SVKM'S
Mithibai College of Arts, Chauhan Institute of Science &
Amrutben Jivanlal College of Commerce and Economics (Autonomous)
Academic Year (2022-23)
Class: TYBSC Semester: VI

Program: B.Sc Computer Science **Max. Marks: 75**
Course Name: Cyber Forensics **Time:**
Course Code: USMACS602 **Duration: 2 hrs 30 minutes**
Date:

SOLUTION SET

Q1	ATTEMPT ANY 3 FROM THE FOLLOWING:	[21]
A	Describe the standard procedure for computer forensics. standard procedure 7 points 7M Make an initial assessment about the type of case you're investigating— Determine a preliminary design or approach to the case— Create a detailed checklist— Determine the resources you need— Obtain and copy an evidence drive— Identify the risks Mitigate or minimize the risks Test the design	7
B	Describe Computer Forensics with the following points i. Disk Imaging ii. Preservation Data Encryption and Compression 3.5M each − Disk Imaging is the process of copying a hard drive as a backup copy or an archive. − The process entails copying all the data stored on the source drive including data like the master boot record and table allocation information. − This image, however, is a single file that can be stored in any storage device and not necessarily an identical hard drive. − In the event that a restoration is necessary, the image will have to be applied to the hard drive. The Uses of Disk Imaging − The primary use of disk imaging software is to provide quick and easy back-ups of computer software and data stored on hard disks. − While most people think of backing up data, disk imaging programs back up not only data but also the computer's systems and configuration. − In effect, a disk imaging program captures an 'image' of an active computer system - its structure, registry programs, 'tweaks', software, etc.	7

	• Preservation – Data preservation is the process of ensuring the retention and protection from destruction or deletion all potentially relevant electronically stored evidence using forensically sound processes. – A forensically sound process will ensure the electronically stored evidence is not changed, including electronic metadata. – The obligation is to make sure that all electronic and information that may be relevant is protected from deletion. – The obligation to preserve begins when there is a reasonable expectation of future litigation. – Reasonable efforts to preserve include suspension of routine deletion policies, issuing adequate preservation instructions to the organization, and oversight as appropriate.	
C	Explain procedures for network forensics. Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics is as follows: 1. Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files. 2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening. 3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off. 4. Acquire the compromised drive and make a forensic image of it. 5. Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.	7
D	List and explain knoppix commands for Unix. 5 to 7 commands for 7M A few of the Knoppix-STD tools include the following: • dcfldd—The U.S. DOD computer forensics lab version of the dd command • memfetch—Forces a memory dump • photorec—Retrieves files from a digital camera • snort—A popular IDS that performs packet capture and analysis in real time (www.snort.org) • oinkmaster—Helps manage snort rules so that you can specify what items to ignore as regular traffic and what items should raise alarms • john—The latest version of John the Ripper, a password cracker • chntpw—Enables you to reset passwords on a Windows computer, including the administrator password • tcpdump and ethereal—Packet sniffers	7
Q2	ATTEMPT ANY 3 FROM THE FOLLOWING:	[21]
A	Define Internet forensics. "Browser Forensics Analysis is a separate, large area of expertise". Justify. Internet forensics- 2M +justification 5M	7

