Ethical Hacking

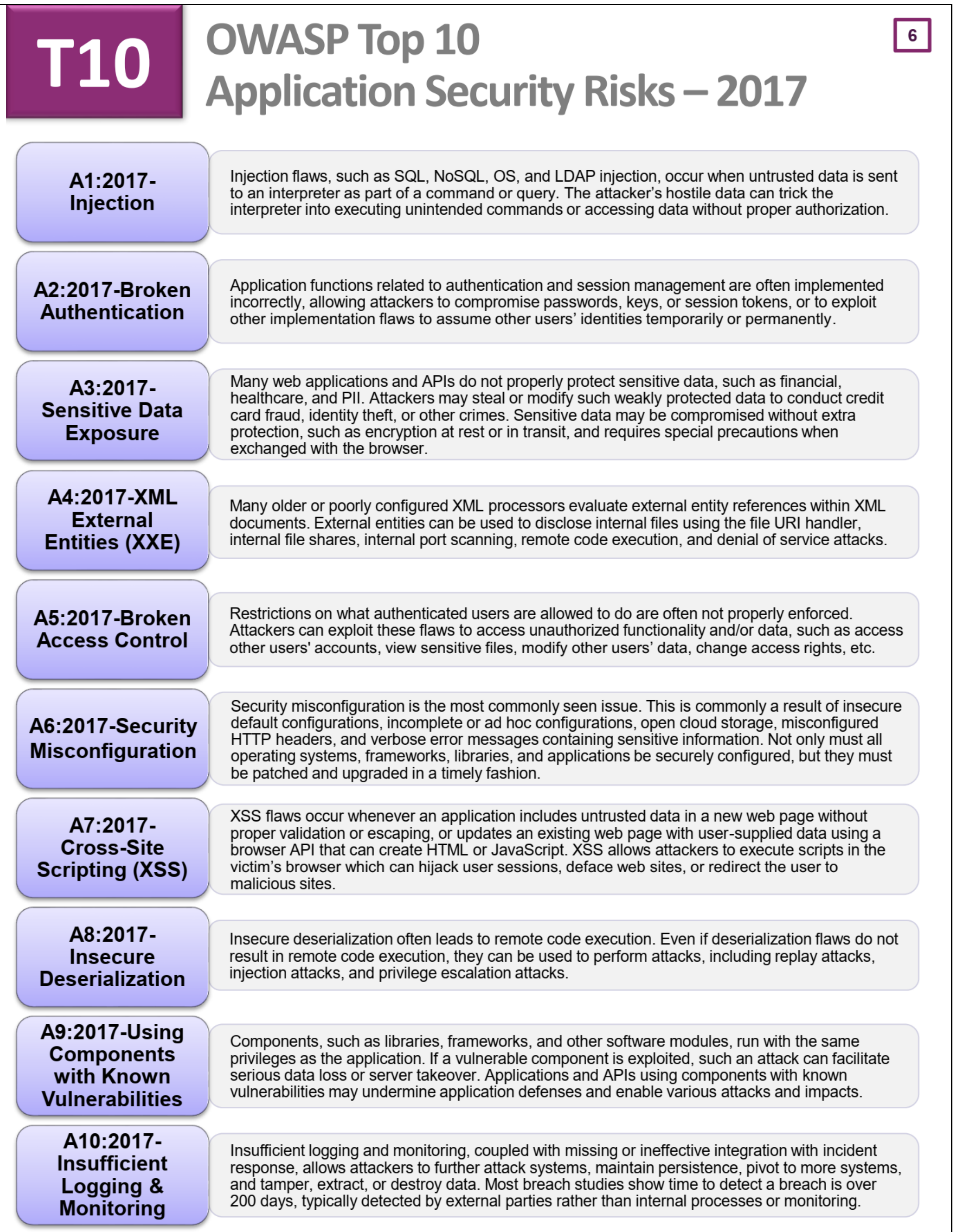
Information Security: Attacks and Vulnerabilities Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Malware, Worms, viruses, Trojans, Spyware, Rootkits, Types of vulnerabilities: Top 10 OWASP.

Types of attacks and their common prevention mechanisms: Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs

Case-studies: Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit, Media Markt, Kaseya, JBS, Colonial Pipeline, The University of California at San Francisco.

UNIT 1

1	
ANS:	
2	What is OWASP Top 10? List the Ten Most Critical Web Application Security Risks.
ANS:	• The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. • At OWASP, you'll find free and open: – Application security tools and standards. – Complete books on application security testing, secure code development, and secure code review. – Presentations and videos. – Cheat sheets on many common topics. – Standard security controls and libraries. – Local chapters worldwide. – Cutting edge research. – Extensive conferences worldwide. – Mailing lists. • A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. • The Top 10 provides basic techniques to protect against these high risk problem areas, and provides guidance on where to go from here.



T10

OWASP Top 10
Application Security Risks – 2017

6

A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

3	What is OWASP Top 10? Explain in brief any one of the Ten Most Critical Web Application Security Risks.
ANS:	OWASP TOP 10 pdf
4	W.r.t to attacks in security explain the following with an example: a. Keystroke Logging b. Denial of Service (DoS /DDoS) c. brute force d. phishing and fake WAP e. Eavesdropping f. Man-in-the-middle

g. Session Hijacking
h. Cookie Theft
i. Buffer Overflow
j. ARP poisoning
k. Identity Theft
l. Waterhole attack
m. Clickjacking.
n. URL Obfuscation
o. IoT Attacks

ANS:

a. Keystroke Logging

- Keylogger is spy software to be installed on a computer or a spying device to be plugged into a computer.
- Basic keylogger saves all text typed using a computer keyboard.
- Advanced models have more functions like taking screenshots, sending reports to e-mail, storing history of browsing and opened apps.
- Installation of **software keylogger, which sends logs on a pre-defined e-mail address**, usually takes less than a minute.
- Thanks to a **keylogger that sends stored data straight to your e-mail**, you just need to open your inbox to learn what pages a person spied on visited, what messages they wrote and to whom and more.
- **Keylogger sends report to a predefined e-mail address**.
- It is **super simple – just type in the address** in an appropriate place.
- Hardware keylogger also **stores files with computer logs**.
- If you have access to the monitored computer, all you need to do is press the **appropriate key combination** to see the whole log.
- In this way, you can also check if the keylogger works correctly after plugging it into a computer.
- A keylogger (short for keystroke logger) is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don’t know that your actions are being monitored.
- This is usually done with malicious intent to collect your account information, credit card numbers, user names, passwords, and other private data.
- Legitimate uses do exist for keyloggers.
- Parents can monitor their children’s online activity or law enforcement may use it to analyse and track incidents linked to the use of personal

computers, and employers can make sure their employees are working instead of surfing the web all day.

- Nevertheless, keyloggers can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard.
- As a result, cybercriminals can get PIN codes and account numbers for your financial accounts, passwords to your email and social networking accounts and then use this information to take your money, steal your identity and possibly extort information and money from your friends and family.
- **How would I get a keylogger?**
  - Keyloggers spread in much the same way that other malicious programs spread.
  - Excluding cases where keyloggers are purchased and installed by a jealous spouse or partner, and the use of keyloggers by security services, keyloggers are installed on your system when you open a file attachment that you received via email, text message, P2P networks, instant message or social networks.
  - Keyloggers can also be installed just by you visiting a website if that site is infected.
- **How do you detect a keylogger?**
  - Keyloggers are tricky to detect. Some signs that you may have a keylogger on your device include: slower performance when web browsing, your mouse or keystrokes pause or don’t show up onscreen as what you are typing or if you receive error screens when loading graphics or web pages.
- **What can you do to protect yourself?**
  - Just as you maintain your own health on a daily basis by eating well-balanced meals, getting plenty of rest and exercising, you must also maintain your computer or mobile device’s health.
  - That means avoiding keyloggers by avoiding actions that could negatively affect your computer, smartphone or tablet, like visiting dangerous websites or downloading infected programs, videos or games.
  - Here are some tips:
    - **Use caution when opening attachments** – files received via email, P2P networks, chat, social networks, or even text

messages (for mobile devices) can be embedded with malicious software that has a keylogger.

- **Watch your passwords** – Consider using one-time passwords and make sure key sites you log into offer two-step verification. You could also use a password manager like McAfee SafeKey that is available with McAfee LiveSafe™ service, which will automatically remember your user name and passwords, but also prevent keylogging since you are not typing in any information on the site as the password manager will do that for you.

- **Try an alternative keyboard layout** – Most of the keylogger software available is based on the traditional QWERTY layout so if you use a keyboard layout such as DVORAK, the captured keystrokes do not make sense unless converted.

- **Use a comprehensive security solution** – Protect all your devices—PCs, Macs, smartphones and tablets—with a solution like McAfee LiveSafe, that offers antivirus, firewall, as well as identity and data protection.

b. Denial of Service (DoS /DDoS)

- A “denial of service” or DoS attack is used to tie up a website’s resources so that users who need to access the site cannot do so.
- Many major companies have been the focus of DoS attacks.
- Because a DoS attack can be easily engineered from nearly any location, finding those responsible can be extremely difficult.
- DoS attacks have evolved into the more complex and sophisticated “distributed denial of service” (DDoS) attacks.
- Attackers include hacktivists (hackers whose activity is aimed at promoting a social or political cause), profit-motivated cybercriminals, and nation states.
- DoS attacks generally take one of two forms. They either flood web services or crash them.
- Flooding attacks
  - Flooding is the more common form DoS attack.
  - It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle.
  - The system eventually stops.
  - An ICMP flood — also known as a ping flood — is a type of DoS attack that sends spoofed packets of information that hit every computer in a targeted network, taking advantage of misconfigured network devices.

    - A SYN flood is a variation that exploits a vulnerability in the TCP connection sequence.
    - This is often referred to as the three-way handshake connection with the host and the server.
    - Here’s how it works:
        - The targeted server receives a request to begin the handshake.
        - But, in a SYN flood, the handshake is never completed.
        - That leaves the connected port as occupied and unavailable to process further requests.
        - Meanwhile, the cybercriminal continues to send more and more requests, overwhelming all open ports and shutting down the server.
- Crash attacks
    - Crash attacks occur less often, when cybercriminals transmit bugs that exploit flaws in the targeted system.
    - The result? The system crashes.
    - Crash attacks — and flooding attacks — prevent legitimate users from accessing online services such as websites, gaming sites, email, and bank accounts.
- How a DoS attack works
    - Unlike a virus or malware, a DoS attack doesn’t depend on a special program to run.
    - Instead, it takes advantage of an inherent vulnerability in the way computer networks communicate.
    - Here’s an example.
    - Suppose you wish to visit an e-commerce site to shop for a gift.
    - Your computer sends a small packet of information to the website.
    - The packet works as a “hello” – basically, your computer says, “Hi, I’d like to visit you, please let me in.”
    - When the server receives your computer’s message, it sends a short one back, saying in a sense, “OK, are you real?” Your computer responds — “Yes!” — and communication is established.
    - The website’s homepage then pops up on your screen, and you can explore the site.
    - Your computer and the server continue communicating as you click links, place orders, and carry out other business.
    - In a DoS attack, a computer is rigged to send not just one “introduction” to a server, but hundreds or thousands.
    - The server — which cannot tell that the introductions are fake — sends back its usual response, waiting up to a minute in each case to hear a reply.
    - When it gets no reply, the server shuts down the connection, and the computer executing the attack repeats, sending a new batch of fake requests.
    - DoS attacks mostly affect organizations and how they run in a connected world.

    - For consumers, the attacks hinder their ability to access services and information.
- Other types of attacks: DDoS
    - Distributed denial of service (DDoS) attacks represent the next step in the evolution of DoS attacks as a way of disrupting the Internet.
    - Here’s why DDoS attacks have become the weapon of choice for disrupting networks, servers, and websites.
    - The attacks use large numbers of compromised computers, as well as other electronic devices — such as webcams and smart televisions that make up the ever-increasing Internet of Things — to force the shutdown of the targeted website, server or network.
    - Security vulnerabilities in Internet-of-Things devices can make them accessible to cybercriminals seeking to anonymously and easily launch DDoS attacks.
    - In contrast, a DoS attack generally uses a single computer and a single IP address to attack its target, making it easier to defend against.
- How to help prevent DoS attacks
    - If you rely on a website to do business, you probably want to know about DoS attack prevention.
    - A general rule: The earlier you can identify an attack-in-progress, the quicker you can contain the damage.
    - Here are some things you can do.
        - *Method 1: Get help recognizing attacks*
            - Companies often use technology or anti-DDoS services to help defend themselves.
            - These can help you recognize between legitimate spikes in network traffic and a DDoS attack.
        - *Method 2: Contact your Internet Service provider*
            - If you find your company is under attack, you should notify your Internet Service Provider as soon as possible to determine if your traffic can be rerouted.
            - Having a backup ISP is a good idea, too.
            - Also, consider services that can disperse the massive DDoS traffic among a network of servers.
            - That can help render an attack ineffective.
        - *Method 3: Investigate black hole routing*
            - Internet service providers can use “black hole routing.”
            - It directs excessive traffic into a null route, sometimes referred to as a black hole.
            - T0his can help prevent the targeted website or network from crashing.
            - The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.
        - *Method 4: Configure firewalls and routers*

        - Firewalls and routers should be configured to reject bogus traffic.
        - Remember to keep your routers and firewalls updated with the latest security patches.
    - *Method 5: Consider front-end hardware*
        - Application front-end hardware that's integrated into the network before traffic reaches a server can help analyse and screen data packets.
        - The hardware classifies the data as priority, regular, or dangerous as they enter a system.
        - It can also help block threatening data.

c. brute force

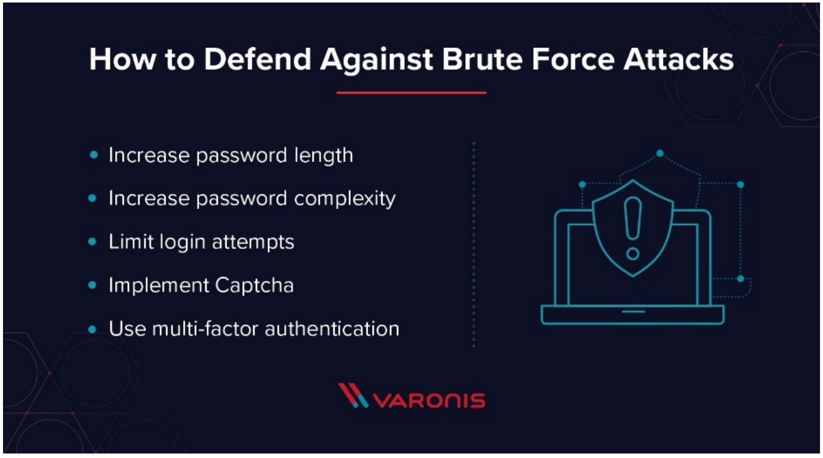
- An attacker could launch a brute force attack by trying to guess the user ID and password for a valid user account on the web application.
- If the brute force attempt is successful, the attacker might be able to access:
- Confidential information, such as profile data for users or confidential documents stored on the web application
- Administration tools used by the System Administrator for the web application to manage (modify, delete, add) web application content, manage user provisioning, or to assign different privileges to users
- Sections of the web application that might expose vulnerabilities or advanced functions not available to non-Administrator users
- Types of brute force attacks
- An attacker might try the following attack methods to find out valid authentication credentials for a web application:

Attack type	**Attack description**
Dictionary attacks	Automated tools that try to guess user names and passwords from a dictionary file. A dictionary file might contain words gathered by the attacker to understand the user of the account about to be attacked, or to build a list of all the unique words available on the web site.
Search attacks	Covers all possible combinations of a character set and ranges of password length. This attack might take some time because of the large amount of possible combinations.
Rule-based search attacks	Uses rules to generate possible password variations from part of a user name or from modifying pre-configured mask words in the input.

Table 1. Brute force attacks

- Brute force attacks are simple and reliable.
- Attackers let a computer do the work – trying different combinations of usernames and passwords, for example – until they find one that works.
- Catching and neutralizing a brute force attack in progress is the best counter: once attackers have access to the network, they're much harder to catch.
- Types of Brute Force Attacks

    - The most basic brute force attack is a dictionary attack, where the attacker works through a dictionary of possible passwords and tries them all.
    - Dictionary attacks start with some assumptions about common passwords to try to guess from the list in the dictionary.
    - These attacks tend to be somewhat outdated, given newer and more effective techniques.
    - Computers are so fast that they can brute force decrypt a weak encryption hash in mere months.
    - These kinds of brute force attacks are known as an exhaustive key search, where the computer tries every possible combination of every possible character to find the right combination.
    - Credential recycling is another type of brute force attack that reuses usernames and passwords from other data breaches to try to break into other systems.
    - The reverse brute-force attack uses a common password like "password," and subsequently tries to brute force a username to go with that password.
- How to Defend Against Brute Force Attacks



How to Defend Against Brute Force Attacks

- Increase password length
- Increase password complexity
- Limit login attempts
- Implement Captcha
- Use multi-factor authentication

VARONIS

- Brute force attacks need time to run.
- Some attacks can take weeks or even months to provide anything usable.

– Most of the defences against brute force attacks involve increasing the time required for success beyond what is technically possible, but that is not the only defence.

  - ✦ **Increase password length**: More characters equal more time to brute force crack
  - ✦ **Increase password complexity**: More options for each character also increase the time to brute force crack
  - ✦ **Limit login attempts**: Brute force attacks increment a counter of failed login attempts on most directory services – a good defence against brute force attacks is to lock out users after a few failed attempts, thus nullifying a brute force attack in progress
  - ✦ **Implement Captcha**: Captcha is a common system to verify a human is a human on websites and can stop brute force attacks in progress
  - ✦ **Use multi-factor authentication**: Multi-factor authentication adds a second layer of security to each login attempt that requires human intervention which can stop a brute force attack from success

– The proactive way to stop brute force attacks starts with monitoring.

– It’s better to detect an attack in progress and actively stop the attack than it is to hope your passwords are un-crackable.

– Once you detect and stop the attack, you can even blacklist IP addresses and prevent further attacks from the same computer.

d. phishing and fake WAP

PHISHING

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Common Features of Phishing Emails

  → **Too Good To Be True -** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people’s attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true, it probably is!

  → **Sense of Urgency -** A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just

	ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email. → **Hyperlinks -** A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully. → **Attachments -** If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file. → **Unusual Sender -** Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it! ➢ *What is phishing* • Phishing is a devious approach that cybercrooks use to trick you into revealing personal information, such as passwords or credit card, social security, and bank account numbers. • They do this by sending you fake emails or directing you to a fake website. ➢ *Where phishing attacks come from* • Phishing messages seem to be from legitimate organizations like PayPal, UPS, a government agency or your bank; however, these are in fact clever cons. • The emails politely request updates, validation or confirmation of account information, often suggesting that there is a problem. • You're then redirected to a fake site and tricked into entering account information, which can result in identity theft. ➢ *How to recognize a phishing scam* • You get messages asking you to reveal personal information, usually via email or via a website. • Anti-phishing tools help detect **phishing emails and websites**. Avast Internet Security offers you the best anti-phishing software. ➢ *How to remove phishing* • While phishing lures can't be "removed," they can be detected. • Monitor your website and be aware of what should and shouldn't be there. • If possible, change the core files of your website on a regular basis. ➢ *How to prevent phishing* • Have good habits and don't respond to links in unsolicited emails or on Facebook.

- Don't open attachments from unsolicited emails.
- Protect your passwords and don't reveal them to anyone.
- Don't give sensitive information to anyone—on the phone, in person or through email.
- Look at a website's URL (web address). In many phishing cases, the web address may look legitimate, but the URL may be misspelled or the domain may be different (.com when it should be .gov).
- Keep your browser up to date and apply security patches.
- Use anti-phishing software to detect phishing emails and websites.

FAKE WAP

- Everyone always hears about hackers and hacking and thinks that it is something that only happens to big companies.
- Or they think it only happens to important people.
- This is not the case, especially when we start looking at public WiFi.
- More than anything, hackers love a vulnerable audience.
- They want an audience that is going to take something without thinking.
- Who doesn't want to take free WiFi at every opportunity? Hackers know this, and that's why they have come up with a common hack known as a fake WAP.

