UNIVERSITY OF GHANA

BA/B.SC INFORMATION TECHNOLOGY, FIRST SEMESTER EXAMINATIONS: 2016/2017

CSIT425: COMPUTER CRIME, FORENSICS AND AUDITING

INSRUCTIONS

ANSWER ANY THREE OF THE QUESTIONS. EACH QUESTION 20 MARKS

TIME ALLOWED:

TWO AND A HALF (2½) HOURS

[60 MARKS TOTAL]

1. The Principles of Computer Forensics is to recover, analyse, and present computer based material in such a way that it is useable as evidence in a court of law. There fore it is essential that none of the equipment or procedures used during the examination of the computer prevent this.

a. Define computer forensics and briefly explain the five phases that are used in digital forensic investigation process.

b. Using you understanding explain why Computer evidence must be Authentic, Accurate, Complete and Convincing to juries and in conformity with common law and legislative rules and admissible at court.

c. Explain the theory behind the searching process in the evidence searching phase.

d. Explain the search techniques after you have after you have taken steps to preserve the data?

(20 MARKS)

1. To effectively combat cybercrime, greater emphasis must be placed in the compute r forensic field of study. Therefore the professional must know who the cyber criminal's pri mary targets are and who can use Computer Forensic Evidence.

a. With your understanding and using examples, explain the four roles the computer can play in a Cybercrime

b. Identify about three groups that require Computer Forensic Evidence and briefly explain what they use them for?

c. Explain the importance of digital forensics Tools

d. Explain the importance of Documenting searches procedures.

(20 MARKS)

1. An ethical hacker possesses the skills, mindset and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems. Also the intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. Therefore the attacker must have Methods, Opportunity and Motive(MOM)

a. Explain with examples the acronym 'MOM' and why the malicious attacker must have these three things to penetrate a system?

b. Identify and briefly explain the four types of threats that can be used to penetrate a system.

c. Using the acronym 'MOM' explain the differences between a hacker and an ethical hacker.

d. Briefly explain the three main types hackers (crackers) techniques that the hacker can technically commit to network connections.

(20 MARKS)

1. When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role. To ensure this as the digital forensic investigator: Use any case studies such as the Roman Case study, EOCO and GFA case, and the Two Nigerians Verses Ghana Arm Forces cases as examples to answer the questions:

a. Explain what Life Analysis is and the methodologies used in evidence gathering

b. Explain what Dead Analysis is and the methodologies used in evidence gathering

c. Explain with examples the PICL guidelines in you digital forensic investigations?

d. Why is important that data saved during a dead or live analysis, a cryptographic hash should be calculated

(20 MARKS)

1. The board of directors of a technical research company demoted the company's founder and chief executive officer CEO. The executive, disgruntled because of his demotion, was later terminated; it was subsequently determined that the executive had planned to quit about the same time he was fired and establish a competitive company. Upon his termination, the executive took home two computers; he returned them to the company four days later, along with another company computer that he had previously used at home. Suspicious that critical information had been taken; the company's attorneys sent the computers to a Computer Forensics Specialist Team (CFST) for examination.

a. Using the acquired evidence generated, discusses the analysis techniques and steps the CFS Team used in their quest to gather the table of information usage?

b. Applying the scientific method to digital forensics analysis, explain the methods involve to objectively and critically assessing digital evidence to gain an understanding of and reach conclusions about the crime.

c. Define what type of analysis this is required and what methodology that should be applied.

d. How do you analyse a server that has been compromised in your digital investigation to supports or refutes a hypothesis.