B.E. (Computer) (Sem-VIII) (CBSGS)

Paper / Subject Code: 52704 / 4) Digital Forensic Date- 4/12/19

(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) Explain the category "cybercrimes against persons". **05**
   (b) Define term Digital Forensic and Digital forensic investigation. **05**
   (c) Define digital evidence and its types of digital evidences. **05**
   (d) What is DOS attack? How to achieve recovery from DOS attack? **05**

2. (a)What steps or activities are done in an initial response phase? **10**
   (b) What are the steps involved in computer evidence handling? Explain in detail. **10**

3. (a) What is Address Spoofing explain it types ? **10**
   (b) What are possible investigation phase carried out in Data Collection and Analysis? **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) Difference Between Network based IDS and Host based IDS. **10**

5. (a) Explain how law enforcement is done in computer forensics. **10**
   (b) What are the goals of network monitoring? What are the different types of network monitoring? Explain with examples. **10**

6. Write a short note on **20**
   (1) Steps of Unix system investigation
   (2) How to collect network based evidence Log files?

4B5860DF6148AB46DA06129EE2CF66B0