|  |  |
| --- | --- |
| LOGO.jpg | **GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY**  (**AN AUTONOMOUS INSTITUTION**)  **(Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu)**  **(Accredited by NAAC with “A” Grade, NBA (EEE,ECE &ME) & ISO 9001:2008Certified Institution)** |
| **QUESTIONBANK(DESCRIPTIVE)**  **Subject Name with Code: DIGITAL FORENSIC (22A3705T)**  **Course & Branch: B.TECH & CS Year& Semester: III-II Regulation: RG22** | |

**UNIT - I**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Question** | **[BT Level] [CO][ Marks]** |
| **2 Marks Questions (Short)** | | |
| 1. | What is hacking? List out different types hackings | L1/CO1/2M |
| 2. | Define Computer crime? | L1/CO1/2M |
| 3. | List out the common situations to conduct digital investigation in private sector environment? | L1/CO1/2M |
| 4. | What is Search and Seizure in Digital Forensics | L1/CO1/2M |
| 5. | What is Chain of Custody for Digital Evidence | L1/CO1/2M |
| 6. | List out the text used in internal warning banners | L1/CO1/2M |
| 7. | List out the types of Digital evidences | L1/CO1/2M |
| 8. | What are the Key Principles to Ensure the Integrity of Digital Evidence | L1/CO1/2M |
| **Descriptive Questions (Long)** | | |
| **1** | What are the key steps involved in a typical digital forensics investigation? | L1/CO1/12M |
| **2** | Explain the Benefits of forensics | L2/CO1/12M |
| **3** | What is computer crime? Discus about different types of computer crimes | L2/CO1/12M |
| **4** | What are the different types of digital forensics, and how do they differ from one another? | L2/CO1/12M |
| **5** | Explain different types of Digital investigation process | L2/CO1/12M |
| **6** | Describe History of Digital Forensics | L2/CO1/12M |
| **7** | Describe the Steps in Handling Digital Evidence | L2/C01/12M |
| **8** | What is Digital evidence? Explain Types of Digital Evidence in Court | L2/CO1/12M |
| **9** | Discuss the legal concerns and private issues in forensic | L2/CO1/12M |

**UNIT - II**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Question** | **[BT Level] [CO][ Marks]** |
| **2 Marks Questions (Short)** | | |
| **1** | What are the basic parameters of software cost model? | L1/CO2/2M |
| **2** | What are the advantages and disadvantages of commercial components? | L1/CO2/2M |
| **3** | Write a short note on software processes | L1/CO2/2M |
| **4.** | List out the attributes of three distinct process | L1/CO2/2M |
| **5.** | Explain peer inspections. | L2/CO2/2M |
| **6.** | What is Boehm five staffing principle | L1/CO2/2M |
| **7.** | List out the top five principles of modern process | L1/C02/2M |
| **8.** | Explain micro process | L2/CO2/2M |
| **9.** | What is meta process | L1/CO2/2M |
| **Descriptive Questions (Long)** | | |

|  |  |  |
| --- | --- | --- |
| **1.** | What is the significance of reducing the size of a software product, and how does it impact maintainability? | L2/CO2/12M |
| **2.** | Can you explain how streamlining software processes can contribute to overall project efficiency? | L2/CO2/12M |
| **3.** | What are some common practices that can be adopted to improve team effectiveness in software development projects? | L1/CO2/12M |
| **4.** | How does automation in software development processes help in reducing human error and increasing productivity? | L2/CO2/12M |
| **5** | What role does continuous testing play in ensuring that software meets the required quality standards? | L1/CO2/12M |
| **6.** | How do peer inspections improve the quality of software development compared to individual review processes? | L2/CO2/12M |
| **7.** | What are the main characteristics of conventional software engineering principles, and how do they differ from modern approaches? | L2/CO2/12M |
| **8.** | How does modern software management differ from traditional methods in terms of team collaboration and adaptability? | L2/CO2/12M |
| **9.** | Can you describe how modern software management encourages automation, and what impact it has on time-to-market? | L2/CO2/12M |
| **10.** | In what ways does modern software management emphasize continuous improvement of software processes and adaptability in a rapidly changing environment? | L2/CO2/12M |

