices, along with the NetHunter App and NetHunter App Store. Additionally, we can boot into a full desktop environment using chroot and containers, and leverage the "Kali NetHunter Desktop Experience (KeX)".

6. **Over 600 Penetration Testing Tools Pre-installed**

   Kali Linux includes more than 600 useful tools, such as Crunch, Aircrack-ng, Wireshark, and Nmap. After evaluating each tool from BackTrack, Kali removed many that were either non-functional or duplicated the functionality of others.

7. **Developed in a Secure Environment**

   The Kali Linux team consists of a small group of developers who are the only ones authorized to commit packages and communicate with repositories, all through secure protocols.

8. **Free (as in beer) and Always Will Be**

   Like BackTrack, Kali Linux is and always will be absolutely free. There will never be a charge for using Kali Linux.

9. **Wide-Ranging Wireless Device Support**

   Support for wireless interfaces has traditionally been a challenge for Linux distributions. Kali Linux is designed to work with as many wireless devices as possible, allowing it to run on a wide range of hardware and connect with various USB and other wireless devices.

10. **Custom Kernel, Patched for Injection**

    The development team often needs to perform wireless assessments as penetration testers, so the kernel includes the latest injection patches.

11. **GPG Signed Packages and Repositories**

    In Kali Linux, each package is signed by the developer who built and committed it, and the repositories subsequently sign the packages as well.

12. **A Trustworthy Operating System**

    Users of a security distribution need to trust that it has been developed with transparency and best security practices. Kali Linux is developed by a small team of skilled developers who upload signed source packages built on a dedicated build daemon. These packages are then checked for integrity and distributed as part of a signed repository. The work done on the packages can be thoroughly reviewed using the Kali source package packaging Git repositories, which include signed tags. The Kali package tracker can also be used to track the evolution of each package.

13. **Forensics Mode**

    When performing forensic work on a system, it is crucial to avoid altering the data on the analyzed system in any way. However, modern desktop environments tend to obstruct this goal by attempting to auto-mount any detected disks. Kali Linux offers a forensics mode, which can be enabled from the boot menu to disable all such functions. The live system is especially useful for forensic purposes, as any computer can be rebooted into a Kali Linux system without accessing or altering its hard disks.

14. **Kali Linux Full Disk Encryption**

    Kali Linux LUKS Full Disk Encryption (FDE) allows us to encrypt the entire hard drive

of our critical penetration testing computer, a vital feature in the industry.

15. **Kali Linux Metapackages**

    Mastering Kali Linux toolsets with Kali Metapackages is simplified through various metapackage collections that combine different toolsets. This makes it easy to set up custom, minimal environments. For example, `apt-get install kali-linux-wireless` can be used if only wireless utilities are needed for an evaluation.

16. **Kali Linux Accessibility Features**

    Kali is one of the few Linux distributions that include both voice feedback and braille hardware support for blind or visually impaired users, ensuring accessibility for all.

Advantages of Kali Linux

- It offers high-level security and stability.
- It is a good distribution for experts only.
- Kali Linux is capable of performing a wide range of tasks.
- The Kali Linux distribution includes over 600 penetration tools, all designed to help network security teams evaluate the security of their networks.
- It is a completely free and open-source operating system, allowing us to use it freely and contribute to its development.
- Kali Linux supports numerous languages.

Disadvantages of Kali Linux

- Kali Linux takes up a lot of space.
- Kali Linux is not suitable for beginners.
- Some software may malfunction.
- It can be a bit slower.

Kali NetHunter: Mobile device forensic tool

As we continue through this section, we will shift our attention towards mobile devices (Kali NetHunter). The core components of Kali NetHunter, included in all three editions, consist of:

Figure 2: Kali Linux desktop sessions with support for screen mirroring via HDMI.

1. **Kali Linux Container:** This container encompasses all the tools and applications provided by Kali Linux.
2. **Kali NetHunter App Store:** A dedicated app store featuring dozens of purpose-built security applications.
3. **Android Client:** This client facilitates access to the Kali NetHunter App Store.
4. **Kali NetHunter Desktop Experience (KeX):** This feature allows users to run full Kali Linux desktop sessions, with support for screen mirroring via HDMI or wireless screen casting (see Fig 3).

