Computer Forensics

Week 11: Mobile Device Forensics and the internet of anything

Lecturer: Lemi Agrey Oliver

codingissweet@gmail.com

KUMI UNIVERSITY

Content

- Understanding Mobile Device Forensics
- Understanding Acquisition Procedures for Mobile Devices
- Understanding Forensics in the Internet of Anything

Understanding Mobile Device Forensics

- People store extensive personal information on cell phones and smartphones.
- Despite the fear of losing their phones, many people do not secure their phones as they do their laptops or desktops.

Types of Stored Information:

- Call logs (incoming, outgoing, missed)
- MMS and SMS messages
- Email accounts
- Instant messaging logs
- Web pages

Understanding Mobile Device Forensics +

- Photos, videos, and music files
- Calendars and address books
- Social media information
- GPS data
- Voice recordings and voicemail
- Bank account logins
- Home security access
- Smartphones often store more data than computers and have computing power similar to older desktop computers.

Understanding Mobile Device Forensics++

- In many countries, smartphones are used for banking tasks, increasing the potential evidence they can hold.

Search Warrant Requirement

- Previously, police routinely searched phones upon arrest.
- But things have changed over there. For example, the Supreme Courts of Oregon and Ohio require a search warrant for phone searches.
- The 2014 U.S. Supreme Court decision in Riley v. California mandates a search warrant before examining phone contents.
- Private information unrelated to the case must be redacted from public records.

Understanding Mobile Device Forensics+++

Challenges in Digital Forensics

- No single standard for data storage on phones.
- Phones frequently use similar but not identical storage methods.
- New phone models are released every six months, often incompatible with older models.
- Forensic tools and accessories can become obsolete quickly due to rapid technological advancements

Introduction to Mobile Phone Basics

- **Rapid Advancements:** Mobile technology has evolved significantly over the past few decades, transforming from bulky, expensive devices to the sleek, affordable phones of today.
- **Historical Context:** In 2008, mobile phones had already gone through three generations: analog, digital PCS, and 3G, each introducing new capabilities.
- **Enhancements with 3G:** 3G brought about unprecedented features such as downloading while on the move, revolutionizing the mobile experience.
- **Transition to 4G:** Sprint Nextel introduced 4G networks in 2009, setting the stage for further advancements.

Mobile Network Technologies

- **GSM** (Global System for Mobile Communications): Uses Time Division Multiple Access (TDMA), where multiple users share the same frequency channel by dividing the signal into different time slots.
- Operates on 800 to 1000 MHz and 1900 MHz bands.
- Widely adopted around the world, making it easier for international roaming.
- Utilizes SIM cards for storing user information, making it easy to switch devices
- **CDMA (Code Division Multiple Access):** Uses a spread-spectrum technology where multiple calls are transmitted simultaneously over the same frequency range, each encoded with a unique key.

Mobile Network Technologies

- Includes IS-95 (CDMAOne) and later CDMA2000 for 3G.
- Typically managed by the carrier, with phones often locked to a specific network.
- Generally offers better call quality and network capacity in crowded areas compared to GSM.

Evolution to 4G

- The move from 3G to 4G marked a significant leap in data speeds and multimedia capabilities.
- In 2009, Sprint Nextel introduced the fourth-generation (4G) network, setting a new standard for mobile connectivity.

Key Enhancements:

- **Increased Data Speeds:** 4G networks offered substantially faster data speeds compared to their predecessors, facilitating seamless multimedia streaming and faster downloads.
- **Enhanced Multimedia Capabilities:** With 4G, users could enjoy high-quality video streaming, online gaming, and other data-intensive applications with minimal lag or buffering.

Evolution to 4G+

- **Improved Network Efficiency:** 4G technologies optimized network efficiency, allowing for more simultaneous connections and better utilization of available bandwidth.

