Digital Forensics 2

(SPY 2010)

Assignment 1

Submitted By-

Your Name
University Number: 123456

Submitted To-

Dr. Mohammad Shoab
Department of Computer Science
Shaqra University

Instructions:

- *The assignment must be handwritten.*
- *Use A4 papers to write the assignment.*
- *Draw diagrams wherever relevant. Explain your notations explicitly and clearly.*
- *An incomplete assignment is NOT acceptable for submission.*
- *Arrange all the papers of your assignment into a file to submit.*
- *Once you submit your assignment, you will be expected to answer all the questions there INDEPENDENTLY. You may be asked to answer any question of the assignment in the class.*

Q1. What are the key differences between live data acquisition and static data acquisition in digital evidence collection? When would each method be appropriate in a forensic investigation?

Q2. Explain the typical steps involved in a cybercrime investigation. How is digital evidence handled to ensure its admissibility in court?

Q3. Discuss the main legal and ethical challenges that a digital forensic investigator may face. How do chain of custody and jurisdictional issues impact investigations?

Q4. What is reverse engineering in the context of malware analysis? Describe the tools and techniques used to analyze advanced malware.

Q5. Define memory forensics. What kinds of evidence can be extracted from volatile memory, and why is it critical in modern investigations?