University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions

Lecture 07: Digital Forensics and Incident Response

Question 1

a. How can somebody working in a company know what to do when he/she discovers a security incident ?
b. What are the main elements of an IR Policy (Incident Response Policy) ?
c. Describe the 3 main types of IR teams.

Question 2

The following are steps of the incident response process. Briefly explain each concept and provide a Norwegian translation. The steps can often be executed in parallel.

a) Triage
b) Investigation
c) Containment
d) Analysis
e) Tracking
f) Recovery

Question 3

Briefly explain and provide a Norwegian translation for the following terms:

a) Forensics
b) Digital Forensics
c) Computer Forensics
d) Network Forensics
e) Electronic data discovery
f) Cyber Forensics
g) Computational Forensics

Question 4

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 function of their OOV.

Question 5

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.

Question 6

Explain the basic steps of the forensic investigation process.

Question 7

Explain the basic scientific principles for the forensic investigation process.