

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Digital Forensics: Anti Forensics Techniques

*Technical Project
(ACCA7053)*

Applied Computing - WISA

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk



- **Understand Anti-Forensics Techniques**
- ~~**Data Deletion and Recycle Bin Forensics**~~
- ~~**File Carving**~~
- **Password Cracking**
- **Detecting Steganography**
- **Artifact Wiping Techniques**
- **Countermeasures**
- **Understanding Mobile Forensics**

Lab/ Tutorials

- **NA**

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

In continuation to our earlier lectures, where we discussed about various Digital Forensics aspects, today, lets discuss about “Anti-forensics techniques”.

They are used by cyber-criminals to complicate or prevent proper forensics investigation. Cyber-criminals employ these techniques to make evidence collection extremely difficult and to compromise the accuracy of a forensics report.

Let's discuss and try to understand what AFT is? Its Goals, Techniques and concepts around this.

Discuss about various digital forensics capabilities and the appropriate method to acquire data. We shall also discuss the challenges in acquiring data and the area in which keen attention is required. Our discussion this week will cover digital evidences storage formats, Acquisition Methods, Contingency Planning for Data Acquisition, Use and Validate Data Acquisition, RAID Acquisition, Remote Network Acquisition and Forensic Tools used for Data Acquisition.

Recall...

Let's talk about scenarios:

What will happen if the attackers or perpetrators use certain techniques to sidetrack the forensic investigation process

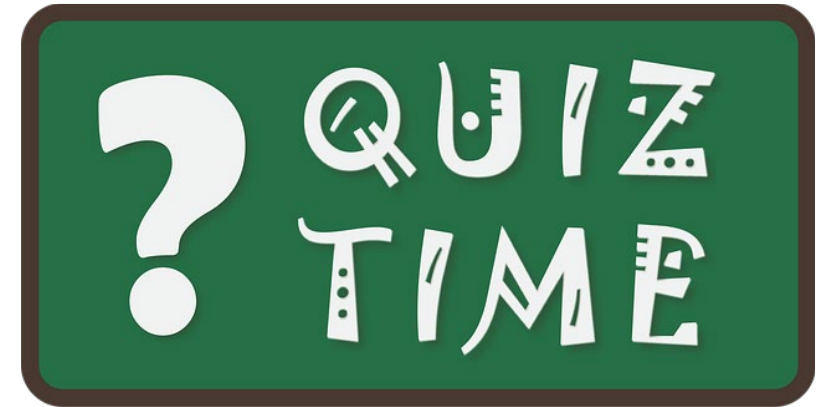
- a. It makes the investigations much harder
- b. It accelerates the forensic investigation process
- c. It raises the risk of investigators being misled by intentional obfuscation
- d. It could result in the loss or destruction of crucial digital evidence

Does use of anti-forensics techniques impact the integrity of digital evidence?

- a. It has no impact on the integrity of digital evidence
- b. It enhances the reliability of forensic findings
- c. It compromises the integrity of digital evidence
- d. It accelerates the forensic investigation process

How can file and data obfuscation impede forensic investigations?

- a. It has no impact on the identification of attackers
- b. It conceals the true nature of files, making them less recognizable
- c. It enhances the accuracy of forensic analysis
- d. It simplifies the interpretation of digital files



Anti Forensics

- Anti-forensics, also known as counter forensics,
- It is a set of techniques that attackers or perpetrators use to sidetrack the forensic investigation process

(try to make the investigations much harder).

- It will negatively affect the quantity and quality of evidence from a crime scene.

(making the forensic investigation process difficult).

- As an investigator, you might have to perform additional steps to fetch the data.

(leading to a delay in the investigation process).

Anti Forensics

Goals

- Interrupt and prevent information collection
- Make the investigator's task of finding evidence difficult
- Hide traces of crime or illegal activity
- Compromise the accuracy of a forensics report or testimony
- Delete evidence that an anti-forensics tool has been run

Techniques

- Data/File Deletion
- Password Protection
- Steganography
- Data Hiding in File System Structures
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption
- Program Packers
- Minimizing Footprint

Anti Forensics – Deletion

Deleting files/data is a common anti-forensics technique used by attackers.

- What happens when a file is deleted from the hard drive?
- How will you try to recover the deleted data?
- What tools will you use?

Discuss with your group and share your thoughts!!!

Duration: 5 Mins Discussion – 5 Mins Presentation

Anti Forensics – Deletion

E5h!

Rings a bell? What is it?

\$BitMap

Rings a bell? What is it?

Recycle Bin

What is it? – Storage Location – Maximum Limit – How it restores?

Anti Forensics – Deletion

- INFO2 is the master database file and is very crucial for the recovery of data.
- It contains various details of deleted files such as their original file name, original file size, date and time of deletion, unique identifying number, and the drive number in which the file was stored.

```
C:\Windows\system32>dir /a /p %systemdrive%\$Recycle
Volume in drive C is Local Disk
Volume Serial Number is 0E67-EEA4

Directory of C:\$Recycle.bin

12/09/2023  13:25    <DIR>        .
12/09/2023  13:25    <DIR>        ..
07/12/2023  06:20    <DIR>        S-1-12-1-6733117
12/09/2023  13:25    <DIR>        S-1-5-18
               0 File(s)                0 bytes
               4 Dir(s)  9,313,476,608 bytes free
```

```
Directory of C:\$Recycle.bin\S-1-12-1-673311706-123

07/12/2023  06:20    <DIR>        .
07/12/2023  06:20    <DIR>        ..
14/11/2023  06:55                270 $I0EBOXE.lck
14/11/2023  06:55                328 $I18LN4C.lck
07/12/2023  06:20                182 $I1XPG46.docx
14/11/2023  07:04                370 $I21Y0B4.lck
14/11/2023  06:55                256 $I3KMVD9.lck
14/11/2023  07:05                292 $IAP249Y
14/11/2023  06:57                236 $IBEHK49
10/11/2023  19:40                256 $IC2FUCT.lck
14/11/2023  07:04                384 $IF27WHD.lck
21/11/2023  14:34                260 $IL0CE51.pdf
07/11/2023  13:46                238 $INM2166.lnk
07/12/2023  06:20                146 $IUACFEC.pdf
14/11/2023  07:03                374 $IUQG0CS.lck
07/12/2023  06:20                130 $IX9E1TH.PNG
14/11/2023  07:05                374 $IY91PG0.lck
14/11/2023  06:55    <DIR>        $R0EBOXE.lck
14/11/2023  06:55    <DIR>        $R18LN4C.lck
06/11/2023  17:57            203,332 $R1XPG46.docx
14/11/2023  07:04    <DIR>        $R21Y0B4.lck
14/11/2023  06:55    <DIR>        $R3KMVD9.lck
14/11/2023  07:05    <DIR>        $RAP249Y
14/11/2023  06:57    <DIR>        $RBEHK49
Press any key to continue . . .
08/11/2023  21:30    <DIR>        $RC2FUCT.lck
14/11/2023  07:04    <DIR>        $RF27WHD.lck
21/11/2023  06:03            272,770 $RL0CE51.pdf
12/09/2023  15:49            2,432 $RNM2166.lnk
21/11/2023  06:08            164,726 $RUACFEC.pdf
14/11/2023  07:03    <DIR>        $RUQG0CS.lck
21/11/2023  20:07            130,516 $RX9E1TH.PNG
14/11/2023  07:04    <DIR>        $RY91PG0.lck
12/09/2023  13:10                129 desktop.ini
               21 File(s)            778,001 bytes
               12 Dir(s)  9,315,942,400 bytes free
```

Anti Forensics – Deletion

Recycle Bin Forensics

- The original files pertaining to the \$I files are not visible in the Recycle Bin folder when \$I file is corrupted or damaged
(The attacker/insider deletes \$I files from the Recycle Bin)
- Check for the \$R files in the Recycle Bin directory
(to counter the anti-forensic technique used by the attacker)
- If the metadata files related to the original files are not present in the folder,
 - Recover the deleted files from Recycle Bin for further analysis.

Anti Forensics – Deletion

Deleting files/data is a common anti-forensics technique used by attackers.

- During your investigation, the file system metadata is not present. What will you do? Or How will you proceed further?

Discuss with your group and share your thoughts!!!

Duration: 5 Mins Discussion – 5 Mins Presentation

File carving refers to a technique that is used to recover deleted/lost files and fragments of files from the hard disk when file system metadata is missing.

Anti Forensics – Deletion

File Carving Techniques

- helps to ***extract data from a storage medium without any support from the file system*** used in the creation of the file.

