University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions

Lecture 11: Digital Forensics

QUESTION 1

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

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

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.

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.