Unit - 4

E-mail Forensics

- **Phishing -** e-mails contain links to text on a Web page
- **Pharming** - DNS poisoning takes user to a fake site
- **Spoofing** - e-mail can be used to commit fraud

Investigators can use the **Enhanced/Extended Simple Mail Transfer Protocol** (ESMTP) number in the message's header to check for legitimacy

From a digital forensics perspective, our focus lies in locating and retrieving emails from a suspect forensic image file or device. We analyze the email headers, extracting valuable information such as IP addresses and the date/time of when a particular email was sent. Ultimately, our goal is to trace the email back to its origin, identifying the sender.

Investigating Email Crimes and Violations

Digital forensics, particularly concerning email investigations, shares similarities with other types of investigations. The goals are clear:

- Identify the perpetrator of the crime
- Gather evidence
- Present findings
- Build a case

It's crucial to recognize that laws such as the **Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA)** apply to email investigations. However, email crimes may vary in legality depending on the jurisdiction:

- For instance, spam might not be considered a crime in some states.
- Therefore, it's imperative to consult with an attorney.

Understanding the applicable privacy laws for your jurisdiction is paramount.

Examples of crimes involving emails include:

- Narcotics trafficking
- Extortion
- Sexual harassment and stalking
- Fraud
- Child abductions and pornography
- Terrorism

Understanding Forensic Linguistics

Forensic linguistics is an emerging field where language intersects with the law. The International Association of Forensic Linguists categorizes this field into four main areas:

- Language and law
- Language in the legal process
- Language as evidence
- Research/teaching

Consider the following:

- When receiving emails from acquaintances, the choice of words can convey facial expressions such as smiles or frowns. Deviations from their usual language could indicate the email wasn't authored by them.
- Forensic linguistics trains professionals to analyze voice recordings to determine the speaker's identity and to assess whether a particular email or letter was written by a specific person.

Forensic linguistics is pertinent in civil cases, criminal cases, cyberterrorism cases, and various other legal contexts.

Protocol Name	Role
SMTP	Simple Mail Transfer Protocol: Used to transfer e-mail messages from client to server and between servers.
POP3	Post Office Protocol: Clients use it to download their incoming e-mail from their e-mailbox to their local machine (using a proper e-mail client like MS Outlook or Thunderbird) without saving a copy on the POP3 server.
IMAP	Internet Message Access Protocol: This is another incoming mail protocol (like POP3) and plays the same role; however, it differs from the POP3 protocol in allowing a user to store a copy of his/her incoming e-mail message on the mail server even after a user downloads it to his/her local machine.
HTTP	HyperText Transfer Protocol: When a user sends and receive e-mails using the webmail interface (Web browser), like Google and Yahoo!, the HTTP protocol will be used.

When conducting forensic analysis on e-mails, examining the e-mail header is essential to gather valuable information, such as its origin.

The e-mail header contains a wealth of forensically useful information:

- The route the e-mail took over the Internet
- Stops or delays during delivery
- The IP address of the sending machine
- The client (e.g., e-mail program) and the type of operating system used

It's crucial to note that while most of the information in the e-mail header, including technical details, can be forged, tech-savvy criminals can manipulate the origin of their e-mails. They can even make them appear similar to genuine e-mails, such as in phishing attempts.

When analyzing an e-mail, understanding the information contained within the e-mail header is crucial:

1. **Message-ID**: This is a unique number assigned by the sending e-mail server.
2. **Sender's E-mail Address**: This can be falsified, as the sender's "e-mail address" can be adjusted from their end.
3. **Originating IP Address:** This is the IP address of the sender. Note that this IP address can be forged or spoofed.
    - Expect to see multiple "Received" lines. Read the e-mail header from bottom to top; the first "Received" line typically points to the sender.
4. **Recipient IP Address.**
5. **Recipient's E-mail Address.**

- When an e-mail travels through the Internet, each mail server it passes through adds information to the header. Therefore, the e-mail header can contain additional information such as the e-mail client and the operating system used to send the message.
- Additionally, an e-mail header can reveal more information about the message, such as the name and version of the e-mail client and the operating system used to compose and send the message.

```
Date: Sun, 7 Oct 2018 00:22:02 +0300
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101
 Thunderbird/45.8.0
```

Determining a Sender's Geographic Location

To ascertain a sender's geographical location:

- Extract the sender's IP address from the e-mail header, typically found in the "Received: from" line, starting from the bottom header.
- Use online services like Wolfram Alpha or Ipfingerprints to map the IP address to a geographical location.

If the sender's IP address is unavailable in the header, or if it's missed:

- Check the sender's computer time zone information, which can provide clues about their location.
- Utilize tools like the Google Apps Message Header Analyzer, focusing on the "Created at:" field.

Examining Additional E-mail Files

E-mail programs store messages either on the client computer or the server, depending on settings:

- Clients may save e-mails in separate folders for record-keeping.
- For example, **Outlook can save e-mails in .pst or .ost files**, facilitating offline access.
- Some companies host Exchange servers in the cloud, storing .ost files locally and .pst files on the server, requiring network administrator access.
- **Web-based e-mail providers store messages as web pages in the browser's cache folders.**
- Instant messaging (IM) services offered by web-based e-mail providers, like Yahoo! Messenger and Google Talk, can save messages in various file formats.

E-mail Investigations Challenges

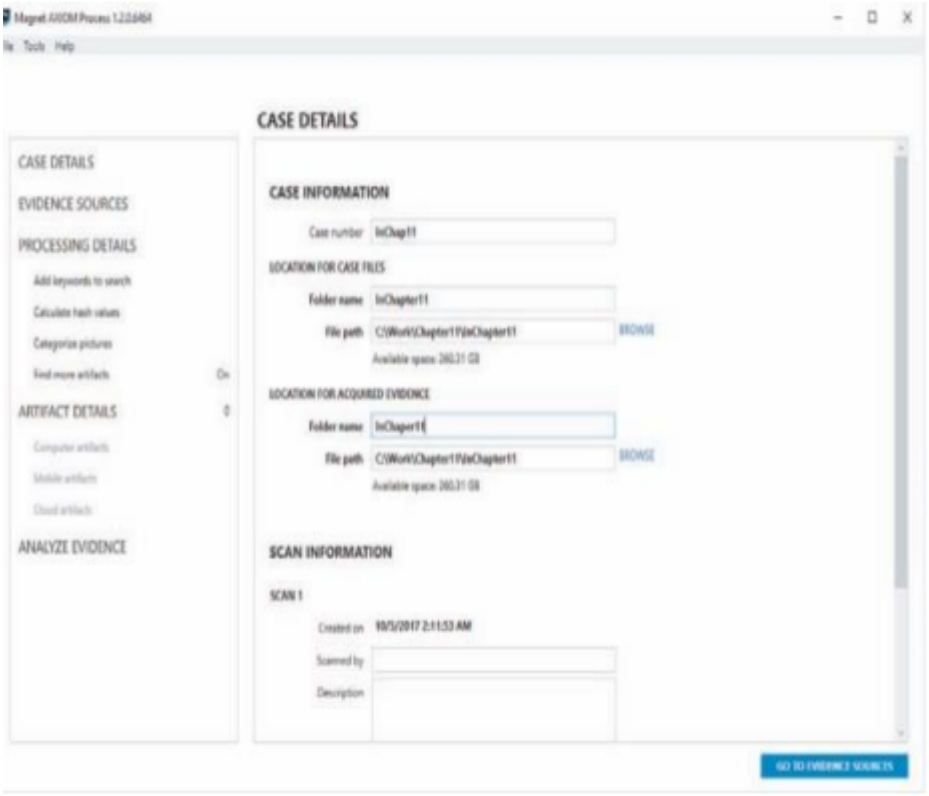
Investigating e-mails and tracing their source or origin can be challenging due to various factors:

1. Disposable E-mail Addresses:
    - Tracking disposable (temporary) e-mail addresses is extremely difficult, if not impossible, as they exist for a short time and are often used for one-time contact only.
2. Anonymous E-mails:
    - Some individuals use the TOR network to send anonymous e-mails, making tracking nearly impossible due to strict precautionary measures.
3. Shared E-mail Accounts:
    - Suspects may create an e-mail account using a free service like Yahoo! or Gmail and share access with a partner.
    - Instead of exchanging e-mails, the suspect leaves instructions for criminal activity in the draft folder. The partner accesses the account, reads the instructions, and deletes the draft message.
4. Different Jurisdictions:
    - Cloud e-mail providers may store e-mails on servers located in countries other than the user's residence.
    - For example, if a suspect involved in criminal activity in the United States has an e-mail account with a provider in Switzerland, can U.S. law enforcement compel the Swiss provider to release suspect data?

