

--	--	--	--	--	--	--	--

**M.Sc DEGREE THIRD SEMESTER EXAMINATION IN COMPUTER SCIENCE
(SOFT COMPUTING), JANUARY 2021
19-323-0320 CYBER FORENCICS**

Time: 3 Hours

Maximum Marks: 50

**(Answer ANY FIVE questions)
(Each Question carries 10 Marks)
(Regular)**

- I A What are different roles of computer in a crime. Give one example for each role. (6 Marks)
 B Differentiate Identity theft and Identity fraud with suitable example. (4 Marks)
- II A cybercrime involves accessing of databanks of a corporate company where credit card numbers are stored. Using the stolen information, a hacker may attempt to extort or threaten the victim with the release of the information. To avoid the consequences, the company filed a cyber case. Explain the accepted procedure that an investigator follows to prepare the case. (10 Marks)
- III A What are different possibilities to collect the evidence when a compromise has been detected? Explain with possible dangers while collecting evidence. (6 Marks)
 B Explain about backup obstacles. (4 Marks)
- IV A What are different types of evidence? From the following identify the type of evidence
 i. A forensic investigator collected evidence from log file as last log on, network log on data, recently accessed files etc.
 ii. On 26th January 2019 I had a conversation with my supervisor. He said: I paid enough for the work.
 iii. The employment contract signed by an employer. (6 Marks)
 B What are 6 steps of incident handler methodology? Briefly explain each. (4 Marks)
- V Explain different tools and commands used for forensic process improvements. (10 Marks)
- VI A Differentiate forensic duplicate and qualified forensic duplicate. (2 Marks)
 B Give the dd commands used for creating forensic duplicate and qualified forensic duplicate. (4Marks)
 C What are different file formats supported by FTK imager? Explain steps to create an image using FTK (4 Marks)
- VII Briefly explain the steps for analysing an email header. (5 Marks)
 Why do we need separate forensics procedure for mobile phones ? List and briefly explain systematic procedure for mobile forensics.
