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**

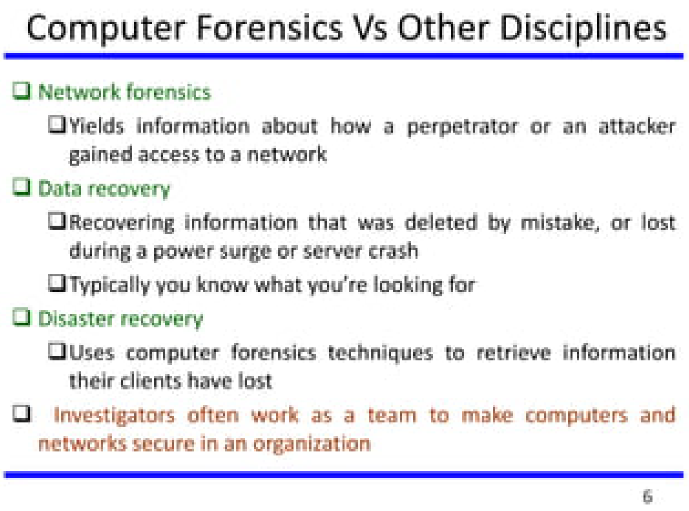
Course Name: Cyber Forensics **Time:**

Course Code: USMACS602 **Duration: 2 hrs 30 minutes**

Date:

SOLUTION SET

Q1	ATTEMPT ANY 3 FROM THE FOLLOWING:	[21]
A	Define computer forensics? How it is different from other Forensics? Explain with an example. computer forensics 2M+differences 4M+ 1M Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Digital forensics: Computer Forensics specifically means the Computing Devices. While Digital Forensics Means all the Devices that works on 0 and 1 it includes Mobile Phones, PDA's, Smart Watches, Printers, Scanners, Secondary Storage Media, Biometric Devices. Network Forensics: network forensic investigations deal with volatile and dynamic information. Disk or computer forensics primarily deals with data at rest.	7

	 Computer Forensics Vs Other Disciplines ❑ Network forensics ❑Yields information about how a perpetrator or an attacker gained access to a network ❑ Data recovery ❑Recovering information that was deleted by mistake, or lost during a power surge or server crash ❑Typically you know what you're looking for ❑ Disaster recovery ❑Uses computer forensics techniques to retrieve information their clients have lost ❑ Investigators often work as a team to make computers and networks secure in an organization 6	
B	Explain the three modes of protection of defense in depth. Concept 1M+ 3 modes 6M The National Security Agency (NSA) developed a approach, called the defense in depth (DiD) strategy. DiD has three modes of protection: • People • Technology • Operations	7
C	What is Chain of Custody? Explain Acquisition Procedures for Cell Phones and Mobile Devices. Chain of Custody 2M+ Acquisition Procedures 5M Before a piece of evidence gets in front of a jury, it must first meet a series of strict legal requirements. One of those is a well-documented chain of custody. A computer taken in as evidence makes many stops on its road to trial. It's collected, logged in at the lab, stored, checked out for analysis, checked back in for storage, and so on. Each of these stops must be noted, tracking each and every time the evidence item changes hands or locations. Without this detailed accounting, the evidence will be deemed untrustworthy and inadmissible. It's this detailed trail that makes up the chain of custody. Acquisition is the process of cloning or copying digital data evidence from mobile devices. The process of acquiring digital media and obtaining information from a mobile device and its associated media is precisely known as "imaging." The evidence image can be stored in different formats which can be used for further analysis. A hash value is generated to make sure that the image is not tampered with at any given point in time.	7
D	Describe Data Recovery and write its steps. Data Recovery 3M + steps 4M	7

- The data recovery process varies, depending on the circumstances of the data loss, the data recovery software used to create the backup and the backup target media.
- For example, many desktop and laptop backup software platforms allow users to restore lost files themselves, while restoration of a corrupted database from a tape backup is a more complicated process that requires IT intervention.
- Data recovery services can also be used to retrieve files that were not backed up and accidentally deleted from a computer's file system, but still remain on the hard disk in fragments.
- Data recovery is possible because a file and the information about that file are stored in different places.
- For example, the Windows operating system uses a file allocation table to track which files are on the hard drive and where they are stored.
- The allocation table is like a book's table of contents, while the actual files on the hard drive are like the pages in the book.
- When data needs to be recovered, it's usually only the file allocation table that's not working properly.
- The actual file to be recovered may still be on the hard drive in flawless condition.

