RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -6

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- What are the Steps in the Mobile Forensics Process?
- Acquisition
- MCQ
- References

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

5. Acquisition

/Identification + Extraction/

The goal of this phase is to retrieve data from the mobile device. A locked screen can be unlocked with the right PIN, password, pattern, or biometrics (Note that biometric approaches while convenient are not always protected by the fifth amendment of the U.S. Constitution). According to a ruling by the Virginia Circuit Court, pass codes are protected, fingerprints not. Also, similar lock measures may exist on apps, images, SMSs, or messengers. Encryption, on the other hand, provides security on a software and/or hardware level that is often impossible to circumvent. It is hard to be in control of data on mobile devices because the data is mobile as well. Once communications or files are sent from a Smartphone, control is lost. Although there are different devices having the capability to store considerable amounts of data, the data in itself may physically be in another location.

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

5. Acquisition

/Identification + Extraction/

To give an example, data synchronization among devices and applications can take place directly but also via the cloud. Services such as Apple's iCloud and Microsoft's One Drive are prevalent among mobile device users, which leave open the possibility for data acquisition from there. For that reason, investigators should be attentive to any indications that data may transcend the mobile device as a physical object, because such an occurrence may affect the collection and even preservation process. Since data is constantly being synchronized, hardware and software may be able to bridge the data gap. Consider Uber – it has both an app and a fully functional website. All the information that can be accessed through the Uber app on a phone may be pulled off the Uber website instead, or even the Uber software program installed on a computer.

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

5. Acquisition

/Identification + Extraction/

Regardless of the type of the device, identifying the location of the data can be further impeded due to the fragmentation of operating systems and item specifications. The open-source Android operating system alone comes in several different versions, and even Apple’s iOS may vary from version to version.

Another challenge that forensic experts need to overcome is the abundant and ever-changing landscape of mobile apps. Create a full list of all installed apps. Some apps archive and backup data.

WHAT ARE THE STEPS IN THE MOBILE FORENSICS PROCESS?

5. Acquisition

/Identification + Extraction/

After one identifies the data sources, the next step is to collect the information properly. There are certain unique challenges concerning gathering information in the context of mobile technology. Many mobile devices cannot be collected by creating an image and instead they may have to undergo a process called acquisition of data. Thera are various protocols for collecting data from mobile devices as certain design specifications may only allow one type of acquisition.

The forensic examiner should make a use of SIM Card imagining – a procedure that recreates a replica image of the SIM Card content. As with other replicas, the original evidence will remain intact while the replica image is being used for analysis. All image files should be hashed to ensure data remains accurate and unchanged.

MCQ

11. Data ___________ is used to ensure confidentiality.

a) Encryption

b) Locking

c) Deleting

d) Backup

12. Which of these is not a proper method of maintaining confidentiality?

a) Biometric verification

b) ID and password based verification

c) 2-factor authentication

d) switching off the phone

13. Data integrity gets compromised when _____ and _____ are taken control off.

a) Access control, file deletion

b) Network, file permission

c) Access control, file permission

d) Network, system

14. ______ is the latest technology that faces an extra challenge because of CIA paradigm.

a) Big data

b) Database systems

c) Cloud storages

d) Smart dust

15. One common way to maintain data availability is __________

a) Data clustering

b) Data backup

c) Data recovery

d) Data Altering

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/