- Understand – Unallocated Space

- Observe – Characteristics of file headers and footer

identify the files using file header and footer (the first and last few bytes)

- Identify – the elements

- Fragments of data present

- Deletion Technique used

- Type of Storage



Tools such as 010 Editor, CI Hex Viewer, Hexinator, Hex Editor Neo, Qiew, WinHex, etc.



File carving does not require file system structure to recover data from the disk whereas file recovery requires knowledge of the file system structure to recover deleted data.

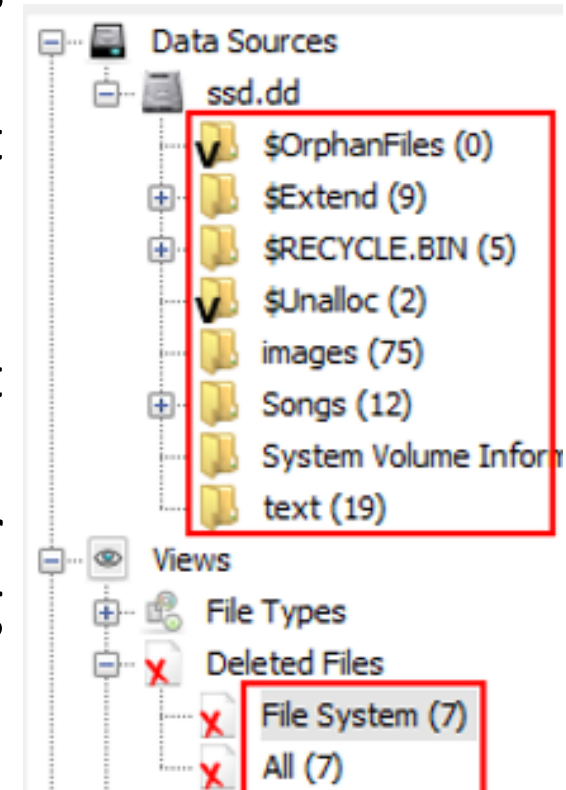
Anti Forensics – Deletion

File Carving – Windows SSD/HDD File

- **The recovery of deleted files in SSD becomes difficult as TRIM is enabled by default** (*mostly not possible*)
- With Autopsy, the file names are listed but the deleted data cannot be recovered
- Check status of the SSD's TRIM feature
- In TRIM disabled SSD's, you can perform file carving to recover lost data from the drive

Discuss with your group about TRIM Feature and share your thoughts!!! – Recommendations on Disabling and Enabling TRIM Feature. What it is?

Duration: 5 Mins Discussion – 5 Mins Presentation



Recall...

Using File Recovery Tools like Recover my Files etc, you can recover

- a. Files even if emptied from Recycle Bin Data
- b. Files after accidental format or reinstallation
- c. Files after a Hard Disk Crash
- d. Files after a partitioning error
- e. Files from RAW hard drives
- f. Files from HD, Memory Card, USB, Floppy or any media

Using Autopsy Tool, which is an end-to-end platform

- a. Timeline Analysis
- b. Hash Filtering
- c. Keyword Search
- d. Web Artifacts
- e. Data Carving
- f. Multimedia



Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack is applicable in two situations:

- In cryptanalysis (*it helps find out the decryption key for obtaining the plaintext from the ciphertext*)
- In computer security, (*it helps avoid authentication and access to a computer by guessing passwords*)

Dictionary Attacks

Methods to improve the success of a dictionary attack:

- Using a greater number of dictionaries, (technical dictionaries and foreign dictionaries etc)
- Using string manipulation

Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack

- involves testing all possible keys to recover the plaintext, which is the base for producing a particular ciphertext.
- Brute-force attacks need more processing power compared to other attacks. The detection of keys or plaintext at a rapid pace in a brute-force attack results in breaking of the cipher.

Brute Force Attacks

Some considerations for brute-force attack are as follows:

- It is a time-consuming process
- It can eventually trace all passwords
- An attack against Networking Technology (NT) hash is much harder against LAN Manager (LM) hash

Anti Forensics – Passwords

- **Cleartext Passwords**
- **Obfuscated passwords**
- **Password hashes**

This attack

- Is possible with some credible information about the password
- *Eg: Password Rule, Algorithms, Strings, Characters etc*

Rule Based Attack

- This technique involves brute-force, dictionary, and syllable attacks
- The attackers may use multiple dictionaries, brute-force techniques, or simply try to guess the password.

Anti Forensics – Passwords

BIOS Passwords

- A BIOS password protects the computer system from unauthorized access.
- In the BIOS setup, there are three types of passwords
 - System Password
 - Admin Password
 - HDD Password
- Bypassing BIOS password can unlock System and Admin password but not the HDD password
- Using a manufacturers' backdoor password to access the BIOS password
- Using password cracking software
- Resetting the CMOS using the jumpers or solder beads
- Removing the CMOS battery for at least 10 minutes

Anti Forensics – Steganography



Medium/ Message



Embedding
Function



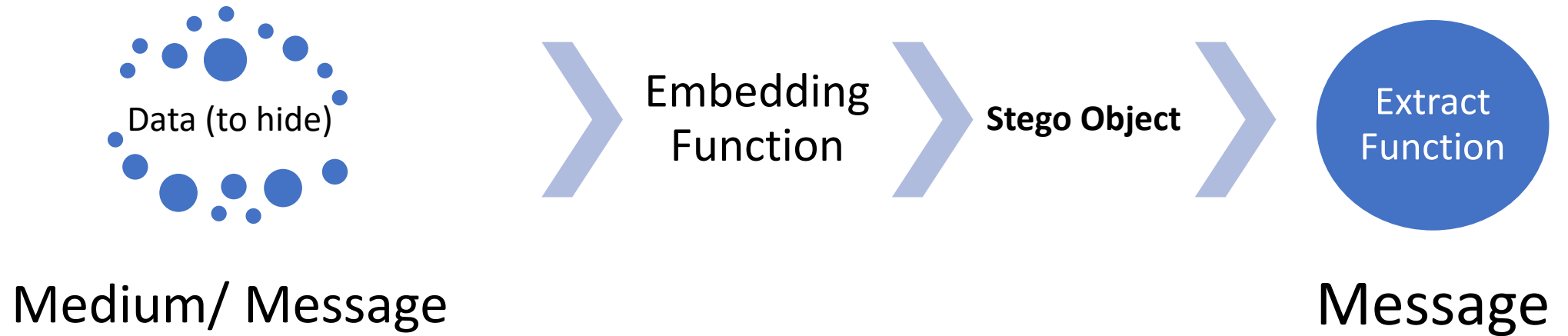
Stego Object



Message

- Steganography refers to the art of hiding data “behind” other data without the target’s knowledge
- It replaces bits of unused data in usual files such as graphic, sound, text, audio, video, etc. with some other surreptitious bits. The hidden data can be plaintext or cipher text, or it can be an image.
- Utilizing a graphic image as a cover is the most popular method to conceal data in files.
- Steganography is preferred by attackers because, unlike encryption, it is not easy to detect.

Anti Forensics – Steganography



Steganalysis

- Process of discovering the existence of the hidden information in a medium.
- Steganalysis is the reverse process of steganography
- A Steganalyst tries to detect the hidden messages embedded in images, text, audio and video carrier mediums using steganography.
- Locate encoded hidden message and recovers it if recovery is possible.
- It can identify the hidden message by comparing the differences in the bit patterns of files.

Anti Forensics – Steganography

Steganalysis

- Detection and Distortion of messages.
 - In the detection phase, relationships between the steganography tools, stego-media, cover, and message is observed.
 - In the distortion phase, the stego-media is manipulated to extract the embedded message and decides whether it is of any use or whether it should be removed altogether.
- The first step in steganalysis is to discover a suspicious image that may be harboring a message.
- There also are other types of attack against steganography such as **Stego-only, Known-stego, known-message, known-cover, chosen-message, and chosen-stego.**

Anti Forensics – Steganography

Steganalysis

- Challenges
- Suspect information stream may or may not have encoded hidden data
- Efficient and accurate detection of hidden content within digital images is difficult
- The message might have been encrypted before being inserted into a file or signal
- Some of the suspect signals or files may have irrelevant data or noise encoded into them

Anti Forensics – Steganography

Text Files

- The positions of characters are altered in the text files to hide the data.
- Investigators can detect these changes by looking for text patterns, the language used, height of lines and unusual number of blank spaces.
- A simple word processor can reveal text steganography sometimes as it displays the spaces, tabs, and other characters that distort the text's presentation during text steganography.