➢ **The fake WAP: Stealing your information made easy**

- A fake WAP hack takes place in public spaces where there is free WiFi.
- This includes your local coffee shop, the airport, and shopping centers.
- Most fake WAP hacks start when a hacker downloads a program.
- You don't need any special hacking skills. You just download a program.
- In some instances, you don't even have to download a program as most phones already have this built into them. It is called a 'hot spot' in common parlance.
- Once a device is setup to broadcast its own WiFi signal is when the true hacking will start.
- Hackers will then use another tool, one which is usually built into Aircrack-NG Suite, for jamming and deauthentication.
- Once the local Wi-Fi signal has been jammed or deauthenticated they can then force you to connect to the wireless access point that they have set up.
- This is where problems start.

➢ **What is the point of a fake WAP?**

– There are three main things that hackers are trying to do with a fake WAP:

- **Steal your password and login:** Since so many people use the same password and login for all of their accounts, hackers will require you to enter one to connect to their fake WiFi. They will then take that information and try to use it to sign into other websites. Think about your Amazon account, eBay, banking, etc. This will be done using basic brute force tools.

- **Man in the middle attack:** Hackers will use something like Ettercap for a man-in-the-middle attack. This hack will sniff any data that you send over their wireless access point, giving them free access to your data. Again, they're looking for login details and passwords. If you do any banking over this public WiFi you can say goodbye to your money.
- **Device control:** Hackers can take control of your device using a tool like the Metasploit Project. You won't have to worry about your passwords or logins anymore, you will no longer have control of your computer.

➢ **Defend against the fake WAP**

- Here are the steps you need to take to protect yourself from a fake WAP in a public setting:

– **Get the correct WiFi:** When you are in a public setting you will no doubt find a number of open WiFi networks. Be sure to find the person responsible for administering it before you connect. Talk to a security guard in the mall. Talk to the librarian. Make sure that you are connecting to an official WiFi account using the correct name.

– **Unique passwords:** The most basic fake WAP hack can be easily thwarted by simply creating new passwords for each account. If you can't do that, do yourself a favor and do not connect to the wireless access point if it asks for signin details. 1Password can help you with this as well.

– **Using encryption:** Encryption does not have to be scary. It is just another tool that is used in today's modern world. The easiest way to get encryption on public WiFi is by using a VPN service. These tools will automatically encrypt all of the data that you send over any WiFi network. This isn't just beneficial to protect yourself against a fake WAP, but a number of other possible hacks and online tracking activities.

– **VPN blockage:** You will know for certain that you do not want to be on a WiFi network when it blocks you from using a VPN. Even if it is a legitimate WiFi access point, the owner still doesn't want you to protect yourself. Would you get into a car on the condition that you not put on a seatbelt? I hope not…

– **Spoofing:** Another common problem is that once you connect to a WiFi network it sends you to spoof websites. Again, this can be where they ask for login details.

– **Becoming free:** This is when you go to a place where you know the WiFi is regularly paid, or guarded. A hacker can see this and try to play into your gullibility by suddenly changing it to being free available… Using their own WAP with the same name.

– **Auto connect:** You have to turn off the auto connect on your computer. It will want to connect to the most powerful signal in your area. A hacker can make their WAP the most powerful quite easily with a single command line.

e. Eavesdropping

➢ *What is an Eavesdropping Attack*

- An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network.
- An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

➢ *BREAKING DOWN Eavesdropping Attack*

- Eavesdropping attacks involve a weakened connection between client and server that allows the attacker to send network traffic to itself.
- Attackers can install network monitoring software (a sniffer) on a computer or a server to carry out an eavesdropping attack and intercept data during transmission.
- Any device in the network between the transmitting device and the receiving device is a point of weakness, as are the initial and terminal devices themselves.
- Knowing what devices are connected to a network and what software is installed on those devices is one way to protect against eavesdropping attacks.
- Using personal firewalls, updated antivirus software, and virtual private networks (VPN) – and avoiding public networks, especially for sensitive transactions – can help prevent eavesdropping attacks as well.
- Public Wi-Fi networks are an easy target for eavesdropping attacks.
- Anyone with the easily available password can join the network and use free software to monitor network activity and steal login credentials and valuable data that users transmit over the network.
- This is one-way people get their Facebook and email accounts hacked.
- Users can sometimes limit their exposure to such attacks by making sure their phones are running the most recent operating system version.
- However, sometimes users do not have access to the latest software version because the phone vendor does not make it available immediately.

➢ *Examples of Eavesdropping Attacks*

- In May 2011, most Android smartphones were vulnerable to an eavesdropping attack involving authentication tokens sent over unencrypted Wi-Fi networks.
- Eavesdroppers using a sniffing program called Wireshark could view, steal, modify, and delete private calendar data, contact data, and Picasa Web Album data this way.
- The attacker could change a victim’s contact data to trick the victim's contacts into sending sensitive data to the attacker.
- HTTP should not be used to transmit sensitive information such as passwords or credit card numbers because it is not encrypted and is therefore

vulnerable to attack; HTTPS or SSH (secure shell) encryption should be used instead to offer a measure of protection against eavesdropping attacks.

- However, attackers may still be able to decrypt encrypted communications to gain access to confidential information.
- In April 2015, at least 25,000 iOS apps were vulnerable to eavesdropping attacks because of a bug in an open-source code library called AFNetworking that could take down HTTPS encryption.
- The attacker only needed a valid certificate to eavesdrop on or modify an encrypted SSL (secure socket layer) session involving one of the affected apps.

f. Man-in-the-middle

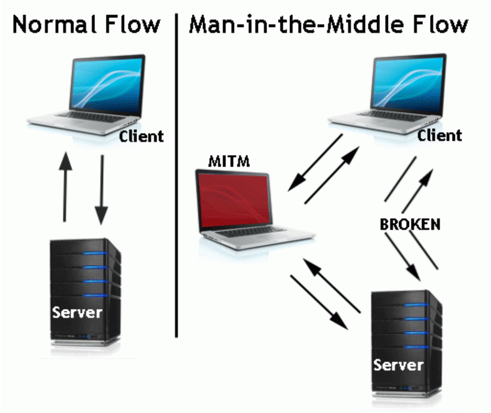
➢ *What Is a Man-in-the-Middle Attack?*

- ✦ A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other.
- ✦ A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.
- ✦ Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.

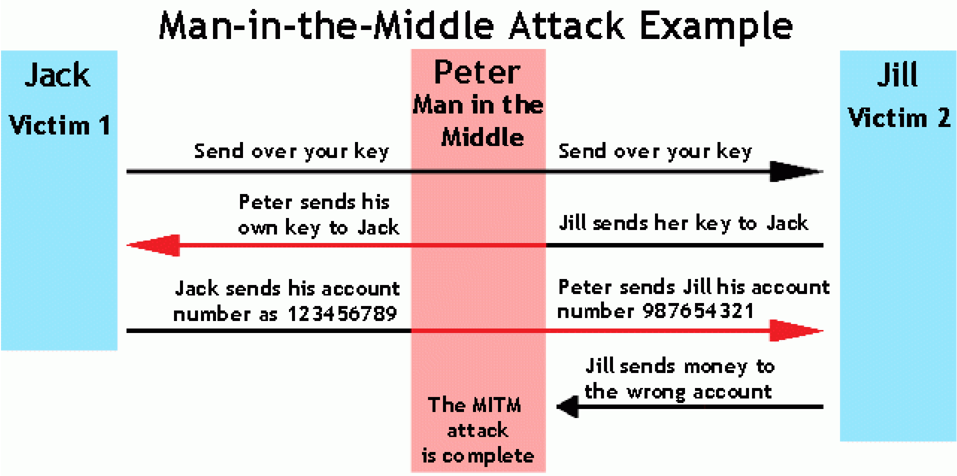
➢ *Key Concepts of a Man-in-the-Middle Attack*

- ✦ Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
- ✦ A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
- ✦ Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

➢ *Man-in-the-Middle Attack Examples*



- In the image above, you will notice that the attacker inserted him/herself in-between the flow of traffic between client and server.
- Now that the attacker has intruded into the communication between the two endpoints, he/she can inject false information and intercept the data transferred between them.
- Below is another example of what might happen once the man in the middle has inserted him/herself.


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

- The hacker is impersonating both sides of the conversation to gain access to funds.
- This example holds true for a conversation with a client and server as well as person-to-person conversations.
- In the example above, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.

➢ *Interactions Susceptible to MITM Attacks*

✦ Financial sites – between login and authentication

✦ Connections meant to be secured by public or private keys

✦ Other sites that require logins – where there is something to be gained by having access

g. Session Hijacking

- ***What is Session Hijacking?***

- The session hijacking is a type of web attack.
- It works based on the principle of computer sessions. The attack takes advantage of the active sessions.

- ***How Does Session Hijacking Works?***

- As we know, the http communication uses many TCP connections and so that the server needs a method to recognize every user's connections.
- The most used method is the authentication process and then the server sends a token to the client browser.
- This token is composed of a set of variable width and it could be used in different ways, like in the URL, in the header of http requisition as a cookie, in other part of the header of the http request or in the body of the http requisition.
- The attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the web server.
- This compromising of session token can occur in different ways.

- ***Session Sniffing***

- The first step by the attacker is getting this session id.
- The attacker uses a sniffer to get the session id. When the session id is captured, the attacker uses this session id to gain unauthorized access to the web server.

- ***The Cross-Site Script Attack***

- The cross-site script attack is a way to get the session id with the helping of running malicious code or script from the client side.
- In this attack, the attacker executes malicious scripts, also known as malicious payloads into a legitimate website or web application.
- By using this attack, the attacker does not target a victim directly, but the attacker could exploit a vulnerability in a website that the victim would visit and use the website to deliver malicious script to the victim's browser.

- ***How to prevent the Session Hijacking?***

- The method often used to steal session id is by installing a malicious code on the client website and then the cookie is stealing.
- The best way to prevent session hijacking is enabling the protection from the client side.
- It is recommended that taking preventive measures for the session hijacking on the client side.
- The users should have efficient antivirus, anti-malware software, and should keep the software up to date.
- There is a technique that uses engines which fingerprints all requests of a session.

- In addition to tracking the IP address and SSL session id, the engines also track the http headers.
- Each change in the header adds penalty points to the session and the session gets terminated as soon as the points exceeds a certain limit.
- This limit can be configured.
- This is effective because when intrusion occurs, it will have a different http header order.
- These are the recommended preventive measures to be taken from both the client and server sides to prevent the session hijacking attack.

h. **ARP poisoning**

- **ARP is the acronym for Address Resolution Protocol**.
- It is used to convert IP address to physical addresses [MAC address] on a switch.
- The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address].
- The resolved IP/MAC address is then used to communicate.
- **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic**.

➢ *ARP Poisoning Countermeasures*

  → Static ARP entries:

  - ∗ These can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets.
  - ∗ The disadvantage of this method is, it's difficult to maintain on large networks.
  - ∗ IP/MAC address mapping has to be distributed to all the computers on the network.

  → ARP poisoning detection software:

  - ∗ These systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated.
  - ∗ Uncertified IP/MAC address resolutions can then be blocked.

  → Operating System Security:

  - ∗ This measure is dependent on the operating system been used.
  - ∗ The following are the basic techniques used by various operating systems.

- **Linux based**: these work by ignoring unsolicited ARP reply packets.

- **Microsoft Windows**: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;

    - **AntiARP**– provides protection against both passive and active sniffing
    - **Agnitum Outpost Firewall**–provides protection against passive sniffing
    - **XArp**– provides protection against both passive and active sniffing

- **Mac OS**: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses.
- All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses.
- ARP Poisoning is also known as **ARP Spoofing**.
- Here is how ARP works −

    - When one machine needs to communicate with another, it looks up its ARP table.
    - If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.
    - All machines on the network will compare this IP address to MAC address.
    - If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
    - The requesting computer will store the address pair in its ARP table and communication will take place.

➢ *What is ARP Spoofing?*

✦ ARP packets can be forged to send data to the attacker's machine.

✦ ARP spoofing constructs many forged ARP request and reply packets to overload the switch.

✦ The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

✦ Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

i. Identity Theft

- Identity theft occurs when someone steals your personal information, such as your date of birth, name, and address history.
- Criminals can then use this information to commit identity fraud, typically using your identity to gain financially.
- Unfortunately, identity theft can happen to anyone. If your identity is stolen and used to commit identity fraud, you could face serious consequences.
- Perpetrators may:
- – Max out your bank or credit card funds.
- – Leave you liable for debts you didn't accrue.
- – Use your identity to commit non-financial crimes.
- – Severely damage your credit score so you are unable to take out loans or mortgages.
- Though it might be possible for you to clear your name or regain lost funds, the emotional toll and financial worries can linger for a long time.
- Therefore, it's important that you are aware of the common types of identity theft and how criminals steal information, so you can protect yourself.

➢ *Common Types of Identity Theft*

  - Identity thieves are always finding new ways to steal and use personal and confidential information. Below are some examples of how a criminal might commit identity fraud.
  - Driver's license fraud. Driver's license fraud occurs when a criminal has a driver's license issued to themselves under another person's identity. They might use the license to commit traffic violations that end up on your record and you could lose your license.
  - Financial identity theft. Criminals are able to use your stolen personal information to take over your financial accounts or create their own, which can be very serious and stressful. It can take you months or years to rectify the effects of financial identity theft and it could result in large volumes of debt and a poor credit score.
  - Child identity theft. Child identity theft is usually committed by a relative who will take out loans and credit cards in the child's name. As children have no reason to check or monitor their credit reports, they will usually remain unaware of the fraudulent activity until they come of age and require loans. This type of fraud can take years to sort out and could stop you from being able to buy a house or car. It's also likely to increase the interest rates on any loans you might be offered.
  - Change of address fraud. A fraudster could change your mailing address, diverting it to themselves instead. This allows them to look through all your mail and find out bank details, credit card details and other personal information.
  - Employment identity theft. Criminals, illegal immigrants and the jobless use stolen identification and personal details to obtain

employment. By using stolen identification, they are able to conceal their real personal history from their employers.

- *How does Identity Theft Happen?*
    - Identity theft can happen to anyone.
    - Because of this, it's important that you understand how criminals steal data so you know how to protect yourself.
    - *Theft*
        - Theft of your personal belongings, such as a purse or wallet, or of credit card or bank statements can provide criminals with your sensitive information.
        - Criminals might even go rooting through your rubbish in search of discarded bank statements, so be cautious and shred them or block out sensitive information like your name, address and account numbers.
        - Alternatively, they might attempt to steal new statements or cards directly from your mailbox.
        - You should inform your local post office immediately if you notice your mailbox has been tampered with.
    - *Phishing*
        - Phishing is a type of email scam.
        - The sender might pose as a real company, organisation or agency and prompt you to enter your personal information.
        - If an email asks you for a large amount of personal data, such as your name, address, card details or bank account numbers, do not click on any links and register the email as spam.
        - Additionally, if the email contains poor spelling or grammar, claims you won contests you didn't enter, has offers that are too good to be true or makes unrealistic threats, it's probably spam.
    - *Cold Calling*
        - Cold calling is when a criminal call you, pretending to be a real company, organisation or agency, and coerces you into providing them with your personal information.
        - You should always ignore unsolicited phone calls and assume they have bad intentions.
        - Never give them any of your personal details.
    - *Hacking*
        - From banks to retail chains, criminals can hack into computer systems and steal personal credit card and bank information.
        - Organisations will have systems in place to warn you in the event of a security breach, but before reacting to a message check with the company that your data has been compromised.

	– Once you know the alert is legitimate, takes steps to close any affected cards if necessary. ∗ *Identity fraud can be costly, both emotionally and financially.* ∗ *However, by understanding the ways criminals go about committing identity fraud and taking measures to stop people getting hold of your personal information, you can reduce the risks of being the victim of identity theft.*
5	What are BOTs and BOTNETs? Explain. From book
6	Cross site scripting
7	Sql injection
8	Example any 4 recent attacks.

CYBER FORENSICS

UNIT 3

1. Computer Forensics? How it is different from other Forensics?

ANS:

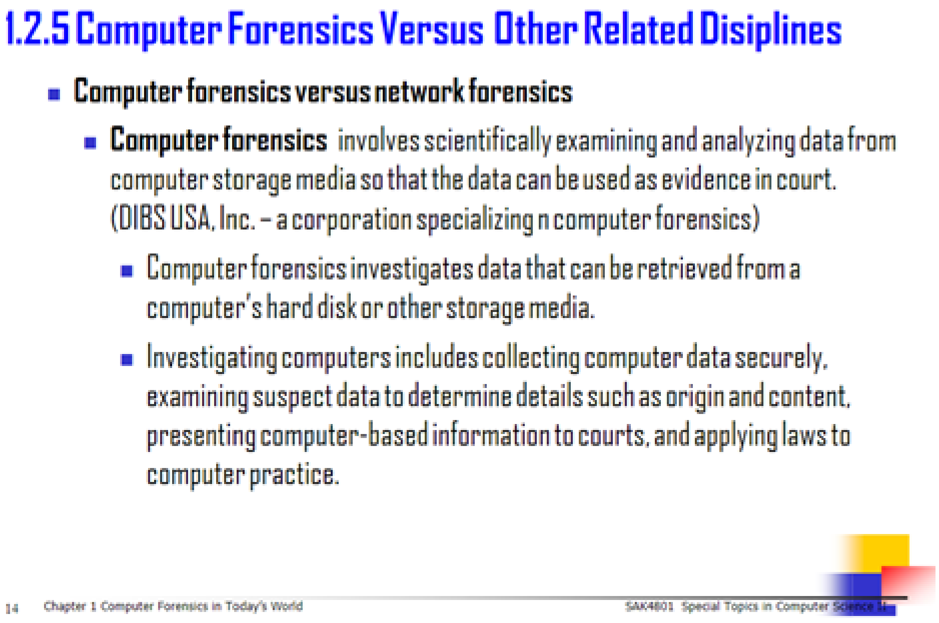
Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Although it is most often associated with the investigation of a wide variety of computer crime, 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:

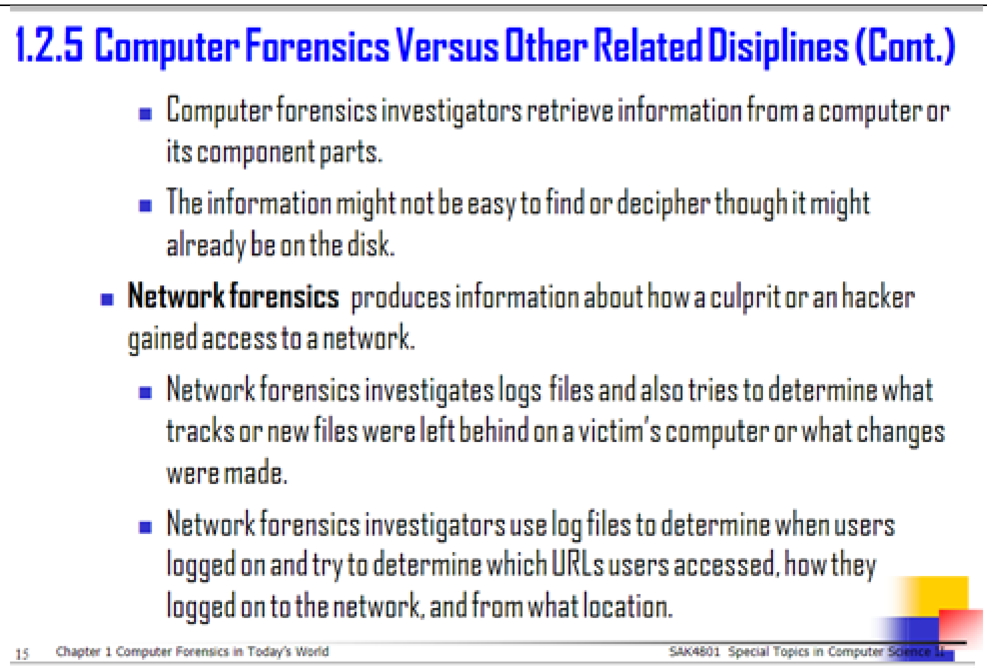
network forensic investigations deal with volatile and dynamic information. Disk or computer forensics primarily deals with data at rest.



