
RAMA UNIVERSITY

www.ramauniversity.ac.in

# FACULTY OF EGINEERING & TECHNOLOGY

## MOBILE SECURITY

## LECTURE -7

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

# OUTLINE

- What are the Steps in the Mobile Forensics Process?
- Examination & Analysis
- The New Digital Reality of Mobile Forensics
- MCQ
- References

# WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

## 6. Examination & Analysis

As the first step of every digital investigation involving a mobile device(s), the forensic expert needs to identify:

- ❑Type of the mobile device(s) – e.g., GPS, Smartphone, tablet, etc.
- ❑Type of network – GSM, CDMA, and TDMA
- ❑Carrier
- ❑Service provider (Reverse Lookup)

# WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

## 6. Examination & Analysis

The examiner may need to use numerous forensic tools to acquire and analyze data residing in the machine. Due to the sheer diversity of mobile devices, there is no one-size-fits-all solution regarding mobile forensic tools. Consequently, it is advisable to use more than one tool for examination. Access Data, Sleuth kit, and Encase are some popular forensic software products that have analytic capabilities. The most appropriate tool(s) is being chosen depending on the type and model of mobile device.

Timeline and link analysis available in many mobile forensic tools could tie each of the most significant events, from a forensic analyst's point of view.

All of the information, evidence, and other findings extracted, analyzed, and documented throughout the investigation should be presented to any other forensic examiner or a court in a clear, concise, and complete manner.

# WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

## The New Digital Reality of Mobile Forensics

“On May 17, 2015, a biker gang shootout erupted at the Twin Peaks Restaurant near Waco, Texas, killing nine and injuring dozens. More than a hundred mobile phones were recovered from the incident, setting the wheels in motion for one of the state’s largest and most challenging investigations to date.

The events that unfolded at the Twin Peaks restaurant thrust McLennan County law enforcement into a new urgent reality.

Within days of the decision to deploy, [the Celebrity's New UFED Analytics Platform] allowed both investigators and prosecutors to import and decode all extracted mobile digital forensics data from one centralized location for fast and efficient analysis. Call records, text messages, photos, videos and social media posts could be filtered by keywords and tagged for other members of the investigative team to view instantly.

“… [the solution] allowed us to go back and more quickly comb through the data to find the bigger picture details we needed to confirm the motives, plans and goals of these motorcycle organizations [,]” said the McLennan County prosecutor.”

# WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

## App Risks

- Apps are the primary attack surface for mobile devices
- Major security issues
  - Fragmentation
  - Sensitive information leakage
  - "Secure" on-device storage
  - Weak authentication
  - Failure to properly implement specs
  - BYOD

# WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

## Open vs. Closed Platforms

- ❑Apple is closed and more secure
  - ✓Code must be signed by Apple to run
  - ✓Has Address Space Layout Randomization (ASLR)
  - ✓Better code sandbox
  - ✓No shell
- ❑Android is open and less secure
  - ✓Custom OS versions for each device manufacturer
  - ✓Updates often blocked by MNOs

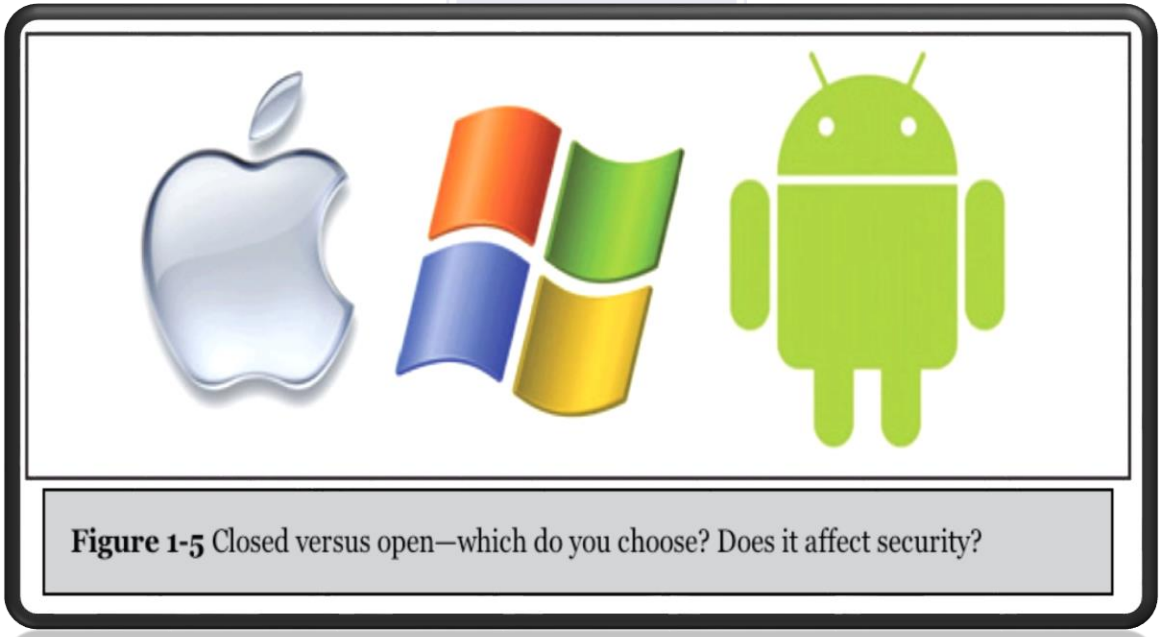

**Figure 1-5** Closed versus open—which do you choose? Does it affect security?

# MCQ

1. _____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
   a) Network Security
   b) Database Security
   c) Information Security
   d) Physical Security

2. From the options below, which of them is not a threat to information security?
   a) Disaster
   b) Eavesdropping
   c) Information leakage
   d) Unchanged default password

3. From the options below, which of them is not a vulnerability to information security?
   a) flood
   b) without deleting data, disposal of storage media
   c) unchanged default password
   d) latest patches and updates not done

4. _____ platforms are used for safety and protection of information in the cloud.
   a) Cloud workload protection platforms
   b) Cloud security protocols
   c) AWS
   d) One Drive

5. Which of the following information security technology is used for avoiding browser-based hacking?
   a) Anti-malware in browsers
   b) Remote browser access
   c) Adware remover in browsers
   d) Incognito mode in a browser

# REFERENCES


- https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref