DIGITAL EVIDENCE

Why is it important?

UNODC
United Nations Office on Drugs and Crime

- **Work Experience**

I’m currently a Cyber Crime Consultant at UNODC

Lectured at Catholic University of Eastern Africa.

I have worked in different areas in the IT field

- **Education**

MSc. Advanced Security and Digital Forensics- Edinburgh Napier University, UK

MSc. Cyber Security (GCHQ Certified) –Edinburgh Napier University, UK

BSc. Information Technology- JKUAT Kenya

- **Skills:**

Host-based Forensics, Digital Forensics, Cloud Forensics, Penetration Testing, Network Security, Security Audit, Digital Investigations, Offensive Security, Ethical Hacking.

DIGITAL EVIDENCE

An Introduction by Claudia
@claudiajematia

CONTEXT:

FIRST SESSION

- Introduction – Digital Evidence
- First Responder
- ACPO Guidelines
- Triage
- Mobile Phone Evidence
- Analysis Of Digital Evidence

DIGITAL EVIDENCE

- What is a Digital Evidence?

  -Digital Evidence: also known as electronic evidence, is data or information that exist in digital form.

  -Evidence that ‘can prove’ or ‘reveal the truth’ about a crime and can be relied upon and used in a court of law.

TYPES OF DIGITAL EVIDENCE

- There are different types of digital evidence offering unique type of information. They are broadly categorized into two groups:

1**. Evidence from data at rest** – (obtained from any device that stores digital information).

2**. Data intercepted while being transmitted** (interception of data transmission/communications)

THE LOCARD’S EXCHANGE PRINCIPLE

- The Locard's Exchange Principle states that "with contact between two items, there will be an exchange."

- For Example, burglars will leave traces of their presence behind and will also take traces with them.

SOURCES OF DIGITAL EVIDENCE

- Internet
- Computers
- Portable Devices

1. INTERNET

- Evidence obtained from the internet includes information collected from website communications, emails, message boards, chat rooms, file sharing networks and intercepted communications.
- Message boards and chat rooms contain wealth of information both in real time as well as archives.
- However, due to jurisdiction challenges, some culprits may not be easily tracked and identified. Also, some websites are designed for user anonymity making culprit identification more difficult.

2. COMPUTERS

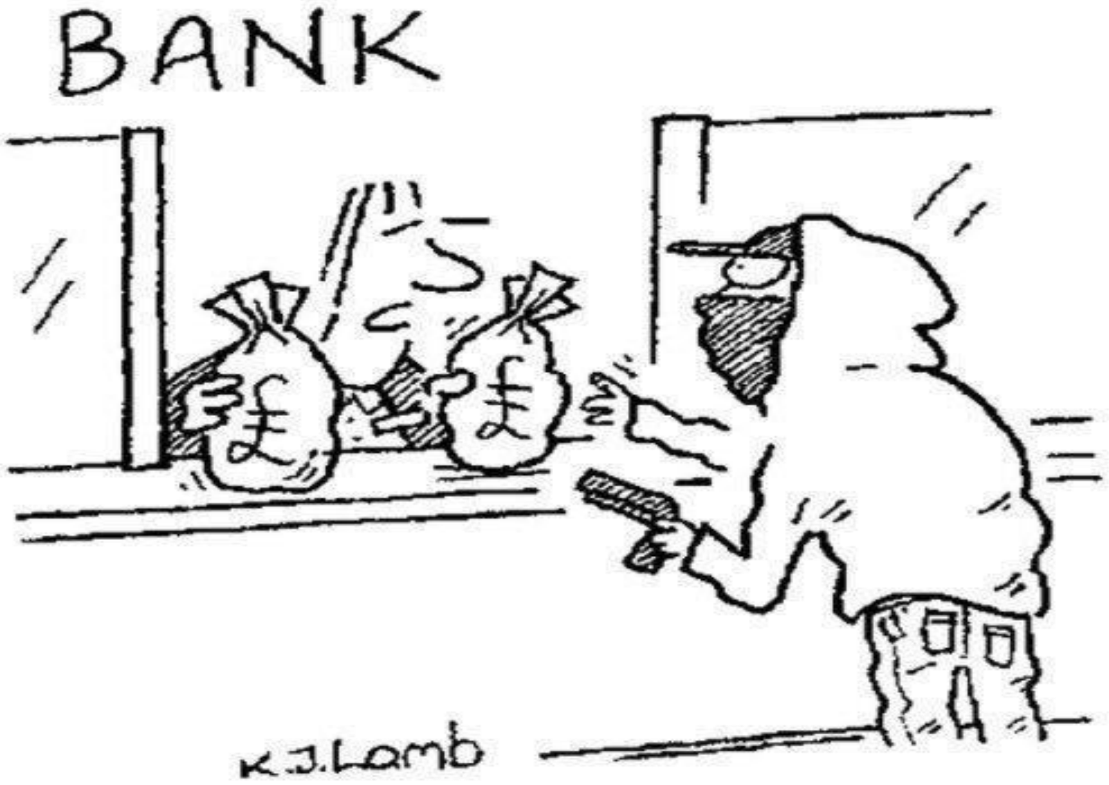
- Computers are a repository of information with evidence obtained using special extraction methods.