Technological Innovations:

- **OFDM (Orthogonal Frequency Division Multiplexing):** Introduced parallel carriers to transmit data more efficiently, reducing interference and improving overall network performance.
- **Mobile WiMAX:** Adopted by Sprint for its 4G network, Mobile WiMAX offered high-speed data transmission with support for speeds up to 12 Mbps, enabling a wide range of multimedia applications.
- **UMB (CDMA2000 EV-DO):** Initially considered for 4G transition, UMB provided blazing-fast downlink speeds of up to 275 Mbps, although it was eventually superseded by LTE technology.

Evolution to 4G++

- **MIMO (Multiple Input Multiple Output):** Leveraged by 4G networks to increase data throughput and improve signal reliability by using multiple antennas for transmission and reception.
- **LTE (Long Term Evolution):** Emerged as the leading 4G technology, offering peak data rates ranging from 45 Mbps to 144 Mbps, and paving the way for the modern era of high-speed mobile connectivity.

Impact on User Experience:

- The transition to 4G revolutionized the mobile experience, enabling users to enjoy seamless connectivity and access to a wide range of multimedia content on the go.
- Faster data speeds and enhanced network capabilities opened up new possibilities for communication, entertainment, and productivity, driving the widespread adoption of smartphones and mobile applications.

5G Technology

- 5G represents the fifth generation of mobile network technology, poised to revolutionize connectivity and enable a wide range of transformative applications.
- Finalized in 2020, 5G promises to deliver unparalleled speed, ultra-low latency, and massive connectivity, transforming the way we communicate, work, and live.

Key Features

- **Ultra-Fast Speeds:** 5G networks offer blazing-fast data speeds, potentially reaching up to 20 Gbps, enabling seamless streaming of high-definition video, real-time gaming, and rapid downloads.
- **Low Latency:** With latency as low as 1 millisecond, 5G minimizes delays in data transmission, facilitating real-time interactions for applications like autonomous vehicles, remote surgery, and augmented reality.

5G Technology+

- **Massive Connectivity:** 5G networks support massive connectivity, connecting billions of devices simultaneously and enabling the Internet of Things (IoT) to reach its full potential, powering smart cities, industrial automation, and more.

Technological Innovations

- **Millimeter-Wave Technology:** Utilizes high-frequency radio waves in the millimeter-wave spectrum to achieve ultra-fast speeds and high bandwidth, albeit with shorter range and susceptibility to blockages.
- **Beamforming:** Directs signals towards specific devices rather than broadcasting uniformly, increasing network efficiency and improving coverage in dense urban areas.

5G Technology++

- **Small Cell Deployment:** Relies on a dense network of small cells to enhance coverage and capacity in high-traffic areas, complementing traditional macrocells for seamless connectivity.
- **Network Slicing:** Allows for the creation of virtual network slices tailored to specific applications or users, ensuring optimal performance and resource allocation for diverse use cases.

Inside Mobile Devices

- Mobile devices encompass a wide range, including simple phones, smartphones, tablets, and smartwatches.
- Hardware components include a microprocessor, ROM, RAM, digital signal processor, radio module, microphone, speaker, hardware interfaces (keypads, cameras, GPS), and LCD display.
- Many devices offer removable memory cards and up to 64 GB of internal memory, along with Bluetooth and Wi-Fi connectivity.
- Basic phones often run on proprietary operating systems, while smartphones typically use OSs like Windows Mobile, RIM OS, Android (Linux-based), Google OS, or iOS (for Apple devices).

Mobile Network Architecture

- **Cellular Structure:** Dividing geographic areas into cells for efficient coverage and resource allocation.

Key Components:

- **Base Transceiver Station (BTS), a**cts as the interface between mobile devices and the network, defining cell boundaries.
- **Base Station Controller (BSC), c**oordinates BTSs, managing resources and connections.
- **Mobile Switching Center (MSC), r**outing calls, managing subscriber data, and facilitating seamless connectivity.

Importance of Search and Seizure Procedures

- Critical for Mobile Devices: Procedures for seizing mobile devices are as crucial as those for computers due to the significant amount of personal and sensitive information they contain.

