Final Assessment Test – November 2019

Course: CSE4004 - Digital Forensics

Class NBR(s): 0796/1481

Time: Three Hours

Slot: G1+TG1

Max. Marks: 100

KEEPING MOBILE PHONE/SMART WATCH, EVEN IN 'OFF' POSITION, IS EXAM MALPRACTICE

Answer ALL Questions

(10 X 10 = 100 Marks)

1. Media leak investigations can be time consuming and resource intensive. Because the management wants to find who leaked the information, scope creep during the investigation is not uncommon. Elaborate the proper guidelines for media leak investigations.

2. Retrieving only the data relevant to the investigation with the sparse or logical acquisition method is the only practical solution. When dealing with very large RAID servers, consult the computer forensics vendor to determine how to best capture RAID data. Considering the above scenario, illustrate the all the RAID systems and identify the best retrieval for your data retrieval.

3. In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

   Discuss elaborately the tasks that you should complete before you search for evidence.

4. In a criminal matter, investigators seize entire drives to preserve as much information as possible and ensure that no evidence is overlooked. Exemplify the precautionary measures and steps that you would take while seizing and storing the criminal data that will act as valuable evidences.

5. To help prevent loss of information, software vendors now provide whole disk encryption. Explore and examine the new challenges in examining and recovering data from drives.

   Demarcate the organization of windows registry and its importance.

6. A threat email had been delivered to the BSE and NSE, at 10:44 am on Monday. With the MRA Marg police and the Cyber Crime Investigation Cell (CCIC) working together on the cyber crime case, the accused has been detained. The IP address had been traced to Patna, Bihar. When checked for any personal details, two contact numbers were found, which belonged to a photo frame maker in Patna.

   Determine what kind of data is to be collected for proper evidence and exemplify how you will analyze the collected evidence for solving the case.

7. Using the trojan or malware, a woman's webcam was accessed to capture her private videos and posted on an illegal website. The incident came into light when the Mumbai resident appeared for an interview.

   Considering the above case, Compare and contrast Pro-Discover Basic and FTK with respect to validating the criminal evidence data.

8. Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for prosecution or arbitration.

9. People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect. Illustrate the intricacies involved with the mobile forensic investigation.

10. Elaborate the key features and limitations of SANS SIFT Investigative tool. How does it help the forensic investigator to solve a criminal case.

⇔⇔⇔