Using Magnet AXIOM to Recover E-mail

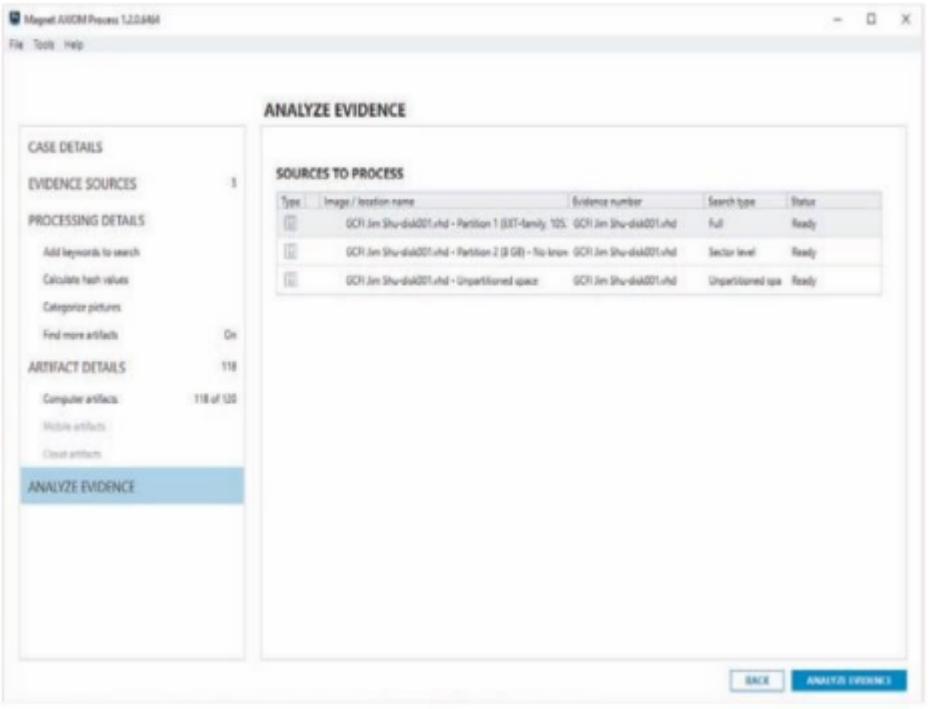
Magnet AXIOM is a comprehensive tool designed to retrieve evidence from PCs, mobile devices, and the cloud. Here's how you can use Magnet AXIOM to recover e-mails:

1. **Start Magnet AXIOM Process**:
    - Click the **CREATE NEW CASE** button.
    - In the **Case number** text box, enter the case number.
    - In the **LOCATION FOR CASE FILES** section, enter the folder name.
    - Click **BROWSE** next to the **File path** text box, navigate to your work folder, and click **Select Folder**.
    - Click the **GO TO EVIDENCE SOURCES** button.



1. **Select Evidence Source**:
   - In the **EVIDENCE SOURCES** window, choose **COMPUTER**.
   - Click the **LOAD EVIDENCE** icon and then click **NEXT**.
   - Choose **IMAGE**, navigate to your work folder, select the hard drive file, and click **OK**.
2. **Add Files and Folders**:
   - In the **Add Files and Folders** window, click **NEXT**.
3. **Specify Search Type**:
   - Leave all search types selected (full, sector level, unpartitioned space), and click **NEXT**.
4. **Processing Details**:
   - Click **GO TO PROCESSING DETAILS**.
   - Add keyword lists, hash values, and other details as needed.
   - Click **GO TO ARTIFACT DETAILS**.
5. **Analyze Evidence**:

- Click **GO TO ANALYZE EVIDENCE**.
- Click **ANALYZE EVIDENCE**. This process may take around two hours.



6. **Examine E-mail**:
   - Once processing is complete, Magnet AXIOM Examine starts automatically.
   - Click to expand **EMAIL** on the left.
   - Click an e-mail with the desired address in the **EVIDENCE** pane.
   - Copy the e-mail header from the pane on the far right.
   - Open a web browser and go to https://mxtoolbox.com/EmailHeaders.aspx.
   - Paste the e-mail header into the **E-mail Header Analyzer** text box and click **Analyze Header**.
7. **Exit Magnet AXIOM**:
   - After examining the e-mail, exit Magnet AXIOM.

Email Forensics: Phishing

Phishing scams aim to gather sensitive information such as bank account details, credit card numbers, and social security numbers for illegal misuse or

sale. Here's how phishing attacks typically unfold:

1. **Attack Method**:
    - Phishing attacks are often delivered via email communications that are spoofed to appear legitimate, mimicking well-known entities like banks, shopping portals, hotels, or even authoritative figures or personal acquaintances.
2. **Modus Operandi**:
    - Cybercriminals, posing as trusted entities, deceive recipients into opening the email. Once opened, recipients are enticed to click on a malicious link or document, leading to the installation of malware. Consequently, sensitive information on the victim's system is compromised.

Types of Phishing Attacks:

1. **Spear Phishing**:
    - Targets a specific person or organization. Phishers meticulously gather information about their target to craft a believable and legitimate-looking email to extract information or money.
2. **Whaling**:
    - A form of spear phishing targeted at high-profile individuals such as executives (e.g., COO, CEO) who have access to financial data or assets. CFO fraud is a common example of whaling, where critical and sensitive information is stolen from a company.
3. **Smishing and Vishing**:
    - **Smishing**: SMS phishing conducted via SMS text messaging on mobile devices.
    - **Vishing**: Voice phishing conducted via phone calls.
4. **Deceptive Phishing**:
    - The sender disguises email IDs as official company email addresses, encouraging users to click on fake links provided in the email. Cybercriminals typically target victims via bulk email processes.
5. **Pharming (DNS-based phishing)**:

- Involves the modification or tampering of a system's host files or domain name system to redirect URL requests to a fake site. Users are unaware that the website they are entering their personal details into is fake.

6. **Content-injection Phishing**:
    - Scamsters/phishers insert malicious code or misleading content into legitimate websites, asking users to enter their credentials or personal information. This phishing attack occurs as part of content spoofing.
7. **Search Engine Phishing**:
    - Scamsters or phishers create malicious websites with enticing offers, which are then indexed by search engines. Innocent victims are lured to these sites, unknowingly sharing all their personal information.

A Possible Way to Spot a Phishing Email:

1. **Example Scenario**:
    - Cybercriminals send an email claiming that there has been an error in calculating your tax, and a refund needs to be issued. The email includes a link that redirects you to a banking login page. If you log in by entering your account details, your bank account could be hacked.
2. **Spotting the Phishing Attempt**:
    - Check the sender's email address.
    - In this case, the sender's address appears as donotreply@incometaxindiafilling.gov.in, not donotreply@incometaxindiaefiling.gov.in, which is the legitimate email address of the income tax department.
    - Note the misspellings:
        - The letter "e" is missing from the word "efiling."
        - "Filing" is misspelled as "filling."

To check if the sender email address is legitimate or spoofed use a free online utility called **Email Dossier**

- **OST and PST Files**: These are data files used to store emails, attachments, contacts, notes, and other data in Microsoft Outlook.
- **OST Files**:

- Used to interact with the Exchange Server while offline.
- Created when you configure Outlook to work in caching exchange mode.

- **PST Files**:
  - Used to store data on your local computer.
  - Created when you create a new Outlook data file.

OST vs PST

Characteristics	OST	PST
Definition	OST files are used to interact with the Exchange Server while offline.	PST files are used to store data on your local computer.
Creation	OST files are created when you configure Outlook to work in caching exchange mode.	PST files are created when you create a new Outlook data file.
File Size	Due to synchronization, the file size is large.	Due to synchronization, the file size is small.
Backup	Backups will be taken automatically.	Need to take backup manually
Secure	It is more secure due to the presence of encryption.	Due to data files stored on a local computer, it is less secure.
Usage	It is used in Exchange Server environments.	It is used in non-Exchange Server environments.
Data Access	OST allows offline access to previously downloaded data files such as emails, contacts, notes, and other data.	PST allows you to archive old emails, contacts, and notes.

Mobile Forensics

Understanding Mobile Device Forensics

Investigating cell phones and mobile devices poses several challenges in digital forensics:

- **No Standardization**:
  - There is no single standard for how and where phones store messages.
  - New phones are released approximately every six months, and they are rarely compatible with previous models.
- **Variety of Devices**:
  - Cell phone stores offer a vast array of makes, models, and operating systems.
  - Different devices support various services and applications.
- **Lack of Established Hardware Interface**:

    - There is no established hardware interface for mobile devices.
    - Upgrading phones often requires purchasing new chargers and data cables.
- **Improvements**:
    - Many phones now include a mini-USB in their handsets, which simplifies compatibility.