To detect text steganography

- Unusual patterns used in stego-object
- Appended extra spaces and invisible characters

Anti Forensics – Steganography

Image Files

- The information that is hidden in the image can be detected by observing changes in size, file format, last modified time stamp, and color palette of the file.

The following points can help detect image steganography:

- Too many display distortions in images
- Sometimes images may become grossly degraded
- Detection of anomalies when evaluating original images and stego-images with respect to color composition, luminance, pixel relationships, etc.
- Exaggerated "noise"
- Observe the LSB's
 - By using statistical analysis on the LSB, the difference between random values and real values can be identified.

Anti Forensics – Steganography

Audio Files

- Audio steganography is the process of embedding confidential information such as private documents and files in digital sound.
- Statistical analysis methods can be used for detecting audio steganography as it too modifies LSB.
- Especially, inaudible frequencies should be scanned for hidden information.
- Odd distortions and patterns can also indicate the presence of secret data.

Anti Forensics – Steganography

Video Files

- Detection of secret data in video files involves a combination of methods used in image and audio files.
- Special code signs and gestures help in detecting secret data.
- Both audio and video steganography are quite difficult to detect, as compared to the other types.
- Moreover, it is very hard to detect any type of steganography that has been well executed.
- However, careful analysis of audio and video signals for hidden information may increase the chances of detection.

Anti Forensics – Data Hiding

- Data hiding is making the data inaccessible.
- NTFS-based hard disks contain
 - bad clusters in a metadata file as \$BadClus and the MFT entry 8 represents these bad clusters.
 - \$BadClus is a sparse file, which allows attackers to hide unlimited data as they can allocate more clusters to \$BadClus to hide more data.
- Some hard disks have a **host protected area** (HPA) in which the developers can store data they want to protect (and hide) from normal use.
- The attackers use DPAs, DCOs, and slack spaces to hide data, which will not be visible to either BIOS or OS and requires special tools to detect and view.

Anti Forensics – Data Hiding

- ADS, or an alternate data stream, is a NTFS file system feature that helps users find a file using alternate metadata information such as author title.
- It allows files to have more than one stream of data, which are invisible to Windows Explorer and require special tools to view.
- Files/ Data/ Executables may be hidden and accessed when required using CL - Utility.
- An ADS contains metadata such as access timestamps, file attributes, etc.
- Investigators need to **find ADS and extract the information**.
 - Retrieving ADS can offer raw details of the file and execution of malware.
 - Use software tools to identify ADS files and extract the additional streams.

Anti Forensics – Program Packers

- Program packers are to hide their data. (*similar to cryptography*)
- The packers compress the files using various algorithms. Unless the investigators know the tool that has been used to pack the file and have a tool to unpack it, they will not be able to access it.
- Evidence files may be hidden into containers, (*making them hard to detect*)
- As an Investigator,
 - mount compound files.
 - Program packers that are password-protected is a challenge
 - You need to first decrypt the password to unpack the file.
- Intruders use packers to hide attack tools by reverse engineering or scanning techniques.

Anti Forensics – Program Packers

- Packers can carry executable files, malware, and other attack elements.
- In case of executable files, these programs carry unpackers built into them, which unpack the file when user tries to run it and installs the executable on the host system.
- Some of the widely used packers are UPX, PECompact, BurnEye, Exe Stealth Packer, Smart Packer Pro, etc.
- You can dynamically analyze these packed executables by running them in a controlled environment and observing their behavior.
- Packed programs that are not password-protected are vulnerable to static analysis.

Anti Forensics – Countermeasures

- Train and educate the forensic investigators about anti-forensics
- Validate the results of examination using multiple tools
- Impose strict laws against illegal use of anti-forensics tools
- Understand the anti-forensic techniques and their weaknesses
- Use latest and updated CFTs and test them for vulnerabilities
- Save data in secure locations
- Use intelligent decompression libraries to defend against compression bombs
- Replace weak file identification techniques with stronger ones

Recall...

What is the primary goal of mobile forensics?

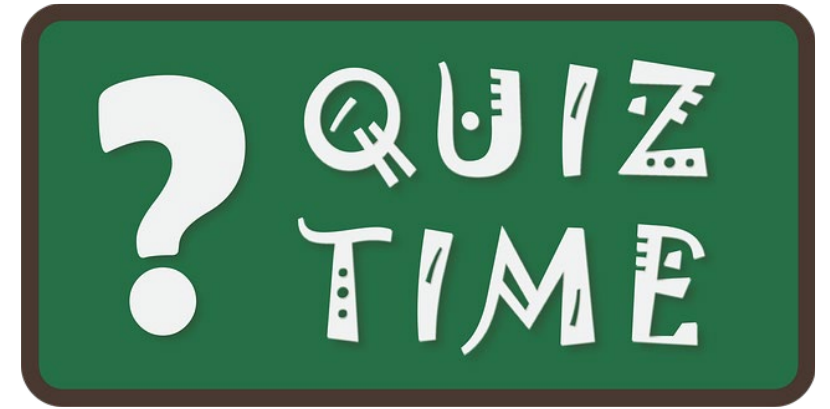
- a. Enhancing mobile device performance
- b. Investigating and analyzing digital evidence on mobile devices
- c. Recovering lost contacts from mobile phones
- d. Improving mobile network connectivity

What is the first step in the mobile forensic process?

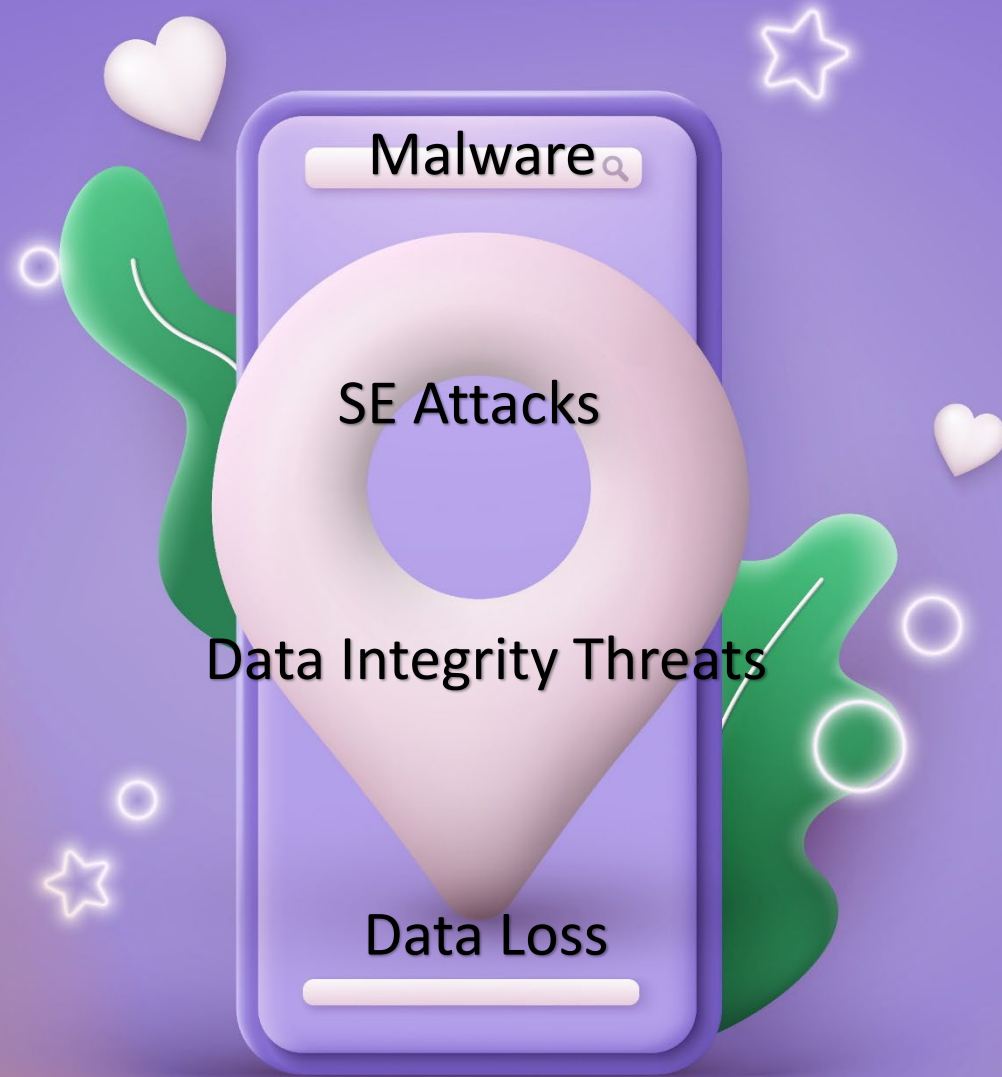
- a. Analyzing data
- b. Acquiring the device
- c. Presenting findings
- d. Collecting evidence

Which of the following is a volatile data source in mobile forensics?