1.2.5 Computer Forensics Versus Other Related Disiplines

- Computer forensics versus network forensics
  - **Computer forensics** involves scientifically examining and analyzing data from computer storage media so that the data can be used as evidence in court. (DIBS USA, Inc. – a corporation specializing n computer forensics)
    - Computer forensics investigates data that can be retrieved from a computer's hard disk or other storage media.
    - Investigating computers includes collecting computer data securely, examining suspect data to determine details such as origin and content, presenting computer-based information to courts, and applying laws to computer practice.

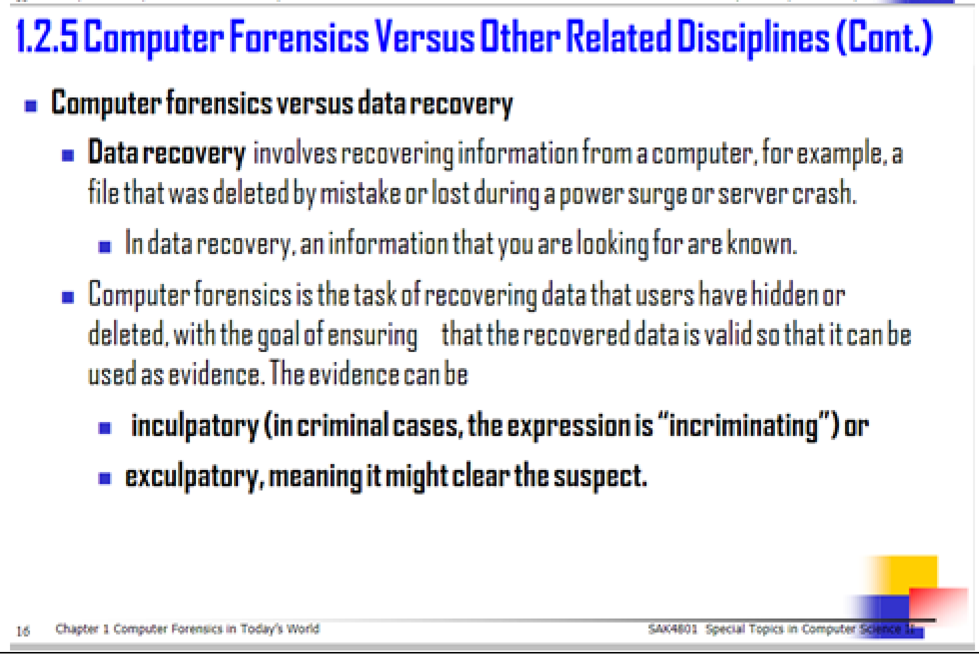
14 Chapter 1 Computer Forensics in Today's World SAK4801 Special Topics in Computer Science II



1.2.5 Computer Forensics Versus Other Related Disiplines (Cont.)

  - Computer forensics investigators retrieve information from a computer or its component parts.
  - The information might not be easy to find or decipher though it might already be on the disk.
- **Network forensics** produces information about how a culprit or an hacker gained access to a network.
  - Network forensics investigates logs files and also tries to determine what tracks or new files were left behind on a victim's computer or what changes were made.
  - Network forensics investigators use log files to determine when users logged on and try to determine which URLs users accessed, how they logged on to the network, and from what location.

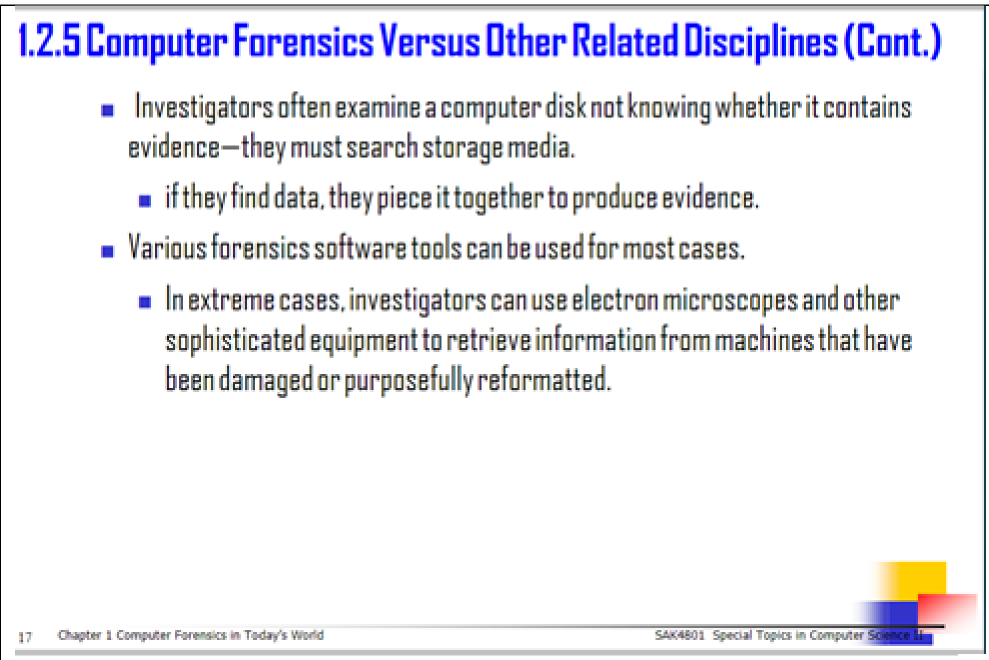
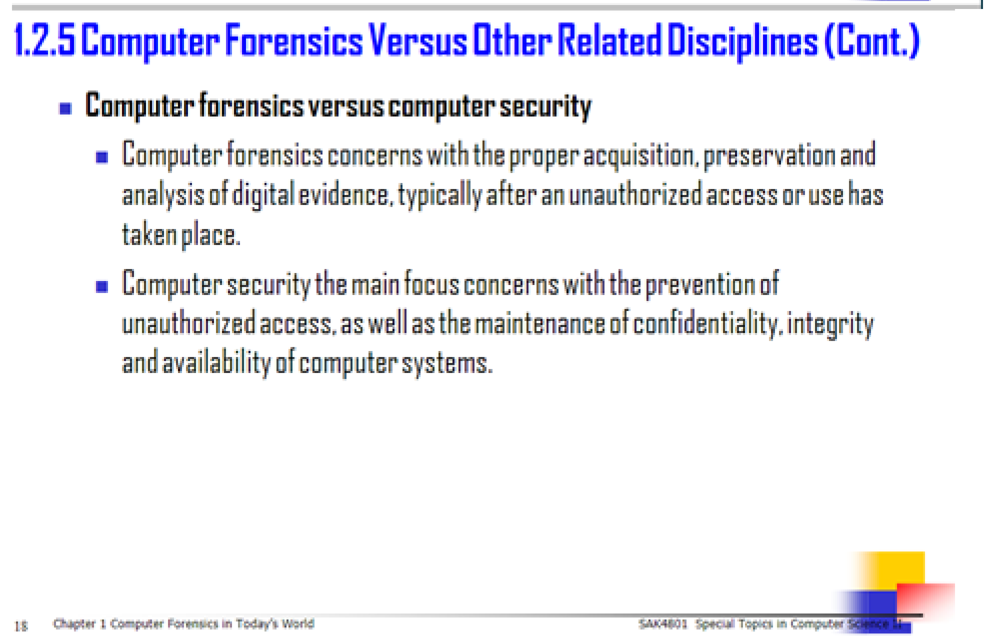
15 Chapter 1 Computer Forensics in Today's World SAK4801 Special Topics in Computer Science II



1.2.5 Computer Forensics Versus Other Related Disciplines (Cont.)

- **Computer forensics versus data recovery**
  - **Data recovery** involves recovering information from a computer, for example, a file that was deleted by mistake or lost during a power surge or server crash.
    - In data recovery, an information that you are looking for are known.
  - Computer forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence. The evidence can be
    - **inculpatory (in criminal cases, the expression is "incriminating") or**
    - **exculpatory, meaning it might clear the suspect.**

16 Chapter 1 Computer Forensics in Today's World SAK4801 Special Topics in Computer Science II

	 **1.2.5 Computer Forensics Versus Other Related Disciplines (Cont.)** ▪ Investigators often examine a computer disk not knowing whether it contains evidence—they must search storage media. ▪ if they find data, they piece it together to produce evidence. ▪ Various forensics software tools can be used for most cases. ▪ In extreme cases, investigators can use electron microscopes and other sophisticated equipment to retrieve information from machines that have been damaged or purposefully reformatted. 17 Chapter 1 Computer Forensics in Today's World SAK4801 Special Topics in Computer Science II  **1.2.5 Computer Forensics Versus Other Related Disciplines (Cont.)** ▪ **Computer forensics versus computer security** ▪ Computer forensics concerns with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place. ▪ Computer security the main focus concerns with the prevention of unauthorized access, as well as the maintenance of confidentiality, integrity and availability of computer systems. 18 Chapter 1 Computer Forensics in Today's World SAK4801 Special Topics in Computer Science II
2.	E procedures for Network Forensics.
ANS:	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.
3.	Data Recovery and write its steps.
ANS:	● Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible. ● How data recovery works ■ 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.

  - If the file still exists -- and it is not damaged or encrypted -- it can be recovered.
  - If the file is damaged, missing or encrypted, there are other ways of recovering it.
  - If the file is physically damaged, it can still be reconstructed.
  - Many applications, such as Microsoft Office, put uniform headers at the beginning of files to designate that they belong to that application.
  - Some utilities can be used to reconstruct the file headers manually, so at least some of the file can be recovered.
  - Most data recovery processes combine technologies, so organizations aren't solely recovering data by tape.
  - Recovering core applications and data from tape takes time, and you may need to access your data immediately after a disaster.
  - There are also risks involved with transporting tapes.
  - In addition, not all production data at a remote location may be needed to resume operations.
  - Therefore, it's wise to identify what can be left behind and what data must be recovered.

- Data recovery techniques
  - Instant recovery, also known as *recovery in place*, tries to eliminate the recovery window by redirecting user workloads to the backup server. A snapshot is created so the backup remains in a pristine state and all user write operations are redirected to that snapshot; users then work off the backup virtual machine (VM) and the recovery process begins in the background.
  - Users have no idea the recovery is taking place, and once the recovery is complete, the user workload is redirected back to the original VM.
  - One way to avoid the time-consuming and costly process of data recovery is to prevent the data loss from ever taking place.

	■ Data loss prevention (DLP) products help companies identify and stop data leaks, and come in two versions: stand-alone and integrated. ■ Stand-alone DLP products can reside on specialized appliances or be sold as software. ■ Integrated DLP products are usually found on perimeter security gateways and are useful for detecting sensitive data at rest and in motion. ■ Unlike stand-alone data loss prevention products, integrated DLP products usually do not share the same management consoles, policy management engines and data storage.
4.	Order of volatility.
ANS:	***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. ● Many forensic tools include the ability to capture volatile data. ● Once it’s captured, experts can analyse it and gain insight into what the computer and user were doing. ● You might not be the forensic expert capturing and analysing the data, but you certainly don’t want to be the technician that destroyed it. ● You should know the order of volatility of data and what you can do to protect evidence. ● A processor can only work on data in random access memory (RAM), so all the data in RAM indicates what the system was doing. ● This includes data a user has been working on, system processes, network processes, application remnants, and much more. ● All of this can be valuable evidence in an investigation, but the evidence is lost when the computer is turned off.

- Due to this, it is important to realize you shouldn’t power a computer down if it’s suspected to be involved in a security incident.
- Data worked on by the central processing unit (CPU) is held in the CPU cache.
- A system has less cache than regular RAM so data in cache is more likely to be overwritten sooner than data in regular RAM.
- In other words, the CPU cache is more volatile than regular RAM and should be collected first if possible.
- In contrast, data on hard disk drives (HDDs) remains on the HDD even after powering a system down.
- This includes any files and even low-level data such as the master boot record on a disk.
- While a computer is running, it maintains a paging file (also called a swap file) as an extension of memory.
- The paging file is stored on the HDD so it is less volatile than RAM.
- However, the paging file is rebuilt after rebooting a computer so it is more volatile than regular files stored on a HDD.
- Any data stored on a remote system is less volatile than data stored directly on a computer.
- As an example, many servers send log files to remote systems for centralized collection.
- Even if the original computer is completely destroyed, these log files are still available.
- Last, data stored on archive media such as backup tapes of optical media is the least volatile.
- This data is offline and much less likely to be destroyed or corrupted than any online data.
- The order of volatility from most volatile to least volatile is:
    - Data in RAM, including CPU cache and recently used data and applications
    - Data in RAM, including system and network processes
    - Swap files (also known as paging files) stored on local disk drives
    - Data stored on local disk drives
    - Logs stored on remote systems

- Archive media

5. Standard procedure for computer forensics.

ANS:

- □ *Make an initial assessment about the type of case you’re investigating—*
  - ▪ To assess the type of case you’re handling, talk to others involved in the case and ask questions about the incident.
  - ▪ Have law enforcement or company security officers already seized the computer, disks, and other components?
  - ▪ Do you need to visit an office or another location?
  - ▪ Was the computer used to commit a crime, or does it contain evidence about another crime?
- □ *Determine a preliminary design or approach to the case—*
  - ▪ Outline the general steps you need to follow to investigate the case.
  - ▪ If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours.
  - ▪ If you’re preparing a criminal case, determine what information law enforcement officers have already gathered.
- □ *Create a detailed checklist—*
  - ▪ Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step.
  - ▪ This outline helps you stay on track during the investigation.
- □ *Determine the resources you need—*
  - ▪ Based on the OS of the computer you’re investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.
- □ *Obtain and copy an evidence drive—*
  - ▪ In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, USB drives, PDAs, and other removable media.
  - ▪ Make a forensic copy of the disk.
- □ *Identify the risks—*

- ▪ List the problems you normally expect in the type of case you’re handling.
- ▪ This list is known as a standard risk assessment.
- ▪ For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.

□ *Mitigate or minimize the risks—*

- ▪ Identify how you can minimize the risks.
- ▪ For example, if you’re working with a computer on which the suspect has likely password protected the hard drive, you can make multiple copies of the original media before starting.
- ▪ Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.

□ *Test the design—*

- ▪ Review the decisions you’ve made and the steps you’ve completed.
- ▪ If you have already copied the original media, a standard part of testing the design involves comparing hash values to ensure that you copied the original media correctly.

□ *Analyze and recover the digital evidence—*

- ▪ Using the software tools and other resources you’ve gathered, and making sure you’ve addressed any risks and obstacles, examine the disk to find digital evidence.

□ *Investigate the data you recover—*

- ▪ View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect’s guilt or innocence.

□ *Complete the case report—*

- ▪ Write a complete report detailing what you did and what you found.

□ *Critique the case—*

- ▪ Self-evaluation is an essential part of professional growth.

After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.

6. Chain of Custody in detail with example.

ANS:

- 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.

CHAIN OF CUSTODY CHECKLIST

+ Have a plan before an incident occurs. Identify your “go-to” people, whether in-house or outside, while the waters are still calm.

+ Do not touch the computer unless you are experienced in digital forensics. Thousands of files are altered simply by turning it on.

+ Document the location and condition of everything before touching anything. A digital camera can help.

+ Systematically collect items of evidence, marking and recording each item with a unique number.

+ Record the date, time, personnel and purpose for every transfer of custody.

+ Store evidence in a secured, climate-controlled location, away from other items that might alter or destroy digital evidence.

+ Computer forensic examiners should be able to testify that they have validated that their tools and processes do not create alterations to the data.

+ Hash values of files and/or media should be created as early as possible.

An example of *chain of custody* would be the recovery of a bloody knife at a murder scene:

1. Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill.
2. Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene.
3. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).

The chain of custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented *and* that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible.

In the courtroom, if the defendant questions the chain of custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the chain of custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

Chain of Custody is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.

7. In what way Live Acquisitions are performed in network forensics.

ANS:

Live Acquisitions:

- A data acquisition method used when a suspect computer can’t be shut down to perform a static acquisition.
- Data is collected from the local computer or over a remote network connection.
- The captured data might be altered during the acquisition because it’s not write-protected.
- Live acquisitions aren’t repeatable because data is continually being altered by the suspect computer’s OS.
- Live acquisitions are especially useful when you’re dealing with active network intrusions or attacks or you suspect employees are accessing network areas they shouldn’t.
- Live acquisitions done before taking a system offline are also becoming a necessity because attacks might leave footprints only in

running processes or RAM; for example, some malware disappears after a system is restarted.

- In addition, information in RAM is lost after you turn off a suspect system.
- However, after you do a live acquisition, information on the system has changed because your actions affect RAM and running processes, which also means the information can’t be reproduced.
- Therefore, live acquisitions don’t follow typical forensics procedures.
- The problem investigators face is the order of volatility (OOV), meaning how long a piece of information lasts on a system.
- Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years.
- The following steps show the general procedure for a live acquisition, although investigators differ on exact steps:

A. Create or download a bootable forensic CD, and test it before using it on a suspect drive.

If the suspect system is on your network and you can access it remotely, add the appropriate network forensics tools to your workstation.

If not, insert the bootable forensics CD in the suspect system.

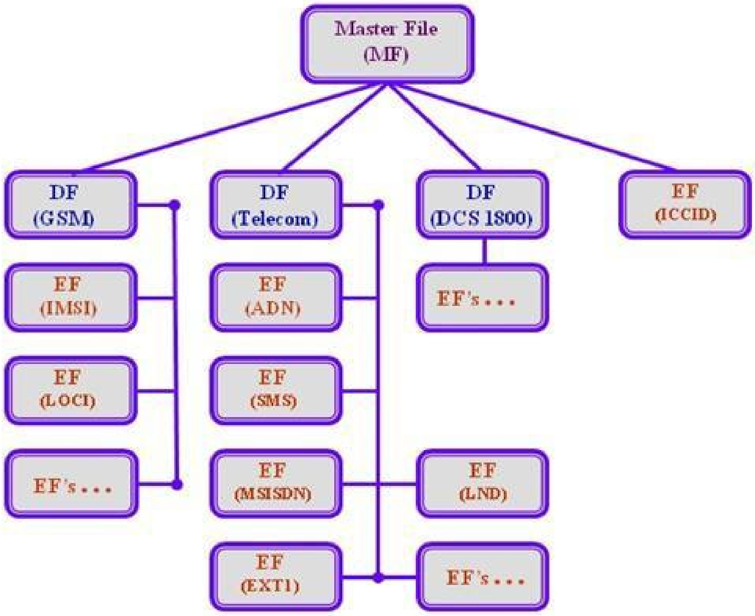
B. Make sure you keep a log of all your actions; documenting your actions and reasons for these actions is critical.

C. A network drive is ideal as a place to send the information you collect.

If you don’t have one available, connect a USB thumb drive to the suspect system for collecting data. Be sure to note this step in your log.

D. Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or you can use available freeware tools, such as memfetch and BackTrack.

	E. The next step varies, depending on the incident you're investigating. With an intrusion, for example, you might want to see whether a rootkit is present by using a tool such as RootKit Revealer. You can also access the system's firmware to see whether it has changed, create an image of the drive over the network, or shut the system down and make a static acquisition later. Be sure to get a forensically sound digital hash value of all files you recover during the live acquisition to make sure they aren't altered later.
8.	SIM File Structure in detail.
ANS:	A SIM card contains a processor and operating system with between 16 and 256 KB of persistent, electronically erasable, programmable read-only memory (EEPROM). It also contains RAM (random access memory) and ROM (read-only memory). RAM controls the program execution flow and the ROM controls the operating system work flow, user authentication, data encryption algorithm, and other applications. The hierarchically organized file system of a SIM resides in persistent memory and stores data as names and phone number entries, text messages, and network service settings. Depending on the phone used, some information on the SIM may coexist in the memory of the phone. Alternatively, information may reside entirely in the memory of the phone instead of available memory on the SIM. The hierarchical file system resides in EEPROM. The file system consists of three types of files: master file(MF), dedicated files, and elementary files. The master file is the root of the file system. Dedicated files are the subordinate directories of master files. Elementary files contain various types of data, structured as either a sequence of data bytes, a sequence of fixed-size records, or a fixed set of fixed-size records used cyclically.