Main Concerns

- Loss of Power: Ensuring mobile devices don't lose power before retrieving RAM data is essential, as volatile memory requires power to maintain data.
- Synchronization with Cloud Services: Preventing automatic synchronization with cloud services is crucial to avoid data being overwritten.
- Remote Wiping: Protecting the device from remote wiping actions that can erase valuable evidence is a priority.

Initial Steps at the Investigation Scene

- Determine Device Status
- If the device is off, Leave it off to prevent data alteration. Find and connect the charger as soon as possible.
- If the device is on, check the battery level to assess how urgent it is to take action to preserve the data.
- Attach Charger, connect the charger to ensure the device remains powered. Document this step if it's unclear whether the device was charged at the time of seizure.

Preventing Synchronization and Data Loss

- Disconnect from PCs or Tablets: Immediately disconnect mobile devices from any connected PCs or tablets to prevent automatic data synchronization and potential data loss.
- Collect Peripherals: Gather associated laptops, tablets, and peripherals to check for transferred and deleted data, providing a comprehensive understanding of the digital evidence.

Isolating the Device from Signals

- Why Isolate?
- To prevent data alteration or loss due to incoming signals or remote actions.

Methods of Isolation

- Airplane Mode: Disables all wireless communication, stopping synchronization and remote access.
- Faraday Bag or Paint Can: Blocks electromagnetic signals, ensuring complete isolation.
- Turning Off the Device: Prevents signal reception, but this method may increase battery drainage.

Handling Battery Drainage

- **Roaming Mode**: Isolation methods may trigger roaming mode, which can accelerate battery drainage.
- **Automatic Shutdown**: Devices may shut off or enter sleep mode when the battery is low, necessitating prompt action to prevent data loss.

SANS DFIR (Digital Forensics and Incident Response) Procedures

- The SANS Digital Forensics and Incident Response (DFIR) procedures are a set of guidelines and best practices developed by the SANS Institute to assist professionals in managing and responding to cybersecurity incidents.
- These procedures provide a structured approach to effectively handle digital forensics and incident response tasks.
- Key components of SANS DFIR procedures:

Preparation

- **Develop Policies and Procedures**: Establish clear policies and procedures for incident response.

SANS DFIR (Digital Forensics and Incident Response) Procedures+

- **Create an Incident Response Team (IRT)**: Form a team with defined roles and responsibilities.
- **Conduct Training and Awareness**: Train staff on incident response processes and awareness.
- **Maintain Tools and Resources**: Ensure all tools, software, and hardware required for incident response are available and up-to-date.

Identification

- **Detect and Report Incidents**: Monitor systems and networks to detect suspicious activities.
- **Analyze Events**: Assess and analyze logs, alerts, and indicators to identify potential incidents.
- **Confirm Incidents**: Validate whether an event is an actual security incident.

SANS DFIR (Digital Forensics and Incident Response) Procedures++

Containment

- **Short-Term Containment**: Take immediate steps to limit the damage and prevent the incident from spreading.
- **Long-Term Containment**: Implement measures that allow the organization to continue operations while dealing with the incident.

Eradication

- **Identify Root Cause**: Determine the cause of the incident and how it penetrated the defenses.
- **Remove Threats**: Eliminate the components of the threat from the environment.
- **Patch Vulnerabilities**: Apply patches and fixes to prevent the incident from recurring.

SANS DFIR (Digital Forensics and Incident Response) Procedures+++

Recovery

- **Restore Systems**: Return affected systems and services to normal operation.
- **Validate Security**: Ensure that the systems are secure and that the incident has been fully eradicated.
- **Monitor Systems**: Continuously monitor the environment for any signs of residual or new threats.

Lessons Learned

- **Conduct a Post-Incident Review**: Hold a debrief to analyze the incident and response.
- **Document Findings**: Record what happened, how it was handled, and what can be improved.

SANS DFIR (Digital Forensics and Incident Response) Procedures++++

- **Update Policies and Procedures**: Revise incident response plans and protocols based on lessons learned.
- **Improve Training**: Incorporate findings into training programs to better prepare for future incidents.