Mobile Phone Basics

Mobile phone technology has rapidly advanced over the years:

- **Generations of Mobile Phones**:
    - By the end of 2008, mobile phones had gone through three generations:
        - Analog
        - Digital Personal Communications Service (PCS)
        - Third-generation (3G)
    - Fourth-generation (4G) was introduced in 2009.
    - Fifth-generation (5G) cellular networks are currently being implemented.
- **Digital Networks**:
    - Several digital networks are used in the mobile phone industry.
- **CDMA and GSM Networks**:
    - Most Code Division Multiple Access (CDMA) networks conform to IS-95.
        - CDMA systems are referred to as CDMAOne, and when they upgraded to 3G services, they became CDMA2000.
    - Global System for Mobile Communications (GSM) uses the Time Division Multiple Access (TDMA) technique, where multiple phones take turns sharing a channel.
- **3G Standard**:
    - The 3G standard was developed by the International Telecommunications Union (ITU) under the United Nations.

    - It is compatible with CDMA, GSM, and TDMA.
    - Enhanced Data GSM Environment (EDGE) standard was developed specifically for 3G.
- **4G Network Technologies**:
    - 4G networks can use various technologies, including:
        - Orthogonal Frequency Division Multiplexing (OFDM)
        - Mobile WiMAX
        - Ultra Mobile Broadband (UMB)
        - Multiple Input Multiple Output (MIMO)
        - Long Term Evolution (LTE)

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. In the United States, Sprint, U.S. Cellular, and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile in the United States and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots; GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEN)	This Motorola protocol combines several services, including data transmission, into one network.
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

Cellular Network Components

Understanding the components of a cellular network is crucial for digital forensics:

- **Base Station**:
    - Consists of antennas and related equipment.
- **Base Station Controller (BSC)**:
    - Manages Base Transceiver Stations (BTSs) and assigns channels by connecting to the Mobile Switching Center (MSC).
- **Mobile Switching Center (MSC)**:

    - Connects calls by routing digital packets for the network.
    - Relies on a central database containing subscriber account data, location data, and other key information needed during investigations.
    - Retrieving information from a carrier's central database typically requires a warrant or subpoena.
- **Base Transceiver Station (BTS)**:
    - Made up of radio transceiver equipment that defines cells and communicates with mobile phones.
    - Often referred to as a "cell phone tower."
- **Visitor Location Register (VLR)**:
    - Linked to a MSC.
    - Records all mobile devices currently being controlled by that MSC.
    - Interworking Functions serve as gateways outside data networks such as the Internet.
- **Home Location Register (HLR)**:
    - Collects information about individual subscribers, including subscriber identification, billing, services received, and the current location of the device.
    - Stores encryption keys.
    - Supports the Authentication Center (AuC), which controls access to the network by screening connections and blocking unauthorized users.

Inside Mobile Devices

Mobile devices, ranging from simple phones to smartphones, tablets, and smartwatches, contain various hardware components:

- **Hardware Components**:
    - Microprocessor, ROM, RAM, digital signal processor, radio module, microphone, speaker, hardware interfaces, and LCD display.
    - Most basic phones have a proprietary OS, while smartphones typically use the same OSs as PCs.
- **Storage and Operating System**:

    - Phones store system data in electronically erasable programmable read-only memory (EEPROM), allowing service providers to reprogram phones without physically accessing memory chips.
    - The OS is stored in ROM, which is nonvolatile memory and remains available even if the phone loses power.
- **Evolution of Personal Digital Assistants (PDAs)**:
    - PDAs have been largely replaced by iPods, iPads, and other mobile devices.
    - Their use has shifted to more specific markets such as medical or industrial PDAs.
- **Peripheral Memory Cards**:
    - Used with PDAs, including Compact Flash (CF), MultiMediaCard (MMC), and Secure Digital (SD) cards.
- **Subscriber Identity Module (SIM) Cards**:
    - Found most commonly in GSM devices.
    - Consist of a microprocessor and internal memory.
    - GSM divides a mobile station into two parts: the SIM card and the mobile equipment (ME).
    - SIM cards come in three sizes and are necessary for the ME to work.
    - Functions of SIM cards include identifying the subscriber to the network and storing service-related information.

SIM Card and Acquisition Procedures for Mobile Devices

SIM Card Content:

- The SIM card contains several pieces of valuable information, including:
    - International Mobile Subscriber Identity (IMSI) used to identify subscriber account information and services.
    - Integrated Circuit Card Identifier (ICC-ID), the serial number of the SIM card.

- Subscriber identification, service provider, language preferences, phone location when powered off, user-stored phone numbers, numbers dialed by the user, SMS text messages, and potentially deleted SMS text messages.

SIM PIN:

- A Personal Identification Number (PIN) may protect the SIM data.
- PINs are typically four to eight digits long, with only three attempts allowed to enter the correct PIN.
- After three unsuccessful attempts, access requires an eight-digit Pin Unblocking Key (PUK) along with a new PIN.
- After 10 failed PUK attempts, many SIM cards permanently deny access.

Acquisition Procedures for Mobile Devices:

- All mobile devices have volatile memory, so ensuring they don't lose power before retrieving RAM data is critical.
- Concerns include loss of power, synchronization with cloud services, and remote wiping.
- Suggested procedures:
  - Disconnect a mobile device attached to a PC via USB cable immediately.
  - Isolate the device from incoming signals to prevent automatic synchronization and data overwrite.
  - Depending on the warrant or subpoena, the time of seizure might be relevant, as messages might be received on the device afterward.
  - Isolation methods include airplane mode, a paint can, Faraday bag, or turning the device off.
- SANS DFIR Forensics recommends various actions depending on the device's status (on/unlocked, on/locked, off) to ensure effective acquisition.
  - If device is on and unlocked - isolate it from the network, disable the screen lock, remove passcode
  - If device is on and locked - what you can do varies depending on the type of device

    - If device is off - attempt a physical static acquisition and turn the device on, determine whether it’s locked, and then follow the procedure for either a locked or unlocked condition
- In the forensics lab, assess what can be retrieved, considering logical and physical acquisition methods, and check areas such as internal memory, SIM card, external memory cards, and network provider data.
- Retrieving information from the network provider often requires a search warrant or subpoena.
- GPS data retrieval from the device is usually possible if the device is available, eliminating the need for triangulation through a cell tower from the provider.

Triangulation in Mobile Device Forensics

Triangulation is a key method used to locate cell phones in digital forensics:

- **Method**: Triangulation involves determining the approximate location of a phone by measuring its distance from three different cell towers.
- **Signal Delay Calculation**: The distance is calculated by measuring the signal delay from the phone to the three towers.
- **Directional Antenna**: Alternatively, a directional antenna can be used to determine the phone's location by measuring signal delays from only two towers. The directional antenna helps determine the direction of the signal.
- **GPS**: Finally, the phone's location can also be determined using GPS coordinates, providing precise latitude and longitude information.

Understanding Acquisition Procedures for Mobile Devices

As mobile devices evolve, acquiring data from them becomes increasingly complex:

- **Cloud Backups**: Mobile device backups are often stored in carrier or third-party clouds, adding a new layer of complication to the acquisition process.
- **Remote Wiping**: Due to the rise in mobile device thefts, service providers now employ remote wiping to erase a user's personal data from stolen devices.

- **Memory Storage**: Mobile devices typically utilize a combination of volatile and nonvolatile memory. Volatile memory contains frequently changing data like missed calls and text messages, while nonvolatile memory stores OS files and user data.
- **SIM Card**: Memory resides not only in the phone but also in the SIM card, which has a hierarchical file system structure.
- **Retrievable Information**: The data that can be retrieved from a mobile device falls into four main categories: service-related data, call data, message information, and location information.
- **Accessing SIM Card**: If power is lost, PINs or access codes may be required to access SIM card files. Typically, users retain the original PIN, so look for user manuals or documentation at the scene to assist in accessing the SIM card.
- **PIN Unlock Key (PUK)**: After three unsuccessful attempts, a locked SIM card requires a PUK from the service provider to unlock. Common PINs to try are 1-1-1-1 or 1-2-3-4.

Call Detail Records (CDR)

- **Provider Use**: CDRs are primarily used by service providers to troubleshoot and enhance network performance.
- **Forensic Use**: For examiners, CDRs provide crucial information such as:
  - Date and time of call initiation and termination
  - Caller and recipient information
  - Call duration
  - Call direction (incoming or outgoing)
  - Originating and terminating cell towers

Subscriber Information Records are distinct from CDRs:

- **Subscriber Information**: Includes subscriber details such as name, address, telephone numbers, account numbers, email addresses, and services subscribed to.