	Typical SIM Card File System  Master File (MF) DF (GSM) DF (Telecom) DF (DCS 1800) EF (ICCID) EF (IMSI) EF (ADN) EF's... EF (LOCI) EF (SMS) EF's... EF (MSISDN) EF (LND) EF (EXT1) EF's... As can be seen in the above figure, dedicated files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF are EFs (ICCID). Subordinate to each of the DFs are supporting EFs, which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network-related information and the EFs under DF (Telecom) contain the service-related information. All the files have headers, but only EFs contain data. The first byte of every header identifies the file type and the header contains the information related to the structure of the files. The body of an EF contains information related to the application. Files can be either administrative- or application-specific and access to stored data is controlled by the operating system.
9.	Network Forensics and Sysinternal tool commands.
10.	Investigation Triad in computer forensics.
Ans:	– Investigators often work as a team to make computers and networks secure in an organization. – The computer investigations function is one of three in a triad that makes up computing security.

- In an enterprise network environment, the triad consists of the following parts
  (shown in Figure 1-2):
  - * Vulnerability assessment and risk management
  - * Network intrusion detection and incident response
  - * Computer investigations

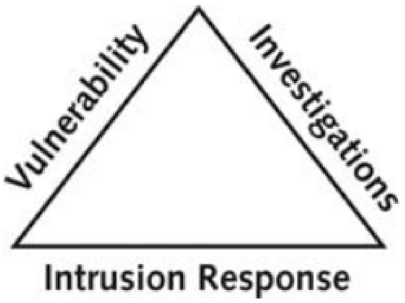
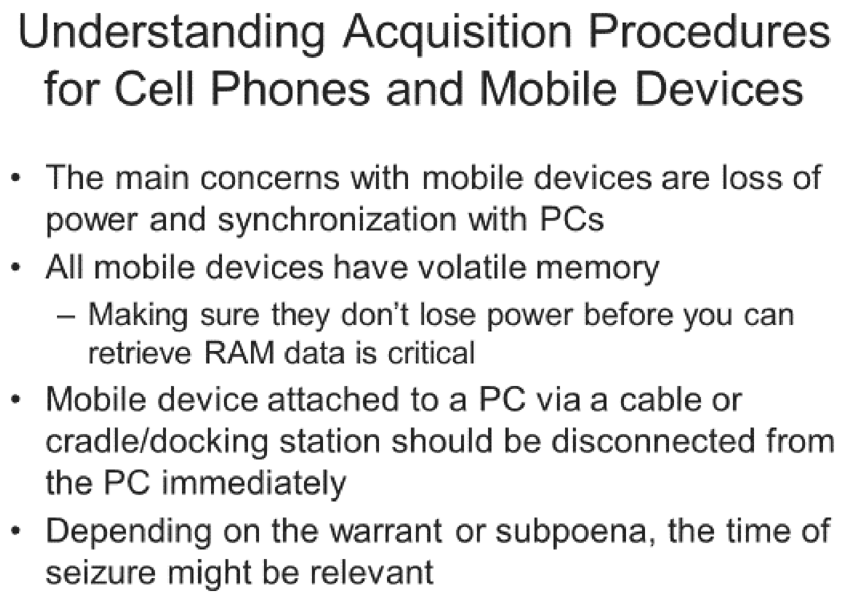


Figure 1-2 The investigations triad

- Each side of the triad in Figure 1-2 represents a group or department responsible for performing the associated tasks.
- Although each function operates independently, all three groups draw from one another when a large-scale computing investigation is being conducted.
- By combining these three groups into a team, all aspects of a high-technology investigation are
  addressed without calling in outside specialists.
- The term enterprise network environment refers to large corporate computing systems that might include disparate or formerly independent systems.
- In smaller companies, one group might perform the tasks shown in the investigations triad, or a small company might contract with other companies for these services.
- When you work in the vulnerability assessment and risk management group, you test and verify the integrity of standalone workstations and network servers.

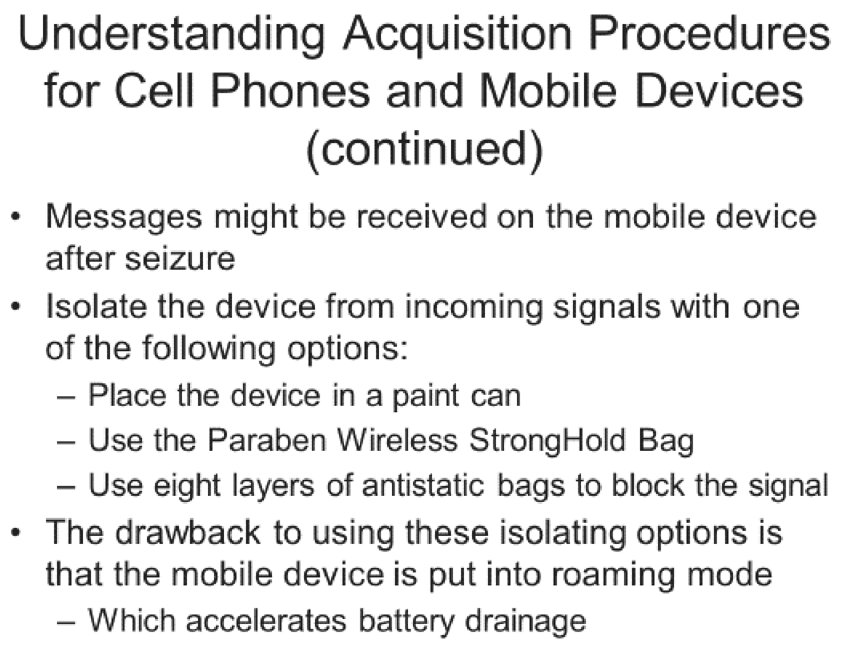
- This integrity check covers the physical security of systems and the security of operating systems (OSs) and applications.
- People who work in this group test for known vulnerabilities of OSs and applications used in the network.
- This group also launches attacks on the network and its workstations and servers to assess vulnerabilities.
- Typically, people performing this task have several years of experience in UNIX and Windows administration.
- Professionals in the vulnerability assessment and risk management group also need skills in network intrusion detection and incident response.
- This group detects intruder attacks by using automated tools and monitoring network firewall logs manually.
- When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network.
- If an intruder launches an attack that causes damage or potential damage, this team collects the necessary evidence, which can be used for civil or criminal litigation against the intruder.
- Litigation is the legal process of establishing criminal or civil liability in court.
- If an internal user is engaged in illegal acts, the network intrusion detection and incident response group respond by locating the user and blocking his or her access.
- For example, someone at a community college sends inflammatory e-mails to other users on the network.
- The network team realizes that the e-mails are coming from a node on the internal network and dispatches a security team to the location.
- Vulnerability assessment staff often contribute significantly to computing investigations.

	– The computer investigations group manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime. – For complex casework, the computer investigations group draws on resources from those involved in vulnerability assessment, risk management, and network intrusion detection and incident response. This group resolves or terminates all case investigations.
11.	Case-How could you apply DiD principles to your office network?
ANS:	
12.	Acquisition Procedures for Cell Phones and Mobile Devices.



Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- The main concerns with mobile devices are loss of power and synchronization with PCs
- All mobile devices have volatile memory
  - Making sure they don't lose power before you can retrieve RAM data is critical
- Mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately
- Depending on the warrant or subpoena, the time of seizure might be relevant



Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)

- Messages might be received on the mobile device after seizure
- Isolate the device from incoming signals with one of the following options:
  - Place the device in a paint can
  - Use the Paraben Wireless StrongHold Bag
  - Use eight layers of antistatic bags to block the signal
- The drawback to using these isolating options is that the mobile device is put into roaming mode
  - Which accelerates battery drainage

ANS:

Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)

- Check these areas in the forensics lab :
  - Internal memory
  - SIM card
  - Removable or external memory cards
  - System server
- Checking system servers requires a search warrant or subpoena
- SIM card file system is a hierarchical structure

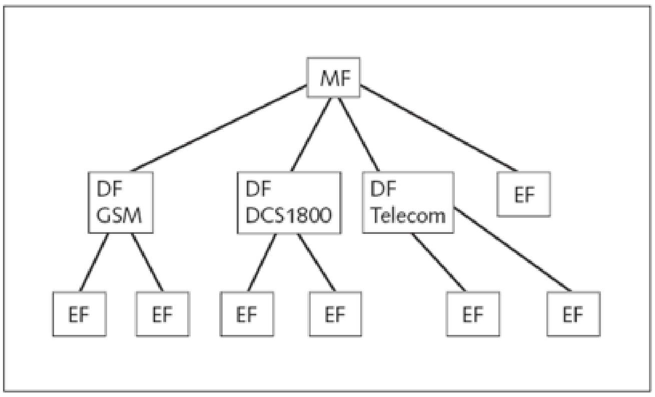
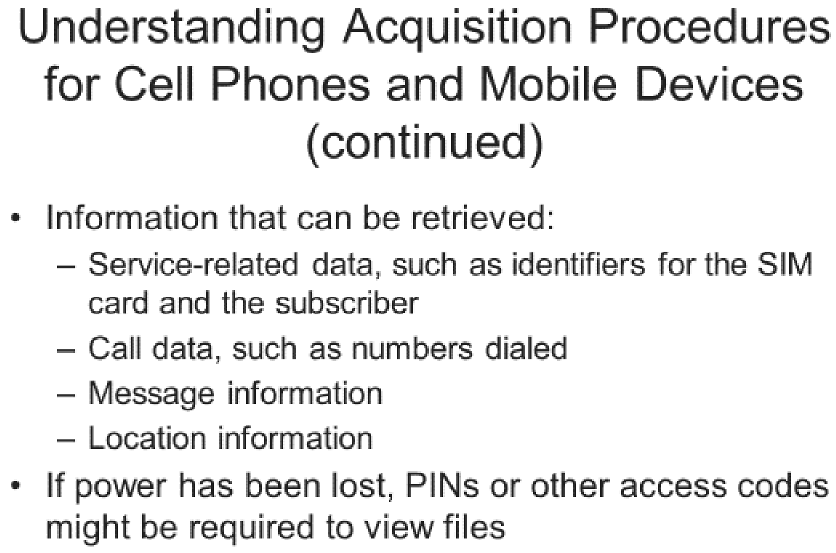


Figure 13-1 SIM file structure

- MF: root of the system
- DF: directory files
- EF: elementary data

13.	Knoppix commands for UNIX.
ANS:	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
14.	Computer forensics with respect to Falsification of data.
ANS:	**Data falsification**: Manipulating research data with the intention of giving a false impression. This includes manipulating images (e.g. micrographs, gels, radiological images), removing outliers or “inconvenient” results, changing, adding or omitting data points, etc.

	 Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued) • Information that can be retrieved: – Service-related data, such as identifiers for the SIM card and the subscriber – Call data, such as numbers dialed – Message information – Location information • If power has been lost, PINs or other access codes might be required to view files With regard to image manipulation it is allowed to technically improve images for readability. Proper technical manipulation refers to adjusting the contrast and/or brightness or color balance if it is applied to the complete digital image (and not parts of the image). Private or corporate investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination. When conducting a computer investigation for a private company, remember that business must continue with minimal interruption from your investigation. Because businesses usually focus on continuing their usual operations and making profits, many in a private corporate environment consider your investigation and apprehension of a suspect secondary to stopping the violation and minimizing damage or loss to the business. Businesses also strive to minimize or eliminate litigation, which is an expensive way to address criminal or civil issues. Corporate computer crimes can involve e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage, which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.
15.	Steps for systematic approach for computer forensics.

ANS:

- When preparing a case, you can apply standard systems analysis steps, explained in the following list, to problem solving.
    - Make an initial assessment about the type of case you’re investigating—To assess the type of case you’re handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, and other components? Do you need to visit an office or another location? Was the computer used to commit a crime, or does it contain evidence about another crime?
    - Determine a preliminary design or approach to the case—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. If you’re preparing a criminal case, determine what information law enforcement officers have already gathered.
    - Create a detailed checklist—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step. This outline helps you stay on track during the investigation.
    - Determine the resources you need—Based on the OS of the computer you’re investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.
    - Obtain and copy an evidence drive—In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, USB drives, PDAs, and other removable media. Make a forensic copy of the disk.
    - Identify the risks—List the problems you normally expect in the type of case you’re

handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.

- Mitigate or minimize the risks—Identify how you can minimize the risks. For example, if you’re working with a computer on which the suspect has likely passwordprotected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.
- Test the design—Review the decisions you’ve made and the steps you’ve completed. If you have already copied the original media, a standard part of testing the design involves comparing hash values to ensure that you copied the original media correctly.
- Analyze and recover the digital evidence—Using the software tools and other resources you’ve gathered, and making sure you’ve addressed any risks and obstacles, examine the disk to find digital evidence.
- Investigate the data you recover—View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect’s guilt or innocence.
- Complete the case report—Write a complete report detailing what you did and what you found.
- Critique the case—Self-evaluation is an essential part of professional growth. After you complete a case, review it to

	identify successful decisions and actions and determine how you could have improved your performance. – The amount of time and effort you put into each step varies, depending on the nature of the investigation. – For example, in most cases, you need to create a simple investigation plan so that you don’t overlook any steps. – However, if a case involves many computers with complex issues to identify and examine, a detailed plan with periodic review and updates is essential. – A systematic approach helps you discover the information you need for your case, and you should gather as much information as possible. For all computing investigations, you must be prepared for the unexpected, so you should always have a contingency plan for the investigation. A contingency plan can consist of anything to help you complete the investigation, from alternative software and hardware tools to other methods of approaching the investigation.
16.	Describe Computer Forensics with Disk Imaging, Preservation Data Encryption and Compression.
ANS:	● *Disk Imaging* – **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.

- Unlike the cloned drive, system restore is not possible by just copying the image file on the hard drive.
- A software imaging program will have to be employed to install and open the image on the hard drive.
- The backup device can therefore be used to store multiple image files, unlike the cloned drive where only a single clone can be stored on the duplicate drive.
- Disk imaging refers to copying the contents of a data storage device or medium, and transferring this to another, similar medium or device.
- In its original context, disk imaging implies the creation of an exact duplicate of a computer's hard disk drive - including its programs, setup and data then storing this in a special, compressed file format.
- Disk imaging aims to provide the user with an exact replica of a computer's systems and data - needed in case of a catastrophic disk crash where the user needs to recover systems or data (e.g. in the event of a virus attack or accident), to 'clone' a systems set-up for installation in another computer or to move these to another 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.

- This is especially useful in case of problems encountered during the life of the system - deliberate virus attacks which may erase systems or data, software or hardware glitches which may require formatting or erasure of the hard disk, installation of beta (test) software that may conflict with a computer system, catastrophic incidents like man-made disasters or accidents (e.g. fire, floods, and the like).

- In other words, a disk image means having an updated 'rescue disk' that one uses to easily reinstall the system to what it was at the time of 'duplication,' without having to go through the involved process of installing software and resetting or tweaking settings once again to the desired configuration.

- A second application for disk imaging software is for systems administrators who oversee multiple computers with similar configurations.

- Rather than spending time in transferring and configuring systems on different computers, a disk imaging software makes the task easy and quick - duplicate the systems on one machine and install the 'disk image' on another computer.

● *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.

- Delegation is not a defence when electronic evidence is lost, altered and/or destroyed once the duty to preserve is known.
- You need to consult with your attorney and computer forensic examiner to ensure there is a well-documented process to protect the data.
- Proper evidence handling and chain of custody provide both a shield and a sword for the credibility and persuasiveness of your digital evidence.
- First, opposing counsel is either going to shy away from this line of attack because a strong chain of custody makes it apparent that you have handled the evidence properly, or they are going to lose credibility with the judge or jury by wasting their time on a pointless matter.
- Second, the persuasive value of your digital evidence is bolstered, and your credibility is enhanced.
- With all the responsibilities placed on busy professionals today, there are going to be times when it's very tempting to forgo collecting and maintaining the chain of custody.
- Don't succumb!
- Take the time to develop and implement your chain of custody and evidence handling protocols.
- You will be thankful when you're in court and your smoking gun email nails a conviction.

CHAIN OF CUSTODY CHECKLIST

+ Have a plan before an incident occurs. Identify your “go-to” people, whether in-house or outside, while the waters are still calm.

+ Do not touch the computer unless you are experienced in digital forensics. Thousands of files are altered simply by turning it on.

+ Document the location and condition of everything before touching anything. A digital camera can help.

+ Systematically collect items of evidence, marking and recording each item with a unique number.

- Record the date, time, personnel and purpose for every transfer of custody.
- Store evidence in a secured, climate-controlled location, away from other items that might alter or destroy digital evidence.
- Computer forensic examiners should be able to testify that they have validated that their tools and processes do not create alterations to the data.
- Hash values of files and/or media should be created as early as possible.

- *Data Encryption and Compression*

ENCRYPTION

- The use of encryption technology to protect computer data is growing—and that fact presents a challenge for forensic investigators.
- Without a decryption key, forensic tools cannot be used to find digital evidence.
- Even with the key, searching encrypted data can be tricky and time consuming.

Q: Why is the use of encryption growing in popularity?

A: Corporations and computer users like the idea of encryption as a way to protect their sensitive or personal data from breaches, but the average user still sees this technology as burdensome or too time consuming to implement on a constant basis. So the move to encryption is not necessarily coming from the users. Instead it is coming from hardware and software companies who are embedding encryption technology into their products. The BlackBerry is a good example because all data is encrypted and this protection is automatic. More important, the use of the encryption technology is completely invisible to the user.

Q: What is the impact of encryption on forensic investigation?

A: As investigators, we are limited to the information on the device that we can access. If a hard drive is fully encrypted, we have no easy access to the stored data and our investigative options become limited. The first thing an investigator must do is to determine the level and extent of the encryption. Weak passwords can be cracked, but if the user has implemented a strong password it becomes almost impossible to access via brute force methods. It could be that just a few files are encrypted and there could be unencrypted copies elsewhere on the device. The user could also be a creature of habit and use the same set of passwords. These passwords can be quickly located in easily decipherable formats throughout the system. In all cases, though, I tell investigators that digital evidence is just one piece of the body of evidence in a case. Don't fall into a trap where you spend too much time trying to decrypt a potentially probative item, when valuable unencrypted data may be found by simply continuing your examination.

Q: Is there a greater chance of damaging or corrupting the encrypted evidence?

A: There is always a slight chance when working with electronic media that data may be damaged or corrupted. The best advice I can give is to keep your evidence-handling procedure reasonable and defensible. Reasonable means using industry-standard tools. Defensible means you thoroughly document the process.

The bigger concern is that all of the data on the drive must be decrypted—and that can take hours. As you work a drive to decrypt this data, that drive could fail. Thus, it is important to be sure that your forensics tool supports encrypted data, which makes the process more seamless while contributing to the defensibility of the procedure.

Q: What new techniques do investigators need to consider when they come across an encrypted drive?

A: For many investigators this is a new area. First, they should try to determine the extent of the encryption. There are many tools that allow you to encrypt the whole hard drive, a portion of the disk space, or even individual files. An investigator should first determine whether the whole drive is encrypted; if not, then they can scan for encrypted files. If encryption software like Encrypt It or TrueCrypt is on the drive, then there is a reasonable expectation that the user may have encrypted some of the content. Examiners can analyze the use of these applications and learn just how often and when an encryption program has been run. This can lead to a search for other digital files that were being accessed around the same time periods.

If there is encrypted information on the disk, the next step is to use any known passwords. So far courts in the United States have been reluctant to force defendants to divulge their personal passwords, but people are creatures of habit and they tend to use a single small set of passwords for everything. These can be found in many places on the hard drive where they are easily deciphered. For example, many web browsers allow a user to store their passwords for various websites. The repository where those passwords are stored is generally easy to crack.