Additional SANS DFIR Resources

- **Incident Response Playbooks**: Detailed guides for specific types of incidents (e.g., malware infections, data breaches).
- **Digital Forensics Techniques**: Methods for collecting, preserving, and analyzing digital evidence.
- **Threat Intelligence Integration**: Using threat intelligence to enhance incident detection and response.
- **Legal and Compliance Considerations**: Ensuring that incident response efforts comply with legal and regulatory requirements.

Acquisition Methods in the Forensics Lab

- Assess Retrievable Data: Determine whether to perform a logical or physical acquisition based on data storage locations and investigation requirements.
- Logical Acquisition: Access files and folders as they appear in the file system, suitable for general data retrieval.
- Physical Acquisition: Conduct a bit-by-bit acquisition to recover deleted files or folders, providing a more comprehensive forensic analysis.

Key Data Locations

- Internal memory
- SIM card
- Removable/external memory cards
- Network provider's servers (requires a warrant)

Remote wiping

- What is Remote Wiping?
- Remote wiping is a feature that allows the owner of a mobile device to remotely erase data from the device.
- Primarily used to protect personal information if the device is lost or stolen.
- Remote wiping can erase contacts, calendars, photos, bank logins, and other personal data, often restoring the device to factory settings.

Data Recovery Post-Remote Wipe

- If a device has been remotely wiped, there are still some strategies to recover data:
- **Physical Acquisition**: A bit-by-bit copy of the device's storage might still recover deleted files and fragments of data.
- This requires specialized forensic tools that can access and extract data from the device's flash memory.
- **Cloud Backups**: Check if the device has backups stored in cloud services (e.g., iCloud, Google Drive). Access to these backups typically requires legal authorization (e.g., search warrant or subpoena).
- **Service Provider Records**: Obtain call logs, SMS records, and other relevant data from the service provider. This also requires legal authorization.
- **Deleted Data Recovery**: Use forensic tools capable of recovering deleted files and data remnants from the device's storage.

Forensic Tools for Handling Remote Wipe Challenges

- Several forensic tools are designed to handle the complexities of remote wiping and data recovery, including:
- **Cellebrite UFED,** Provides comprehensive extraction and decoding capabilities, even for devices that have been wiped.
- **Oxygen Forensic Detective,** Offers data recovery features for wiped devices and supports cloud extraction.
- **Magnet AXIOM,** Specializes in recovering data from devices, cloud services, and encrypted containers.

Preventive Measures in Forensic Investigations

- To mitigate the risk of remote wiping, forensic investigators can take several preventive measures:
- **Faraday Bags/Boxes**: Place the device in a Faraday bag or box immediately to block any remote wiping commands. These containers prevent the device from connecting to any network by blocking electromagnetic signals.
- **Airplane Mode**: If possible, put the device into airplane mode to disable all wireless communications, including cellular, Wi-Fi, and Bluetooth. This prevents the device from receiving remote wipe commands.
- **Isolation**: Remove the SIM card and disable Wi-Fi to ensure the device cannot receive remote commands.

Preventive Measures in Forensic Investigations+

- **Immediate Data Extraction**: Perform a quick data extraction as soon as possible to capture volatile data that could be lost if the device is wiped.
- **Regular Backups**: If the investigation permits, create regular backups of the device data to ensure that recent data is preserved.

Memory Storage in Mobile Devices

- Mobile devices utilize various types of memory storage to store data, ranging from system files to user-generated content.
- Understanding how data is stored in mobile devices is crucial for forensic investigations and data recovery processes.

Types of Memory

- Volatile Memory:
  - Requires continuous power to retain data.
  - Examples include Random Access Memory (RAM) and cache memory.

Memory Storage in Mobile Devices+

- Nonvolatile Memory
  - Retains data even when power is removed.
  - Includes internal storage, external memory cards, and SIM cards.

SIM Card Memory

Subscriber Identity Module (SIM)

- Contains subscriber information and network-related data.
- Provides authentication for network access and stores contacts and text messages.