Q2 ATTEMPT ANY 3 FROM THE FOLLOWING: [21]

A Explain WWW threats with respect to internet forensics. 7

WWW threats with respect to internet forensics categories 7M

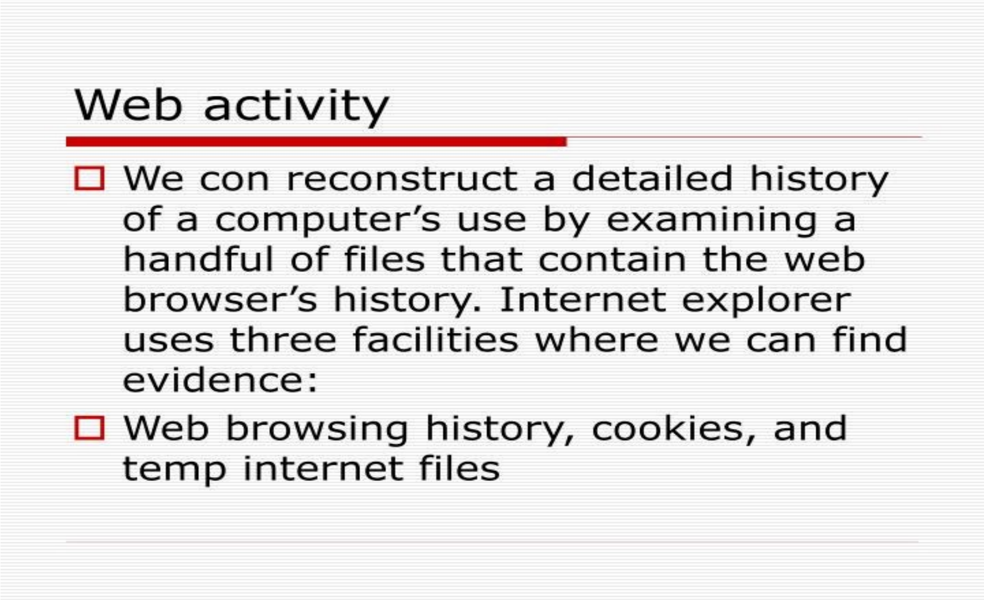
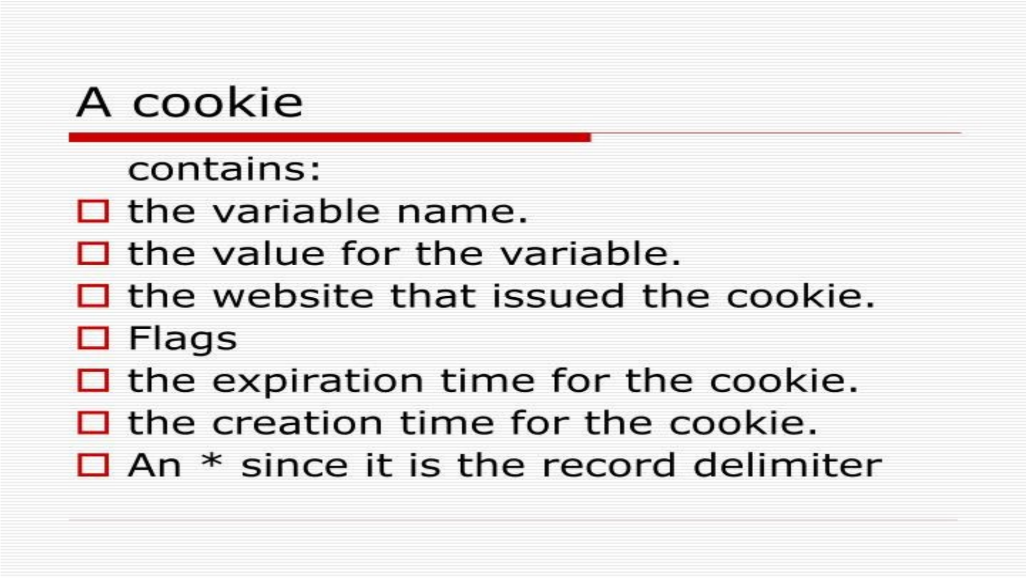
Web-based threats, or online threats, are a category of cybersecurity risks that may cause an undesirable event or action via the internet.