The investigator has more options if certain files are encrypted. Computers are redundant by nature. The data that is inside the encrypted volume had to come from somewhere (another device for example) or it might be spread across the drive outside of the encrypted file.

For example, Microsoft Word automatically writes copies of a document to a hard drive as it is being modified. This way, the user has a backup if the computer fails. When that document is closed, the program deletes all the temporary versions. If you encrypt the document and you delete the original document, your machine still has the deleted files that can be accessed by using forensics. Another example: When a suspect is working with digital photos, thumbnail images are always being created. Finding non-encrypted copies of files will not always be possible, but investigators can and should look for copies of the data across all relevant devices.

COMPRESSION

- Lossless compression techniques reduce file size without removing data.
- When you uncompress a file that uses lossless compression, you restore all its information.
- GIF and Portable Network Graphics (PNG) file formats reduce file size with lossless compression, which saves file space by using mathematical formulas to represent data in a file.
- These formulas generally use one of two algorithms: Huffman or Lempel-Ziv-Welch (LZW) coding.

- Each algorithm uses a code to represent redundant bits of data.
- For example, if a graphics file contains a large red area, instead of having to store 200 red bytes, the algorithm can set one byte to red and set another byte to specify 200 red bytes.
- Therefore, only 2 bytes are used.
- Lossy compression is much different because it compresses data by permanently discarding bits of information in the file.
- Some discarded bits are redundant, but others are not.
- When you uncompress a graphics file that uses lossy compression, you lose information, although most people don't notice the difference unless they print the image on a high-resolution printer or increase the image size.
- In either case, the removed bits of information reduce image quality.
- The JPEG format is one that uses lossy compression.
- If you open a JPEG file in a graphics program, for example, and save it as a JPEG file with a different name, lossy compression is reapplied automatically, which removes more bits of data and, therefore, reduces image quality.
- If you simply rename a file by using Windows Explorer or the command line, however, the file doesn't lose any more data.
- Another form of lossy compression, vector quantization (VQ), uses complex algorithms to determine what data to discard based on vectors in the graphics file.
- In simple terms, VQ discards bits in much the same way rounding off decimal values discards numbers.
- Some popular lossless compression utilities include WinZip, PKZip, StuffIt, and FreeZip. Lzip is a lossy compression utility.
- You use compression tools to compact folders and files for data storage and transmission.
- Remember that the difference between lossless and lossy compression is the way data is represented after it has been uncompressed.
- Lossless compression produces an exact replica of the original data after it has been uncompressed, whereas lossy compression typically produces an altered replica of the data.

18. Explain computer forensics and clarify how it is different other forensics.

ANS:

- Computer forensics involves obtaining and analysing digital information for use as evidence in civil, criminal, or administrative cases.
- In general, computer forensics investigates data that can be retrieved from a computer’s hard drive or other storage media. Computer investigators retrieve information from a computer or its component parts.
- The information you retrieve might already be on the drive, but it might not be easy to find or decipher.
- Computer forensics vs Mobile device forensics
  - Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device.
  - It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms.
  - Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
  - Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range.

- Computer forensics vs Network forensics
  - Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection.
  - Unlike other areas of digital forensics, network forensic investigations deal with volatile and dynamic information.
  - Disk or computer forensics primarily deals with data at rest.
  - Network forensics by its very nature is dynamic.
  - In fact, it would not be possible to conduct a network forensic investigation if prior arrangements were not made to capture and store network traffic

- o Additionally, network forensics involves the analysis of logs. This can be a bit of art as well as science.

Ø Computer forensics vs data recovery

Computer forensics is also different from data recovery, which involves recovering information from a computer that was deleted by mistake or lost during a power surge or server crash, for example. In data recovery, typically you know what you're looking for.

19. State the three modes of protection of defence in depth.

ANS:

The National Security Agency (NSA) developed a approach, called the defense in depth (DiD) strategy. DiD has three modes of protection:

- **People**
- **Technology**
- **Operations**

If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge. In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organization's security policy. Physical and personnel security measures are included in this mode of protection.

The technology mode includes choosing a strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

Finally, the operations mode addresses day-to-day operations. Updating security patches, antivirus software, and OSs falls into this category, as does assessment and monitoring procedures and disaster recovery plans.

20. Describe Main components of Mobile device.

ANS:

- Mobile devices can range from simple phones to small computers
  - Also called **smart phones**
- Hardware components
  - Microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces, and an LCD display

- Most basic phones have a proprietary OS
  - Although smart phones use stripped-down versions of PC operating systems
- Phones store system data in **electronically erasable programmable read-only memory (EEPROM)**
  - Enables service providers to reprogram phones without having to physically access memory chips
- OS is stored in ROM
  - Nonvolatile memory
- **Subscriber identity module (SIM) cards**
  - Found most commonly in GSM devices
  - Microprocessor and from 16 KB to 4 MB EEPROM
    - Sometimes even more, up go 1 GB EEPROM
  - GSM refers to mobile phones as “mobile stations” and divides a station into two parts:
    - The SIM card and the mobile equipment (ME)
  - SIM cards come in two sizes
  - Portability of information makes SIM cards versatile
  - Additional SIM card purposes:
    - Identifies the subscriber to the network
    - Stores personal information
    - Stores address books and messages

	• Stores service-related information
21.	Explain the following cases with respect to Computer forensics. Sabotage, Industrial espionage
ANS:	Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracies, such as drug and human trafficking. According to the Federal Bureau of Investigation, computer sabotage costs billions of dollars in legal fees to recover damages such as identity theft and to repair vital infrastructure that serves hospitals, banks and 911 services. Committing computer sabotage can be as simple as deliberately infecting a computer with a virus to keep authorized users from logging in. Although not always, much computer sabotage involves the use of malware, such as bots, worms, viruses and other spyware, which enables hackers to gain illegal access to personal and corporate computers. Apart from theft of services and wire fraud, such sabotage facilitates pedophiles who stalk children online at school and at home, identity thieves who duplicate fake IDs for illegal immigrants, and home invasion rings and other criminals who use malware to identify potential victims. **Cyber spying**, or **cyber espionage**, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods

	on the Internet, networks or individual computers through the use of proxy servers[1], cracking techniques and malicious software including Trojan horses and spyware.[2][3] It may wholly be perpetrated online from computer desks of professionals on bases in far away countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmer.
22.	Enumerate the basic steps for computer forensics investigations.
ANS:	● Obtain authorization to search and seize. ● Secure the area, which may be a crime scene. ● Document the chain of custody of every item that was seized. ● Bag, tag, and safely transport the equipment and e-evidence. ● Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence. ● Keep the original material in a safe, secured location. ● Design your review strategy of the e-evidence, including lists of keywords and search terms. ● Examine and analyze forensic images of the e-evidence (never the original!) according to your strategy. ● Interpret and draw inferences based on facts gathered from the e-evidence. Check your work. ● Describe your analysis and findings in an easy-to-understand and clearly written report. ● Give testimony under oath in a deposition or courtroom.

CYBER FORENSICS

UNIT 4

1. Internet forensics and internet crimes.

ANS: Internet forensics

- Internet forensics shifts that focus from an individual machine to the Internet at large.
- With a single massive network that spans the globe, the challenge of identifying criminal activity and the people behind it becomes immense.
- A con artist in the United States can use a web server in Korea to steal the credit card number of a victim in Germany.
- Unfortunately, the underlying protocols that handle Internet traffic were not designed to address the problems of spam, viruses, and so forth.
- It can be difficult, often impossible, to verify the source of a message or the operator of a web site.
- In cases like this the minor details become important.
- The layout of files on a web site or the way that email headers are forged can play the same role as a fingerprint at a physical crime scene.
- 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.
- All those who own websites, store vital information online or transact over the internet are always under constant threat of falling victims of internet attack.
- Internet forensic is therefore very important in making the internet a safe platform of transacting.

- Internet forensics has become an important part of safe and secure internet usage and an integral part of criminal investigation, where money transfers and communication between parties can provide evidence, especially in white-collar crime.
- Internet forensic consultants can use their expertise to monitor the activities in which employees engage while logged onto the company's network, this is especially important if there are employees who have access to information the company would consider as volatile or sensitive.
- As the internet is growing exponentially, with more people using it every day, there are more people at risk, and more people looking to take advantage of others web insecurity.
- The need to protect your internet presence has necessitated the emergence and emphasized the importance of internet forensics.

Internet Crimes

- Internet crime is any crime or illegal online activity committed on the Internet, through the Internet or using the Internet.
- The widespread Internet crime phenomenon encompasses multiple global levels of legislation and oversight.
- In the demanding and continuously changing IT field, security experts are committed to combating Internet crime through preventative technologies, such as intrusion detection networks and packet sniffers.
- Internet crime is a strong branch of cybercrime.
- Identity theft, Internet scams and cyberstalking are the primary types of Internet crime.
- Because Internet crimes usually engage people from various geographic areas, finding and penalizing guilty participants is complicated.
- Types of Internet crime include:
    - Cyberbullying and harassment

	- Financial extortion - Internet bomb threats - Classified global security data theft - Password trafficking - Enterprise trade secret theft - Personal data hacking - Copyright violations, such as software piracy - Counterfeit trademarks - Illegal weapon trafficking - Online child pornography - Credit card theft and fraud - Email phishing - Domain name hijacking - Virus spreading ● To prevent becoming an Internet crime, online vigilance and common sense are critical. ● Under no circumstances should a user share personal information (like full name, address, birth date and Social Security number) to unknown recipients. ● Moreover, while online, a user should remain suspicious about exaggerated or unverifiable claims.
2.	By what method Browser Forensics Analysis is a separate, large area of expertise.
ANS:	● 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.
- One of the most famous web browsers is Internet Explorer.
- This browser is a component of the Windows operating system and is often used as a default web browser.
- In Windows 10, Microsoft replaced Internet Explorer with Microsoft EDGE.
- Microsoft EDGE is a web browser that contains new features.
- Internet Explorer and Microsoft EDGE can work in InPrivate mode, without storing information about web resources visited by the user.
- Another popular web browser is Google Chrome. It has the following features:
    - Integration with Google services.
    - Synchronization of user passwords between devices.
    - The ability to use extensions and plugins.
    - Fast operation.
    - Gathers user data.
    - Consumes large amounts of memory.

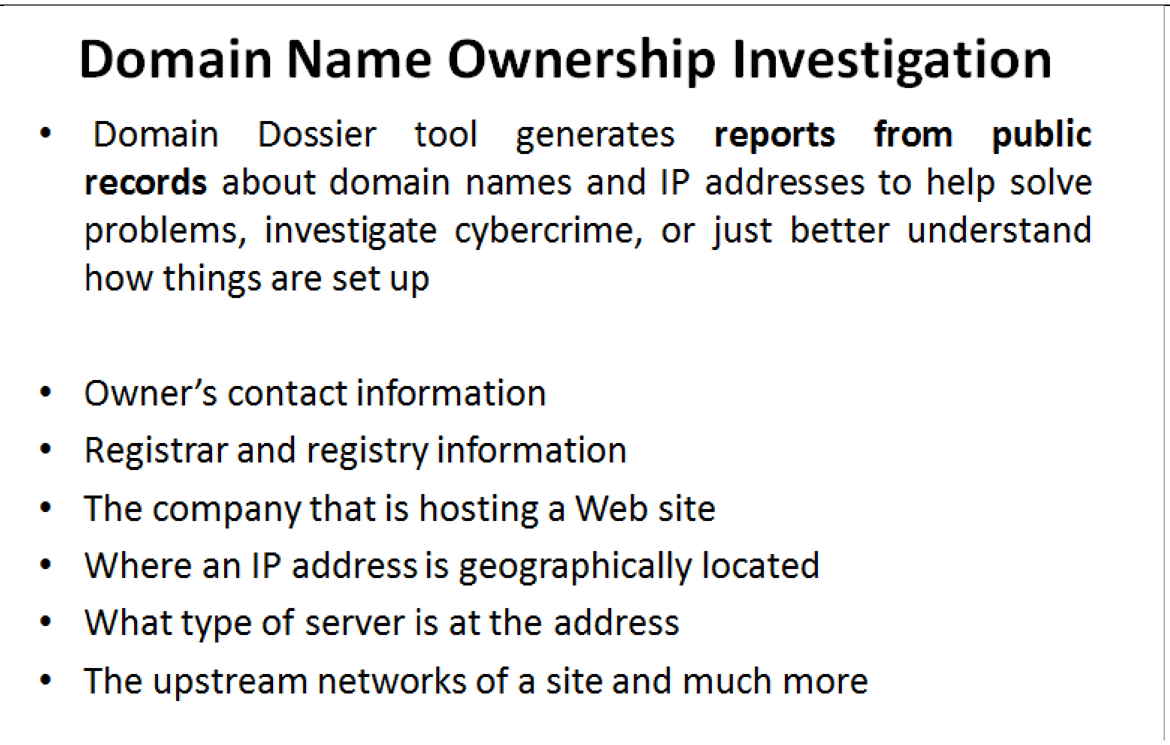
- Google Chrome can work in Incognito mode, which prevents the browser from permanently storing any history information, cookies, site data or form inputs.
- Encryption of data
    - Part of the data in web browsers is encrypted (for example, passwords to websites).
    - You need a user password to decrypt the encrypted data.
    - If the password is logged into your account using the login and the password, the operating system uses the hash of the password to decrypt the encrypted data.
    - As a rule, data encryption is carried out using the SHA1 algorithm, however, in some cases, the data is encrypted using a less crypto-resistant algorithm.
- Difficulties of web browsers forensic analysis
    - An examiner can have the following difficulties when analysing web browsers:
        - ❖ Many browsers, lots of data
        - ❖ Different data
        - ❖ Encryption used to protect user data
        - ❖ User's use of Private mode (or Incognito mode), in which the examined computer does not have web browser artifacts.
- Web browser forensic artifacts
    - Of course, each web browser leaves its own individual artifacts in the operating system.
    - Types of artifacts from the web browser can vary depending on the version of the web browser.
    - Typically, when researching artifacts of web browsers, you can extract the following types of artifacts:
        - ★ History

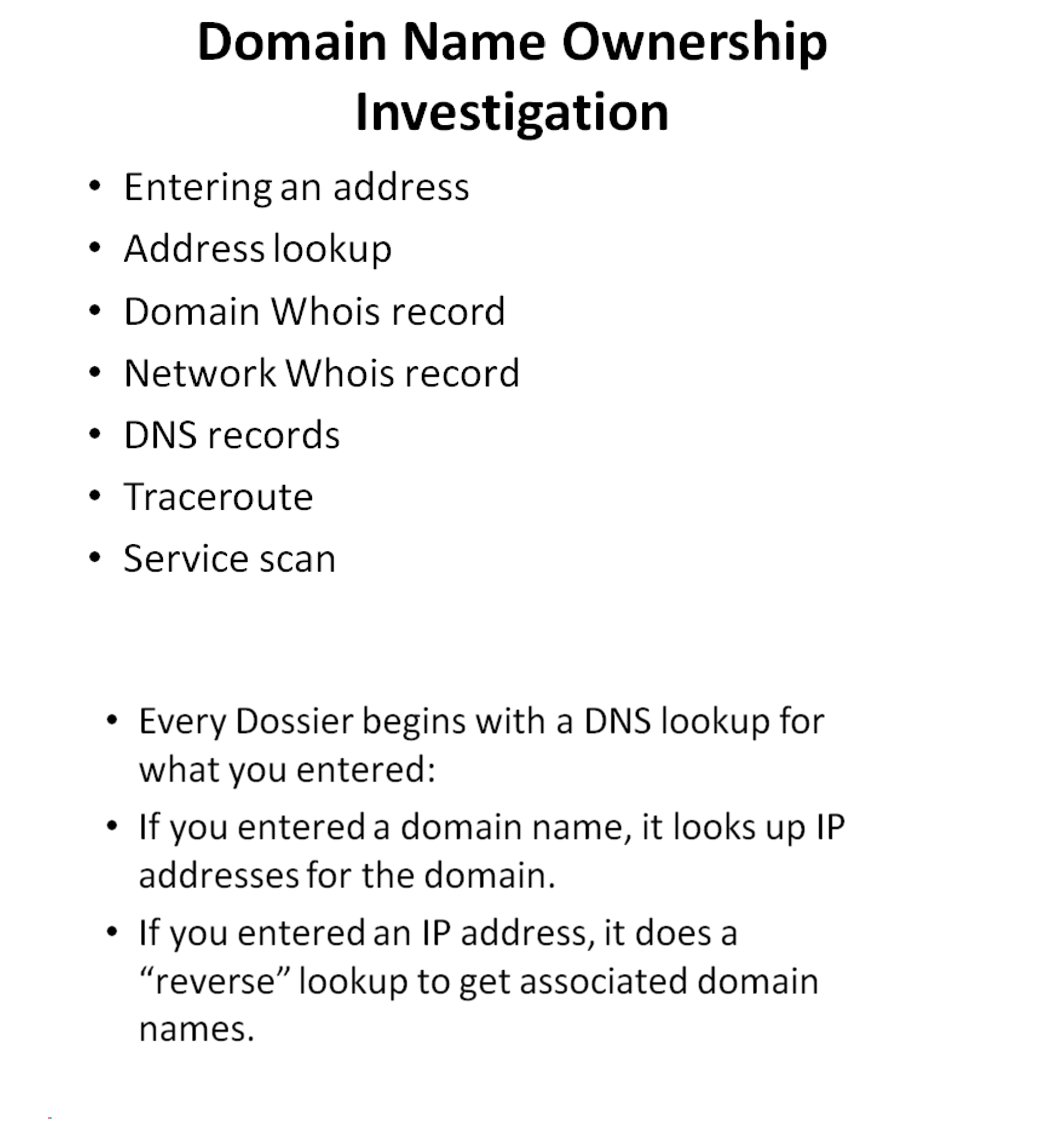
	★ Cache ★ Cookies ★ Typed URLs ★ Sessions ★ Most visited sites ★ Screenshots ★ Financial info ★ Form values (Searches, Autofill) ★ Downloaded files (Downloads) ★ Favourites
3.	In what way to reconstruct past internet activities and events?
ANS:	Forensics Checklist ● Create a timeline to reconstruct the events that led to your system being corrupted. This can be particularly difficult when it comes to computers—clock drift, delayed reporting, and differing time zones can create confusion in abundance. ● Do not change the clock on an affected system ● Record any clock drift and the time zone in use, as you will need this later, but changing the clock just adds in an extra level of complexity that is best avoided. ● Synchronize the log files. Log files usually use timestamps to indicate when an entry was added, and these must be synchronized to make sense. ● Use timestamps. You're not just reconstructing events; you are making a chain of events that must be accounted for as well. ● Use the GMT time zone when creating your timestamps, because the incident may involve other time zones than your own. Using a common reference point can make things much easier. ● Make sure you have a dedicated host for the job when analysing backups. This examination host should be secure, clean (a fresh,

	hardened install of the operating system is a good idea), and isolated from any network—you don’t want it tampered with while you work, and you don’t want to accidentally send something nasty down the line. ● Commence analysis of the backups once the system is available. Making mistakes at this point shouldn’t be a problem—you can simply restore the backups again if required. ● Document everything you do. Remember the mantra. ● Ensure that what you do is not only repeatable, but that you always get the same results. ● Reconstruct the chain of events leading to and following the attacker’s break-in now that you have collected the data. Make sure you correlate all the evidence you have gathered (which is why accurate timestamps are critical). It’s probably best to use graphical tools, diagrams, and spreadsheets. ● Include all of the evidence you’ve found when reconstructing the attack—no matter how small it is, you may miss something if you leave a piece of evidence out. ● Review audit trails of system activity to pinpoint how, when, and why the incident occurred, since the amount of damage that occurred with an incident can be assessed.
4.	Describe Social media forensics in detail.
ANS:	1. With 1.2 billion monthly active users on Facebook alone, it’s not surprising that social media networks can be a rich source of information for investigators. And because Americans spend more time on social media than any other major Internet activity, including email, social media information and evidence is plentiful. You just need to know how to get it. 2. Finding, preserving and collecting social media evidence often requires some forensic skills, as well as an understanding of the laws

that govern its collection and use. It's important for investigators to be aware of both the possibilities and limitations of social media forensics. A key point to understand is the fact that forensics happens where the data is. One great example is social network forensics and it really makes sense: The growth of social networks during the last decade has being astonishing, to say the least. Aside from the well-established brands such as Facebook, LinkedIn, Twitter, Instagram, and YouTube.

3. Social network forensics is nothing more than the application of computer investigation and analysis techniques, such as collecting information from online sources (e.g., Facebook, Twitter, LinkedIn and any other form of social network, no matter its size) and subsequently storing, analyzing, and preserving it as evidence that may have to be presented in a court of law.
4. Sometime investigators have time due to lack of information during an investigation, but that is not the case here. For social network forensics, there is usually plenty of data to collect, but the problem is knowing how to do it. It is no simple task knowing where to find it, the best way to sort what may actually be useful, and how to properly collect and preserve information from a live environment that you have little to no control over.
5. The work is not limited to major social media outlets, it is also possible to recover information from online services, blogs, company or personal websites, forums, and even government web sites that may be connected to social networks or provide similar functions.
6. Basically, from the investigator point of view, social network forensics will be a question of finding where the evidence lies and collecting it without violating any law.
7. Evidence collection may be done manually (which may be quite time-consuming) using simple techniques, such as visiting a website and taking a screenshot, or aided by open source tools (e.g., HTTrack), or

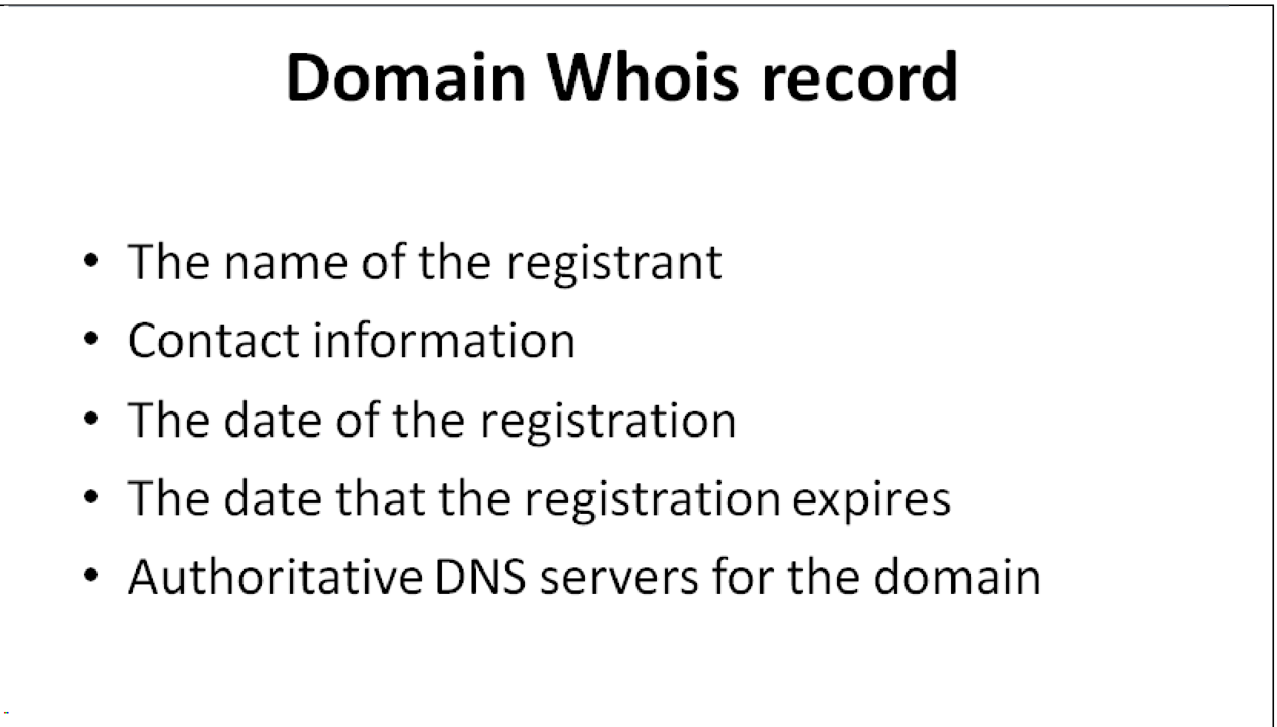
	even commercial solutions. It is also important to understand that an investigator will be dealing with live content, so another great option is using services that content archiving (e.g., websites, blog, and social media archiving) so information cannot be altered or tampered.
5.	Domain name investigation in detail.
ANS:	 **Domain Name Ownership Investigation** - Domain Dossier tool generates **reports from public records** about domain names and IP addresses to help solve problems, investigate cybercrime, or just better understand how things are set up - Owner's contact information - Registrar and registry information - The company that is hosting a Web site - Where an IP address is geographically located - What type of server is at the address - The upstream networks of a site and much more



Domain Name Ownership Investigation

- Entering an address
- Address lookup
- Domain Whois record
- Network Whois record
- DNS records
- Traceroute
- Service scan

- Every Dossier begins with a DNS lookup for what you entered:
- If you entered a domain name, it looks up IP addresses for the domain.
- If you entered an IP address, it does a “reverse” lookup to get associated domain names.

	 **Domain Whois record** • The name of the registrant • Contact information • The date of the registration • The date that the registration expires • Authoritative DNS servers for the domain
6.	Social Media Forensics with respect to yahoo messenger.
ANS:	● 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. ● In that regard, perhaps the only means of identifying the fact that the message came via Yahoo Messenger is in the layout of the text itself, with the message prefixed by a user name and colon.
7.	Examine the steps in Email Investigation.
ANS:	In email forensics, the source and content of emails is considered as evidence. 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* 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

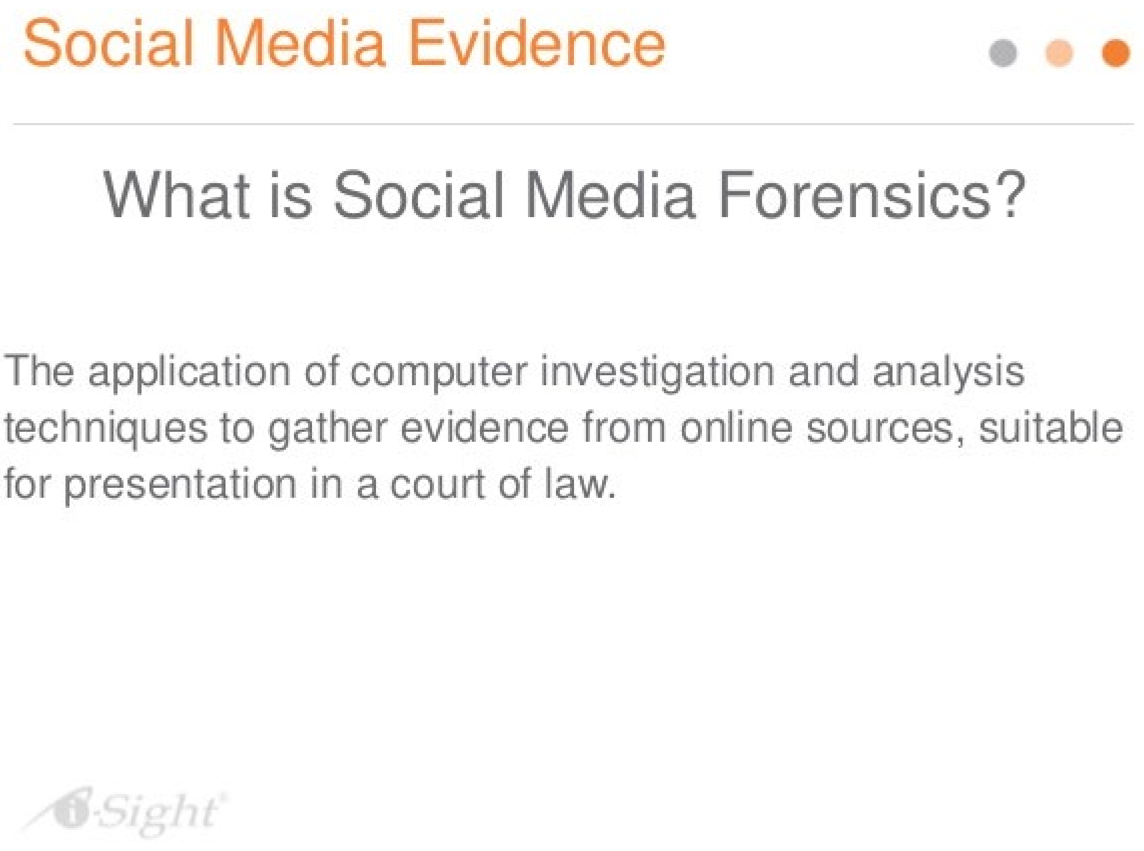
The source of an email message can also be investigated with the help of logs maintained by network devices such as routers, firewalls and switches. Owing to its complexity, this technique is only deployed in the absence of logs of ISP or proxy servers. Unavailability of server logs may occur due to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

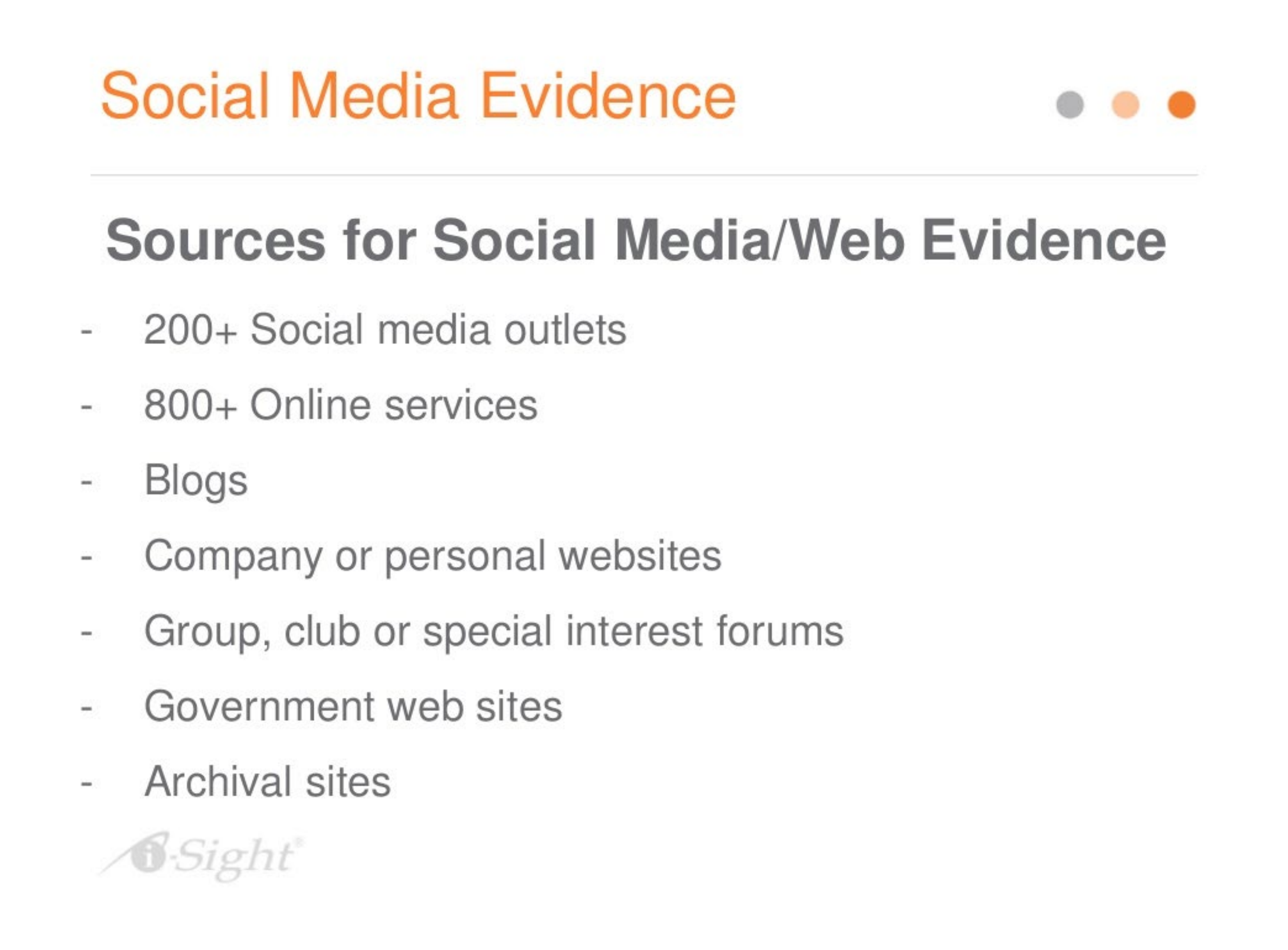
Fingerprints Of Sender Mailers

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.
8.	Describe Social media forensics in detail.
ANS:	 Social Media Evidence What is Social Media Forensics? The application of computer investigation and analysis techniques to gather evidence from online sources, suitable for presentation in a court of law.

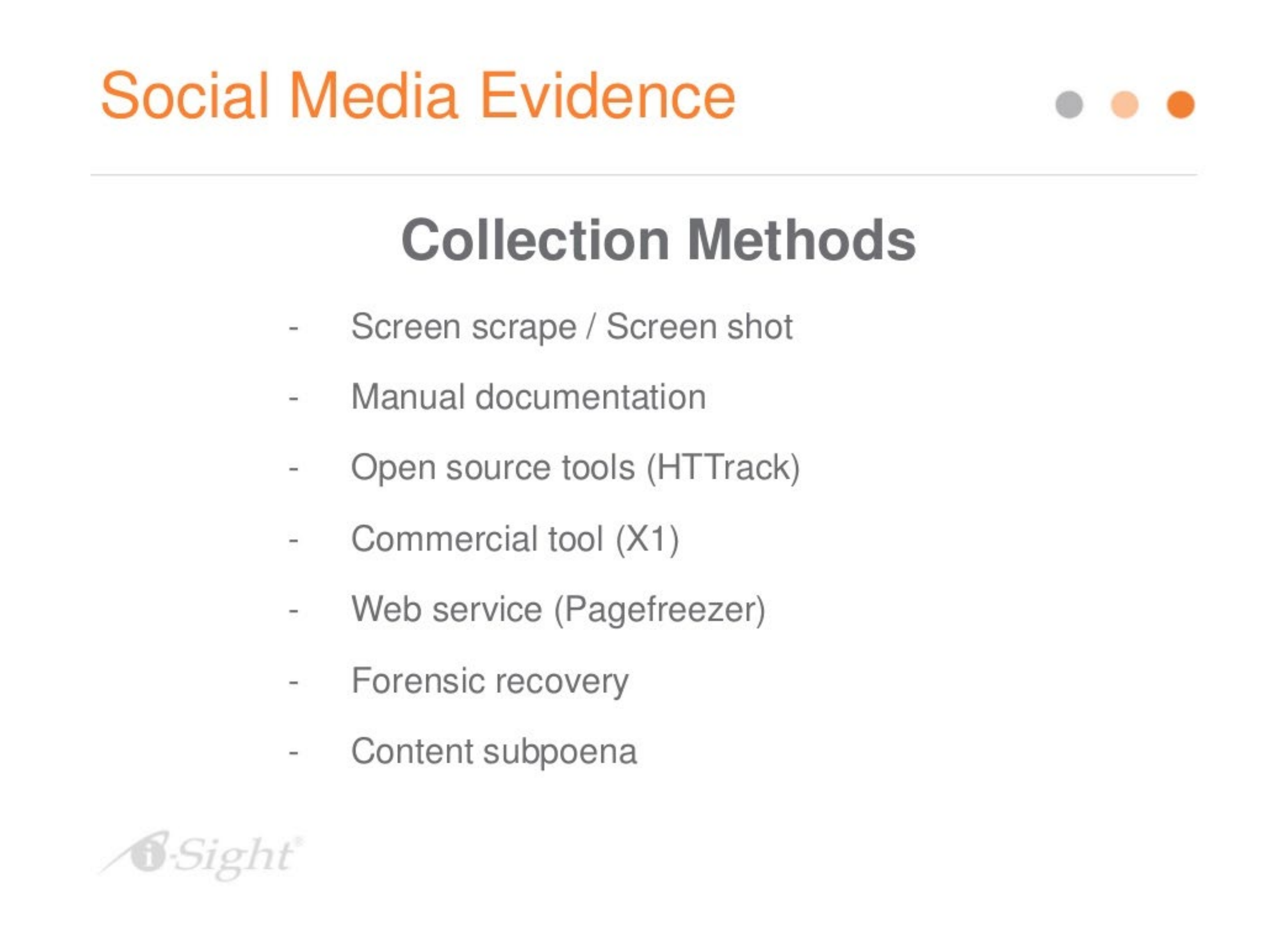


Social Media Evidence

Sources for Social Media/Web Evidence

- 200+ Social media outlets
- 800+ Online services
- Blogs
- Company or personal websites
- Group, club or special interest forums
- Government web sites
- Archival sites