Kali Linux NetHunter is a free and open-source platform designed to provide mobile penetration testing capabilities for **Android devices**, based on the Kali Linux distribution. NetHunter is compatible with a wide range of Android devices, including popular models from OnePlus, Samsung, and Google Nexus. The platform is maintained by a community of volunteers, with project funding provided by Offensive Security. NetHunter is available for both rooted and unrooted devices, with different versions tailored to each. For unrooted devices, the "NetHunter Rootless" edition is available, while rooted devices with custom recovery can use "NetHunter Lite."

In today's society, any organization, or even an individual, is vulnerable to external attacks and security breaches. Cyber attackers frequently carry out these acts. Once an attack has

been executed, computer forensics is used to determine the root cause of the attack and the appropriate course of action to respond to it.

This is where the Kali Linux distribution comes in, offering tools for penetration testing as well as tools for forensics. Some of the important tools include:

- **Bulk Extractor Tool**

  Bulk extractor is a C++ program that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The results are stored in feature files that can be easily inspected, parsed, or processed with automated tools. bulk extractor also creates histograms of features that it finds, as features that are more common tend to be more important.

- **Scalpel Tool**

  Scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is filesystem-independent and will carve files from FAT16, FAT32, exFAT, NTFS, Ext2, Ext3, Ext4, JFS, XFS, ReiserFS, raw partitions, etc. scalpel is a complete rewrite of the Foremost 0.69 file carver and is useful for both digital forensics investigations and file recovery.

- **Binwalk Tool**

  Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. Binwalk uses the libmagic library, so it is compatible with magic signatures created for the Unix file utility. Binwalk also includes a custom magic signature file which contains improved signatures for files that are commonly found in firmware images such as compressed/archived files, firmware headers, Linux kernels, bootloaders, filesystems, etc. This package is an empty package, because the binary tool is already provided with the library, dependency of this package.

- **Guymager Tool**

  The forensic imager contained in this package, guymager, was designed to support different image file formats, to be most user-friendly and to run really fast. It has a high speed multi-threaded engine using parallel compression for best performance on multi-processor and hyper-threading machines.

- **Pdfid Tool**

  This tool is not a PDF parser, but it will scan a file to look for certain PDF keywords, allowing you to identify PDF documents that contain (for example) JavaScript or execute an action when opened. PDFiD will also handle name obfuscation.

- **Magic Rescue Tool**

  Magic Rescue scans a block device for file types it knows how to recover and calls an external program to extract them. It looks at "magic bytes" (file patterns) in file contents, so it can be used both as an undelete utility and for recovering a corrupted drive or partition. As long as the file data is there, it will find it. Magic Rescue uses files called 'recipes'. These files have strings and commands to identify and extract data from devices or forensics images. So, you can write your own recipes. Currently, there are the following recipes: avi, canon-cr2, elf, flac, gpl, gzip, jpeg-exif, jpeg-jfif, mbox, mbox-mozilla-inbox, mbox-mozilla-sent, mp3-id3v1, mp3-id3v2, msoffice, nikon-raw, perl, png, ppm, sqlite and zip. This package provides magicrescue, dupemap and magicsort commands. magicrescue is a carver and it is useful in forensics investigations.

- **HashDeep Tool**

  HashDeep is a set of tools to compute MD5, SHA1, SHA256, tiger and whirlpool hashsums of arbitrary number of files recursively.

  The main hashdeep features are:

  It can compare those hashsums with a list of known hashes;

  The tools can display those that match the list or those that does not match;

  It can display a time estimation when processing large files.

  It can do piecewise hashing (hash input files in arbitrary sized blocks).

  This package is useful in forensics investigations.

- **Autopsy Tool**

  The Autopsy Forensic Browser is a graphical interface to the command line digital forensic analysis tools in The Sleuth Kit. Together, The Sleuth Kit and Autopsy provide many of the same features as commercial digital forensics tools for the analysis of Windows and UNIX file systems (NTFS, FAT, FFS, EXT2FS, and EXT3FS).

