University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions

Lecture 11: Digital Forensics

QUESTION 1

Briefly explain the following terms

a) Forensics
b) Digital Forensics
c) Computer Forensics
d) Network Forensics
e) Digital Investigations
f) Internet Investigations
g) Computational Forensics

Answer

a) Forensics:
Application of a broad spectrum of sciences to answer questions of interest to a legal system. This may be in relation to a crime or a civil action. “Forensic” Comes from the Latin “forēnsis”, meaning “before the forum”, i.e. presented to forum of judges.
b) Digital Forensics:
Recovery and investigation of material and legal evidence found in digital devices, often, but not necessarily, related to computer crime
c) Computer Forensics:
Recovery and investigation of material and legal evidence found in computers and digital storage media used with computers.
d) Network Forensics:
Monitoring and analysis of computer network traffic for the purposes of gathering legal evidence and information about events, or for intrusion detection. Unlike other areas of digital forensics, network forensics deals with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.
e) Digital Investigations:
To use digital tools to conduct investigation, or to investigate digital material and systems, without necessarily aiming to produce legal evidence.
f) Internet Investigations:
To investigate events taking place in the Internet or with relation to the Internet, without necessarily aiming to produce legal evidence.
g) Computational Forensics:
Quantitative approach to the methodology of the forensic sciences. It involves computer-based modeling, computer simulation, analysis, and recognition in studying and solving problems posed in various forensic disciplines. CF integrates expertise from computational science and forensic sciences.

QUESTION 2

Evidence integrity is essential in order for digital evidence to be admissible in court and to carry weight as evidence.

a. What is CoC (Chain of Custody) and why is it important for evidence integrity?
b. Assuming that a forensic team follows the right steps for preserving evidence integrity and for keeping an unbroken CoC, what must they do in order to convince the court that they have done so?
c. What is OOV (order of volatility), and how does it influence decisions regarding which evidence should be preserved first?
d. List various data storage media as a funciton of their OOV.

Answer

a. Chain of custody (CoC) refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.
b. Document it.
c. Data stored on media can be modified or erased due to various factors. The volatility expresses the rapidity and ease with which such factors can modify or erase data. The OOV expresses the relative ranking of media according to volatility.
d. OOV of variuouis media: Microprocessor registers, microprocessor cache, RAM, HD cache, HD, peripheral memory (R/W), Write once.

QUESTION 3

a. Explain the difference between “live acquisition” and “post mortem acquisition”.
b. What are the advantages and disadvantages of live and post mortem acquisition?
c. Give an example when “live acquisition” is necessary.

Answer

a. In case of live acquisition, the evidence is collected from a system where the microprocessor is running. In case of post mortem acquisition, the evidence is collected from storage media of a system that is shut down.
b. Post mortem provides better integrity preservation and does not influence the data. However, volatile data can be lost in the process of shutting down a system. Live acquisition enables the collection of volatile data, but also influences the data.
c. In case the HD is encrypted, it is better to collect the data from the HD while it is running.