

**EXAMINATION PAPER**

**FACULTY: COMPUTER SCIENCE & MULTIMEDIA**

**COURSE: MASTER OF COMPUTER SCIENCE**

**YEAR/SEMESTER: SECOND / THIRD**

**MODULE TITLE & CODE: DIGITAL FORENSICS : DFS 232**

**DATE:**

**TIME ALLOWED: 3 HOURS  START: 1:00 PM FINISH: 4:00 PM**

**Instruction to candidates**

1. This question paper has THREE (3) Sections.
2. Answer all **7** questions in Section A, VSAQ
3. Answer **7** questions out of 9 in Section B, SAQ.
4. Answer **2** questions out of 3 in Section C, LAQ.
5. No scripts or answer sheets are to be taken out of the Examination Hall.
6. Lengthy answers do not win more marks. Students are advised to write the clear and concise answers with valid relevant examples

***Do not open this question paper until instructed***

*(Candidates are required to give their answers in their own words as far as practicable)*

**SECTION A**

**Very Short Answer Questions**

**Attempt all seven (7) questions [2 × 7 = 14]**

1. What are the bad sectors?
2. List different types of network attacks.
3. What is the importance of cybercrime investigation
4. What is the difference between threat, vulnerability and attack?
5. Explain the function of SQL Server Management Studio(SSMS).
6. Original evidence should **NEVER** be used for analysis. Provide your thought process for agreement or disagreement.
7. Mention some cloud computing threats.

**SECTION B**

**Short Answer Questions**

**Attempt only seven (7) questions out of eight (9) questions [7 × 8 = 56]**

**Q. 1**   (Unit 1: Forensic Science)

Explain the basic steps of the Digital Forensic Investigation Process?

**Q. 2**   (Unit 1: Forensic Science)

You are taking an interview of forensics investigators to hire in your organization, what are the different traits, roles, and responsibilities you will search on him/her during the process?

**Q. 3**  (Unit 2: Regulations, Policies, and Ethics)

You have hired a digital forensics expert for setting up a computer forensic Lab. Briefly describes different items that you will take into account and build a computer forensic Lab.

**Q. 4** (Unit 2: Regulations, Policies, and Ethics)

Explain different steps that are involved while performing an investigation of email crimes and violations.

**Q. 5** (Unit 2: Regulations, Policies, and Ethics)

What are the guidelines for writing a good forensic report?

**Q.6** (Unit 3: Digital Evidence)

When you are conducting a forensics investigation explain how you will deal with these items briefly

* Dealing with powered on computers
* Dealing with powered off computers
* Dealing with networked computers
* Dealing with network open and startup files

**Q.7**( Unit 4:Procedure and Methodology)

Why is chain of custody important? Explain what happens when a chain of custody is broken?

**Q. 8**  ( Unit 5:Digital Forensics)

Explain Web Application Architecture. Why log is important in forensic investigation? Explain with some log files stored in apache web server.

**Q. 9** (Unit 5:Digital Forensics)

What do you understand about cloud forensics and describe different challenges that are faced by investigators while performing cloud forensics?

**Group C**

**Long Analytical or Case Question**

**Attempt any two (2) questions out of three (3) questions [2 × 15 = 30]**

**Q. 1** (Unit 1: Forensic Science,Unit 2: Regulations, Policies, and Ethics, Unit 3: Digital Evidence,Unit 4:Procedure and Methodology, Unit 5:Digital Forensic)

Suppose you were recently hired for a new position as the computer forensics specialist at a medium sized communications company. You have been asked to prepare a presentation to the BOD on your main duties for the company and how your position could help achieve business goals based on security and confidentiality. You are also aware that the company has just had some issues with employee complaints of ongoing sexual harassment over email and instant messaging systems but has been unable to obtain adequate evidence of any kind.

1. Explain the basic primary tasks, high – level investigation processes, and challenges of a computer forensics specialist.
2. Provide an overview of how computing devices are used in crimes of today and how these crimes can affect a company data and information.
3. Discuss how computer forensics investigations pertain the law and trying of cases. (5+5+5)

**Q.2**  (Unit 4:Procedure and Methodology)

You are working as a forensics investigator expert at MNO college. You have been recently onboarded last week. All of sudden you come across a situation where you have to perform a computer forensics investigation process. Describe briefly the methodology of the computer forensics investigation you will go through to handle the incident. (15)

**Q.3** (Unit 3: Digital Evidence)

You have been hired as a malware analyst for an educational organization. Your job is to perform malware analysis for the organization. There are a few scoped machine which has been affected by malware. What different dynamic and static malware analysis techniques you will use to investigate these machines. (8+7)

Good Luck