Name:

Enrolment No:

UPES

End Semester Examination, May 2023

Course:	**Digital Forensics-1**	**Semester : VI**
Program:	**B.Tech (CSE)+ LLB**	**Time : 03 hrs.**
Course Code:	**CSSF3017**	**Max. Marks: 100**

Instructions:

SECTION A
(5Qx2M=10Marks)

S. No.		Marks	CO
Q 1	How can the Recovery of Erased and Damaged data be accomplished during the process of Computer Forensics? What are the techniques and tools used?	**2**	**CO1**
Q 2	Can you explain the standard procedures that are followed during the process of Computer Forensics for Incident Verification and System Identification?	**2**	**CO2**
Q 3	What techniques can be used to authenticate digital evidence and ensure its integrity?	**2**	**CO3**
Q 4	What is the Information Technology Act, and what are its key provisions? How does the act impact the collection, preservation, and analysis of digital evidence?	**2**	**CO5**
Q 5	What is the role of laws and regulations in shaping the practice of digital forensics?	**2**	**CO4**

SECTION B
(4Qx5M= 20 Marks)

Q 6	How do Automated Search Techniques assist in the process of Computer Forensics investigations? What are the advantages and limitations of using automated tools in searching for digital evidence?	**5**	**CO4**
Q 7	Can you discuss the impact of Data Encryption and Compression on the process of Computer Forensics? How do these techniques complicate the recovery and analysis of digital evidence?	**5**	**CO3**
Q 8	What are the steps involved in conducting a Computer Forensics investigation using Forensics Software? How does the use of these tools aid in the collection, preservation, analysis, and presentation of digital evidence?	**5**	**CO5**
Q 9	Can you explain the key concepts and principles of Internet Forensics? How do Forensics Investigators collect, preserve, analyze, and present digital evidence related to online activities and communications?	**5**	**CO4**

SECTION-C
(2Qx10M=20 Marks)

Q 10	Discuss the various threats facing the World Wide Web, and how do they pose a risk to individuals, organizations, and society at large? How do cybercriminals exploit vulnerabilities in web applications, databases, and networks to carry out attacks such as phishing, malware, distributed denial-of-service (DDoS), and ransomware? What are the best practices and tools that can help mitigate these	**10**	**CO5**

	threats, and what steps can be taken to ensure the security and privacy of users' data online? **OR** You have been hired as a forensic investigator by a law enforcement agency to investigate a cybercrime that involves the use of a web browser. The suspects are believed to have used the browser to access and download sensitive information from a company's server. As part of your investigation, you need to analyze the browser's cache and temporary internet files and cookie storage to gather evidence related to the suspects' activities. A. What techniques and tools can you use to analyze the browser's cache and temporary internet files and cookie storage in this case, and how do they work? B. How do you collect, preserve, analyze, and present digital evidence related to browser activities, and what are the challenges associated with these investigations?		
Q11	A forensic investigator is tasked with analyzing a computer system that has been infected with a sophisticated malware that has encrypted all the files on the system. The malware creators are demanding a ransom payment to provide the decryption key. The investigator cannot afford to pay the ransom and must find a way to recover the encrypted files. What strategies and approaches can the investigator use to overcome this challenge? A) Conduct a memory analysis to identify any running processes related to the malware and attempt to reverse engineer the encryption algorithm. B) Use file carving techniques to recover any deleted or hidden files on the system that may contain important information. C) Use network forensics to track down the source of the malware and gather evidence for a criminal case against the perpetrators. D) All of the above. Which of the strategies or approaches would be the most effective in this scenario and why? What potential challenges or limitations could the investigator encounter when trying to implement these strategies?	**10**	**CO3**
SECTION-D **(2Qx25M=50 Marks)**			
Q 12	How can an organization or individual investigate cases of hacking and illegal access, obscene and incident transmission, and domain name ownership to identify the responsible party and gather evidence for legal action? What tools and techniques can be used to track down the source of the attack or transmission, such as IP address and metadata analysis, digital forensics, and network traffic monitoring? How can the investigation be conducted while ensuring the privacy and security of the organization's or individual's own data? Finally, how can the results of the investigation be presented in a clear and convincing manner to law enforcement or legal authorities, and what steps can be taken to prevent similar incidents in the future? **OR** Recently, a company has been sued by a former employee for wrongful termination, and the employee claims that the company used Yahoo Messenger	**25**	**CO2**

	to communicate about their termination in a discriminatory manner. The company has hired a Forensics Investigator to conduct a Messenger Forensics investigation to determine if any such communication took place. Can you explain the key concepts and principles of Messenger Forensics, specifically related to Yahoo Messenger, and how they can be applied in this case? How do Forensics Investigators collect, preserve, analyze, and present digital evidence related to Messenger communications, such as chat logs, attachments, and user account information? How can the investigator ensure that the evidence is admissible in court, and what measures can be taken to protect the privacy of the company and its employees? Finally, what factors should be considered in determining the severity of any wrongdoing and the appropriate legal penalties, such as the intent of the parties, the impact on the plaintiff, and the potential damages to the company's reputation?		
Q 13	**Case Study: The 2017 Equifax Data Breach** In 2017, Equifax, one of the largest credit reporting agencies in the United States, suffered a massive data breach that exposed the personal information of 143 million Americans. The breach occurred due to a vulnerability in Equifax's web application software, which allowed hackers to gain access to sensitive data such as Social Security numbers, birth dates, and addresses. The breach had far-reaching consequences for individuals, financial institutions, and even the US government. Equifax faced significant legal and financial repercussions, including a $700 million settlement with the US Federal Trade Commission and other government agencies. Questions related to Cyber Crime cases: A. How did Equifax respond to the breach, both in terms of addressing the technical vulnerability and communicating with affected individuals and stakeholders? B. List and discuss the steps that can individuals and organizations take to protect themselves from cyber crimes such as data breaches, identity theft, and ransomware attacks? C. Anticipate and discuss how has the Equifax data breach influenced public perceptions of cybersecurity and data privacy, and what implications does this have for policy and regulation in the field?	**25**	**CO1**