- **google-nexus-tools**

  Nexus Tools is an installer for the Android debug/development command-line tools ADB

(Android Device Bridge) and Fastboot for Mac OS X, Linux, and Google Chrome/Chromium OS.

- **Sleuthkit Tool**

  The Sleuth Kit, also known as TSK, is a collection of UNIX-based command line file and volume system forensic analysis tools. The filesystem tools allow you to examine filesystems of a suspect computer in a non-intrusive fashion. Because the tools do not rely on the operating system to process the filesystems, deleted and hidden content is shown. The volume system (media management) tools allow you to examine the layout of disks and other media. You can also recover deleted files, get information stored in slack spaces, examine filesystems journal, see partitions layout on disks or images etc. But is very important clarify that the TSK acts over the current filesystem only.The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with filesystem analysis tools.Currently, TSK supports several filesystems, as NTFS, FAT, exFAT, HFS+, Ext3, Ext4, UFS and YAFFS2.This package contains the set of command line tools in The Sleuth Kit.

- **Scrounge-NTFS Tool**

  Scrounge NTFS is a data recovery program for NTFS filesystems. It reads each block of the hard disk and try to rebuild the original filesystem tree into a directory. This package is useful in forensics investigations.

An important tool in kali is *Autopsy* [6]. Autopsy is an open-source digital forensic tool, prominently featured in the Kali Linux toolkit, designed for the investigation of cyber-crimes. This robust tool aids in uncovering vital information that can be pivotal in forensic examinations. Key features of Autopsy include comprehensive case management, maintaining the integrity of disk images, powerful search capabilities, and detailed timeline analysis.

With Autopsy, investigators can thoroughly examine mobile phones to retrieve essential data such as SMS messages, contacts, media files, calendar entries, and notes. This makes it an indispensable tool for digital forensics professionals seeking to gather and analyze evidence in cyber-crime investigations.

[6] https://www.sleuthkit.org/autopsy/

The following table shows some features of Autopsy.

Parameter	**Autopsy**
Operating System platform	Windows, Linux and OSX
Supported device	Disk images, Local drive, Folder/Directory
Connection via	USB Cable
IMEI Number	No
Physical Data Acquisition	Yes
Logical Data Acquisition	Yes
Type of evidence recovered	SMS, Contacts, Files, Media, Metadata
Output format	Text, XLS, HTML

Cellebrite UFED

Cellebrite DI Ltd. is an Israeli digital intelligence company that provides a comprehensive suite of tools for federal, state, and local law enforcement, as well as enterprise companies and service providers, to collect, review, analyze, and manage digital data. Headquartered in Petah Tikva, Israel, Cellebrite operates fourteen offices worldwide, including key business centers in Washington, D.C., Munich, and Singapore. A fully owned subsidiary of Sun Corporation based in Nagoya, Japan, Cellebrite is known for its flagship product series, the Cellebrite UFED. On April 8, 2021, the company announced plans to go public via a merger with a blank-check firm, valuing Cellebrite at approximately 2.4 billion. While its products are classified as "dual-use civilian services," allowing them to operate without significant oversight from the Israeli government, Cellebrite's mobile forensics division, established in 2007, produces advanced digital forensics and intelligence tools for law enforcement, intelligence agencies, military branches, corporate security, law firms, and private forensic examiners. Additionally, in 2017, Cellebrite's Mobile Lifecycle division was rebranded as Mobilogy, which produces hardware and software for phone-to-phone data transfer, backup, mobile applications, electronic software distribution, and data analysis tools. Mobilogy's products are widely used by mobile operators and deployed in wireless retail points of sale, ensuring compatibility with handset manufacturers before public release.

The Cellebrite UFED[7] (Universal Forensic Extraction Device) is a cutting-edge tool for extracting data from a diverse array of mobile devices, including smartphones, tablets, and GPS units. It provides extensive support for multiple operating systems, such as iOS, Android, BlackBerry, and Windows Phone. Utilizing advanced extraction techniques, the UFED can retrieve a wide range of data, including call logs, messages, contacts, multimedia files, app data, and more.

