**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE COMPUTER SECURITY AND FORENSICS**

**3RD YEAR 1ST SEMESTER 2020/2021 ACADEMIC YEAR**

**SPECIAL RESIT TWO**

**MAIN CAMPUS (REGULAR)**

---

**COURSE CODE:** **IIT 3311**

**COURSE TITLE:** **Computer Forensics II**

**EXAM VENUE:** **STREAM: (BSc. Computer Security & Forensics)**

**DATE:** **EXAM SESSION:**

**TIME: 2.00 HOURS**

---

**Instructions:**

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

**Question 1[ 30 marks]**

a) Explain the meaning of computer forensics. (2 marks)

b) Describe any three computer forensic hardware tools (3 marks)

c) Discuss five threats and vulnerabilities to which a computer system/network may be exposed (5 marks)

d) Discuss the relationship between computer forensics and computer security (3 marks)

e) Imagine that you compose a Word document and save it on your laptop with the filename Practical.doc. The process of saving a file on your hard disk involves three basic events. However when you decide to delete Practical.doc, only two events happen. Considering the above statement, discuss the processes involved in storing a file in a hard disk drive and deleting it from the hard disk. Explain also why deleting the file may not prevent forensic experts from getting the file. (10 marks)

f) Outline the general guidelines that should be followed in the process of seizing evidence. (7 marks)

**Question 2 [20 marks]**

a) There are many computer forensic tools in use today. Discuss the following forensic tools. (8 marks)

   i. SANS SIFT
   ii. ProDiscover Basic
   iii. Volatility
   iv. The Sleuth Kit (+Autopsy)
   v. FTK Imager
   vi. PlainSight

b) Explain the steps you would follow in gathering evidence from a server. (4 marks)

c) Computer hard disk is the most important secondary storage medium in a computer.

   i. Discuss how a computer hard disk works (4 marks)
   ii. Explain how digital data is stored in it and how evidence can be retrieved.(4 marks)

**Question 3 [20 marks]**

a) Computer forensics process has a number of models that can be used. This is due to the diverse situations that digital forensics must address. For simplicity, incident response methodology is overlooked, and an amalgamation of models derived from the Association of Chief Police Officers (ACPO), US Department of Justice and US Air Force (2007) and the work of Sammes and Jenkinson (2007) may be used. Exhaustively discuss this model (8 marks)

d) Discuss the methods of ensuring the chain of custody of evidence is appropriately managed (7 marks)

e) Explain the meaning of slack space and how it conceals digital evidence (5 marks)

**Question 4 [20 marks]**

a) Explain the meaning of computer forensic imaging (2 marks)

b) Discuss the set of activities involved in the process of computer forensic imaging (10 marks)

c) Equipment refers to the non-evidentiary hardware and software the examiner utilizes to conduct the forensic imaging or analysis of the evidence. Discuss the how you would prepare equipment for forensic audit process. (8 marks)

**Question 5 [20 marks]**

a) When conducting digital forensics, you need to understand the two dimensions of the digital underworld and what they hold as potential evidence. The contents of both the visible and invisible dimensions can be recovered with forensics tools. Discuss the typical examples of each category of evidence. (10 marks)

b) Identify intellectual property or confidential information from which a computer incident might arise. (4 marks)

c) Explain how forensic auditor would go about documenting his evidence in a professional manner . (6 marks)