- **Retention Period**: Service providers maintain these records according to their data retention policies, which can vary based on data type. For instance, SMS data might be retained for 7 to 14 days, while cell sector information could be kept for a year or longer.
- **Importance for Investigation**: Subscriber information records provide comprehensive data on subscribers, including personal and billing details.

Key points to remember:

- **Request Timing**: Requesting CDRs within the provider's retention period is crucial, as records might be purged after a certain period.
- **Data Specificity**: CDRs detail each call's specifics, including tower locations, call duration, initiation time, and dialed numbers.
- **Completeness**: CDRs offer more comprehensive call data compared to billing records, including calls not yet invoiced.

Understanding CDRs and subscriber information records is essential for forensic investigators to access and analyze critical call-related data effectively.

Mobile Forensics Equipment

Mobile forensics requires specialized equipment and methods due to the unique challenges posed by constantly changing phone models:

1. **SIM Card Readers**:
    - Hardware/software devices used to access SIM cards.
    - Procedure involves:
        - Removing the device's back panel and battery.
        - Extracting the SIM card and inserting it into the card reader.
    - It's essential to use forensically sound SIM card readers and document unread messages.
2. **Mobile Forensics Tools and Methods**:
    - **AccessData FTK Imager**: A tool for extracting data from mobile devices.
    - **MacLockPick 3.0**: Another tool for mobile data extraction.

3. **NIST Guidelines**:
    - NIST lists six types of mobile forensics methods:
        - Manual extraction
        - Logical extraction
        - Physical extraction
        - Hex dumping and Joint Test Action Group (JTAG) extraction
        - Chip-off
        - Micro read

Mobile forensics software procedures involve:

- Identifying the mobile device.
- Ensuring the appropriate mobile device forensics software is installed.
- Connecting the phone to power and cables.
- Initiating the forensics software and downloading information.

For SIM card extraction, a forensics lab equipped with suitable anti-static devices is necessary. It's crucial to use tools that preserve the integrity of evidence and document unread messages using methods like taking pictures of each screen.

Android Debug Bridge (adb)

Android Debug Bridge (adb) is a command-line tool that enables users to communicate with an Android device connected to a computer host system via a USB cable. It is part of the Android Software Development Kit (SDK) platform tools package and allows users to perform various tasks such as installing, debugging, and removing apps. ADB consists of three components:

1. **Client**: Sends out commands. It can be invoked by issuing an adb command using a command-line terminal.
2. **Daemon (adbd)**: Runs commands on the device. It operates as a background process.
3. **Server**: Manages communication between the client and daemon. It operates as a background process on the computer system.

ADB provides several useful commands for forensic examiners, such as:

- `adb devices`: Lists the devices connected to the system.
- `adb install filename.apk`: Installs an application on an Android device through the system shell.
- `adb uninstall filename.apk`: Uninstalls an application from the device.

Manual Extraction

Manual extraction is a mobile forensic acquisition method that involves directly scrolling through the data on the device and viewing it on the phone's screen. This method is straightforward but prone to human error, as it may lead to missing certain data due to the examiner's unfamiliarity with the device interface. Here are the key points and challenges of manual extraction:

Key Points:

- Device must be turned on and unlocked.
- PIN or password must be known if the device is locked.
- Only visible data can be extracted; hidden or deleted data cannot be accessed.

Challenges:

- Prone to human error.
- Device must be in an unlocked condition.
- PIN or password must be known if the device is locked.
- Hidden or deleted data cannot be extracted.

Demonstration:

- For demonstration, we will use a Sony Xperia phone running on Jelly Bean 4.2.
- Use the `adb devices` command to list all connected devices. ADB drivers are built into the Santoku Operating System.
- Download the AFLogical OSE apk from GitHub.
- Push the apk onto the device to install it by typing the command:

```
adb -d install AFLogical-OSE_1.5.2.apk
```

- Open the application and select the parameters for extraction. Click on "capture" after selecting all the parameters.
- Once data extraction is complete, call records, contacts, and messages will be exported in .csv format, which is accessible via many applications.
- An info file can also be retrieved in .xml format, containing data about the device and the applications stored on it.
- These files can be found in the File Manager:

```
sdcard
forensics folder
```

Results:

- Contacts stored in the phone in the CSV file.
- Call logs with recipient's name, phone number, timestamps, and duration of the call in the CSV file.
- SMS messages sent or received in the CSV file.

Physical and Logical Acquisition

Physical Acquisition:

- Physical acquisition captures all the data stored on a physical piece of storage media.
- It creates a bit-for-bit copy, similar to cloning a hard drive, including deleted information.
- This method captures all data, including deleted files and folders.
- It requires specialized forensic tools to acquire a forensic image of the mobile device.
- Unlike logical acquisition, physical acquisition does not use write-blocking devices. The phone must interact directly with the hardware and software.
- This is a more comprehensive forensic technique and is often the preferred method for deeper analysis.

Logical Acquisition:

- Logical acquisition captures only the files and folders without deleted data.

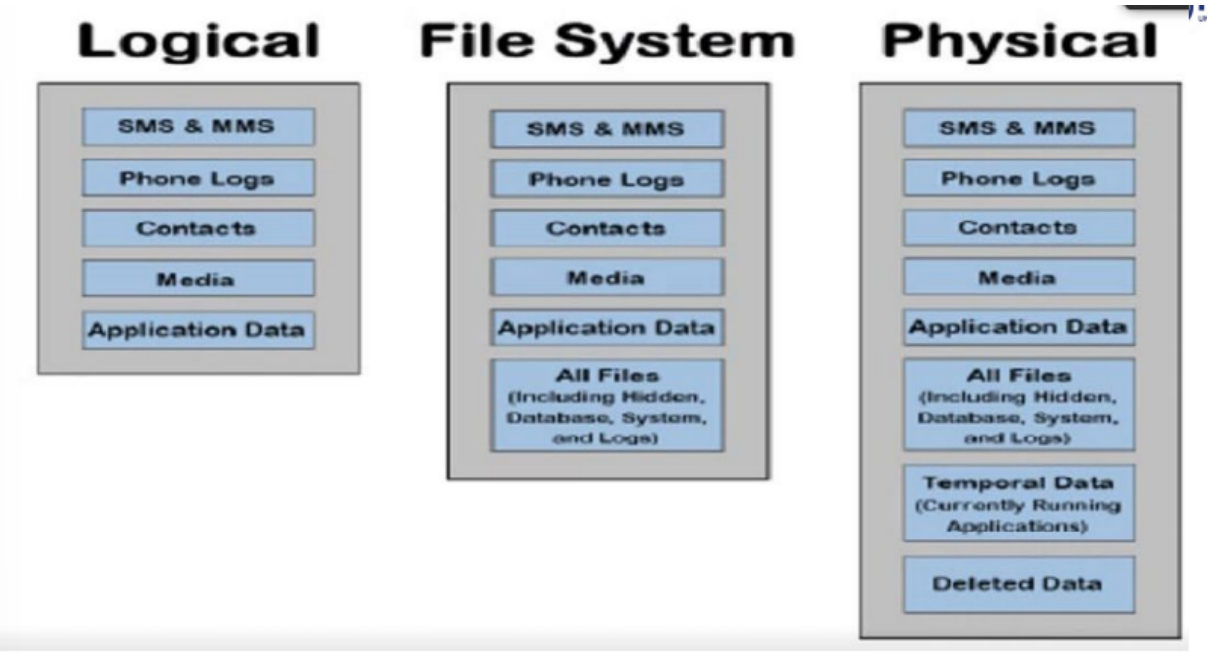
- It does not capture the entire contents of the storage media but focuses on visible files and directories.
- Data can be collected using non-forensic tools used for synchronizing or backing up data on the cell phone.
- Logical acquisition is faster compared to physical acquisition but may not provide as much information.

Difference:

- Physical acquisition captures all data, including deleted files and folders.
- Logical acquisition captures only visible files and directories without deleted data.

Process:

1. **Physical Acquisition:**
    - Forensic investigators use specialized tools to acquire a forensic image of the mobile device.



Joint Test Action Group (JTAG) in Mobile Forensics

Overview:

- JTAG is an advanced data extraction method used in mobile forensics.

- Originally developed by the electronics industry for testing and verifying designs and printed circuit boards.
- JTAG stands for Standard Test Access Port and Boundary-Scan Architecture, recognized as an IEEE standard.
- Provides an interface for direct communication between a computer and the chipboard of a device.
- Allows access to raw data by connecting the evidence mobile device's Test Access Port (TAP) to a JTAG emulator.