File Structure

- **Master File (MF):** The root of the SIM card's file system.
- **Directory Files (DF):** Contain categories of data.
- **Elementary Files (EF): Contain actual**
- SIM Cards Stores service-related data, call logs, messages, and location information.

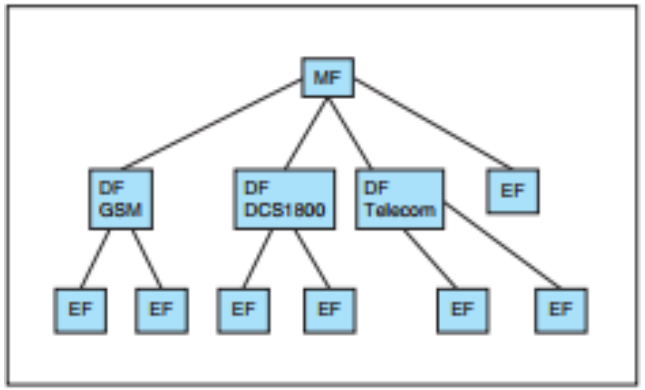

Figure 1: SIM File Structure[1]

Data Retention and Accessibility

Data Persistence

- Nonvolatile memory retains data indefinitely, even when the device is powered off.
- Volatile memory requires continuous power and loses data upon power loss.

Accessibility

- Nonvolatile memory is accessible for data retrieval and forensic analysis.
- Volatile memory may require specialized techniques for data capture before power loss.

Legal Considerations

- Warrants and Subpoenas, Legal authorization is often required to access and examine the device's data.
- Service Provider Cooperation, Collaboration with service providers can help prevent remote wiping by suspending the device's service during an investigation.

Overview of Mobile Forensics Equipment

- Mobile forensics is a constantly evolving field, mainly due to the frequent release of new phone models.
- The text provides an overview of procedures for working with mobile forensics software and discusses specific tools in detail.
- Identifying the mobile device is the first step, and online sources like phonescoop.com can assist in this process.
- Installing mobile device forensics software is crucial, but not all facilities have access to the necessary tools due to cost constraints.
- Some vendors offer tools that capture screenshots while scrolling, though this method is not ideal forensically.

Overview of Mobile Forensics Equipment+

- Connecting the phone to its power supply using the correct cables is the next step, with many newer phones having combined USB/power cables.
- Rigging cables together may be necessary for older phones, and some vendors provide toolkits with various cables.
- After connecting the device, start the forensics software and begin downloading available information.
- If the software doesn't support the model being investigated, acquiring other tools may be necessary, with a focus on ensuring the software's forensic integrity.

Mobile Forensics Equipment

Hardware Tools

- **Forensic Imaging Devices**: These devices create bit-by-bit copies (forensic images) of mobile device storage, preserving all data including deleted files and unallocated space. They often include write-blocking capabilities to prevent data alteration during imaging.
- **Universal Forensic Extraction Devices (UFEDs)**: UFEDs are multifunctional devices capable of extracting data from a wide range of mobile devices. They can perform logical, physical, and file system extractions, bypassing security measures like PINs and passwords.
- **Chip-Off Tools**: In cases where traditional methods fail, chip-off tools allow forensic experts to directly access memory chips on mobile devices, extracting data at the hardware level. This method is typically used as a last resort due to its complexity and potential damage to the device.

Mobile Forensics Equipment+

- **JTAG and ISP Programmers**: These tools enable forensic examiners to bypass security protections and directly access the device's memory via the Joint Test Action Group (JTAG) or In-System Programming (ISP) interfaces.
- **Write Blockers**: Write blockers prevent any write operations to the mobile device during forensic analysis, ensuring the integrity of the data. They are essential for preventing inadvertent changes to evidence.