**UNIT - III**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Question** | **[BT Level] [CO][ Marks]** |
| **2 Marks Questions (Short)** | | |
| 1. | List out the Employee termination cases in Private-Sector High-Tech Investigations | L1/CO3/2M |
| 2. | What are the requirements need to be collected for Internet Abuse Investigations | L1/CO3/2M |
| 3. | List out the steps in internet abuse investigation procedure | L1/CO3/2M |
| 4. | Who are Involve in the Industrial espionage Investigation | L1/CO3/2M |
| 5. | Define Interviews and Interrogations Private-Sector High-Tech Investigations | L1/CO3/2M |
| 6. | What is write-blocker device and its importance | L1/CO3/2M |
| 7. | Explain is data recovery in Private-Sector organization | L2/CO3/2M |
| 8. | Discus Critique phase in conducting an investigation | L2/CO3/2M |
| 9. | What is Bit-stream Copy | L1/CO3/2M |
| 10. | What are the Steps involved in conducting a digital forensics investigation in the Montgomery 72015 case | L1/CO3/2M |
| **Descriptive Questions (Long)** | | |
| **1** | Explain the procedure for corporate High-Tech investigations of internet abuse and email abuse investigation. | L2/CO3/12M |
| **2** | Discuss about Attorney-Client Privilege Investigations and Industrial Espionage Investigations | L2/CO3/12M |
| **3** | Describe the process of Interviews and Interrogations in High-Tech Investigations and employee termination cases. | L2/CO3/12M |
| **4** | How would you configure a data recovery workstation and apply industry best practices and corporate security policies to recover lost files efficiently | L3/CO3/12M |
| **5** | How would you apply email forensics techniques to recover and analyze email data while ensuring evidence integrity and compliance with legal standards? | L3/CO3/12M |
| **6** | How would you implement the company’s privacy policies and legal guidelines when recovering internet activity logs and relevant data during the investigation of suspected misuse? | L3/CO3/12M |
| **7** | Apply the steps to Configure the forensic workstation setup. | L3/CO3/12M |
| **8** | Explanation of the steps you would take for conducting a digital forensics investigation, using the **Montgomery 72015 case** | L2/CO3/12M |

**UNIT-IV**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Question** | **[BT Level] [CO][ Marks]** |
| **2 Marks Questions (Short)** | | |
| 1. | Differentiate between the Raw format and AFF | L4/CO4/2M |
| 2. | Compare RAID level 3 and RAID level 5 | L4/CO4/2M |
| 3. | Write about Advanced Forensic Format | L1/CO4/2M |
| 4. | List out some the best forensic Acquisition Tools | L1/CO4/2M |
| 5. | Short note on windows Validation Methods | L1/CO4/2M |
| 6. | Write about Validating dd Acquired Data | L1/CO4/2M |
| 7. | Write about Proprietary Formats | L2/CO4/2M |
| 8. | Explain Remote Acquisition with ProDiscover | L2/CO4/2M |
| **Descriptive Questions (Long)** | | |
| **1** | How would you differentiate between proprietary and open storage formats in terms of their suitability for digital evidence preservation? | L4/CO4/12M |
| **2** | What factors must be analyzed to determine the most appropriate acquisition method in a scenario involving a networked environment? | L4/CO4/12M |
| **3** | Given a forensic scenario, how would you determine which acquisition tool is most appropriate and why? | L4/CO4/12M |
| **4** | Compare different methods used for validating data acquisitions. What are the strengths and weaknesses of each? | L4/CO4/12M |
| **5** | Analyze the challenges that may arise when acquiring data from a RAID 5 array and explain how the RAID configuration impacts the forensic imaging process. | L4/CO4/12M |
| **6** | Explain the procedure for getting image from a RAID disk and functions provided by the RAID vendors | L2/CO4/12M |
| **7** | Analyze the potential risks and limitations of using remote network acquisition tools during a live forensic investigation | L4/CO6/12M |
| **8** | Explain the following forensic acquisition tools   1. PassMark Software ImageUSB and ILookIX Investigator IXimager 2. ASRData SMART 3. Runtime Software 4. SourceForge | L2/CO4/12M |

**UNIT-V**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Question** | **[BT Level] [CO][ Marks]** |
| **2 Marks Questions (Short)** | | |
| 1. | What are the Sub functions in the acquisition category of digital forensic tools | L1/CO5/2M |
| 2. | List out tasks performed by digital forensic tools | L1/CO5/2M |
| 3. | What is the role of client and server in Email | L1/CO5/2M |
| 4. | List out sub functions in the Extraction activity of digital forensic tool | L1/CO5/2M |
| 5. | Write out the steps involved in Email crime investigation | L1/CO6/2M |
| 6. | What are the methods of reconstruction | L1/CO6/2M |
| 7. | Compare any four properties forensic tools functions | L3/CO6/2M |
| 8. | Explain about Autopsy tool | L2/CO5/2M |
| 9. | List out Specialized Email forensic tools | L1/CO5/2M |
| **Descriptive Questions (Long)** | | |
| **1** | Demonstrate the types of forensic tools | L3/CO5/12M |
| **2** | Explain the Tasks Performed by Digital Forensics Tools | L2/CO5/12M |
| **3** | compare the functions of different forensic tool | L2/CO5/12M |
| **4** | Explain digital Forensics software Tools | L2/CO5/12M |
| **5** | Explain digital Forensics hardware Tools | L2/CO5/12M |
| **6** | Explain why validation and testing are important in forensic software | L2/CO6/12M |
| **7** | Explain about data hiding techniques | L2/CO6/12M |
| **8** | Discuss E-mail Crimes and Violations Investigations | L2/CO6/12M |
| **9** | **Discuss** the importance of email servers. | L2/CO5/12M |
| **10** | **Explain different E-mail forensic tools** | L2/CO5/12M |