15/05/19

(Sem II) M.E. (COMP) Choice Base

Time: 3 Hours **Total Marks: 80**

N.B.: (1) Question No.1 is compulsory.
(2) Attempt any three questions from the remaining five questions.
(3) Make suitable assumptions wherever necessary but justify your assumptions.

1. (a) What is cybercrime? How do we classify cybercrimes? **05**
   (b) Justify the need of 'Forensic Duplication' in digital forensics. **05**
   (c) Explain need of volatile data collection during digital forensic. **05**
   (d) Explain tools & commands for following operations **05**
   I. To know failed console login.
   II. To dump registry.
   III. To transfer data from victim machine to forensics system.
   IV. To know failed remote login.
   V. To identify hidden files.

2. (a) What are the procedures to be adhered to while handling evidence during an investigation? **10**
   (b) What is digital evidence? How to preserve the digital evidence? Explain the role of custodian in handling digital evidence. **10**

3. (a) Briefly explain the process of collecting the volatile data in Unix system. **10**
   (b) Explain handling & recovering mechanism of DoS attack. **10**

4. (a) What are the requirements of forensic duplication tools? Elaborate different ways of creating a forensic duplicate of a hard-disk. **10**
   (b) Describe in detail about uses of tool in E-mail Forensics. **10**

5. (a) Discuss in details pre Incident preparation in organization. **10**
   (b) Briefly explain the role of Windows registry in collecting forensic evidence. **10**

6. Write a short note on: **(any two)** **20**
   (a) Chain of Custody.
   (b) Guidelines for Writing a Report.
   (c) SNORT.

****