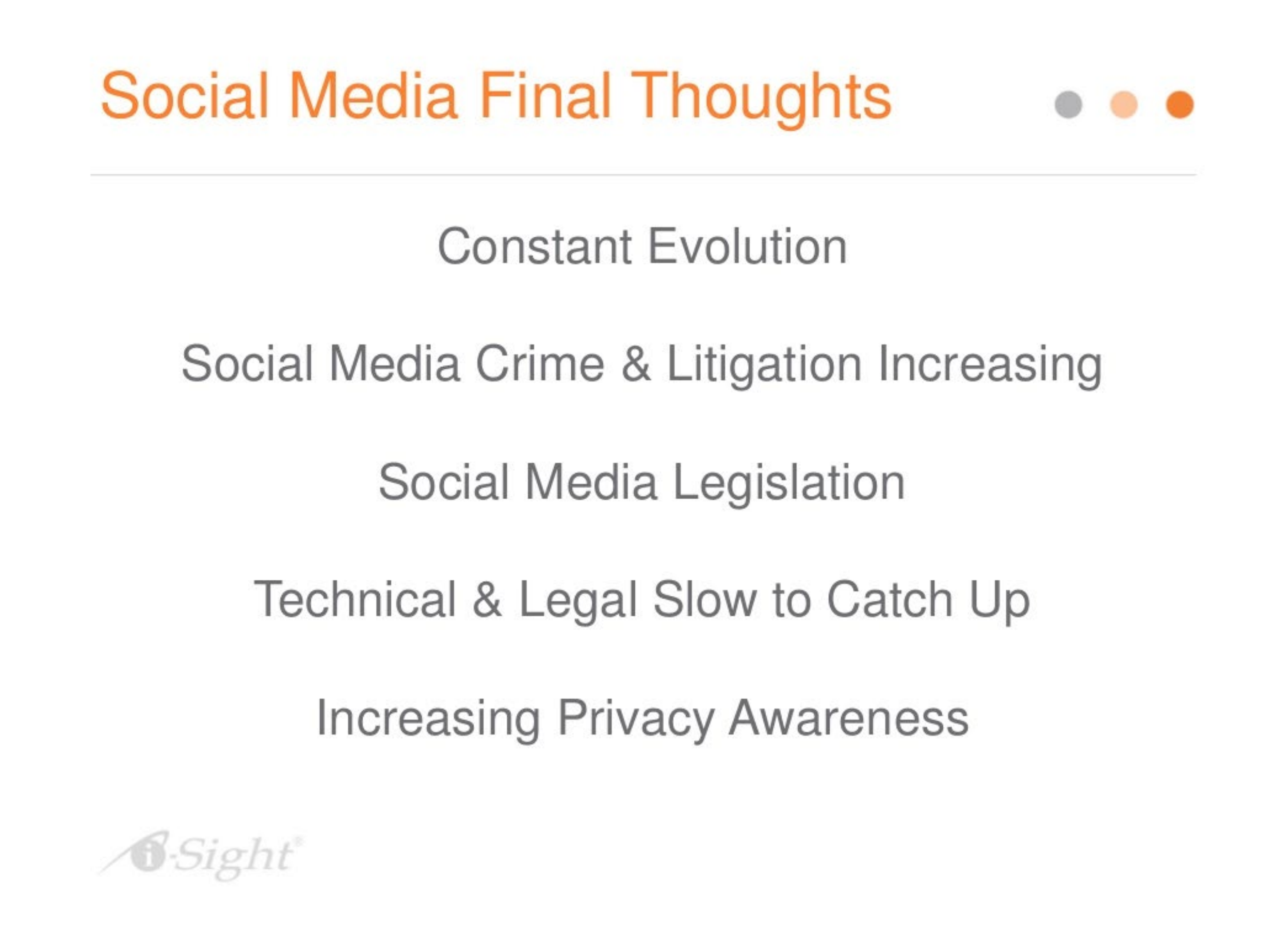
i-Sight

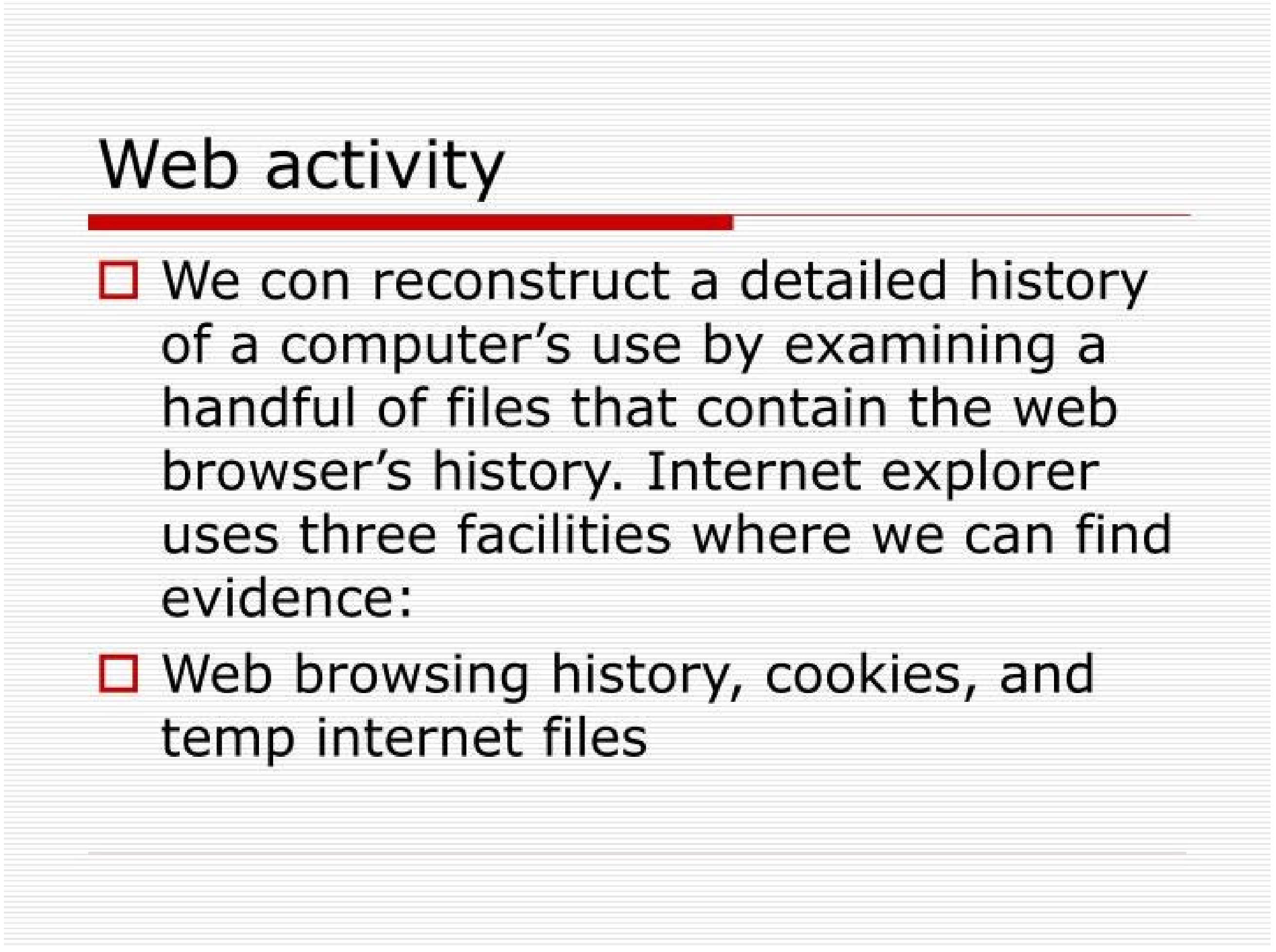


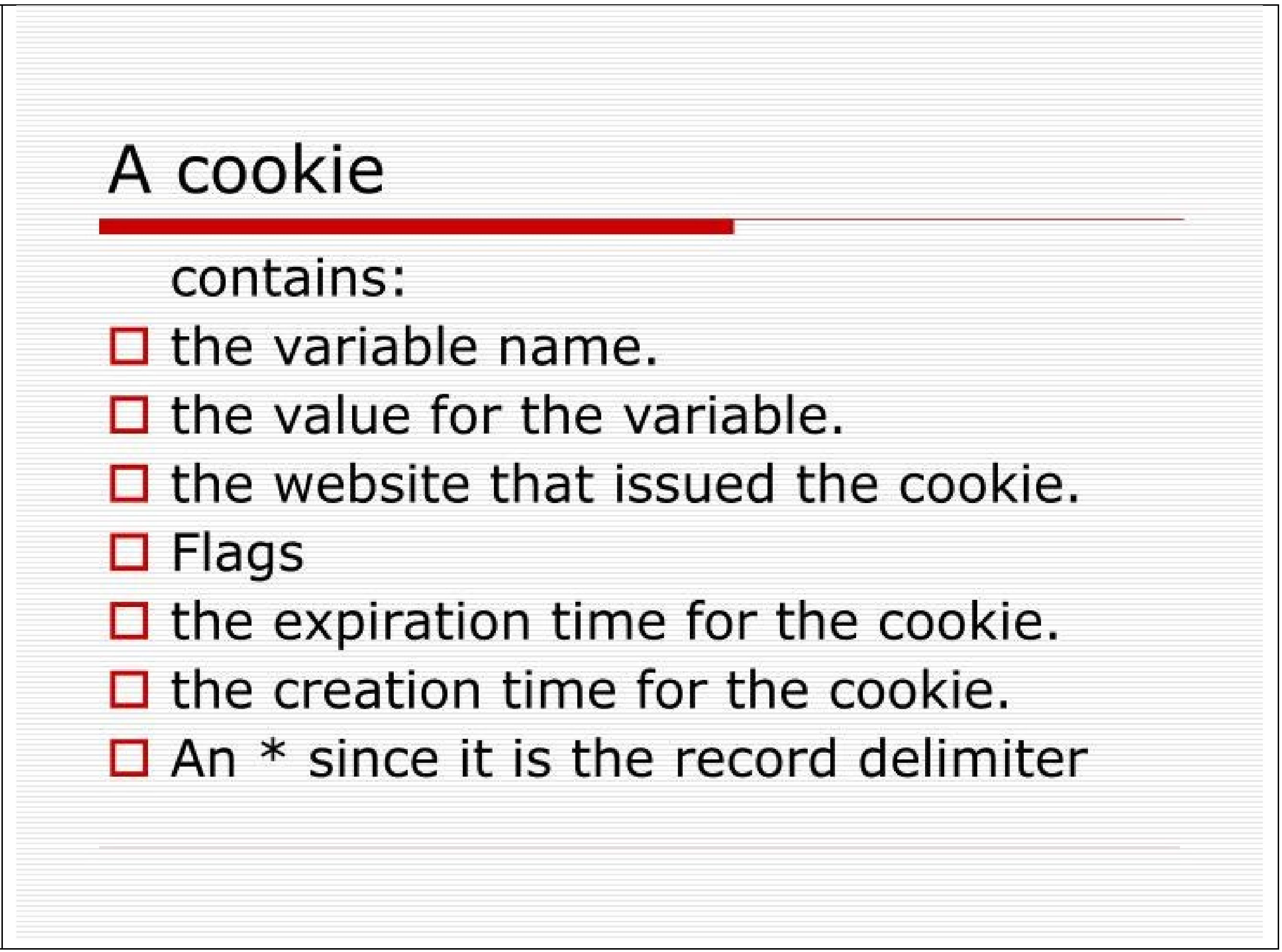
Social Media Evidence

Collection Methods

- Screen scrape / Screen shot
- Manual documentation
- Open source tools (HTTrack)
- Commercial tool (X1)
- Web service (Pagefreezer)
- Forensic recovery
- Content subpoena

	 Social Media Final Thoughts Constant Evolution Social Media Crime & Litigation Increasing Social Media Legislation Technical & Legal Slow to Catch Up Increasing Privacy Awareness i-Sight
9.	Web browser activity reconstruction.

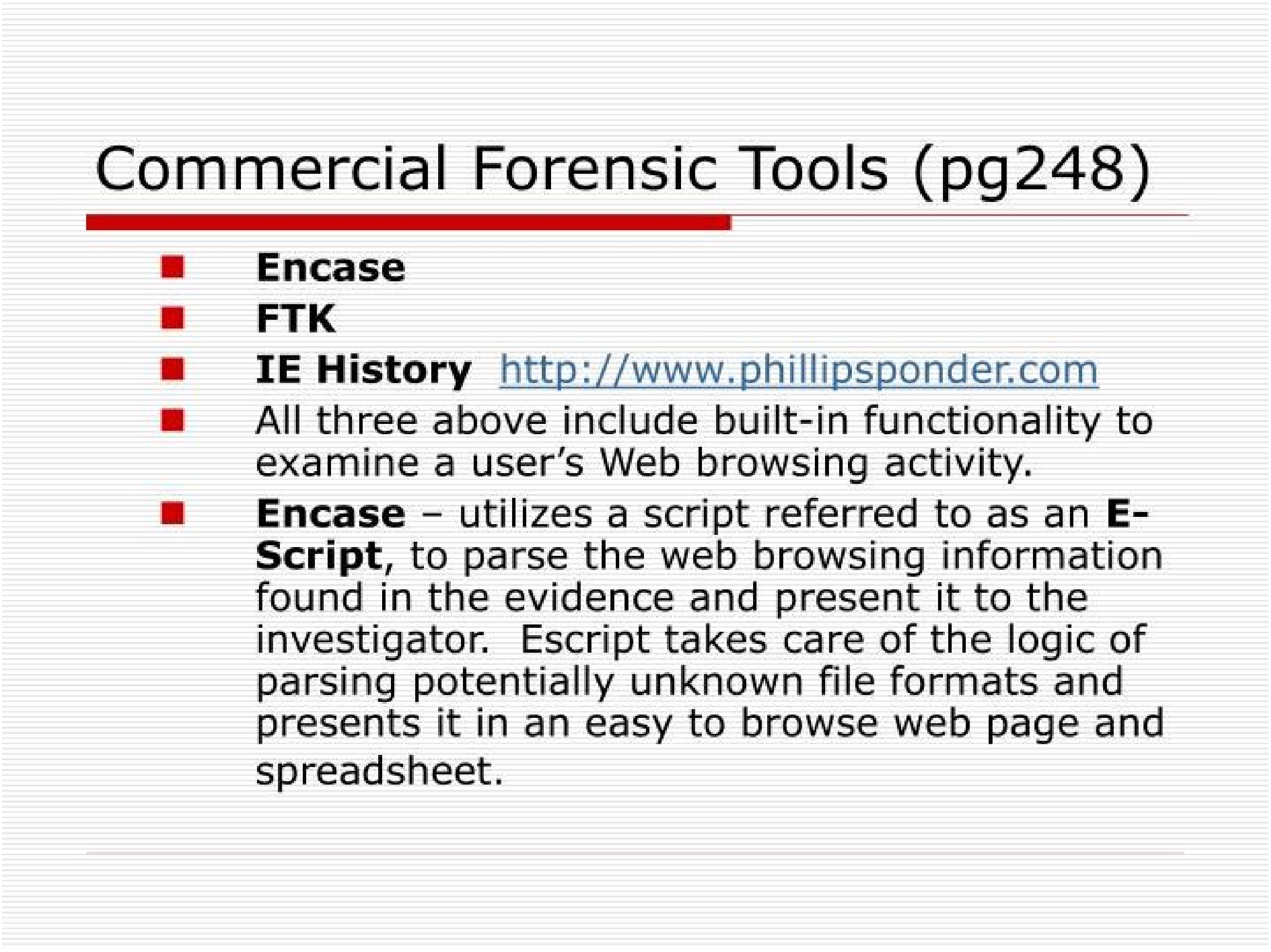
ANS:	 Web activity □ We con reconstruct a detailed history of a computer's use by examining a handful of files that contain the web browser's history. Internet explorer uses three facilities where we can find evidence: □ Web browsing history, cookies, and temp internet files



A cookie

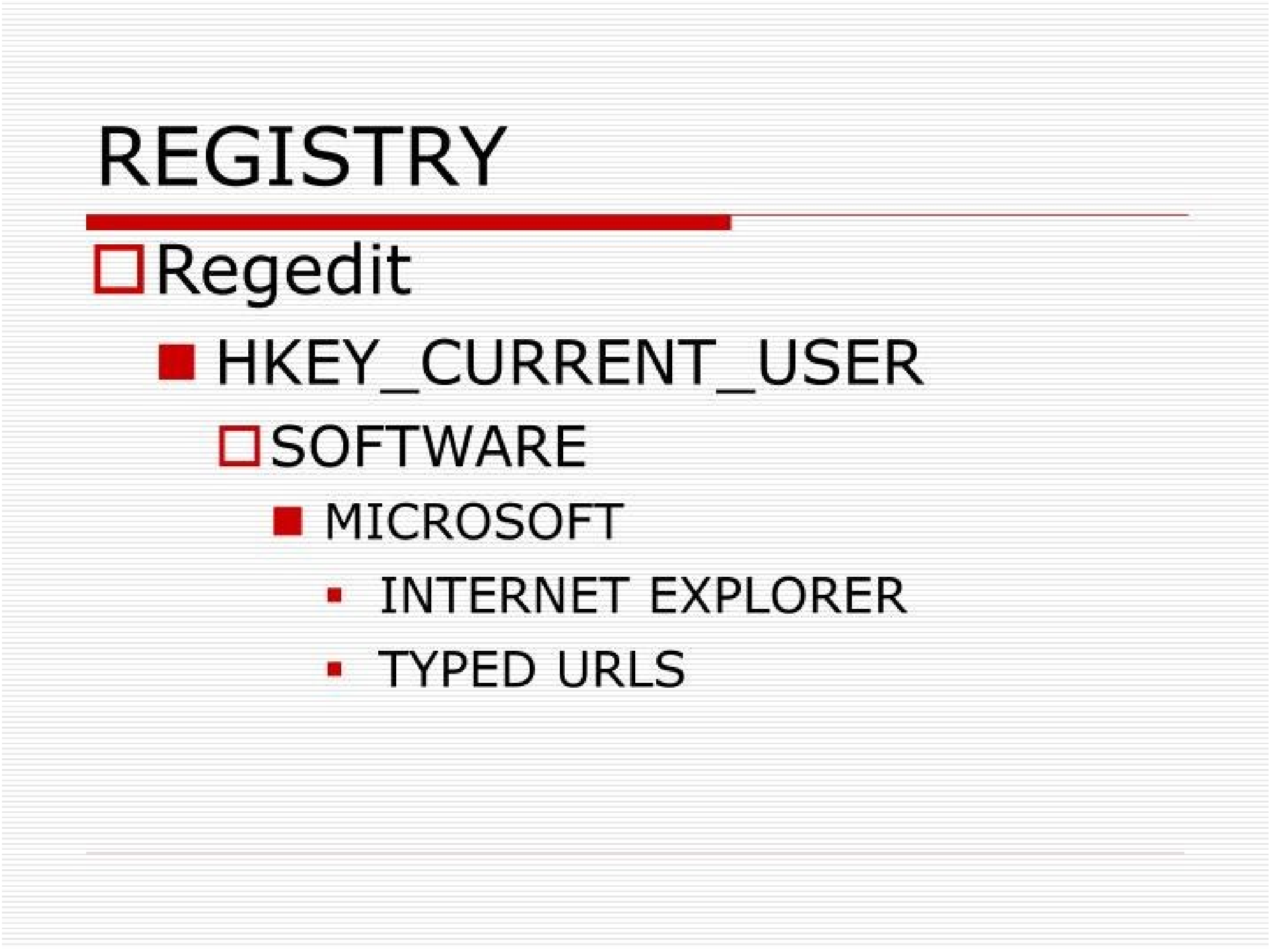
contains:

- 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



Commercial Forensic Tools (pg248)

- **Encase**
- **FTK**
- **IE History** http://www.phillipsponder.com
- All three above include built-in functionality to examine a user’s Web browsing activity.
- **Encase** – utilizes a script referred to as an **E-Script**, to parse the web browsing information found in the evidence and present it to the investigator. Escript takes care of the logic of parsing potentially unknown file formats and presents it in an easy to browse web page and spreadsheet.

	 REGISTRY □ Regedit ■ HKEY_CURRENT_USER □ SOFTWARE ■ MICROSOFT ▪ INTERNET EXPLORER ▪ TYPED URLS
10.	Internet forensics with different the internet crimes.
ANS:	same as Q 1
11.	Web browsers forensic analysis.
ANS:	● Web browser forensics has acquired much importance in digital forensics due to the growing number of internet fraud. ● Forensic analysis of the browser in a user's machine is the primary activity in such investigations as the information generated from web browsers can be of great use in reconstructing the browsing behavior of the user. ● Improper use of the internet can be detected from the information obtained. ● Since browsers are adaptable with the frequent version changes it is highly essential for the digital forensics community to ensure that

they are familiar with the new updates in order to perform a forensic analysis.

- It has been identified that the web browser history, cache, cookies, preferences and the registry are the areas to be searched for evidence.
- Therefore, investigators have to obtain information from numerous locations in order to be confident that they have identified all the digital evidence pertaining to a user’s web browser usage.
- The need for extended privacy in web browsing led to the creation of private browsing mode.
- The motivation for a user to browse privately is to conceal evidence of unusual browsing activity.
- A study on the private browsing artifacts of the installed browsers has shown that the private browsing modes of the Google Chrome, Mozilla Firefox and Microsoft Internet Explorer browsers have left artifacts.
- Microsoft Internet Explorer left forensic artifacts of the private browsing session, in the form of deleted files on the hard disk.
  Mozilla Firefox left artifacts on the hard disk in the pagefile.sys file.
- A recent experiment conducted has shown the weakness of private browsing modes.
- Running a memory leaking program, can pull artifacts from private browsing sessions in to the memory.
- DNS resolutions are cached by the operating system, and an analysis of the cache and Time to live values, it can be concluded if the user visited a particular site.
- Further traces can be obtained by checking the swapped pages.
- With the assistance of advanced browser forensic tools within a few seconds we would be in a position to extract the chosen keywords of most web browsers (Google Chrome, Internet Explorer, Opera Browser, Comodo Dragon, RockMelt) from the local browser history search engine.
- The program will attempt to find the keyword(s) including deleted keywords in the history title and search even the browser history was cleared.

	● If the keyword is present or suspected to be, it will be display in the results list with his URL and Title. ● After Execution, the reports are generated displays date-time folder with subfolders named after the name of the browsers in the suspects system. ● The forensic tools generates various reports in each browser like: ➔ Cookies ➔ Downloads ➔ History ➔ Saved Password ➔ Type of URL's
12.	Write a brief report on how you should proceed for a given case (assume it is given).
ANS:	● *Make an initial assessment about the type of case you're investigating—* - To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident. - Have law enforcement or company security officers already seized the computer, disks, and other components? - Do you need to visit an office or another location? - Was the computer used to commit a crime, or does it contain evidence about another crime? ● *Determine a preliminary design or approach to the case—* - Outline the general steps you need to follow to investigate the case. - If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. - If you're preparing a criminal case, determine what information law enforcement officers have already gathered.