[7] https://cellebrite.com/en/ufed/

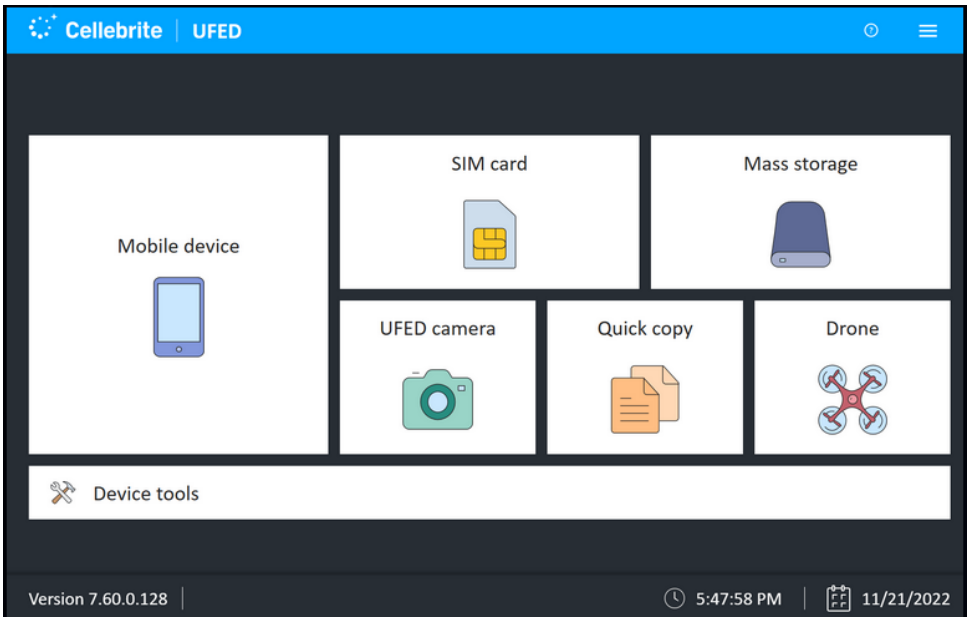

Figure 3: Range of digital devices for collecting data from Cellebrite UFED

The following are the basic features of Cellebrite UFED:

- **Physical and Logical Extractions**

  Cellebrite UFED provides two primary extraction methods: physical and logical. Physical extraction involves creating a bit-by-bit copy of the device's storage, ensuring a complete and accurate representation of the data. Logical extraction focuses on extracting selected data categories without accessing the entire device storage. Both methods offer unique advantages and are tailored to specific investigative needs.

- **Analyzing Extracted Data**

  Once data is extracted using Cellebrite UFED, it can be further analyzed using the tool's built-in analysis capabilities or exported to other forensic software for in-depth examination. UFED provides a user-friendly interface that allows investigators to intuitively explore extracted data. It enables searching, filtering, and sorting capabilities, as well as generating detailed reports for presentation in court.

- **Decrypting and Decoding**

  Cellebrite UFED supports advanced decryption and decoding techniques to access encrypted data and uncover hidden information. It can handle various encryption methods, including device-level encryption, app-specific encryption, and encrypted databases. UFED employs powerful algorithms and databases to decode passwords, recover deleted

data, and bypass security measures.

- **UFED Physical Analyzer**

  Cellebrite UFED comes bundled with a powerful software suite called UFED Physical Analyzer. This software provides enhanced data analysis capabilities, enabling investigators to visualize relationships, timelines, and communication patterns. It offers advanced features like data carving, SQLite and Plist viewers, map analysis, and integrated analytics tools for efficient examination of extracted data.

- **Integration with Other Forensic Tools**

  Cellebrite UFED integrates seamlessly with other digital forensic tools, allowing investigators to combine the strengths of different solutions for a more comprehensive analysis. It can export extracted data to widely used forensic software such as Magnet AXIOM, EnCase, and Oxygen Forensic Detective, enabling cross-tool collaboration and increasing efficiency.

- **Keeping Pace with Device Updates**

  In the rapidly evolving world of mobile devices, new models, operating systems, and security measures are continuously introduced. Cellebrite recognizes this challenge and regularly updates its UFED software to ensure compatibility with the latest devices and operating system versions. This commitment to staying up-to-date ensures that investigators can handle the latest technologies encountered in their cases.