Web threats are made possible by end-user vulnerabilities, web service developers/operators, or web services themselves. Regardless of intent or cause, the consequences of a web threat may damage both individuals and organizations.

This term typically applies to — but is not limited to — network-based threats in the following categories:

- Private network threats - impact sub-networks connected to the wider global internet. Typical examples can include home Wi-Fi or ethernet networks, corporate intranets, and national intranets.
- Host threats - impact specific network host devices. The term *host* often refers to corporate endpoints and personal devices, such as mobile phones, tablets, and traditional computers.
- Web server threats - impact dedicated hardware and software that serve web infrastructure and services.

B	Discuss social media forensics with respect to yahoo messenger. social media forensics with YM 7M ● Yahoo Messenger allows users to communicate using mobile devices. Sending messages to and from a mobile device using Yahoo Messenger is a very simple process and differs only from MSN Messenger in that you must first purchase a messages on account. ● After that the process of sending the messages is transparent. ● To start sending and receiving messages in this manner you must register your mobile phone with Yahoo and validate the phone number via a text message. ● After this the only thing left to do is to purchase a number of text messages from Yahoo, after which the messages can be sent. ● The process is automatic and immediately credits your Yahoo identity with the number of text messages purchased. ● Sending a message is simply a matter of clicking on the ‘text’ icon on the toolbar and type in the text of the message, in this case from the suspect to the victim’s account. ● Forensic examination of the suspect’s computer did not reveal the victim’s telephone number or the text of the message. ● The text of the message is found within the ‘user data’ field of the message, which is preceded by the sender’s Yahoo identity. ● Unfortunately, examination of this data does not show any obvious clue that the message was sourced from Yahoo at all; it could have been sent from any facility.	7
C	What is web browsing 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

	 Web activity □ We con reconstruct a detailed history of a computer's use by examining a handful of files that contain the web browser's history. Internet explorer uses three facilities where we can find evidence: □ Web browsing history, cookies, and temp internet files  A cookie contains: □ the variable name. □ the value for the variable. □ the website that issued the cookie. □ Flags □ the expiration time for the cookie. □ the creation time for the cookie. □ An * since it is the record delimiter	
D	What is Email forensic? Explain CAN-SPAM Act in email crimes. Email forensic 4M + CAN-SPAM Act in email crimes 3M The process includes identifying the actual sender, recipient, date, time and location of mail transaction, intention of the sender, etc. It also involves investigation of metadata, keyword searching, port scanning, etc. various techniques that are used for email investigation are: *Header Analysis OF Emails* While investigating emails, we usually start from a scratch and analyze the headers of the mails. Headers contain information about the senders of the emails and also information about the path through which the emails have travelled. During the time of a crime, the email headers are spoofed in order to hide the identity of the sender. If the messages passing through SMTP server do not possess SMTP idiosyncrasies, then they are faked. *Link Analysis*	7

Link analysis is a graphical data analysis method to evaluate emails exchanged between users. Since a crime can involve multiple suspects, link analysis is used in order examine the link between the suspects. Since there can be thousands of mails that are linked between suspects, therefore it becomes a time consuming task that defeats the purpose of email investigation.

Bait Tactics

The basic aim of the bait tactics is to extract the IP address of the culprit. In this technique, an email with http:<img src>tag which has some image source at a computer that is monitored by investigators is sent to the email address that under investigation. Now the recipient is the one who originally was sender during the crime. When the email is opened, a log entry which contains the IP address of the recipient is recorded on the server which is hosting the image and the recipient is tracked.