- a. SIM card
- b. Internal storage
- c. External SD card



Web and Network based Attacks



Resource Abuse

Understanding Mobile Device Forensics

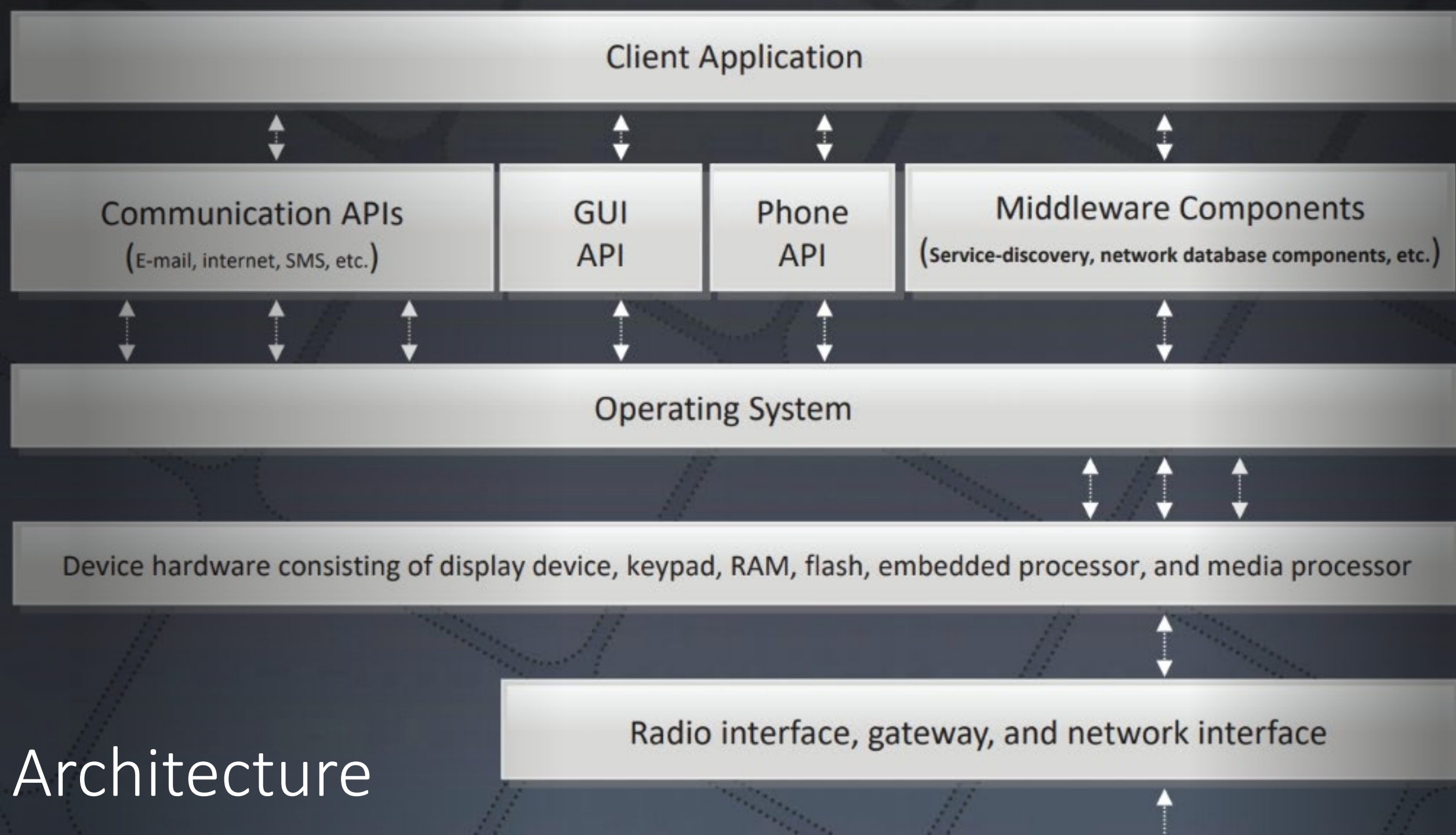
- Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions.
- It includes recovery and analysis of data from mobile device
 - internal memory, SD cards
 - SIM cards
- Mobile forensics aims to trace the perpetrators of crimes that involve the use of mobile phones

Mobile Hardware and Forensics

- Mobile device forensics is highly dependent on the underlying hardware of mobile devices
- Investigators need to take different approaches for mobile forensics depending upon the mobile hardware architecture
- Proprietary hardware of mobile devices makes forensics acquisition difficult
- Knowledge of mobile hardware also becomes essential in case of a broken or damaged device when it is not possible to access device using data ports

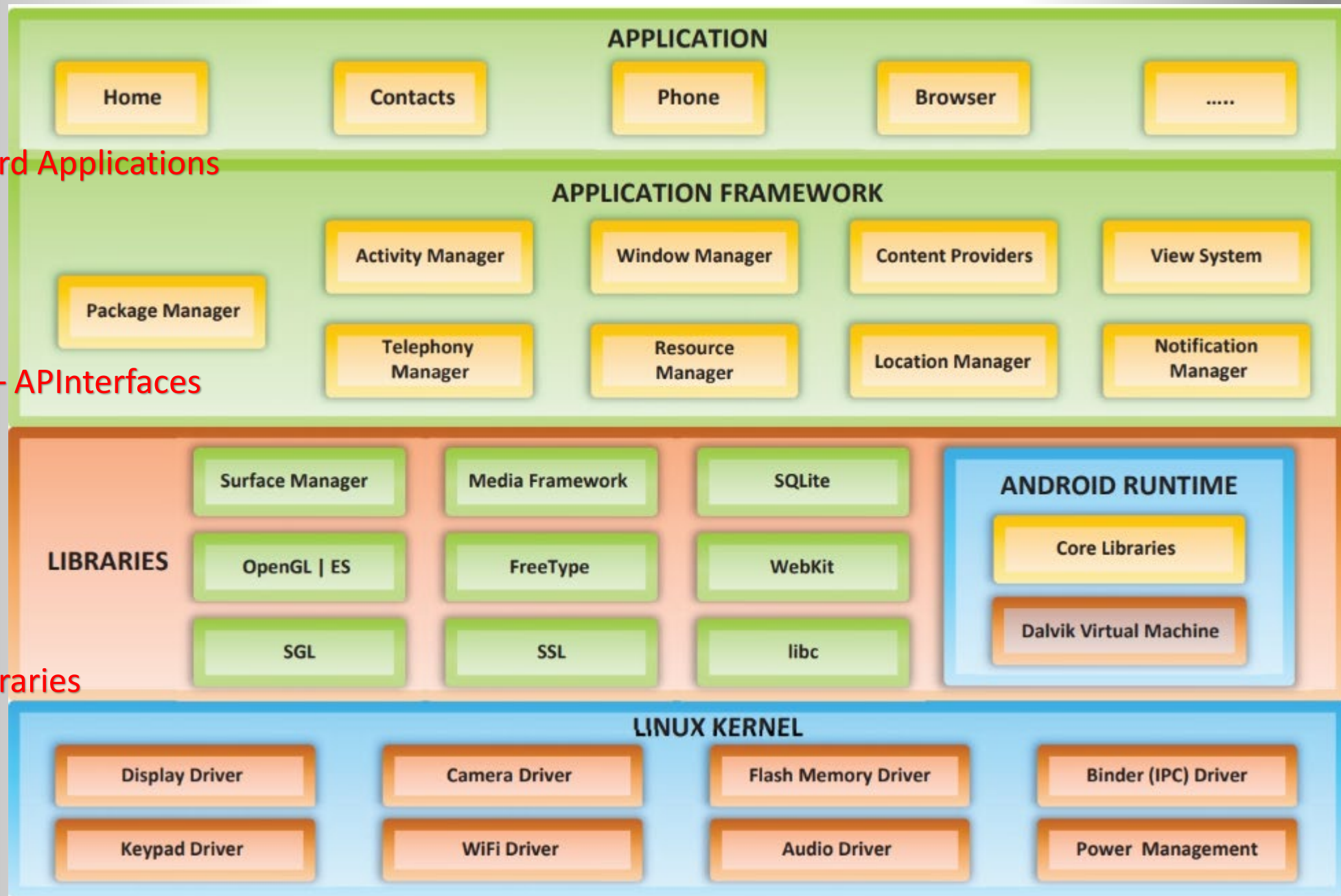
Mobile Hardware and Forensics

- A mobile operating system determines the functions and features available on mobile devices
- It manages the communication between the mobile device and other compatible devices
- This diversity in the mobile OS architecture may impact forensics analysis process
- Investigators require knowledge of underlying OS, architecture, and file systems of mobile device under investigation
- Knowledge of mobile OS booting process helps investigator to gain lower-level access