- **Physical Analyzer Cloud**

  Collect, preserve and analyze public and private-domain, social-media data, instant messaging, file storage, web pages, and other cloud-based content.

- **Pathfinder**

  Pathfinder enables investigators, analysts, and prosecutors to collaborate effectively using a comprehensive, scalable solution to find connections and generate new insights, analyze complex data sets, and identify criminal patternsWith advanced machine learning, Pathfinder automates data ingestion, analyzes and visualizes data from various sources, identifies patterns, reveals connections, and uncovers leads with speed and accuracy. It leverages location data from GPS-enabled apps, photo geo-tags, tower dumps, or Wi-Fi

hotspots to answer critical questions and connect the dots between suspects and victims.

- **Smartphone Biometrics**

  Provides the ability to access mobile devices equipped with advanced biometric features that utilize unique characteristics for user authentication. These include fingerprint scanning, facial recognition, iris scanning, and even voice recognition.

In the realm of digital forensic tools, Cellebrite offers a variety of solutions to meet different investigative needs. The UFED 4PC (Fig. 4) is a cost-effective, flexible, and convenient software solution designed for users who need data access and collection capabilities on their existing PCs or laptops. For those requiring robust field capabilities, the UFED Touch3 Ruggedized Tablet (Fig. 5) provides comprehensive data extraction anywhere—be it in the lab, a remote location, or the field—ensuring quick and secure data retrieval with dedicated hardware that prevents the risk of cross-contaminating digital evidence. Additionally, the UFED Ruggedized Laptop (Fig. 6), equipped with UFED software, comes in a purpose-built rugged case designed to withstand drops, shocks, and extreme temperatures, guaranteeing a seamless workflow regardless of the investigation's environment.

Figure 4: UFED 4PC

Figure 5: UFED Touch3 Ruggedized Tablet.

Figure 6: UFED Ruggedized Laptop

Furthermore, Cellebrite's High-Performance Forensic Workstation, shown in Fig.7 is designed to optimize any digital investigation. It is the most comprehensive workstation available, built to manage the most demanding datasets required for digital intelligence and eDiscovery tasks. This powerful tool ensures that investigators have the capacity and performance needed to handle complex and large-scale digital forensic analyses efficiently.

Figure 7: Cellebrite's High-Performance Forensic Workstation

Smartphone Biometrics

As smartphones continue to evolve and become repositories of our personal information, ensuring their security has become paramount. Recognizing this need, mobile devices are now equipped with advanced biometric features that utilize unique characteristics for user authentication. Biometrics on a phone refer to the authentication methods that use unique physical or behavioral characteristics of an individual to grant access to the device, such as fingerprint scanning, facial recognition, iris scanning, and voice recognition. These biometric systems work by using sensors and algorithms to capture and analyze these unique features, ensuring a higher level of security

compared to traditional PINs or passwords.

Despite the enhanced security offered by smartphone biometrics, they are not entirely foolproof. Biometric data can be subject to vulnerabilities, as sophisticated methods such as high-resolution photos or 3D-printed replicas can potentially spoof biometric systems. Manufacturers continuously improve algorithms to mitigate these risks. Biometric data is typically stored in a secure enclave within the phone's hardware or in an encrypted form in the device's memory. Instead of storing the actual biometric information, the device stores a mathematical representation called a template, which cannot be reversed back into the original biometric data, providing an added layer of security.

In digital forensic investigations, biometric data plays a significant role by linking users to specific activities, such as unlocking the phone or accessing certain applications. This data helps establish timelines, identify suspects, and strengthen the investigative process. Law enforcement agencies can access biometric data on a phone by adhering to legal procedures, obtaining proper authorization, and complying with privacy laws. This often requires specialized tools and expertise to ensure investigations are conducted within legal boundaries. Privacy concerns surrounding smartphone biometrics revolve around the potential misuse or unauthorized access to biometric data, making it crucial for law enforcement and digital forensics examiners to handle this data responsibly and within legal and ethical standards.

Cellebrite offer specialized tools and expertise to aid in extracting and analyzing biometric data, ensuring that investigations are conducted within legal boundaries. Privacy concerns surrounding smartphone biometrics revolve around the potential misuse or unauthorized access to biometric data, making it crucial for law enforcement and digital forensics examiners to handle this data responsibly and within legal and ethical standards.