Steps involved in JTAG forensic examination:

1. **Identification of TAPs:**
    - Research documented devices to identify TAPs.
    - If TAPs are unknown, inspect the device PCB for potential TAPs.
    - Manually trace or probe to pinpoint appropriate connector pins.
2. **Solder wires to TAPs:**
    - Lead wires to the correct connector pins or utilize a solderless jig.
3. **Connect appropriate JTAG emulator with wire leads for the exhibit device.**
4. **Acquire physical image dump.**
5. **Disconnect the wires and reassemble the device.**
6. **Analyze image with forensic software.**

Advantages of JTAG:

- Advanced and non-invasive method of forensic examination.
- Compatible with various types of mobile devices, including Windows phones.
- Less complicated procedure compared to Chip-Off method.

Disadvantages of JTAG:

- Less successful in case of device encryption.
- Resources for JTAG are difficult to find on the internet.

JTAG is an effective method for extracting raw data from mobile devices, offering advantages such as compatibility with various devices and a less

complex procedure. However, it may not be as successful with encrypted devices, and finding resources for JTAG can be challenging.

Chip-Off

Overview:

- Chip-Off is a forensic technique used as a last resort, involving the removal of the memory chip from a mobile device.
- The memory chip is then mounted onto specialized hardware for data acquisition and analysis.
- This method allows examiners to obtain a binary image of the memory chip, which can be analyzed using specialized software.
- Chip-Off is an advanced forensic method that can even be used on bricked or damaged devices.

Steps involved in Chip-Off forensic examination:

1. **Removal of the memory chip:** The memory chip is removed from the device by de-soldering it.
2. **Cleaning and repair:** The chip is cleaned and repaired if necessary.
3. **Mounting the memory chip:** The memory chip is mounted onto special hardware apparatus, and data is acquired.

Advantages of Chip-Off:

- Useful for examining devices in damaged condition.
- High probability of data acquisition even if the device is locked.
- Provides forensic investigators with the flexibility to customize the data acquisition process.

Disadvantages of Chip-Off:

- Heat and adhesive used to remove the memory chips may damage the circuit board.
- Reassembly of the device after examination is very difficult and often unsuccessful.

Chip-Off is a powerful forensic technique that allows examiners to access data from mobile devices, especially in cases where the device is damaged or

locked. However, it carries the risk of damaging the circuit board during the chip removal process, and reassembling the device after examination can be challenging.

Micro-read

Overview:

- Micro-read examination is an advanced forensic technique used to extract data from mobile device memory chips.
- It involves the use of a high-powered electron microscope to observe the output at the gate level.
- The device's memory chip is shaved into extremely thin layers, and data is read bit by bit using an electron microscope or other devices.
- Micro-read examination is a highly sophisticated technique, and only a few entities offer Micro-read examination services.
- It is typically used for high-value devices or damaged memory chips and is reserved for high-profile cases.

Key Points:

- **Technique**: Observes output at the gate level using a high-powered electron microscope.
- **Process**: Memory chip is shaved into thin layers, and data is read bit by bit.
- **Sophistication**: Highly advanced and complex technique.
- **Availability**: Limited availability; very few entities offer Micro-read examination services.
- **Use Cases**: Typically used for high-value devices or damaged memory chips.
- **Future**: Despite being a complicated and expensive technique, Micro-read may become more approachable in the near future.

Mobile Forensics Tools:

- **Paraben Software**: Offers several tools including E3:DS for mobile device investigations, DataPilot for interfacing with phones from different manufacturers, BitPam for viewing data on many CDMA phones, Cellebrite

UFED Forensic System for smartphones, PDAs, tablets, and GPS devices, and MOBILedit Forensic with a built-in write-blocker.

- **Software Tools**: Differ in the information they display and the level of detail; some are designed for updating files rather than retrieving data.
- **Cellebrite**: Often used by law enforcement for data extraction with options for logical, file system, and physical extraction.

Using Mobile Forensics Tools:

- Many mobile forensics tools are available, but most aren't free.
- Methods and techniques for acquiring evidence will change as the market continues to expand and mature.
- Professionals are advised to subscribe to user groups and professional organizations to stay abreast of industry developments.

Rooting an Android Device

- **Android OS**: Android is a Linux-based operating system optimized for touch screen devices.
- **Rooting**: Rooting Android unlocks its core module, providing access to protected areas of the device.
- **Evolution of Rooting**: Initially, rooting was common among Android developers to access device features. Now, it's popular among tech-savvy users for customization.
- **Purpose**: Rooting allows forensic investigators to gain root privileges on the device.
- **Considerations**:
  - Rooting involves installing third-party software that can modify the device state.
  - Improper rooting techniques may accidentally delete or modify data, rendering it unreadable.
- **Admissibility**: Evidence gathered by rooting an Android device is not admissible in court.
- **Image Creation**: Rooting an Android device to create an image is covered in the physical acquisition section.

Methods for Screen Lock Bypass

- **Challenges**: Locked Android devices pose challenges for forensic examiners in image acquisition.
- **Security Standards**: Newer Android versions have stronger security, making previous screen lock bypass methods ineffective.
- **Available Methods**:
  - **Commercial Screen Lock Bypass Tools**: Offer the highest success rate with the lowest risk of data loss.
    - Examples include *dr. fone – unlock*, *iSkysoft ToolBox*, *Pangu FPR Unlocker Tool*, etc.
  - **Flashing Custom Recovery/ROM**:
    - Popular among Android developers.
    - Involves flashing the device with a custom recovery.
    - Important to use the correct custom recovery specific to the device model.
    - Risk involved: Incorrect flashing can destroy data or brick the device.
    - Examples: *Team Win Recovery Project (TWRP)* and *Clockwork* are popular recovery methods.

These methods help forensic investigators bypass screen locks and facilitate image acquisition from locked Android devices.

Anti-Forensics

Introduction to Anti-Forensics

- **Definition**: Anti-forensics is the set of techniques used to fight against forensic analysis. It aims to make acquiring and analyzing digital evidence difficult or impossible.
- **Objective**: Anti-forensics techniques aim to destroy or conceal digital evidence, frustrating forensic investigators and increasing the time needed for analysis.

- **Dr. Marc Rogers' Definition**: "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct."
- **Challenge**: Cyber forensic experts encounter anti-forensics as a significant challenge in dealing with modern cybercriminals.
- **Impact on Investigations**:
  - Anti-forensic measures performed on a device harm the integrity of the data and could compromise the investigation.
  - The common intent of anti-forensics tools is malicious.
- **Purpose of Anti-Forensics**:
  - **For Hackers and Users**: Hackers and computer users practice anti-forensic techniques to hide their trail and protect their data.
  - **Reducing Forensic Artifacts**: The aim of anti-forensics is to significantly reduce the quality and quantity of forensic artifacts present on the disk.
- **Challenges for Investigators**: Anti-forensic activities make digital forensics analysis a nightmare and difficult for investigators.

Users of Antiforensics Techniques

Antiforensics techniques are used by various actors for different purposes. Apart from criminal and terrorist groups, antiforensics is utilized by:

- **Military professionals**
- **Law enforcement**
- **Politicians and diplomats**
- **Security researchers**
- **Journalists and whistleblowers**
- **Business corporations**
- **Casual internet users seeking privacy**

From a digital forensics perspective, it's crucial for examiners to be aware of these techniques and how they function. This knowledge provides a better

understanding of what actions to take if encountering them during investigations.

Criteria for Antiforensics Techniques:
For a tool or technique to be labeled as an antiforensic entity, it must meet one or more of the following criteria:

- Attack the Data
- Attack the Forensic Tools
- Attack the Investigators' Work

Classification of Antiforensics Techniques

Antiforensics has evolved into a broad field, covering various computer security aspects. The main digital antiforensics techniques that forensic examiners may encounter include:

1. **Data hiding techniques** (steganography)
2. **Data destruction techniques** (antirecovery)
3. **Encryption techniques**
4. **Cryptographic anonymity techniques**
5. **Direct attacks against computer forensics tools**
6. **Data wiping**
7. **Trail obfuscation**

Digital Steganography

Definition:
Steganography is the science of concealing a secret message within an ordinary file, maintaining its secrecy during delivery.

Historical Background:

- Old steganographic techniques relied on physical objects like paper, eggs, invisible ink, and even human skin to conceal secret messages.
- With advancements in computing technology and internet communications, modern techniques are largely based on exploiting digital files and IPs to convey secret messages.

How Digital Steganography Works:

- Any digital file type can be used to conceal a secret message within it.
- Most digital steganographic techniques do not alter the appearance of the overt file, ensuring it cannot be detected by an outside observer.

Digital Steganography Techniques:

1. **Injunction:** Embedding a secret message in a trivial, non-readable location of the overt file, such as after the end-of-file marker (EOF). This method does not affect the overt file quality or appearance.
2. **Substitution:** Replacing insignificant bits of the overt file with bits from the secret message. This method is more secure as it does not increase the size of the overt file.
3. **Generation:** Creating a new file that holds the secret message within it. This is the most secure method of digital steganography.