Architecture

Android Architecture



User defined – Standard Applications

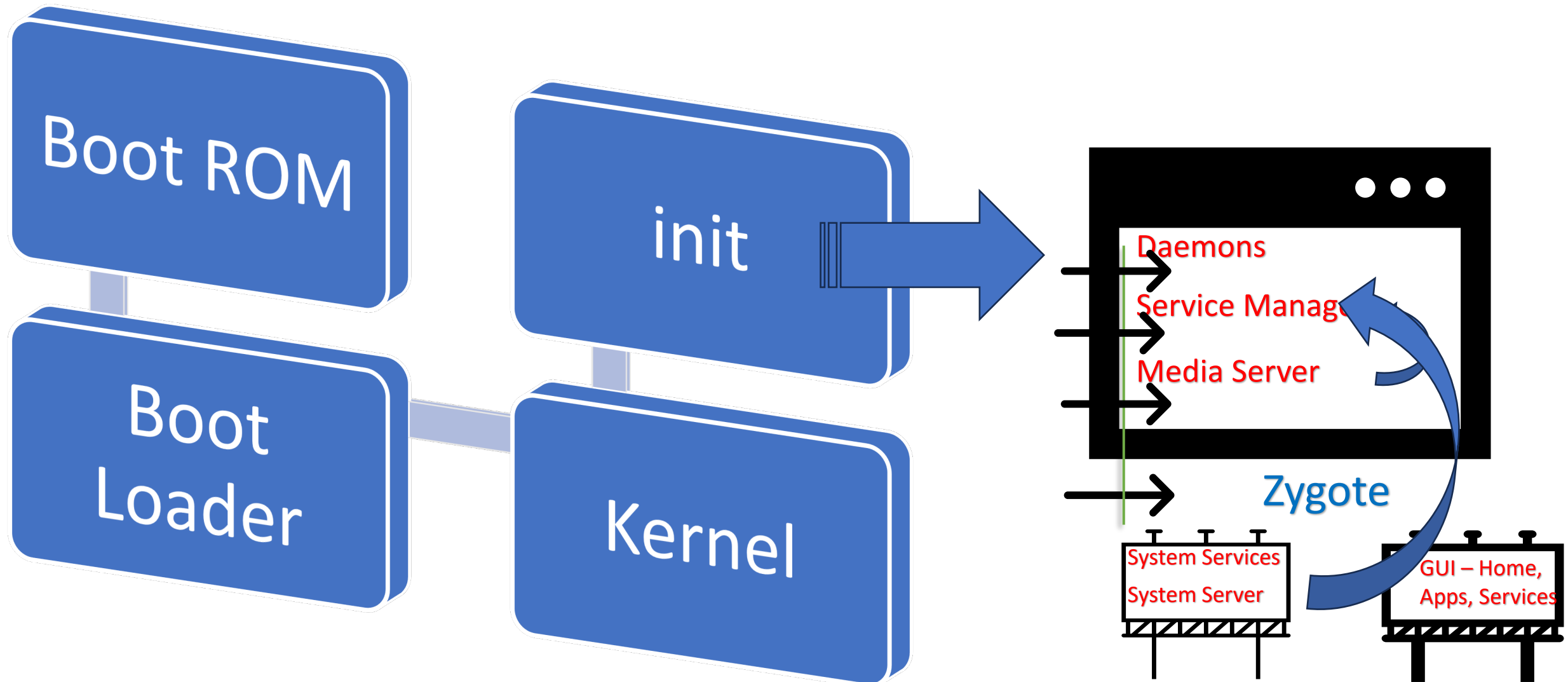
Support Applications – API Interfaces

Custom Built, Native Libraries

Interacting with the Hardware

Architecture

Android Boot Process



iPhone Boot Process

Provides frameworks for iPhone app development

Map Kit, iAD, Game Kit, Events (Touch),
View Controllers, and UIKit

Provide audio, video, animation, and graphics capabilities
to the iPhone

Provide audio, video, animation, and graphics
capabilities to the iPhone

Provides foundation to upper layers

Threading, File Access, Preferences, Collections
(NSArray, NSDictionary, NSSet), Networking,
Address Book, and High Level Features
(iCloud, InApp Purchase, and SQLite)

Provides low-level services

Cocoa
Touch

Media
Services

Core
Services

Core OS

iPhone Hardware

Key Locations

Internal Memory

- RAM, ROM or flash memory (NAND / NOR) is used to store mobile phone's OS, applications and data

SIM Card

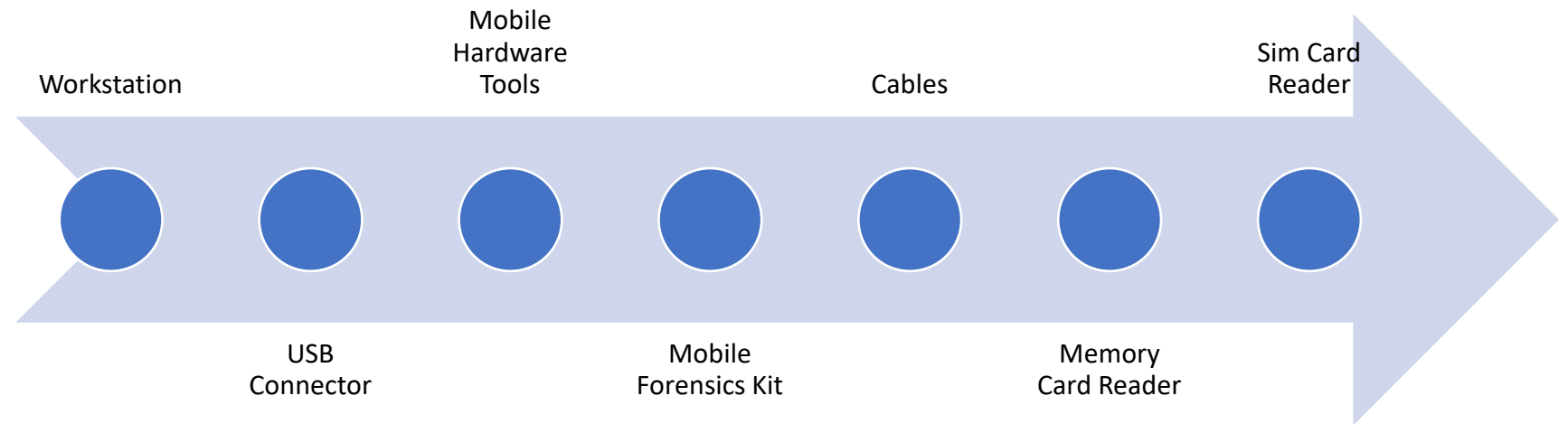
- Stores personal information, address books, messages, and service-related information

