JARAMOGIOGINGA ODINGAUNIVERSITYOFSCIENCEANDTECHNOLOGY

SCHOOLOFINFORMATICSANDINNOVATIVE SYSTEMS

DEPARTMENTOFCOMPUTERSCIENCE
ANDSOFTWAREENGINEERING

UNIVERSITYEXAMINATIONFORTHEDEGREEOFBACHELORSCIENCEINCO MPUTERSECURITY ANDFORENSICS
3RDYEAR1NDSEMESTER2021/2022ACADEMICYEAR
MAINCAMPUS

COURSECODE: **ICB 1301**

COURSETITLE: **COMPUTER FORENSIC II**

INSTRUCTIONS:

1. **AnswerQuestion1(Compulsory)andANYothertwoquestions**

---

2. **Candidatesareadvisednot towriteonthe questionpaper**
3. **Candidatesmusthandintheiranswerbookletstotheinvigilatorwhileintheex amination room**

QUESTIONONE **[30MARKS]**

(a) What is Computer Forensics. [2 Marks]

(b) What are the goals of forensics. [4 Marks]

(c) What is network forensics analysis tool. [2 Marks]

(d) Distinguish between steganography and stegaanalysis [4 Marks]

(e) Outline at least six roles of a forensics investigator [6 Marks]

(f) Give brief explanation to the following terminologies

i. Image file [2 Marks]

ii. Slack space [2 Marks]

iii. Network forensics [2 Marks]

iv. Asymmetric encryption. [2 Marks]

v. Symmetric encryption. [2 Marks]

vi. Data Mining [2 Marks]

QUESTIONTWO **[20MARKS]**

(a) Differentiate between volatile and nonvolatile data giving appropriate examples[4 Marks]

(b) Differentiate between the following. [6 Marks]

i. FAT and NTFS.

ii. FAT16 and FAT32.

(c) Discuss five threats and vulnerabilities to which a computer system/network may be exposed. Describe how the discussed threats and vulnerabilities can be prevented.

[10 Marks]

QUESTIONTHREE **[20MARKS]**

a) There are many computer forensic tools in use today, Discuss any of the three tools.[6 marks]

b) Describe the content of the e-mail header. How is the email header information useful to an investigator. [6 marks]

c) Briefly describe the importance of network forensics in the investigation of cybercrime.

[8 marks]

QUESTIONFOUR **[20MARKS]**

(a) Jooust University has approached you for advice on whether to use patent or trademark property right to protect a software that they are currently working on.

Discuss the advantages and disadvantages of each right and use that to come up with the better of the two Intellectual property rights to recommend to the company

QUESTIONFIVE **[20MARKS]**

(a) What is a file system. [2 Marks]

(b) What is chain of custody and why is it important for evidence integrity. [6 Marks]

(c) How is computer forensics different to data recovery. [4 Marks]

(d) Discuss the methods of ensuring the chain of custody of evidence is appropriately managed. [8 Marks]

- **END–**