Steganography in digital files can occur in various formats, including images, videos, audio, or even a file system like Windows NTFS.

Text Steganography

Description:
Text steganography involves hiding secret messages within ordinary text, preserving its visual appearance while concealing the hidden message.

Techniques:

- **Spelling Changes:** Altering the spelling of certain words while maintaining the visual appearance of the text.
- **Twitter Steganography:** Secret messages can be concealed within Twitter tweets in plain sight using services like http://holloway.co.nz/steg/.

Image Steganography

Description:

- Image steganography is the most commonly used method for concealing secret messages.
- With the prevalence of digital image exchange on social media, this method is less suspicious to outside observers.

Process:

- A user embeds a secret message within an image file using a steganographic algorithm, creating a stego-image.
- The stego-image is sent to the receiver, who extracts the secret message using a similar algorithm.

Audio-Video Steganography

Description:

- **Audio Steganography:** Secret data is concealed within digital audio files.
  - **Popular Tool:** MP3stego conceals secret data in MP3 audio files.
- **Video Steganography:** Techniques used in image and audio files are utilized to conceal secret data in video files.
  - Video files offer a large capacity for secret data without affecting the quality of the original file.

Network Steganography

Description:

- Networking protocols like TCP/IP can be exploited to embed secret messages.
- Many networking protocols allow for this possibility.
- Example: `covert_tcp` is a program used to conceal data within TCP/IP headers. (http://firstmonday.org/ojs/index.php/fm/article/view/528/449)

Data Wiping and Shredding

Description:

- **Wiping:** Erases all data on a hard drive, also known as digital shredding or erasing.
- **Digital Shredding:** Similar to wiping, erasing a portion of the hard disk drive and overwriting it with random data.

Process:

- Formatting or deleting the disk content doesn't remove the data; it's still recoverable.
- In data wiping, the drive is overwritten multiple times to make the data unreadable, ensuring no artifacts are left behind.

Protocol for Disk Wiping:

- **Department of Defense (DoD) Standards:**
  - **Three-Pass Overwrite (DoD 5220.22-M):** Data overwritten by '0's, followed by '1's, and then random characters. A verification pass confirms successful overwriting.
  - **Seven-Pass Overwrite (DoD 5220.22-M ECE):** Similar to three-pass with additional steps of random character passes and verification.

Data Remanence:

- Sometimes data remains on a disk even after deletion, known as data remanence.
- Increasingly complex anti-forensic tools leave hardly any data fragments on a system.
- In rare cases where fragments are obtained, without sufficient details, it's hard to piece together evidence.

Degaussing:

- **Process:** Using strong electromagnets to erase data from a disk, a form of demagnetizing.
- **Effect:** Resets the device to a magnetically neutral state by exposing it to a strong, fluctuating magnetic field.
- **Result:** Device's magnetic structure gets restructured, making it impossible to recover any data.
- **Limitation:** SSDs are immune to degaussing as they don't rely on similar magnetic structures as hard disk drives.

Tools for Data Wiping:

- **USB Oblivion:** Erases all traces of USB-connected drives and CD-ROMs from the Registry in Windows.
- **Eraser:** Open-source tool for Windows that completely removes sensitive data from a hard drive by overwriting it with carefully selected patterns.
- **Disk Wipe:** An open-source portable Windows application for permanent volume data destruction. It can erase all disk data and prevent recovery.

Case Study: Eraser

Overview:

- When a file is deleted, the operating system removes its reference from the file system table but doesn't remove the file from the disk.
- Before the file is overwritten, it can easily be retrieved using undelete utilities or disk maintenance tools.
- **Eraser** is a tool used to completely remove data by overwriting it several times with carefully selected patterns.

Steps for Using Eraser:

1. Open Eraser and select "New Task" under Erase Schedule.
2. Click on "Add Data" and select the file you want to delete. Choose from a variety of erasure methods.
3. Click on any of the Task Type options of your choice.
4. Data will be completely erased.

Data Destruction and Antirecovery Techniques:

- **Offenders** use data destruction techniques to make their incriminating data impossible to recover.
- **Three ways** to destroy data stored on digital devices:
    - **Physical Destruction:** Destroy digital storage media physically using hard drive shredders or destroyers.
    - **Degaussing Technique:** Expose magnetic storage devices like HDD or magnetic tape to a powerful magnetic field using a degausser to eliminate magnetically stored data.
    - **Logical Destruction (Sanitizing):** Use wiping tools to destroy data without affecting the hardware holding the data. However, this method doesn't guarantee 100% removal of data, especially from magnetic storage media like HDD and tapes.

Note:

- The existence of wiping tools on a suspect machine raises suspicions about incriminating data.
- Using wiping tools leaves clear clues about their usage on a hard drive, which can be easily seen when investigating the target hard drive using any Hex editor.

Trail Obfuscation

Overview:

- **Trail Obfuscation** involves the use of tools and techniques to mislead investigations by manipulating evidence.
- Cybercriminals/hackers manipulate evidence to misdirect and confuse forensic investigators.
- Usage of Virtual Private Network (VPN) software like TunnelBlick is an example of trail obfuscation.

Spoofing:

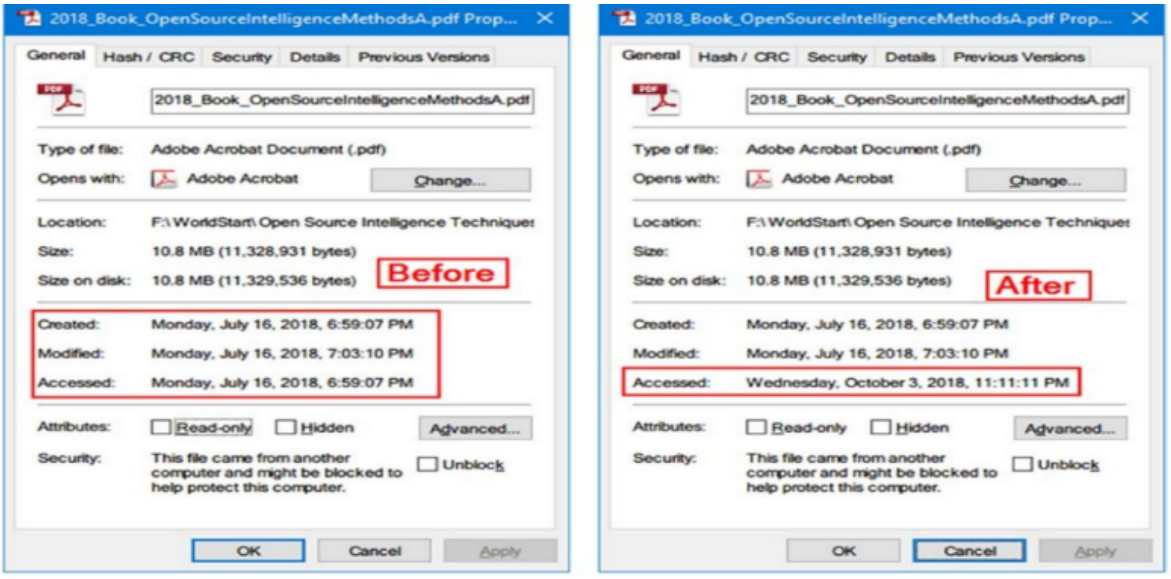
- **Spoofing** is a common trick employed by hackers to pretend to be someone else by changing their IP and MAC address.
- IP spoofing is common and easy to employ, while MAC spoofing hides the identity of the device to a greater extent.

Data Modification:

- **Data Modification** involves manipulating metadata and timestamps of the data.
- Simple timestamp modification can affect the timeline analysis of a case.
- Manipulating metadata can remove forensically significant data.

Files' Metadata Manipulation:

- Metadata timestamps play an important role in computer forensic investigations.
- **BulkFileChanger** is a portable tool from Nirsoft that can modify the main date attributes of any NTFS file, including created/modified/accessed date.
- To change the time attribute using this tool, select the file, and click the “Clock” icon on the program toolbar menu to change attribute values.



Comparison of Date/Time Attribute Values:

- Changing the date/time stamp of files is still an effective method to fight against computer forensics.
- If a professional examiner suspects that a specific file attribute has been changed, they can perform a deep analysis of the file's hidden timestamp attributes located in the Master File Table (MFT).
- This analysis will uncover that the time attributes of the subject file have been changed manually.

Encryption Techniques

Overview:

- **Encryption** is the practice of concealing information by obscuring it, making it unreadable for unintended recipients.
- The process of converting legible data into illegible data is called cryptography.
- With growing concerns about privacy, encryption has become popular.
- Device manufacturers roll out encryption features with their devices to protect users' privacy.
- Advanced encryption protocols and standards are being developed to improve privacy protection.

- Encryption plays a key role in today's IT systems, with both public and private organizations needing to encrypt their data at rest and in transit.
- The widespread use of encryption tools, some with very powerful capabilities, along with their ease of use, makes forensic investigation of encrypted devices difficult, time-consuming, and even impossible without the suspect's cooperation.

Cryptography:

- In cryptography, a **key** is a string of bits used by an algorithm to alter information from plain text into cipher text and vice versa.
- There are two main types of cryptographic systems:
  - **Symmetrical encryption** (Secret Key Cryptography - SKC): Both the sender and the receiver use the same key to encrypt and decrypt the data.
  - **Asymmetrical encryption** (Public Key Cryptography - PKC): This type uses two different keys for encryption and decryption. The encryption key (public key) is available to everyone, while the decryption key (private key) is kept secret.

Full Disk Encryption (FDE):

- **FDE** uses a cryptographic method to encrypt each bit of data on the target drive.
- It has become increasingly required by enterprises and individuals to protect their private data, especially on mobile devices like tablets, laptops, and external drives.
- FDE is integrated into many operating systems (e.g., BitLocker encryption for Windows and FileVault available in Mac OS X 10.3 and later) to protect private user data.
- FDE poses real challenges to computer forensic examiners who become unable to access suspect private data without knowing the decryption key (password).

Windows BitLocker

Overview:

- BitLocker drive encryption is a data protection feature offered by newer editions of Windows beginning with Vista.
- With BitLocker, a user can encrypt the entire disk drive, including the Windows partition and removable USB drives (using BitLocker To Go), securely.
- BitLocker uses the AES encryption algorithm with a default key size of 128 bits, but users can strengthen the encryption by changing the key length to 256 bits for enhanced security.

Trusted Platform Module (TPM):

- BitLocker requires a computer with a **Trusted Platform Module (TPM)**, a small microchip found on the computer motherboard.
- Most modern Windows-certified devices come equipped with this chip.
- The TPM stores BitLocker encryption keys and offers a security mechanism to detect any attempt to change the host OS software or hardware by attackers to decrypt the encrypted drive.

Using BitLocker without TPM:

- If a PC does not contain a TPM chip, BitLocker can still be used, and the encrypted drive can be unlocked using either a password or a key file stored on a thumb drive.

Forensic Considerations:

- Decrypting a machine with BitLocker enabled is nearly impossible.
- When encountering a running machine with BitLocker enabled, it's advisable to capture its RAM memory immediately and then capture the entire hard drive before powering off the machine, as this might be the only chance to get evidence from that computer.

EFS (Encrypting File System):

- EFS is a feature of the Windows NTFS file system.
- It allows a user to enable encryption on a per-file or per-folder basis, or even encrypt the entire volume.
- Using EFS is simple: right-click over the file/folder/volume you want to enable encryption for, select Properties ➤ General tab, click the

"Advanced..." button, and check the option "Encrypt contents to secure data."

- EFS uses a combination of symmetrical and asymmetrical encryption algorithms to encrypt data.
- To secure encrypted data without entering a password, EFS uses the currently logged-on Windows account (username and password) as part of the encryption private key.

Disk Encryption Using Open Source Tools

1. **VeraCrypt** (www.veracrypt.fr/en/Home.html):
    - Free open-source disk encryption software supported on Windows, Mac OSX, and Linux.
    - VeraCrypt allows the creation of hidden volumes within a virtual encrypted disk and hidden operating system partitions.
    - Capable of encrypting entire hard drives and portable storage devices like USB sticks and external HDDs.
2. **CipherShed** (www.ciphershed.org):
    - Open-source encryption software designed for Windows, Mac OSX, and Linux.

Note:
Cracking the encryption of many open-source cryptographic programs is nearly impossible if the offender refuses to disclose the encryption key. As a result, many legal cases have been halted due to the inaccessibility of encrypted files.

Password Cracking

- Digital forensics examiners often encounter encrypted files or volumes during investigations.
- Password cracking tools can be used as a last resort to acquire useful information from suspect encrypted data.
- Popular password cracking software includes:
    - **Cain and Abel** (www.oxid.it/ca_um): Utilizes brute force, dictionary, and cryptanalysis attack techniques, and can sniff passwords from network traffic.

- **Ophcrack** (http://ophcrack.sourceforge.net): Uses rainbow tables to crack Windows passwords.
- **RainbowCrack** (http://project-rainbowcrack.com/table.htm): Speeds up the cracking of password hashes from Windows XP, 2000, Vista, and 7.
- **John the Ripper** (www.openwall.com/john): A password cracker for Unix, Windows, DOS, and OpenVMS.

Cryptographic Anonymity Techniques

- Digital anonymity hides traces between the sender and receiver when communicating over open networks like the Internet.
- It uses encryption algorithms and cryptographic anonymity software to hide the user's identity during transmission.
- Anonymous networks like **TOR** (The Onion Router) help users maintain online privacy by concealing their true IP address from outside observers, including ISPs.
- Other anonymous networks include **I2P** and **Freenet**.

Web Browsers' Private Modes

- Web browsers have introduced Private Browsing (Firefox) or Incognito Mode (Google Chrome) to automatically forget a user’s previous activities.
- Achieving anonymity in cryptographic systems without compromising security is a challenge, but recent results include the design of Pseudonym Systems and Group Blind Digital Signatures.

Report Writing

Understanding the Importance of Reports

1. **Communicate the results of your investigation:**
   - System, network, or digital device.
   - Include expert opinion.
2. **Forensic reports can:**
   - Provide justification for collecting more evidence.
   - Be used at a probable cause hearing.

- Communicate expert opinion.

3. **U.S. district courts require expert witnesses to submit written reports:**
    - State courts are also starting to require them.
4. **Rule 26, Federal Rules of Civil Procedure requires submission of the expert's written report that includes:**
    - Testimony based on sufficient facts or data.
    - Testimony is the product of reliable principles and methods.
    - Witness has applied the principles and methods reliably to the facts of the case.
    - Written report must specify fees paid for the expert's services.
    - List all other civil or criminal cases in which the expert has testified.
5. **Include in the report:**
    - Keep a copy of any deposition notice or subpoena.
        - Jurisdiction.
        - Style of the case.
        - Cause number.
        - Date and location of the deposition.
        - Name of the deponent.
    - Deposition banks.
        - Examples of expert witness' previous testimonies.

Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal:
    - Find information on a specific subject.
    - Recover certain important documents.
    - Recover certain types of files with specific dates and times.
- Before you begin writing, identify your audience and the purpose of the report.

Types of Reports

Digital forensics examiners are required to create different types of reports such as:

1. **Formal Report:**
    - Consists of facts from your findings.
2. **Preliminary Report:**
    - Written or verbal report to your attorney.
3. **Examination Plan:**
    - For the attorney who has retained you.

Verbal Report and Written Report

Verbal Report:

- Less structured.
- Attorneys cannot be forced to release verbal reports.
- Preliminary report:
    - Addresses areas of investigation yet to be completed:
        - Tests that have not been concluded.
        - Interrogatories.
        - Document production.
        - Depositions.

Written Report:

- Affidavit or declaration.
- Limit what you write and pay attention to details.
    - Include thorough documentation and support of what you write.

Examination plan
• What questions to expect when testifying
• Attorney uses the examination plan to guide you in your testimony

• You can propose changes to clarify or define information
• Helps your attorney learn the terms and functions used in computer forensic

Understanding the Purpose of the Report

- It is important to understand the reason why the report has to be written (its purpose).
- Understand what is the subject and who is the audience – all these factors will lead to the selection of the approach, presentation style, and content – and all this is dependent on the purpose behind the creation of the report.
- A report is the record of the detailed account of an investigation and the findings along with evidence, conclusions or analysis, and recommendations, as results of the activities carried out.
- The investigation is commissioned to fulfill a certain objective or need-to-know for which the investigator has made the best effort.
- The investigator must record all this information to make it available to all stakeholders at any time now, or in the near/distant future.
- Hence, there is a need to make another best effort to provide detailed and complete information from and about the investigation, in a simple and logical manner.

Preservation of Lessons Learned:

- The most important reason why reports must have these characteristics is that it preserves lessons learned and approaches to various issues/scenarios/problems.
- If a report is made part of a dynamic (and searchable) document management system or threat library, it can be a valuable resource sometime in the future as an Indicator of Compromise (IoC).
- While the content, language, and presentation of the report are decided based on the purpose being fulfilled by the document, one has to ensure

that the fundamentals (in terms of the expectations of the engagement) are recognized as one begins the task.