External Memory

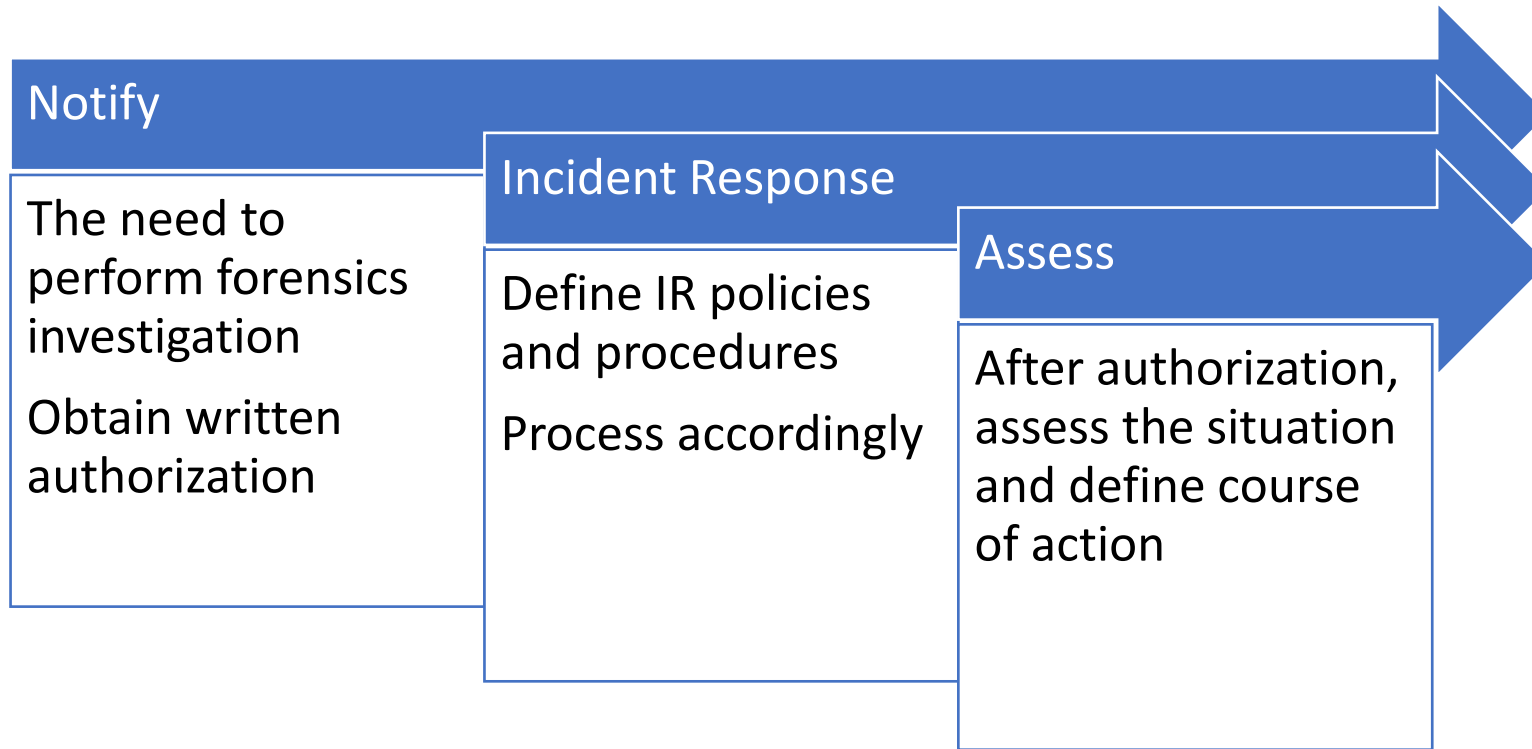
- Stores personal information such as audio, video, images, etc.

Investigations

- Build a Forensics Workstation
- Build the Investigation Team
- Review Policies and Laws
- Notify Decision Makers and Acquire Authorization
- Risk Assessment
- Build a Mobile Forensics Toolkit



Investigations



Risk Assessment

- To prevent new data from contaminating the evidence, **seal the device** in an isolation container properly
- **Do not use plastic bags** to carry out seized mobile device. Use recommended isolation containers
- **Consider the power state** of mobile device seized
- Expiration of the battery would be disastrous as important data may reside in **battery-dependent volatile memory**
- Handle and transport mobile devices carefully as they are **fragile** and can be **easily damaged**



Tools

- Selecting correct tools is the key.
- The mobile forensics toolkit includes both hardware and software tools required to recover and analyze data from mobile devices

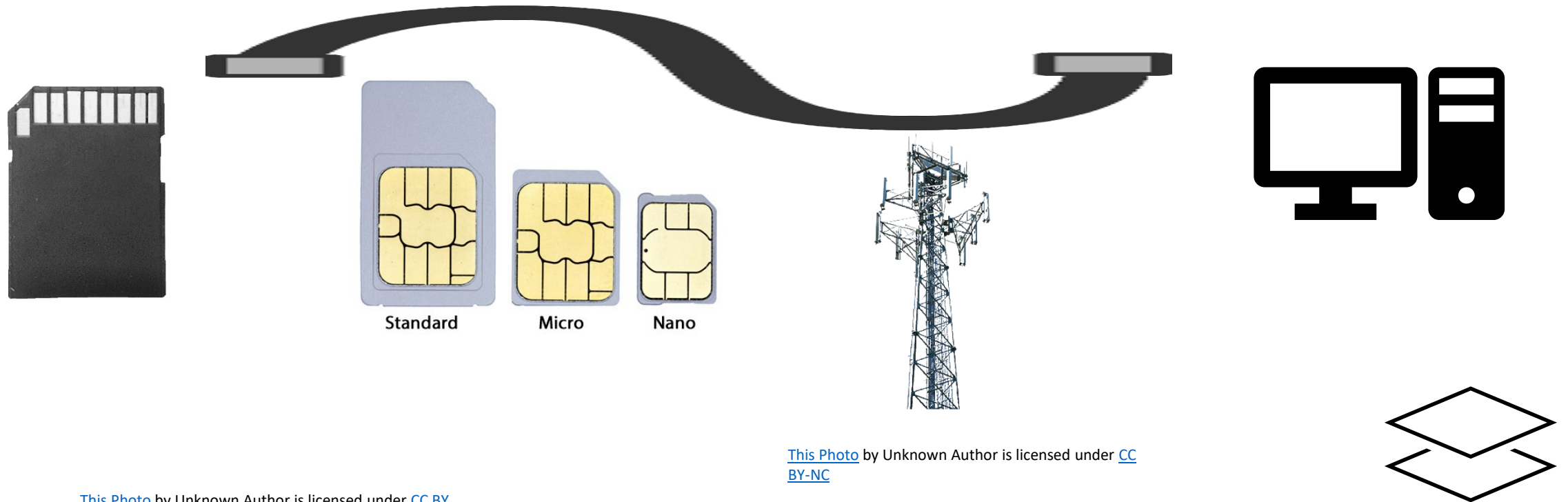
Few Tools are

- Cellebrite UFED System
- Secure ViewKit for Forensics
- DS-Device Seizure & Toolbox
- USB reader for SIM cards
- iGo
- DC Lab Power Supply 0 15V/3A
- Digital Display with Backlight
- Paraben's Phone Recovery Stick

- SEARCH Investigative Toolbar
- BitPim
- Oxygen Forensics Analyst
- Paraben's Sim Card Seizure
- MOBILedit! Forensic
- TULP2G
- iDEN Phonebook Manager
- SUMURI's PALADIN
- XRY Logical & XRY Physical

Process

- Selecting correct tools is the key.
- The mobile forensics toolkit includes both hardware and software tools required to recover and analyze data from mobile devices



Process

- **Collect and Preserve the Evidence**
- Document the Scene
- Imaging and Profiling
- Acquire and Analyze Information
- Generate Report

- Protect the integrity of traditional and electronic evidence
- Prevent unauthorized users from entering at the scene and touching the evidence
- Collect all the electronic devices found at the crime scene
- Check whether the mobile device is connected to a computer
- Confirm the power state of the devices by checking flashing light
- Collect non-electronic evidence such as written passwords, handwritten notes, and computer printouts

Process

- **Collect and Preserve the Evidence**
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - Generate Report
- The aim of the preservation step is to seize the suspect mobile phone and its associated peripherals without altering the data in it
 - It is the first step carried out prior to the actual investigation
 - It involves discovering, recognizing, documenting, and collecting the digital evidence obtained at the crime scene

Process

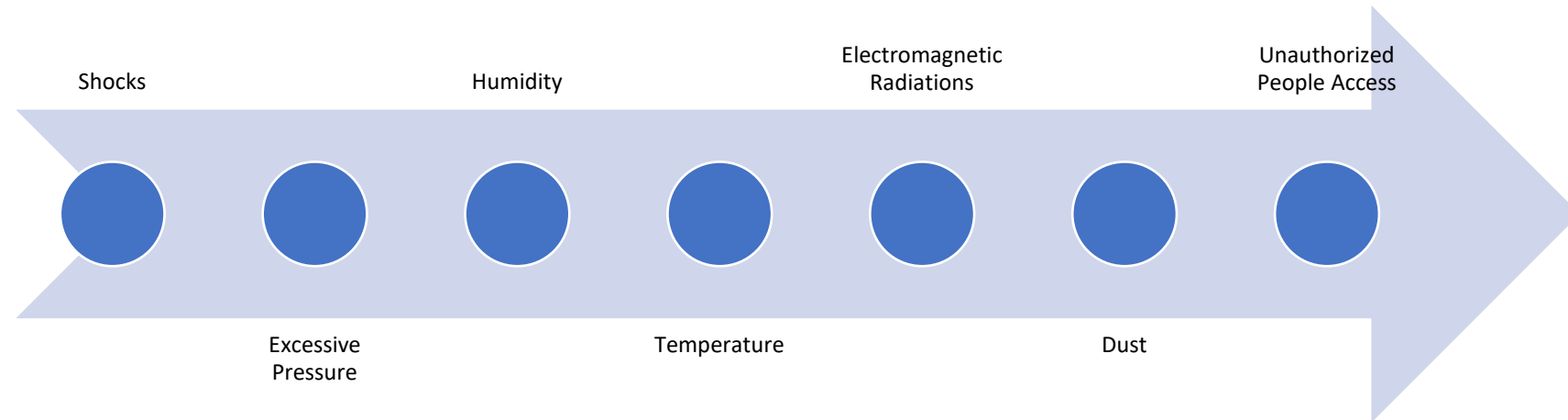
- Collect and Preserve the Evidence
- **Document the Scene**
- Imaging and Profiling
- Acquire and Analyze Information
- Generate Report
- Document all the electronic devices found at the crime scene
- Take photographs of all evidence at the scene, and write notes on what you have seen on the screen
- Document the state of the device during seizure
- Document any activity on the electronic devices found at the crime scene

