



Lecture 11: Digital Forensics

QUESTION 1

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 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 2

- 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.