	Internet Forensics uses the combination of advanced computing techniques and human intuition to uncover clues about people and computers involved in Internet crime, most notably fraud and identity theft. Browser Forensics Analysis is a separate, large area of expertise. ● Web browsers are used in mobile devices, tablets, netbooks, desktops, etc., and often can be used not just for web surfing, but for navigation through the file system of the device. ● The web browser's cache can contain downloaded images, videos, documents, executable files and scripts. ● Web browsers also can contain data entered into forms: search queries, logins and passwords for web email accounts, social networks, other websites and financial information (for example, credit card numbers). ● Favourites and searches can give the researcher an idea of the device owner's interests. ● Browser Forensics is of no small importance in incident response for understanding how an attack on a computer or computer network began and finding the source of compromise. ● The main sources of malware / spyware / adware are emails (including web mails), social networks and other compromised sites. ● Typically, a user accesses all these sources (web emails, social networks, sites) using web browsers.	
B	Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system.Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks. Illegal Access implies that an person has intentional and without right, access of a computer system which the person is not authorized to access.This act is know as hacking and the person commiting the crime is commonly knows as a hacker. llegal access may result in: Damage to computer systems and data Compromise of confidential data Hackers employ a variety of techniques for hacking, including: Vulnerability scanner: checks computers on networks for known weaknesses Password cracking: the process of recovering passwords from data stored or transmitted by computer systems Packet sniffer: applications that capture data packets in order to view data and passwords in transit over networks Spoofing attack: involves websites which falsify data by mimicking legitimate sites, and they are therefore treated as trusted sites by users or other programs Root kit: represents a set of programs which work to subvert control of an operating system from legitimate operators Trojan horse: serves as a back door in a computer system to allow an intruder to gain access to the system later Viruses: self-replicating programs that spread by inserting copies of themselves into other executable code files or documents Key loggers: tools designed to record every keystroke on the affected machine for later retrieval	7

C	What is Social Media Investigation? Explain any two situations, which require Social Media Investigation. Media Investigation 2M+ any two situations 5M A social media investigation looks into the social media posts, status updates, photos, and conversations of an individual. You might require a social media investigation for a court case, custody battle, or as part of a background investigation. Any recent case explanations	7
D	What is activity reconstruction? How to reconstruct past internet activities and events? activity reconstruction 2M + How to reconstruct past internet activities and events 5M Event reconstruction plays a critical role in solving physical crimes by explaining why a piece of physical evidence has certain characteristics. With digital crimes, the current focus has been on the recognition and identification of digital evidence using an object's characteristics, but not on the identification of the events that caused the characteristics 	7
Q3	ATTEMPT ANY 3 FROM THE FOLLOWING:	[21]
A	Define law. Explain the legal process with an example. Definition 1M +6M legal process	7

	the discipline and profession concerned with the customs, practices, and rules of conduct of a community that are recognized as binding by the community. Enforcement of the body of rules is through a controlling authority. ➔ In general Legal process (sometimes simply process) is any formal notice or writ by a court obtain jurisdiction over a person or property. ➔ In computer forensics When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local custom, legislative standards, and rules of evidence. ➔ In general, however, a criminal case follows three stages: the complaint, the investigation, and the prosecution. Someone files a complaint; a specialist investigates the complaint and, with the help of a prosecutor, collects evidence and builds a case. If a crime has been committed, the case is tried in court. ➔ A criminal investigation can begin only when someone finds evidence of an illegal act or witnesses an illegal act. The witness or victim (often referred to as the "complainant") makes an allegation to the police, an accusation or supposition of fact that a crime has been committed. ➔ A police officer interviews the complainant and writes a report about the crime. The police department processes the report, and management decides to start an investigation or log the information into a police blotter. The police blotter provides a record of clues to crimes that have been committed previously. ➔ Criminals often repeat actions in their illegal activities,and these habits can be discovered by examining police blotters. ➔ This historical knowledge is useful when conducting investigations, especially in high-technology crimes. Blotters now are generally electronic files, often databases, so they can be searched more easily than the old paper blotters.	
B	Why is evidence form require? Discuss the sample of multi-evidence form used in corporate environment. evidence form 3M + sample 4M An evidence custody form usually contains the following information: • Case number—The number your organization assigns when an investigation is initiated. • Investigating organization—The name of your organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas. • Investigator—The name of the investigator assigned to the case. If many investigators are assigned, specify the lead investigator's name. • Nature of case—A short description of the case. For example, in the corporate environment, it might be "Data recovery for corporate litigation" or "Employee policy violation case." • Location evidence was obtained—The exact location where the	7
C	Solve the following case study: Connie Dabate was murdered in her home in 2015. According to his arrest warrant, her husband Richard provided an elaborate explanation of the day's events, claiming that he returned home after receiving an alarm alert. Richard went on to claim that, upon	7