- 🧠 Identify the brand, model, operating system, and the network service provider
- 🧠 It helps to choose an appropriate forensics tool for the data acquisition
- 🧠 Identify the type of connection used to connect to the forensics workstation
- 🧠 It may be a cable, Infrared, or Bluetooth
- 🧠 This depends upon the phone, forensics tool and acquisition conditions
- 🧠 Based on the mobile device model and the connection, select a forensics tool that have the following capabilities:

Usable, Comprehensive, Accurate, Deterministic, Verifiable

Process

- If the device is "ON", do not turn it "OFF". Turning it off could activate lockout feature
- Write down all information on display (photograph if possible)
- Power down prior to transport (take any power supply cord present)
- If the device is "OFF", leave it "OFF"
- Turning it on could alter evidence on device (same as computers)
- Mobile device should be protected from signal interruption, and data overwriting
- Use signal containment devices and bags to achieve and maintain network isolation



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - **Imaging and Profiling**
 - Acquire and Analyze Information
 - Generate Report
- A forensics investigator **should not directly work on the original evidence.**
 - He/she should instead create a forensics image of the mobile device obtained at the crime scene
 - File carving and forensics analysis is conducted on forensics image in order to leave the actual evidence intact
 - Possible mobile phone storage for imaging:
 - Mobile phone memory
 - SD card memory
 - SIM card memory

Process

- Collect and Preserve the Evidence
- Document the Scene
- **Imaging and Profiling**
- Acquire and Analyze Information
- Generate Report

Locks

- Mobile phones use three types of phone lock schemes to prevent unauthorized user access
- If phone device obtained at a crime scene is in a locked state, the challenge of unlocking it arises
- Forensics investigator needs to bypass the phone lock to forensically investigate the mobile phone

ByPassing – Locks/ Passwords

Connect the device to the forensics workstation through USB Launch adb shell using ViaExtract Remove password.key file from android directory

Enable USB Debugging

Jail Break (If Necessary)

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- The seized mobile phone undergoes data acquisition and forensics imaging process at the forensics workstation
 - During the acquisition process, all possible data from internal and external memory of the mobile phone is extracted for forensics analysis
 - Data acquisition and forensics analysis requires:
 - Unlocking the device
 - Rooting or Jailbreaking of the device
 - Enabling USB debugging mode in the device

Process

- Collect and Preserve the Evidence
- Document the Scene
- Imaging and Profiling
- **Acquire and Analyze Information**
- Generate Report
- Cellular Data Acquisition
- SIM File System Acquisition
- Logical Acquisition
- Physical Acquisition
- File System Acquisition

Code Division Multiple Access (CDMA) | Enhanced Data Rates for GSM Evolution (EDGE) |

Integrated Digital Enhanced Network (iDEN) | General Packet Radio Service (GPRS) | Global System for Mobile Communications (GSM)

High Speed Downlink Packet Access (HSDPA) | Time Division Multiple Access (TDMA) | Universal Mobile Telecommunications System (UMTS) | Unlicensed Mobile Access (UMA)

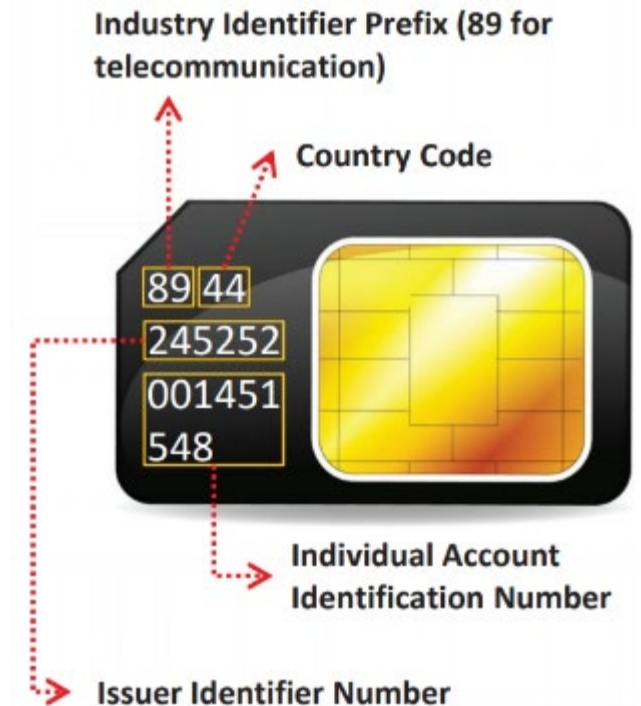
Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
 - Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
-
- Service provider data can act as back up evidence for the mobile forensics' investigator
 - It is useful when the attacker or owner of the mobile phone has deleted call history and/or text messages from the device to wipe out evidence
 - It can also be required in the following cases:
 - When recovering of deleted data is not possible
 - When location-based services are not turned ON in the phone

Process

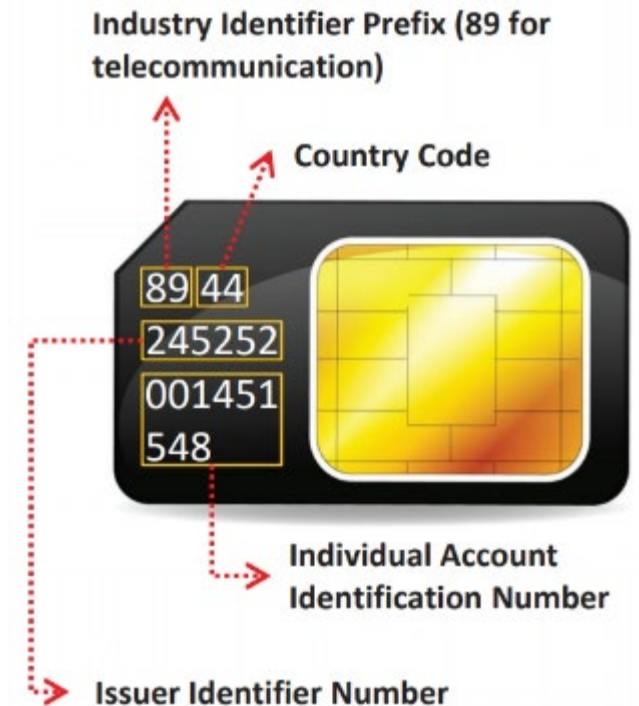
- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition

- SIM is a removable component that contains essential information about the subscriber
- It has both volatile and non-volatile memory
- The file system of a SIM resides in non-volatile memory
- The SIM's main function entails authenticating the user of the cell phone to the network to gain access to subscribed services



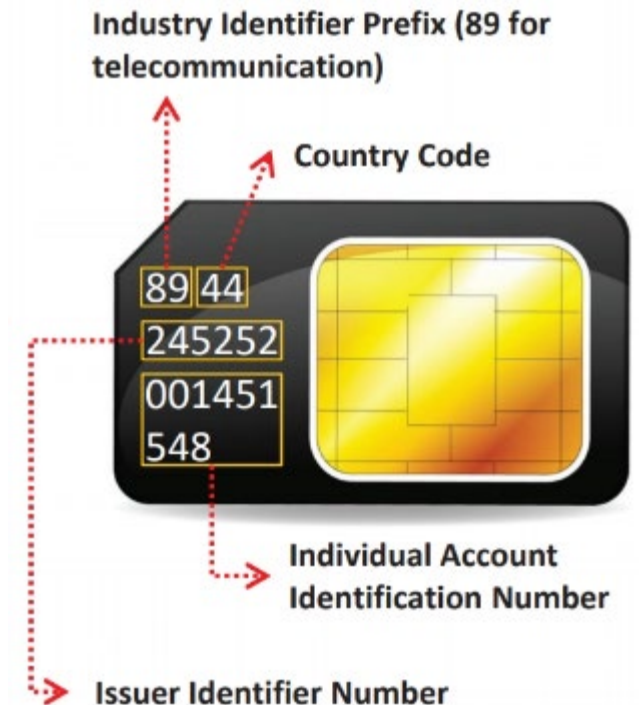
Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
-
- IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices
 - First eight digits, known as the Type Allocation Code (TAC), give the model and origin
 - For powered on GSM and UMTS phones, the IMEI can be obtained by keying in *#06#
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
-
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
-
- Duplicating a SIM card for further investigation in order to avoid accidental tampering of original SIM data



Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
- Logical acquisition involves creating a bit-by-bit copy of logical storage of mobile phone
 - Logical storage includes data stored within mobile files and directories
 - Mobile data is extracted through mobile device's OS, using a known set of commands

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
- Physical acquisition involves creating a bit-by-bit copy of data stored in the internal flash memory of mobile phone
 - It extracts maximum amount of data directly from the mobile device's flash memory(s)
 - It can also extract hidden or deleted data from flash memories
 - It is the most difficult extraction as manufacturers of mobile devices often do not allow arbitrary reading of the device's memory

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- Cellular Data Acquisition
 - SIM File System Acquisition
 - Logical Acquisition
 - Physical Acquisition
 - File System Acquisition
- Logical acquisition **cannot help in extracting deleted data from the file and directory of mobile phone**
 - File system acquisition helps in recovering and extracting deleted data
 - Moreover, the file system acquisition shows file structure, application data, and web artifacts available in the mobile

Process

- Collect and Preserve the Evidence
- Document the Scene
- Imaging and Profiling
- **Acquire and Analyze Information**
- Generate Report

- File carving involves recovering deleted or hidden data from mobile phones
- Persons involved in the incident may delete certain data, and wipe out potential evidence from the mobile phone
- You should try to recover such deleted data for forensics analysis

Use file carving tools to recover:

- Keyboard caches
- Deleted photos
- Browser cache items and other personal data
- Call history data
- Map tiles from maps application
- Cached, and deleted email messages
- SMS messages with timestamp data Deleted voicemails

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - **Acquire and Analyze Information**
 - Generate Report
- After logical, physical, and file system acquisition, forensics examination and analysis is carried out on the extracted data
 - It involves **finding out source of evidence from information obtained by extraction**

The forensics Examiner should investigate:

- ❖ Mobile phone data artifacts such as contacts, call history, browser, SMS/MMS, and geolocation
- ❖ Raw data artifacts
- ❖ Timeline of activities

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - **Generate Report**
- The results obtained in all the steps of forensics process needs to be presented in a **prescribed standard format**
 - A forensics report should include the complete forensics investigation process followed along with supporting documents such as **photographs, notes, and signatures of specialists**
 - A forensics tool is used to prepare reports to present the forensics result in a prescribed format

Your report must include:

Summary, Objectives, Date and time the incident allegedly occurred, Date and time the incident was reported to agency personnel, Name of the person or persons reporting the incident, Examination start date and time, The physical condition of the phone, Photos of the phone and individual components, Phone status when received turned on or off, Make and Model, Mobile Subscriber International ISDN Number (MSISDN), Integrated Circuit Card ID (ICCID), Service Provider Name (SPN), Abbreviated dialing numbers, Last Numbers received.

Process

- Collect and Preserve the Evidence
 - Document the Scene
 - Imaging and Profiling
 - Acquire and Analyze Information
 - **Generate Report**
- The results obtained in all the steps of forensics process needs to be presented in a **prescribed standard format**
 - A forensics report should include the complete forensics investigation process followed along with supporting documents such as **photographs, notes, and signatures of specialists**
 - A forensics tool is used to prepare reports to present the forensics result in a prescribed format

Your report must include: Last Numbers dialed, Missed calls, Short Message Services (SMS), Calendar entries, Photographs stored in the handset, Video stored in the handset Smart Media/ Compact Flash, MMS, International Mobile Subscriber Identity (IMSI), Mobile Country Code (MCC), Mobile Network Code (MNC), Mobile Subscriber Identification Number (MSIN), Preservation of the evidence, Investigative techniques, Tools used for the acquisition, Tools used for the examination, Data found during the examination, Notes from peer review, Supporting expert opinion

Disks

Discussion Point

- With all the knowledge from this session, draft your plan to collect the evidence (mobile phone).



What is a common challenge in mobile forensics related to encryption?

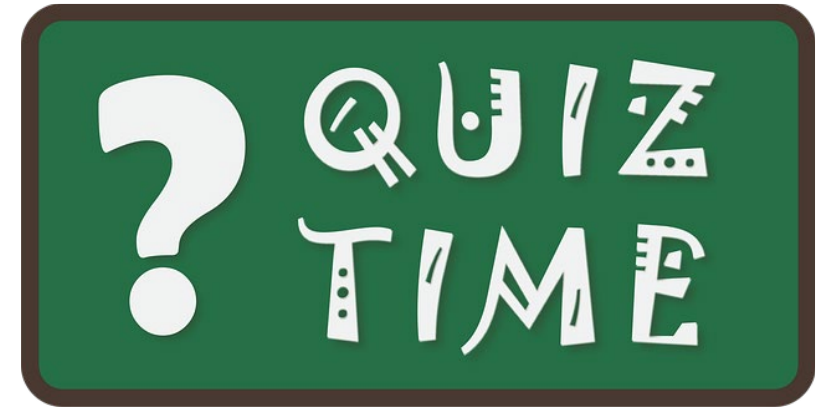
- a. Lack of available tools
- b. Overabundance of data
- c. Complexity of mobile interfaces
- d. Use of encryption to secure data

What does the term "Jailbreaking" refer to in the context of mobile forensics?

- a. Breaking into a physical jail
- b. Unlocking a mobile device's bootloader
- c. Bypassing software restrictions to gain access to the device's file system
- d. Hacking into a social media account

In mobile forensics, what does the acronym IMEI stand for?

- a. International Mobile Equipment Identity
- b. Integrated Mobile Encryption Interface
- c. Internet Message Encryption Index
- d. Internal Memory Erasure Identifier



What is the role of the Chain of Custody in mobile forensics?

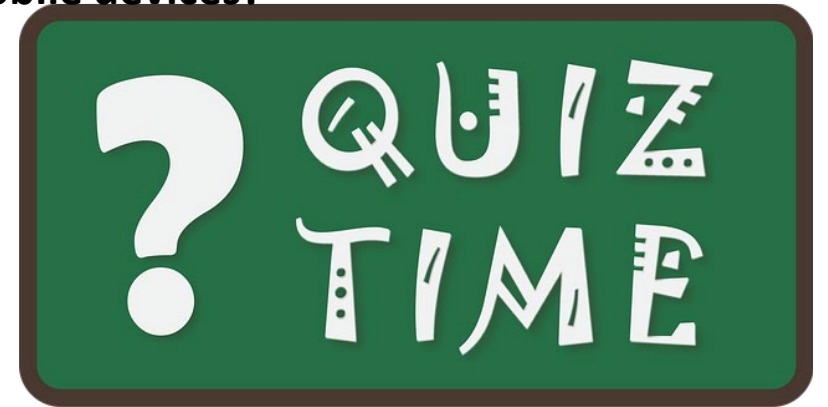
- a. Ensuring the integrity of digital evidence
- b. Investigating network traffic
- c. Conducting mobile device acquisitions
- d. Analyzing cloud storage

Which of the following is a forensic technique for recovering deleted data on mobile devices?

- a. Overwriting data
- b. Data carving
- c. Mobile cloning
- d. Encryption

What is the significance of the mobile device's timestamp in digital forensics?

- a. It indicates the device's manufacturer.
- b. It provides information about the cellular carrier.
- c. It helps establish a timeline of events during an investigation.
- d. It decrypts encrypted data.





Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Any Questions?

Digital Forensics
(ACCA7053)

Applied Computing - WISA

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk



References

- EC Council – CHFI V10 Ebook
- Bossler, Adam M._ Holt, Thomas J._ Seigfried-Spellar, Kathryn C – Cybercrime and digital forensics_ an introduction-Routledge (2017_2018)
- Digital Forensics and Incident Response:
A practical guide to deploying digital forensic techniques in response to cyber security incidents
- Jason Sachowski - Digital Forensics and Investigations – People, Process, and Technologies to Defend the Enterprise
- Whitcomb, C. (2007). The evolution of digital evidence in forensic science laboratories. The Police Chief, 74(11).

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

Digital Forensics
(ACCA7053)

Applied Computing - WISA