- Though information may overlap with internet sources, computers may provide unique and notable pieces of evidence including time stamps, IP addresses, information about VPN and MAC addresses.

3. PORTABLE DEVICES

- These include information sourced from cell phones, tablets and other handheld devices or gadgets.

- Because of the dependency society has on portable devices, these have become the lead source of digital evidence in many court cases.



‘Are you aware that you can now do all of this online?’

Digital Evidence Guide for First Responder

- First Responder is the first person that is responsible to react towards an incident. To be a First Responder, one must know the steps taken to preserve the evidence as best as one could.
- The First Responder should be prepared and his actions should be planned. Deliberate, rush or hurried actions could damage potential evidence. He/she should have a first responder toolkit and a predetermined incident response plan to follow regardless of the type of data being collected.

EVIDENCE ACQUISITION FOR MOBILE DEVICES

STEP 1 : Document the device and all collection procedures

-Photograph

-Video

-Sketch

-Notes

-Chain of custody

Blackberry Classic phone

EVIDENCE ACQUISITION FOR MOBILE DEVICES cont.

STEP 2: Determine if the device is on or off

- Look for lights
- Listen for sounds
- Feel for vibrations or heat

Android unlock screen

EVIDENCE ACQUISITION FOR MOBILE DEVICES cont.

STEP 3: If the device is off, do not turn it

- Collect and package **(see Step 5)**
- Ask for password/pass pattern
- Transport **(see Step 6)**

Apple iPhone 6 and 6 Plus

EVIDENCE ACQUISITION FOR MOBILE DEVICES cont.

STEP 4: If the device is on, proceed with caution.

Important:

The two most significant challenges for officers seizing mobile devices are:

1. Isolating the device from cellular and Wi-Fi networks.

2. Obtaining security passwords or pass patterns for the device so the evidence can be examined forensically.

STEP 4: Cont..

- Always ask if there is any security feature enabled on the phone. These can include passwords (simple or complex), security/wiping apps, pass patterns, or biometrics (facial scan).
- Confirm the password or pass pattern. Turning the device off could result in the loss of evidence. The best option is to keep the device powered, unlocked (if locked, collect any available passwords, PIN codes, or security unlock information), and in airplane mode until it is in the hands of an experience technician.

EVIDENCE ACQUISITION FOR MOBILE DEVICES cont.

STEP 5: Collection and Package

Note:

- You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from smartphones and mobile devices.
- Work with crime scene technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the data on the device. Be sure to advise forensic examiners in advance of submission of the possible existence of hazardous material on the device.

GET THIS

Close for RF Protection
KeyShield
RF Protected
Faraday Bag
faradaybag.com
faradaybag.com
faradaybag.com

EVIDENCE ACQUISITION FOR MOBILE DEVICES cont.

Step 6 – Transport

- Deliver evidence to a secure law enforcement facility or digital evidence/forensic laboratory as soon as possible
- Protect from temperature extremes and moisture

ACPO GUIDELINES

- Association of Chief Police Officers' (ACPO) is a practical guide aimed at police officers, police staff, and private sector investigators working in conjunction with law enforcement.
- These guidelines are essential to agencies and corporate entities involved in the investigation and prosecution of incidents or offences which require the collection and examination of digital evidence.

ACPO GUIDELINES - PRINCIPLES

Principle 1: No action taken by law enforcement agencies or their agents, should change data held on a computer or storage media, which may subsequently be relied upon in court.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

ACPO GUIDELINES – PRINCIPLES …CONT.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

FORENSIC TRIAGE OF MOBILE DEVICES

- Forensic triage/preliminary analysis is emerging as a tool to help investigators find evidence more quickly using fewer resources and taking a load off of the overburdened forensic expert.
- Mobile triage is a technical process to provide information for the forensic examination, but does not involve the evaluation of digital evidence

Why prioritize?