Investigation Of Server

In the server investigation, server logs and copies of delivered messages between sender and receiver are investigated. The emails from the sender and receiver which are not recoverable are received or extracted from proxy or ISP servers, as the servers store a copy of all the emails after their respective delivery.

Investigating Network Device

The source of an email message can also be investigated with the help of logs maintained by network devices such as routers, firewalls and switches. Owing to its complexity, this technique is only deployed in the absence of logs of ISP or proxy servers. Unavailability of server logs may occur due to various reasons like absence of chain of evidences.

Fingerprints Of Sender Mailers

The received header field proves to be helpful in the identification of software which handles email at server. Also different set of headers like "X-Mailers" can be used for the identification of the software which handles email at the client. These headers describe information about the applications and their servers used by the client to send emails.

Software Embedded Identifiers

The information about the creator of emails may be included in the custom headers or in form of MIME contents as a TNEF. The investigation may reveal names of PST files, MAC address, etc. of the computer, which was used to send emails.

1. The CAN-SPAM Act establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations. ... That means all email – for example, a message to former customers announcing a new product line – must comply with the law.
2. The Spam Act 2003 (Cth) is an Act passed by the Australian Parliament in 2003 to regulate commercial e-mail and other types of commercial electronic messages. The Act restricts spam, especially e-mail spam and some types of phone spam, as well as e-mail address harvesting. However, there are broad exemptions.

Q3	ATTEMPT ANY 3 FROM THE FOLLOWING:	[21]
A	State and explain properties of evidence. 3 properties 6M +1M example admissible, authentic, reliable	7
B	Discuss the information technology act in detail. information technology act 3M + 4M for acts The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). · The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In). · This is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. · Objectives of the Act are: • o To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication; o To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law. o To facilitate electronic filing of documents with Government departments o To facilitate electronic storage of data o To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.	7
C	“Warning banners are often easier to present in court than policy manuals are”. Justify with an example.	7

	Justification 7M ● 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 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.	
D	Solve the following case study: Following the Russian annexation of Crimea in February 2014, international tensions built over allegations that Russian troops were operating in other parts of Ukraine. Russian officials repeatedly denied these allegations Starting in late June 2014, Alexander Sotkin, a sergeant in the Russian Army, posted a month-long series of selfies taken from his cell phone to his public Instagram account. The press picked the story up when it was discovered that the jpeg files posted included geotag metadata, and that the geotags and pictures showed the sergeant moving on-duty from a military base in Russia into eastern Ukraine and then back to the base. Analysis-7M Geotags, such as those embedded in Sotkin's pictures, are a form of locational metadata. Geotags generated by smartphones tend to be very accurate and are associated with other types of file metadata, like date- and timestamps. Combine these attributes with the conventional wisdom that a picture is worth a thousand words and reports showing that smartphone users take over 150 pictures per month, and you have a treasure trove of data to pin down who/what/when/where details during an investigation.	7

	Geotags and other types of locational data can also be embedded in other types of files, such as video files and SMS text messages. Other cell phone locational data can be drawn from routes stored in mapping applications, Wi-Fi connections, cell towers in call history and applications like weather or real estate tools.	
Q4	ATTEMPT ANY 3 FROM THE FOLLOWING:	[12]
A	Write a brief note on Order of volatility. Order of volatility refers to the order in which you should collect evidence. Volatile doesn't mean it's explosive, but rather that it is not permanent. In general, you should collect evidence starting with the most volatile and moving to the least volatile.	4
B	What is a search warrant? State its components. A *search warrant* is a document signed by a magistrate giving law enforcement officers the authority to search a specified place for specific items that are particularly described in the warrant. There are three basic parts of a Search Warrant. The Warrant itself, the Affidavit and the Return	4
C	State any two recent cases of Obscenity. 1) Ranbir singh case 2) Raj Kundra case ,etc	4
D	Explain the fourth amendment of United states constitution. The Constitution, through the Fourth Amendment, protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law.	4

****