National Forensics Sciences University, Goa Campus
Mid- semester Examination

Programme – MSC CS
Sem – 2
Subject Name: Incident Response and Digital Forensics
Subject Code- CTMSDFIS S1 P4
Time- 1.5 Hours
Max.Marks- 50
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1 **Solve any four** **20 marks**

a. Explain the difference between malware, ransomware, and phishing attacks. 5 marks

b. How can organizations protect themselves against social engineering attacks? 5 marks

c. Define Windows Events and explain their importance in forensic analysis, focusing on Evt and Evtx file formats. 5 marks

d. What is difference between Windows OS architecture and Linux OS architecture. 5 marks

e. Explain difference between Data recovery and Carving. 5 marks

Q.2 **Attempt all** **30 marks**

a. What is chain of custody and its importance with evidence acquisition. 10 marks

b. Explain standard operating procedures for acquisition and preservation of evidences. 10 marks

c. During a digital forensic investigation of a Windows computer, you discover that the NTFS partition has been deleted. Explain the steps you would take to recreate the NTFS partition and recover any potentially lost data. 10 marks

*** All the best***