- The goal of digital triage is to rapidly review many potential sources of digital evidence for specific information and prioritize for easier analysis.
- The prioritization process is used to determine which devices should be examined first.
- This is important, particularly in life-and-death scenarios when there is need for urgency.

IMPORTANCE OF FORENSIC TRIAGE

1. Field Agents/First Responders can avoid over-collecting on scene, reducing the amount of computers being held in secure storage waiting for investigation.
2. First responders, field agents, and detectives on the scene can gain valuable evidence in real time, allowing them to focus their on-site investigation.
3. The forensic investigators can be given a clear direction in which to focus their investigation, allowing them to build their cases faster.

MOBILE PHONE EVIDENCE

- A Mobile phone can reveal much about a person’s likes, dislikes, habits, hidden secrets, associations and more!
- **Mobile phone data is “Digital DNA”**
- Mobile phone data is so vital that an attorney can use it in just about any case they encounter.
- A mobile phone can also reveal potential witnesses and victims that were not previously known.

Information That Resides On Mobile Devices (A Non-exhaustive List)

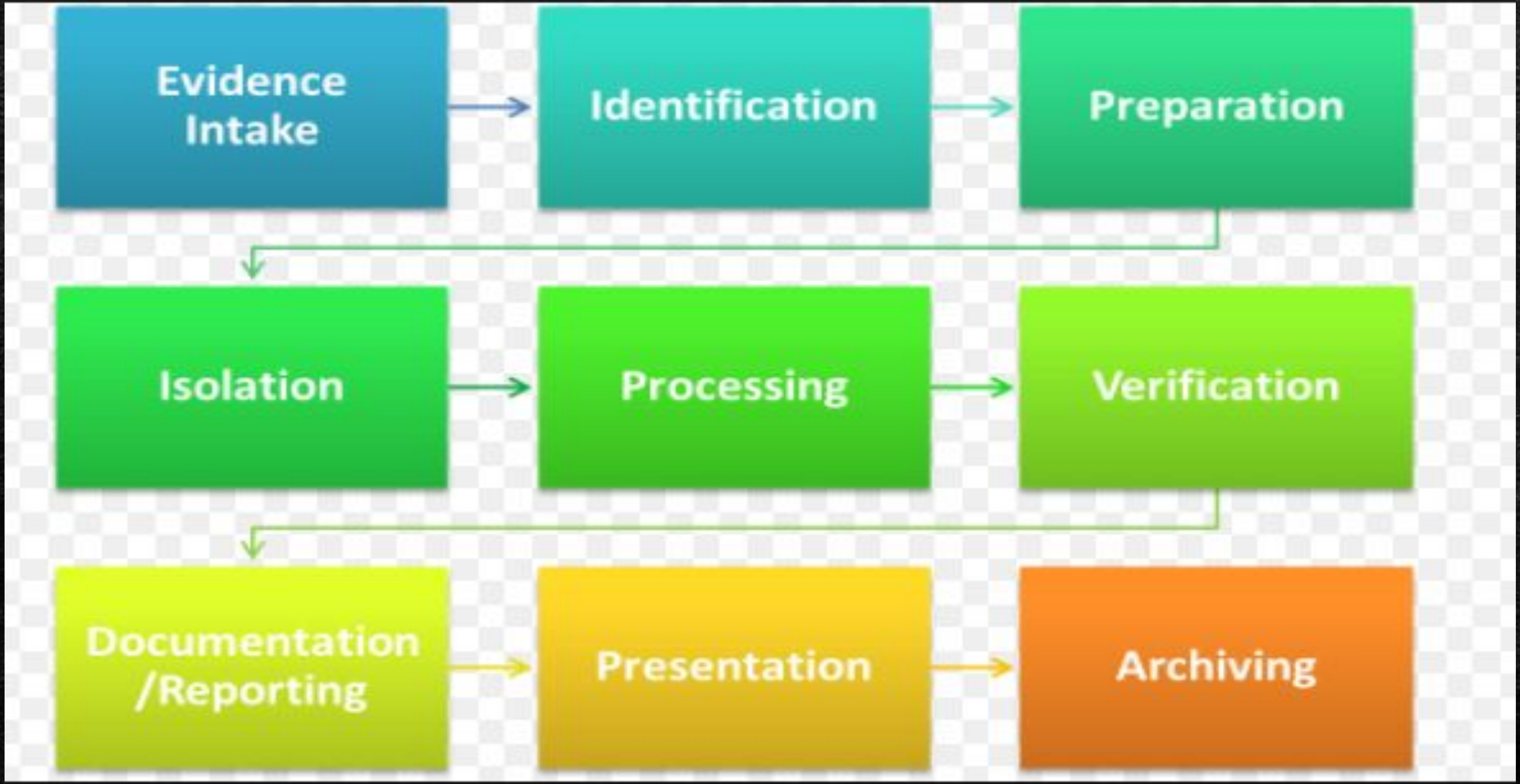
- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones

Information That Resides On Mobile Devices (A Non-exhaustive List)… Cont.

- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related location data, Wi-Fi connection information
- User dictionary content
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above

MOBILE PHONE EVIDENCE EXTRACTION PROCESS

- Evidence extraction and forensic examination of each mobile device may differ.



Evidence Intake

Identification

Preparation

Isolation

Processing

Verification

Documentation /Reporting

Presentation

Archiving

ANALYSIS OF DIGITAL EVIDENCE

There are three main approaches to the extraction of data from a device:

1. Logical Acquisition
2. File System Acquisition
3. Physical Acquisition

1. LOGICAL ACQUISITION

- Logical acquisition allow the retrieval of manually accessible data.
- However, it may not provide deleted data.

Some of the data it does provide include:

1. International Mobile Equipment (IEM). This is used to identify the device not the owner. Stolen devices can be blocked from a network using this number.
2. Integrated Circuit Card ID (ICCID) from the last SIM card. It is unique for each SIM card.
3. Call logs, SMS, MMS, Geodata, Contacts (address book)
4. International Mobile Subscriber Identity (IMSI) from the last SIM card.

2. FILE SYSTEM ACQUISITIONS

- This type of acquisition can retrieve additional data. This is dependent on the type of mobile device and forensic tool capabilities.
- It is more likely to recover deleted data.

Some of the additional data that may be acquired includes:

1. Security codes
2. Database entries
3. Bluetooth pairings
4. Previously inserted ICCID/IMSI

3. PHYSICAL ACQUISITIONS

- Physical acquisition retrieve all of the data on a mobile device, including hidden, deleted and corrupted data.

Physical extraction involves either:

- Cable connection and specific software. For example, Cellebrite UFED Physical Analyzer, XRY Physical)

THREE METHODS TO PRESERVE DIGITAL EVIDENCE FOR COMPUTER FORENSICS

- The most effective methods to ensure legal admissibility while preparing to engage a forensic analyst include the following:
- **Drive Imaging**

  - Forensic image of all digital media helps retain evidence for the investigation.
- **Hash Values**

  - The purpose of a hash value is to verify the authenticity and integrity of the image as an exact duplicate of the original media.
- **Chain of Custody**

  - It is essential to remember chain-of-custody paperwork. This artifact demonstrates that the image has been under known possession since the time the image was created. Any lapse in chain of custody nullifies the legal value of the image, and thus the analysis.

The Use of Social Media Evidence…cont.

In this regard, a distinction must be made between:

- **Evidence in the public domain**

Where information has been posted onto the internet, Facebook (and the user does not have any privacy settings), Twitter or a blog, it is easily accessible and can be exploited by any internet user without authorization.

- **Improperly obtained evidence**

By contrast, the use of evidence that is not in the public domain and that has been obtained in an improper manner would result in the infringement of a legal right or the contravention of a law.

How to Capture Evidence

- Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence.
- Many mobile devices store information about the locations where the device traveled and when it was there.
- Even photos posted to social media such as Facebook may contain location information.

How to Capture Evidence…..cont.

- Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken.

- By gaining a **subpoena** (a writ ordering a person to attend a court) for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

REPORTING:

- It is important to note that a proper forensic report *is not a **legal document*** — it is a technical and scientific document. It does not contain arguments; it contains facts, namely the immutable truths found within the 1s and 0s of digital evidence.
- After the analysis is complete, a forensic neutral will compile a report to outline the processes used and findings.

GENERAL GUIDELINES FOR FORENSIC REPORTS

- Brief summary of information
- Tools used in the investigation process, including their purpose and underlying assumptions associated with the tool
- Repository –(For example person A’s Mobile device)

  - Summary of evidence found in person A’s mobile

  - Analysis of relevant evidence on person A’s mobile device such as email history, internet search history, USB registry analysis
- Repetition of above steps for other evidence items (Laptops, tablets)
- Recommendations and next steps for counsel to continue or cease investigation based on the report findings.

THANK YOU!

ANY QUESTIONS?