University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 6: Incident Response and Digital Forensics

Question 1

a. Regular employees are often key when it comes to discovering incidents. What tools does an organization have to make sure their employees report possible incidents?
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.

a) Detection
b) Triage
c) Collection
d) Containment
e) Analysis and investigation
f) Reporting
g) Recovery

Question 3

Evidence integrity is essential 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?

Question 4

Explain the basic steps of the forensic investigation process.

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 principles for the forensic investigation process.