RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -5

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- What are the Steps in the Mobile Forensics Process?
- Seizure
- Airplane Mode
- Phone Jammer
- Faraday bag
- MCQ
- References

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

What are the Steps in the Mobile Forensics Process?

The term “mobile devices” encompasses a wide array of gadgets ranging from mobile phones, smart phones, tablets, and GPS units to wearable's and PDAs. What they all have in common is the fact that they can contain a lot of user information.

1. Seizure

Digital forensics operates on the principle that evidence should always be adequately preserved, processed, and admissible in a court of law. Some legal considerations go hand in hand with the confiscation of mobile devices.

There are two major risks concerning this phase of the mobile forensic process: Lock activation (by user/suspect/inadvertent third party) and Network / Cellular connection.

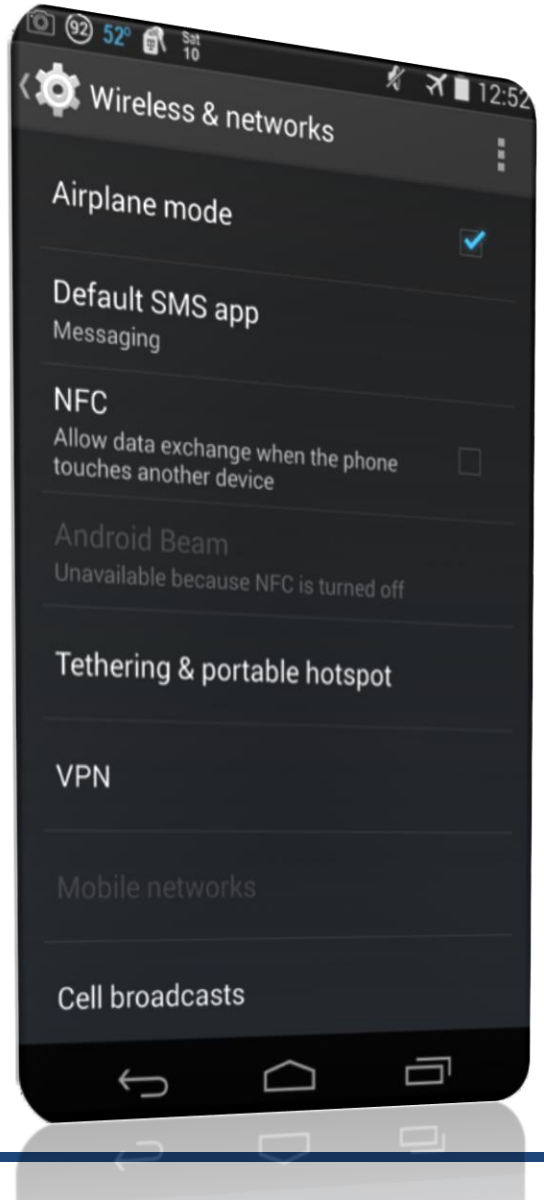
Network isolation is always advisable, and it could be achieved either through 1) Airplane Mode + Disabling Wi-Fi and Hotspots, or

2) Cloning the device SIM card.

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

2. Airplane Mode

Mobile devices are often seized switched on; and since the purpose of their confiscation is to preserve evidence, the best way to transport them is to attempt to keep them turned on to avoid a shutdown, which would inevitably alter files.



WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

3. Phone Jammer

A Faraday box/bag and external power supply are common types of equipment for conducting mobile forensics. While the former is a container specifically designed to isolate mobile devices from network communications and, at the same time, help with the safe transportation of evidence to the laboratory, the latter, is a power source embedded inside the Faraday box/bag. Before putting the phone in the Faraday bag, disconnect it from the network, disable all network connections (Wi-Fi, GPS, Hotspots, etc.), and activate the flight mode to protect the integrity of the evidence.

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

4. Faraday bag

Last but not least, investigators should beware of mobile devices being connected to unknown incendiary devices, as well as any other booby trap set up to cause bodily harm or death to anyone at the crime scene.

MCQ

6. _____ means the protection of data from modification by unknown users.
   a) Confidentiality
   b) Integrity
   c) Authentication
   d) Non-repudiation

7. When integrity is lacking in a security system, _____ occurs.
   a) Database hacking
   b) Data deletion
   c) Data tampering
   d) Data leakage

8. _____ of information means, only authorised users are capable of accessing the information.
   a) Confidentiality
   b) Integrity
   c) Non-repudiation
   d) Availability

9. Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
   a) They help understanding hacking better
   b) They are key elements to a security breach
   c) They help understands security and its components better
   d) They help to understand the cyber-crime better

10. This helps in identifying the origin of information and authentic user. This referred to here as _____
    a) Confidentiality
    b) Integrity
    c) Authenticity
    d) Availability

REFERENCES

- https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref
- https://www.sanfoundry.com/cyber-security-questions-answers-elements-security/