Prep Work for Report Writing:

- Preparation for the report should start at the beginning of the project itself.
- Creating a model of the report based on the scope at the start of the project will help set a focused direction for the investigation team.
- Maintain a logbook or notes: based on the report template, plan the manner in which notes will be captured for the investigation activities.
- Conceptualize a naming and storage convention: how the various files will be named and stored on the network.
- Having a dummy report template that provides the work breakdown for the actual investigation will ensure an error-free and scope-compliant completion of project tasks, collection of indicators (and evidence) of successful task completion, thus contributing to higher efficiency.
- At the end of the project, when it is time to prepare the report, the time for preparation will be greatly reduced, and this small action contributes to higher productivity.
- The logbook with notes will be a point of reference in case of any doubts or sticky questions later.

Writing the Report:

- Report writing is a project within the project that can become a chore if not tackled early.
- It's better that it be tackled at every point in a project!
- Start at the beginning itself and update as you proceed in the investigation.
- It needs to capture all nuances of your investigation, evidence collection, analysis, conclusions in terms of the actions performed, the approach and methods employed.
- Keep the end goal (report) in mind when carrying out the investigation/testing activities.
- The nature and layout of the report should be planned and created at the start of the project – when one begins to collect tools, plan techniques,

envisage scenarios, and generally starts working on getting the project into operational mode.

Key Points - Report Writing:

- Keep full text notes while conducting your investigation/tests making it as descriptive as possible.
- Use your personal investigation logbook to record all your activities as they happen.
- Capture and save the output you are viewing or analyzing as evidence to substantiate your analysis later.
- Reference the source of evidence by way of file/folder name and the section that is being referred to in that document.
- Use your favorite notepad (virtual and physical pen+paper) to log your actions and make notes.
- Computer-based notes will help as you will be able to save much time when creating the final reports.
- Classify these notes so that they are aligned with the headings/sections in the report template created at the start of the project.

Structure of the Report

1. **Title Page**
    - Title of the project
    - Report version number
    - Creator's company name
    - Client name
2. **Document Control**
    - Document information (title, date, release version, etc.)
    - Change tracker indicating document version, changes made, and the name of the author/reviewer
3. **Disclaimer**

- Declaration about the ownership of the contents of the document, liability, and restrictions of use

4. **Table of Contents**
    - Generated using the ToC feature of the word processor, hyperlinked to each section in the document
    - Tables generated from the word processor application, hyperlinked to the appropriate section in the document
5. **Introduction**
    - High-level statements providing the context of the engagement, history, expected outcome, etc.
    - Background of the investigation, how the incident was discovered, etc.
6. **Executive Summary**
    - Summary of the findings, impact, and recommendations using simple language understandable by senior management
    - Recommendations presented at a high level
7. **Scope and Objective of the Engagement/Assignment**
    - Reproduction of the scope and objective from the contract to avoid ambiguity
    - Comments related to the scope/objective highlighting changes, challenges, etc.
    - List of changes made to the scope during the engagement, with an explanation
8. **Findings and Analysis**
    - Classification of findings (critical, high, medium, low risk)
    - List of findings with relevant digital evidence, including analysis, impact, remediation, recommendation, etc.
    - Use of tables or sections to segregate the issues
9. **Investigation Report**
    - Names of investigation officers and their duration on the case

- Details of evidence seized, statement of chain of custody, and present location
- Evidence in digital form accompanied by relevant notes, explanations, origin, date, etc.
- Contact information of all concerned persons

10. **Criminal/Forensic Investigation**
    - Description of the crime, location, time, etc.
    - Details of how the investigation was carried out
    - List of evidence artifacts, their description, and present location
    - Statement of compliance with best practices in evidence collection, transport, storage, and retrieval
11. **Approach and Methodology**
    - Graphic visualization of the investigative process (preferably)
    - Explanation of steps in the investigation and analysis, tools and techniques used, industry standards/frameworks referenced, interviews conducted, process issues considered, etc.
12. **Conclusions and Opinion from the Analysis**
    - Analysis and conclusion for each finding
    - Remediation/mitigation/action required strategy for each area
    - Timeline of the analysis and cross-references
    - Evidence examined for each finding and the result
13. **Project Governance**
    - Project charter, vision, and mission
    - Structure of the project team, roles, responsibilities, qualifications/experience of team members, tasks assigned, internal and interim project status reporting and review schedule, project plan
14. **About Us**
    - Information about the investigator/company, capabilities, testimonials, client references, client list, relevant marketing collaterals
15. **Annexures**

- Evidence and reference content shared within the report, including document scans, large tables or figures, extracts from standards, laws, or regulations, etc.

Plan the Coverage

- When preparing the template for your report, map it to the findings or objectives.
- Revisit the mapping at every iteration when preparing a report.
- Consider the following factors when making the conceptual design for the report:
  - **Audience:** Will they understand technical jargon, or do you need a simplified, non-technical document?
  - **Time:** How much time will you have to present your findings?
  - **Review Status:** Is this a draft report for discussion or has it been reviewed?
  - **Format:** Will you provide a printed copy or only a soft copy? Ensure the soft copy is printable without losing formatting.
  - **Design Issues:** Consider fonts, formatting, tabs, etc.
  - **Data Gathering:** How will you obtain the information? Through interviews, etc.?

Conclusion and Analysis

- The report must provide conclusion statements for the scope requirements.
- Conclusion statements are based on the results from the analysis of findings.
- The investigator tabulates the results.
- Conclusions must factually state whether the investigation has substantiated the allegations arising from the incident.
- The statement of substantiation, or lack thereof, must be supported with credible evidence obtained in the analysis.

Recommendations

- Cyber forensic investigators can provide recommendations based on identified risk factors to prevent or reduce the risk of similar incidents.
- Recommendations should logically follow the conclusion relevant to the investigation and be feasible.
- Recommendations could include a review of current policies, retraining staff, or additional training needs.
- The investigator should address all limitations, provide remedial techniques to correct outstanding security deficiencies, or provide techniques to reduce the risk of loss from cyberattacks.
- Additionally, the investigator can prioritize security measures for the client to overcome security deficits.

Characteristics of a Good Report

- Share the report with a trusted peer for feedback, or allow the report to sit for a couple of days before revisiting it.
- Ensure you have time to delay the submission by a couple of days to check the quality of the report.
- Conduct a self-check dispassionately and without prejudice.
- For a "big" report, have it reviewed by senior investigators and incorporate their changes and recommendations.
- Peer review should be done by trusted peers authorized to access the information in your document.

Essential Characteristics in Any Report

- **Factual Presentation:**
  - Findings are presented factually and focused, supported by evidence.
  - Avoid personal bias in opinions stated in the report.
  - The report can only state the obvious and not pass judgment.
- **Clarity and Detail:**
  - Evidence artifacts must be clearly labeled and described.
  - Statements represent actions taken rather than actions not taken.
  - Spell out acronyms at the first use.

- **Organization and Clarity:**
  - Statements, scenarios, and activities must have a lead-in.
  - Facts and findings are distinctly separated from opinions and analysis.
  - Findings and analysis should be easily understood and reproducible by qualified individuals.
- **Conciseness and Coherence:**
  - Statements should be concise, to the point, and coherent.
  - Save the document with a password and share the password through a separate communication.
- **Language and Professionalism:**
  - Communicate in a simple, clear, concise, and coherent language.
  - Findings and analysis are impartial, professional, and do not draw legal conclusions.
  - Provide analysis along with the listing of files and search terms.
  - Be cautious about using absolutes; use phrases like "It is my professional opinion..." to present information as professional opinion.

Document Design and Good Writing Practices - Writing Reports Clearly

- **Consider:**
  - Communicative quality
  - Ideas and organization
  - Grammar and vocabulary
  - Punctuation and spelling
- Use a natural language style.
- Avoid repetition, vague language, and generalizations.
- Use active rather than passive voice.
- Avoid presenting too many details and personal observations.

Structural Guidelines:

- Lay out ideas in a logical order.
- Build arguments piece by piece.
- Group related ideas and sentences into paragraphs.
- Group paragraphs into sections.
- Avoid jargon, slang, and colloquial terms.
- Define technical terms considering your audience.

Project Objectivity:

- Communicate calm, detached observations.

Including Signposts:

- Draw the reader’s attention to a point.
- Assist readers in scanning the text quickly by highlighting the main points and logical development of information.

Generating Report Findings with Forensics Software Tools

- Commercial and open source tools are available for report generation based on your findings.
- Commercial tools include Encase and Access Data FTK.
- Forensics tools generate reports during analysis, but it's your responsibility to explain the significance of the evidence.

Report Formats:

- Plaintext
- Word processor
- Spreadsheet
- HTML format