Mobile Forensics Equipment++

Software Tools

- **Forensic Analysis Software**: These tools assist in examining and analyzing extracted data from mobile devices. They often provide features for parsing data, recovering deleted files, and generating forensic reports.
- **Mobile Device Management (MDM) Solutions**: MDM solutions allow organizations to remotely manage and monitor mobile devices, including data encryption, remote wiping, and tracking capabilities.
- **Mobile Forensic Software Suites**: Comprehensive software suites like Magnet AXIOM, Oxygen Forensic Detective, and Cellebrite Physical Analyzer provide a wide range of forensic capabilities, including data extraction, analysis, and reporting.

Mobile Forensics Equipment+++

- **Decryption and Password Cracking Tools**: Encryption is a common security feature on mobile devices. Forensic tools may include features to decrypt encrypted data or crack passwords to access protected information.
- **Data Recovery Software**: These tools specialize in recovering deleted or corrupted data from mobile device storage, including messages, images, videos, and application data.

Mobile Forensics Equipment++++

Mobile Device Accessories

- **Faraday Bags:** These shielded bags block incoming and outgoing signals to prevent remote wiping or tampering of mobile devices during transport or storage.
- **Cables and Adapters:** Specialized cables and adapters are often required to connect mobile devices to forensic equipment for data extraction and analysis.
- **Replacement Parts:** In cases where physical examination is necessary, replacement parts such as screens, batteries, and connectors may be needed to repair damaged devices for forensic analysis.

Mobile Forensics Equipment+++++

Important Considerations

- **Compatibility**: Ensure that the equipment supports a wide range of mobile device makes, models, and operating systems to accommodate various forensic scenarios.
- **Reliability and Accuracy**: Choose equipment from reputable manufacturers known for producing reliable and accurate forensic tools.
- **Training and Expertise**: Proper training and expertise are essential for using mobile forensics equipment effectively and interpreting the results accurately.
- **Legal and Ethical Compliance**: Adhere to legal and ethical standards when handling digital evidence, respecting privacy rights and following chain of custody procedures.

SIM Cards

- Subscriber identity module (SIM) cards are commonly found in GSM devices and contain a microprocessor and internal memory. They differ from standard memory cards in connector alignment.
- iPhones and many Android phones support micro SIM and nano SIM slots, but access to these slots may require unlocking the phone.
- In GSM terminology, mobile phones are referred to as "mobile stations," divided into the SIM card and the mobile equipment (ME).
- The SIM card is essential for the ME to function and serves various purposes:
- Identifying the subscriber to the network.
- Storing service-related information.

SIM Cards+

- Providing a backup option for the device.
- SIM cards are available in three sizes: standard, micro, and nano. They facilitate easy transfer of information between compatible phones, allowing users to switch providers or devices without notifying the service provider.
- For example, frequent travelers may use multiple SIM cards, switching between them as needed when traveling between countries.
- Many phones now incorporate SD cards for external storage, typically ranging from 16 GB to 64 GB in size. However, some devices, like Google Nexus models, may not support SD cards

SIM Card Readers

- Accessing the SIM card in GSM phones and newer mobile devices involves using a combination hardware/software device known as a "SIM card reader."
- The use of a SIM card reader requires a forensics lab equipped with antistatic devices, and consultation with the lead investigator regarding potential biological agents on the device.
- The general procedure for using a SIM card reader includes removing the device's back panel and battery, then inserting the SIM card into the card reader, which is connected to a forensic workstation's USB port.
- Various SIM card readers are available, and it's important to note their forensic soundness in the investigation log.

SIM Card Readers+

- An issue with SIM card readers is handling unread text and SMS messages, as viewing a message marks it as opened. Thus, documenting unread messages is crucial.
- Using a tool that captures screenshots of each screen can aid in documenting messages and providing additional evidence.

Mobile Phone Forensics Tools and Methods

- Retrieving information from mobile devices often involves acquiring a forensic image, allowing for the recovery of deleted data like text messages.
- For Android devices, logical acquisition and low-level analysis can be performed using tools like AccessData FTK Imager.
- Similar procedures exist for iPhone acquisition, with tools such as MacLockPick 3.0 designed for iPhones, iPads, and iOS devices.
- The NIST guidelines outline six mobile forensics methods, including manual extraction, logical extraction, physical extraction, hex dumping, JTAG extraction, chip-off, and micro read.
- Various vendors offer mobile forensics software, including Paraben Software's E3 and DataPilot, as well as Susteen Inc.'s Secure View 3.