Unlocking iPhone Devices

Every year, Apple releases new iPhone devices and iOS versions with enhanced security measures, which significantly challenge forensic examiners trying to access these devices. New security mechanisms like iCloud advanced data protection and lockdown mode make it increasingly difficult to extract critical data. Traditional exploit methods, such as Checkm8, have become obsolete for newer devices, emphasizing the need for continuous innovation in forensic tools.

Accessing and extracting data from the latest iOS versions and iPhone devices is a demanding task that necessitates extensive research and development, advanced technical knowledge, and specialized tools. Cellebrite has consistently demonstrated its ability to deliver solutions that enable access to a broad range of iOS and Android devices. Their latest achievement, which includes accessing and extracting data from iOS 16 and iPhone 14 devices, underscores their expertise and dedication to staying ahead in the digital forensics field. This milestone is crucial for agencies and forensic experts, who can now lawfully obtain critical evidence from these devices, thus aiding in criminal investigations and ensuring justice is served.

The significance of Cellebrite's new capabilities extends beyond technological prowess; it marks a pivotal development in the digital forensics industry. With 66 percent of devices arriving at forensic labs being locked, the ability to bypass passcodes and perform full file system extractions on the entire iPhone 14 family is vital. This capability ensures the highest probability of recovering deleted records, third-party application data, iOS biome data, and the iOS keychain. Cellebrite's commitment to providing these advanced solutions not only supports law enforcement and forensic experts but also reinforces the importance of lawful and ethical use of their technology. Strict protocols are in place to ensure that their services are used for legitimate purposes, safeguarding user privacy while helping solve complex cases and protect public safety.

Digital Forensics Credibility

Cellebrite Training [8] offers a comprehensive suite of certification programs designed to enhance the skills and knowledge of digital forensics professionals. These programs cover critical areas such as mobile forensics, computer forensics, and evidence recovery across a wide array of digital devices including smart devices, vehicle GPS systems, drones, and IoT devices. By participating in these specialized training programs, professionals can gain new techniques and stay abreast of the latest developments in the field. Earning certifications from Cellebrite not only solidifies one's expertise but also opens doors for professional growth, networking opportunities, and enhanced credibility within the digital forensics community.

[8] https://cellebrite.com/en/training/

Conclusion

Digital mobile forensics involves the extraction, preservation, and analysis of data from mobile devices to uncover evidence in criminal investigations. With the increasing prevalence of smartphones that store extensive personal information, this field has become crucial for modern law enforcement and investigative processes. Advanced biometric features such as fingerprint scanning and facial recognition enhance device security but also introduce new challenges and opportunities for forensic examiners. They must navigate legal and ethical boundaries to ensure data integrity and privacy protection. Additionally, maintaining certifications and staying current with technological advancements are vital for forensic professionals to ensure their findings are credible and respected in legal contexts.

Kali NetHunter is a groundbreaking mobile penetration testing platform that brings the power of Kali Linux to Android devices, transforming them into highly portable forensic tools. This versatility allows cybersecurity professionals and digital forensic experts to conduct comprehensive investigations on-the-go. With an extensive suite of forensic applications and utilities, NetHunter provides capabilities for data acquisition, analysis, network monitoring, and vulnerability assessment. Its user-friendly interface and customization options make it accessible and adaptable to various investigative needs. Supported by the robust Kali Linux community, NetHunter benefits from continuous updates and a wealth of shared knowledge, ensuring it remains a cutting-edge tool in the fight against digital crime and cyber threats.

Cellebrite's digital forensics tools for mobile devices are indispensable in modern criminal investigations, offering capabilities to extract, preserve, and analyze data from the latest smartphones, even with advanced security features. These tools allow forensic examiners to access encrypted applications and recover critical information, including deleted records and biometric data, which are crucial for identifying suspects and constructing investigative timelines. Additionally,

Cellebrite's comprehensive training and certification programs ensure that forensic professionals stay updated with the latest techniques and technologies, thereby enhancing their credibility and effectiveness in the field and ensuring their findings are respected in legal contexts.