	entering his house, he was immobilized and tortured by an intruder. He told police that the intruder then shot and killed Connie when she returned home from the gym. Relying on evidence collected from Connie's Fitbit, police were able to show that she had been in the house at the time Richard said she was at the gym. According to the Fitbit's data, Connie stopped moving one minute before the home alarm went off. Wearable devices like Fitbits monitor location via GPS and activities like distance traveled, steps taken, sleep time and heart rate. The devices are configured to synchronize data to applications on smartphones and personal computers or to cloud or social media sites. Evidentiary collections can be made from either of these sources using standard digital forensics tools and techniques.	
D	What is the use of warning banner? Explain how warning banners are often easier to present in court than policy manuals. warning banner2M +5M banners are often easier to present in court than policy manuals ● A Warning banner is a text that appears when someone logs on to a company computer that tells them the appropriate use of the machine or Internet access. ● Another way a private or public organization can avoid litigation is to display a warning banner on computer screens. ● A warning banner usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will. ● If this right isn't stated explicitly, employees might have an assumed right of privacy when using a company's computer systems and network accesses. A warning banner establishes the right to conduct an investigation. By displaying a strong,well-worded warning banner, an organization owning computer equipment doesn't need to obtain a search warrant or court order as required under Fourth amendment. ● A warning banner establishes the right to conduct an investigation. By displaying a strong,well-worded warning banner, an organization owning computer equipment doesn't need to obtain a search warrant or court order as required under Fourth Amendment search and seizure rules to seize the equipment. ● In a company with a well-defined policy, this right to inspect or search at will applies to both criminal activity and company policy violations. ● Keep in mind, however, that your country's laws might differ. For example, in some countries, even though the company has the right to seize computers at any time, if employees are suspected of a criminal act, they must be informed at that time. ● Computer system users can include employees or guests. Employees can access the intranet,and guests can typically access only the main network. ● Companies can use two types of warning banners: one for internal employee access (intranet Web page access) and another for external visitor access (Internet Web page access).	7
Q4	ATTEMPT ANY 3 FROM THE FOLLOWING:	[12]
A	Discuss Report Structure. 4M for whole structure	4

	★ Title Page – ❑ This can include information such as the case name, date, investigator name, and contact information. ★ Table of Contents (ToC) – ❑ This is not necessary for short reports or for those without many sections. ❑ However, if your report is long and/or is broken out into many different sections, including a ToC can be of great help to the reader. ★ Executive Summary – ❑ Especially important for longer reports, this allows the reader to get the high level view of important findings without having to delve into specifics. ★ Objectives – ★ Evidence Analyzed – ❑ This should include serial numbers, hash values (MD5, SHA, etc.), and custodian information, if known. ❑ If pictures were taken at the scene, you may want to include them here. ★ Steps Taken - ❑ Be detailed. ❑ Remember, your results should be reproducible. ❑ Include software and hardware used. ❑ Don't forget to include version numbers. ★ Relevant Findings – ❑ This section can be further broken down depending upon the length of your report. ❑ Subcategories will depend on the purpose of the exam, but can include things like: Documents of Interest; Internet Activity; Software of Note; USB Devices, etc. ★ Timeline – ❑ Some reports will benefit from a concise timeline of important events. ❑ A good graphic can go a long way in helping to communicate this information. ★ Conclusion – ❑ Highlight the important issues. ❑ This often comes in the form of a numbered list of concise findings. Signature –	
B	Why should your evidence media be write-protected? To ensure that data isn't altered. List three items that should be in your case report. An explanation of basic computer and network processes, a narrative of what steps you took, a description of your findings, and log files generated from your analysis tools.	4
C	Define the following: i. ESMTP ii. Locard's principle iii. Adversary iv. Victim	4

	1. ESMTP, which stands for "Enhanced Simple Mail Transport Protocol" adds many enhancements to the SMTP protocol. 2. Locard's Exchange Principle states that with contact between two items, there will be an exchange of microscopic material. 3. the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence 4.Person, group, organization, or government that conducts or has the intent to conduct detrimental activities.	
D	Elaborate on the concept of establishing company policies. ● Company policies and procedures establish the rules of conduct within an organization, outlining the responsibilities of both employees and employers. Company policies and procedures are in place to protect the rights of workers as well as the business interests of employers.	4

****