Mobile Phone Forensics Tools and Methods +

- BitPim is a tool for viewing data on CDMA phones and can be used in read-only mode for forensic purposes.
- Cellebrite UFED Forensic System and Micro Systemation XRY are widely used tools for retrieving data from smartphones, tablets, and other devices.
- MOBILedit Forensic is a user-friendly forensics software tool with a built-in write-blocker and SIM card reader capabilities.
- It's essential to note the forensic soundness of software tools, as some tools designed for editing files may not be suitable for forensic purposes.
- Documenting each step of the investigation and being aware of the limitations and idiosyncrasies of the tools used is crucial for conducting a thorough and accurate forensic analysis.

Using the Magnet AXIOM demo software for mobile forensics

- Using the Magnet AXIOM demo software for mobile forensics involves several steps:
- **Download and Install**: Visit the Magnet Forensics website and download the demo version of Magnet AXIOM. Follow the installation instructions provided.
- **Launch the Software**: Once installed, launch Magnet AXIOM on your computer.
- **Select Mobile Forensics**: In the software interface, choose the option for mobile forensics. This typically involves selecting the type of device you want to analyze, such as iOS or Android.
- **Connect the Device**: Connect the mobile device you want to analyze to your computer using a USB cable. Ensure the device is unlocked and configured to allow data access.

Using the Magnet AXIOM demo software for mobile forensics+

- **Begin Acquisition,** Once the device is connected, Magnet AXIOM will begin the acquisition process automatically. This process involves extracting data from the mobile device, including both active and deleted data.
- **Analysis,** After the acquisition is complete, Magnet AXIOM will analyze the data and present the findings in a user-friendly interface. You can explore various categories of data, such as messages, call logs, photos, videos, and app data.
- **Report Generation,** Magnet AXIOM allows you to generate comprehensive reports summarizing the findings of your analysis. These reports can be customized and exported in various formats for further analysis or presentation purposes.

Using the Magnet AXIOM demo software for mobile forensics++

- **Explore Additional Features,** Take some time to explore the additional features and capabilities of Magnet AXIOM, such as keyword searching, timeline analysis, and integration with other forensic tools and databases.
- **Experiment,** Use the demo software to experiment with different scenarios and data types. This will help you familiarize yourself with the software's capabilities and determine if it meets your needs for mobile forensic analysis.

Understanding Forensics in the Internet of Anything

- In 2010, VMware and BlackBerry explored developing type 2 hypervisors for mobile devices, which would enhance security but complicate forensic investigations.
- Personal and business data separation in private-sector investigations is crucial, especially considering privacy laws.
- Though the idea of type 2 hypervisors for mobile devices waned, the challenge of handling private data on personal mobile devices persists, exacerbated by the BYOD trend.
- The Internet of Things (IoT) presents challenges as the number of connected devices surpasses that of people, with potential privacy and security implications.

Understanding Forensics in the Internet of Anything+

- Smart devices interconnected via IoT can complicate investigations, such as determining who made purchases or unlocked doors.
- The IoT has evolved into the Internet of Everything (IoE) and Internet of Anything (IoA), incorporating tangible and intangible elements, further complicating evidence tracking.
- The emergence of 5G smart devices introduces new communication types, posing challenges for digital forensics.
- Gaming consoles and wearable computers like smartwatches and Google Glass present additional data collection challenges for investigators.

Understanding Forensics in the Internet of Anything++

- Vehicle system forensics is a new field addressing the many sensors in cars, raising concerns about privacy and security vulnerabilities.
- Investigations involving IoA devices may be complex due to devices not being designed with investigations or security in mind, requiring thorough research for data access.

Summary

Reference

1. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.
2. Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. *Int. J. Netw. Secur.*, *17*
3. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing Ltd.