- *Create a detailed checklist—*
  - Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step.
  - This outline helps you stay on track during the investigation.
- *Determine the resources you need—*
  - Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.
- *Obtain and copy an evidence drive—*
  - In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, USB drives, PDAs, and other removable media.
  - Make a forensic copy of the disk.
- *Identify the risks—*
  - List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment.
  - For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.
- *Mitigate or minimize the risks—*
  - Identify how you can minimize the risks.
  - For example, if you're working with a computer on which the suspect has likely password protected the hard drive, you can make multiple copies of the original media before starting.
  - Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.
- *Test the design—*
  - Review the decisions you've made and the steps you've completed.

	- If you have already copied the original media, a standard part of testing the design involves comparing hash values to ensure that you copied the original media correctly. ● *Analyze and recover the digital evidence—* - Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence. ● *Investigate the data you recover—* - View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect's guilt or innocence. ● Complete the case report— - Write a complete report detailing what you did and what you found. ● *Critique the case—* - Self-evaluation is an essential part of professional growth. - After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.
13.	What are the Difficulties of web browsers forensic analysis?
ANS:	An examiner can have the following difficulties when analyzing web browsers: 1. There are a many browsers to search from due to which there is lots of data found. 2. Different data is found from all the different browsers that are accessed. 3. Encryption used to protect user data. 4. User's use of Private mode (or Incognito mode), in which the examined computer does not have web browser artifacts. 5. Multiple browsers: Investigators will likely encounter numerous mainstream browsers. There may even be multiple browsers in use on the same machine. 6. Varied storage schemes: Once investigators determine which browsers are being used, they must realize that each browser may store different types of artifacts, differently and in different locations. 7. New/updated architectures: Browser developers may even completely change the architecture between versions, as Mozilla Firefox and Internet Explorer (IE) have done in the past.

8. Non-standard browsers: To further frustrate investigators, attackers may actually install a nonstandard browser in an effort to obfuscate their activities.

14. Explain the law against email crimes.

ANS:

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.
3. **Charges of Wire Fraud for Email Hacking**

   In simple terms, wire fraud involves using a computer, radio, television, or telephone to get money or property from someone else through trickery or deception. This is prohibited and is known as the Wire Fraud Act.

   Although taking money is a common example of wire fraud, such as through various Internet scams, stealing personal and confidential information qualifies as wire fraud, too. One of the keys to wire fraud is that the emails, telephone calls, or wire transmissions have to pass between two or more states or countries.

4. **Charges of Computer Fraud for Email Hacking**

Computer fraud, is similar to wire fraud, except this crime applies only to use of computers, as opposed to telephones and radios. It also requires some sort of interstate connection. However, the law applies only to computers used:

by or for financial institutions, like banks or the U.S. government, and
in such a way that the computer impacts interstate or foreign commerce or communication of the U.S.

5. **Charges of Identity Theft for Email Hacking**

Identity theft is when someone uses fraud, deception, or trickery to get and use another person's personal information. Usually, the information is used by the thief to make money, but money doesn't have to be involved.

6. **Charges of Obstruction of Justice for Email Hacking**

The crime of obstruction of justice covers many things, but it typically means interfering with some legal process or investigation.

7. Additional Laws That Could Be Used Against an Email Hacker

For example, most states have passed criminal and civil identity theft laws. In addition, in some states, like Virginia, it is an invasion of privacy to look at someone's personal information, and this act constitutes a crime. In many states, like Maryland, accessing and telling the world about another person's personal information is an invasion of privacy that may make the hacker liable for money damages to the victim.

15. Internet forensics. Explain WWW threats.

ANS: Internet Forensics:-

•Internet forensics relates to the examination of infrastructure out of one's control,such as servers in other countries.

•Internet forensics applies to both investigations of crimes committed on the Internet and investigations of crimes committed with the Internet.

•computer intrusion, denial-of-service attacks, and bank fraud

•Identity theft, extortion, and money laundering

16. Role of email in forensic investigations.

ANS:	● An increase in e-mail scams and fraud attempts with phishing or spoofing Investigators need to know how to examine and interpret the unique content of e-mail messages. ● Phishing e-mails are in HTML format, which allows creating links to text on a Web page ❖ Many times, the Internet links in a phishing e-mail appear to be correct, such as the U.S. Internal Revenue Service's Web page "www.irs.gov" ❖ Attempts to get personal information from reader ● Pharming - DNS poisoning takes user to a fake site ● A noteworthy e-mail scam was 419, or the Nigerian Scam ● Spoofing e-mail can be used to commit fraud ● Investigators can use the Enhanced/Extended Simple Mail Transfer Protocol (ESMTP) number in the message's header to check for legitimacy of email
17.	Explain Messenger Forensics in detail.
ANS:	
18.	How evidences are collected in social media forensics.
ANS:	● Social media sites, such as Twitter, Facebook, LinkedIn, and YouTube, aren't just a way of communicating with friends and family. ● These online social networks (OSNs) are also used to conduct business, brag about criminal activities, raise money, and have class discussions. ● You can also use OSNs to build a profile of a prospective client, a business partner, a suspect in a murder trial, and more. ● Social media can contain a lot of information, including the following: ❑ • Evidence of cyberbullying and witness tampering ❑ • A company's position on an issue

	❑ • Whether intellectual property rights have been violated ❑ • Who posted information and when ● The number of cases involving social media is growing, and social media evidence often substantiates a party’s claims. ● Social media evidence can be found in several places including the suspect’s computer, smartphone, and the provider’s network. ● Getting evidence from the provider will require relatively quick action along with a subpoena or search warrant. ● Remember, the provider only retains this information for a certain amount of time. At some point, the data you need will be purged without some legal intervention. ● All things considered, collecting the evidence from the provider might yield the best results. ● Recovering evidence on the local machine can be a challenge. The page file (or swap space) is one location that could bear fruit. INDEX.DAT files also hold promise. ● Multiple artifacts can be found here. The confirmation e-mail (sent when the account is created) is found in the History.IE5\Index.dat file. ● The user’s Facebook profile can be found on the local machine in a file named profile[#].htm. ● This is located in the Content.IE5 directories. The History.IE Index.dat file can hold Facebook friend searches.
19.	Explain CAN-SPAM Act in email crimes.
ANS:	● The CAN-SPAM Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations. ● Despite its name, the CAN-SPAM Act doesn’t apply just to bulk email.

- It covers all commercial messages, which the law defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,” including email that promotes content on commercial websites.
- The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.
- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000, so non-compliance can be costly.
- Here’s a rundown of CAN-SPAM’s main requirements:
    - ❑ **Don’t use false or misleading header information:** Your “From,” “To,” “Reply-To,” and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
    - ❑ **Don’t use deceptive subject lines:** The subject line must accurately reflect the content of the message.
    - ❑ **Identify the message as an ad**: The law gives you a lot of leeway in how to do this, but you must disclose clearly and conspicuously that your message is an advertisement.
    - ❑ **Tell recipients where you’re located:** Your message must include your valid physical postal address. This can be your current street address, a post office box you’ve registered with the U.S. Postal Service, or a private mailbox you’ve registered with a commercial mail receiving agency established under Postal Service regulations.
    - ❑ **Tell recipients how to opt out of receiving future email from you:** Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email

from you in the future. Craft the notice in a way that’s easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy Internetbased way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you. Make sure your spam filter doesn’t block these opt-out requests.

❑ **Honor opt-out requests promptly**: Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient’s opt-out request within 10 business days. You can’t charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don’t want to receive more messages from you, you can’t sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you’ve hired to help you comply with the CAN-SPAM Act.

❑ **Monitor what others are doing on your behalf**: The law makes clear that even if you hire another company to handle your email marketing, you can’t contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

20. Explain web browsers forensic analysis with respect to Cookie storage and analysis, Cache and temporary internet files.

ANS: **Cookies**

- A cookie is a small text file that is deposited on a user’s computer by a web server.
- Cookies can serve a variety of purposes. They can be used to track sessions as well as remember a user’s preferences for a particular web site.
- Amazon.com is a great example. When you return to the site you are normally greeted with a “Hello, Susan” as well as customized recommendations based on your buying and browsing history.
- That level of individualization is made possible through cookies.
- Cookies can provide valuable evidence and are tracked in a single INDEX.DAT file.
- They can contain Uniform Resource Locators (URLs), dates and times, user names, and more.
- Deciphering a cookie can be a challenge, as they aren’t normally written in the clear.
- Fortunately for us, tools are available to get this done.
- It’s critical to note that the existence of a web address in a cookie is not necessarily proof that the suspect actually visited the site

Temporary Internet Files, a.k.a. web Cache

- We are an impatient lot. As such, speed is vital to a user’s Internet experience.
- Today, web browsing is expected to be nearly indistinguishable from the applications running on our own machines.
- web cache is one way that the browser makers shave some time off the download times.

- Cache speeds things along by reusing web page components like images, saving time from having to download objects more than once.
- Microsoft’s browser, Internet Explorer, refers to web cache as Temporary Internet Files (TIF).
- In Microsoft Internet Explorer, TIF is organized into sub-folders bearing a random eight-character name. They are organized using a collection of INDEX.DAT files.
- Each file in TIF has a corresponding date and time value associated with it. This includes a “last-checked” time, which is used by the browser to determine if a newer version exists on the server. If so, then it will download the newer version.
- Users can view their TIF anytime using Windows Explorer.
- Inside the TIF folder users will see a listing of its contents. Each item in the list will display an icon showing file type, file name, and the associated URL.
- It’s important to understand that in this instance, what the user sees is a virtualized representation of the content. The actual items are kept in the TIF subdirectories.
- The only file that is actually kept here is the INDEX.DAT that keeps tabs on where the files are located inside the various subdirectories.
- Webmail evidence can also be found in TIF. Hotmail, AOL, and Yahoo! can all leave messages and/or inbox information that can prove useful. These items can be recognized by the file names.
- Here are some examples:

■ Outlook web Access Messages—Read[#].htm

■ AOL Messages—Msgview[#].htm

■ Hotmail messages—getmsg[#].htm

■ Yahoo!—ShowLetter[#].htm

■ Outlook web Access Inbox—Main[#].htm

■ AOL Inbox—Msglist[#].htm

	■ Hotmail Inbox—HoTMail[#].htm ■ Yahoo!—ShowFolder.htm ● web cache can be used to determine both culpability and intent ● Much of what's in web cache will be thumbnails (those small images) along with bits and pieces of web pages. ● Image size can impact a case, particularly those involving child pornography. ● If the suspect images are comprised entirely of small, cache-like images, then some prosecutors may be reluctant to file charges. ● The issue then becomes intent. Those images could have been downloaded automatically, without his consent. ● Images of such a small size can make for a much weaker case. ● Larger images, those not commonly found as part of a web page, are harder to explain away.
UNIT 4	
1.	What are the Components of search warrant?
ANS:	A judge issues a search warrant to authorize law enforcement officers to search a particular location and seize specific items. To obtain a search warrant, police must show probable cause that a crime was committed and that items connected to the crime are likely to be found in the place specified by the warrant. A valid search warrant must meet four requirements: a. the warrant must be filed in good faith by a law enforcement officer; b. the warrant must be based on reliable information showing probable cause to search; c. the warrant must be issued by a neutral and detached magistrate; and the warrant must state specifically the place to be searched and the items to be seized.
2.	Report Structure in detail. (You can also refer pg.521 of textbook)

ANS:

- **Don’t Procrastinate**
  - Start your report before you even begin your examination.
  - There is usually some information that you know before you run a single process.
  - Even if it is filling out serial numbers and contact information, by putting down what you do know in advance you will never be faced with that terrifying blank page once you wrap up your investigation.
  - It is also recommend updating your report as you go along.
  - one can do this by writing down information through each step, or even by keeping notes in a way that will allow for easy transfer to your report.
- **Include Analysis**
  - Don’t fall into the trap of simply listing files and search term hits.
  - While these can undoubtedly be useful, what really adds value to digital forensics is the analysis.
  - Without context, digital evidence is just ones and zeros.
  - If you find the “smoking bit” in a registry key, that’s great, but it won’t do you any good if you can’t explain what it is, how it works, and why it is significant.
- **Be Cautious of Absolutes**
  - There are few times when you can say with certainty that something is always true, or never occurs.
  - Even if you are very sure of a statement, be careful about using absolutes.
  - (Unless you have tested every eventuality and are sure there will be no subsequent research with opposing conclusions, these situations can create havoc during cross-examinations.)
  - Useful phrases include: “This leads me to believe...”, “It is my professional opinion...”, “The evidence indicates...” I’m not saying that you should be wishy-washy.
  - This language is a means of presenting the information as what it is—a professional opinion—because as expert witnesses we are able to express opinions.
- **Create a Template**
  - Templates are easy to create and will end up saving you many hours of work down the road.
  - The template doesn’t have to be set in stone, but just having one will make report writing easier, if for no other reason than because you won’t have to remember to include things that are already built-in.
  - They are a great tool for ensuring consistent formatting and standardized language.
  - Use confidentiality language whenever appropriate.
  - Also, it is recommended to have the word “Draft” in a header, footer, or watermark on every page until the report is finalized.
- **Break it Up**
  - Reports can get long and are often very detailed.
  - For the reader, they can seem dry.
  - Also, it may seem that with almost every report we write, the intended audience tends to focus on one or two items out of the entire report as the items of real interest to them.

- And while we think they marvel at every word as a manifestation of genius, we must know that what they really want to do is zero in on the really juicy bits and be able to navigate easily to other points as needed.
- Breaking up the report into sections is an easy way to accommodate your readers.
- Below are some frequently used sections:
    - **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 –**
        - This section is especially important to include if you were asked to perform a targeted investigation.
        - Other information to include would be search terms requested by the client.
    - **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 –**
  - ❑ Include a signature section that can be printed out and signed.
- ★ **Exhibits –**
  - ❑ We typically reserve exhibits A and B for my Curriculum Vitae and Chain of Custody documentation, respectively.
  - ❑ Certainly not necessary, but it makes it easier to always remember to include them in my reports.
  - ❑ Also, some information can be embedded into the report itself, but if there are items of interest that get long, it is highly recommended to include them as exhibits and simply hyperlink when you refer to them in the report.

The structure of a report and the purpose and contents of each section is shown below.

TITLE PAGE	report title your name submission date
EXECUTIVE SUMMARY	overview of subject matter methods of analysis findings recommendations
TABLE OF CONTENTS	list of numbered sections in report and their page numbers
INTRODUCTION	terms of reference outline of report's structure
BODY	headings and sub-headings which reflect the contents of each section. Includes information on method of data collection (if applicable), the findings of the report and discussion of findings in light of theory
CONCLUSION	states the major inferences that can be drawn from the discussion makes recommendations
REFERENCE LIST	list of reference material consulted during research for report

	APPENDIX information that supports your analysis but is not essential to its explanation
3.	How Warning banners are often easier to present in court than policy manuals
ANS:	● 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.

	● 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).
4.	Establishing company policies.
ANS:	• 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. ● One way that businesses can reduce the risk of litigation is to publish and maintain policies that employees find easy to read and follow. The most important policies are those that set rules for using the company's computers and networks. ● Published company policies provide a line of authority for a business to conduct internal investigations. ● The line of authority states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence. ● Well-defined policies give computer investigators and forensic examiners the authority to conduct an investigation. Policies also demonstrate that an organization intends to be fair minded and objective about how it treats employees and state that the organization will follow due process for all investigations. ("Due process" refers to fairness under the law and is meant to protect the

	innocent.) Without defined policies, a business risks exposing itself to litigation from current or former employees. ● The person or committee in charge of maintaining corporate policies must also stay current with local laws, which can vary depending on the city, state, and country.
5.	Explain Legal process.
ANS:	➔ 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.
- ➔ Not every police officer is a computer expert. Some are computer novices; others might be trained to recognize what they can retrieve from a computer disk. To differentiate the training and experience officers have, CTIN has established three levels of law enforcement expertise:

- Level 1—Acquiring and seizing digital evidence, normally performed by a police officer on the scene.
- Level 2—Managing high-tech investigations, teaching investigators what to ask for,and understanding computer terminology and what can and can’t be retrieved from digital evidence. The assigned detectives usually handle the case.
- Level 3—Specialist training in retrieving digital evidence, normally conducted by a data recovery or computer forensics expert, network forensics expert, or Internet fraud investigator. This person might also be qualified to manage a case, depending on his or her background

6. Evidence and various types of digital evidences.

ANS:

1. Digital evidence can be any information stored or transmitted in digital form.
2. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.
3. The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, spreadsheets, internet

browser histories, computer printouts, Global Positioning System tracks and digital video or audio files.

4. Categories of Digital Evidence
    - i. Because of the many different types of digital evidence, it is usually broken down into four main categories, based upon their source.
    - ii. They are:
        1. Computer forensics:
            - a. The oldest branch, this focuses on digital information from computers, including laptops or desktops, memory, hard drives, operating systems, and logs.
            - b. Usually, a computer device is confiscated and a digital image of drive is created for analysis.
            - c. One of the main aspects of computer forensics is recovering deleted files.
        2. Mobile forensics:
            - a. A mobile device is generally defined as one with a built-in communication system (a la GSM or SMS) as well as location information via GPS; however, mobile devices also include cameras and USB drives.
        3. Network forensics:
            - a. One of the newest categories monitors and collects evidence related to computer networks.
            - b. This is often used to detect intrusions into companies as well as examine packets of data transmitted through the system.
            - c. Information can be gathered in mass and stored for later analysis or collected in real-time and filtered to watch for specific files or events.
        4. Database forensics:
            - a. The analysis of data and metadata contained in databases such as Microsoft SQL, Oracle, and others.

	b. This information can is helpful in tracking financial crime activity as well as establishing timelines of events. 5. There are sub-categories such as email forensics, software-specific forensics, hardware forensics, and web forensics that offer additional niche specialties.
7.	Describe Law Enforcement with example.
ANS:	Ø When conducting public computer investigations, one must understand city, county, state or province, and federal or national laws on computer-related crimes, including standard legal processes and how to build a criminal case. Ø In a criminal case, a suspect is tried for a criminal offense, such as burglary, murder, molestation, or fraud. Ø To determine whether there was a computer crime, an investigator asks questions such as the following: What was the tool used to commit the crime? Was it a simple trespass? Was it a theft, a burglary, or vandalism? Did the perpetrator infringe on someone else's rights by cyberstalking or e-mail harassment? Ø Computers and networks might be only tools used to commit cyber crimes and for this reason, many states have added specific language to criminal codes to define crimes involving computers. Ø For example, they have expanded the definition of laws for crimes such as theft to include taking data from a computer without the owner's permission, so computer theft is now on a par with shoplifting or car theft. Ø Other states have instituted specific criminal statutes that address computer-related crimes but typically don't include computer-related issues in standard trespass, theft, vandalism, or burglary laws. Ø The Computer Fraud and Abuse Act was passed in 1986, but specific state laws weren't formulated until later. Still, many state laws on computer crime have yet to be tested in court. Ø Computers are involved in many serious crimes. The most notorious are those involving sexual exploitation of minors. Ø Digital images are stored on hard disks, Zip disks, floppy disks, USB drives, removable hard drives, and other storage media and circulated on the Internet.

	Ø Other computer crimes concern missing children and adults because information about missing people is often found on computers. Ø Drug dealers often keep information about transactions on their computers or personal digital assistants (PDAs). Ø This information is especially useful because it helps law enforcement officers convict the person they arrested and locate drug suppliers and other dealers. Ø Additionally, in stalking cases, deleted e-mail, digital photos, and other evidence stored on a computer can help solve a case.
8.	Information Technology Act in detail.
ANS:	· **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: •**
  - **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;**
  - **To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.**
  - **To facilitate electronic filing of documents with Government departments**
  - **To facilitate electronic storage of data**
  - **To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.**
  - **To give legal recognition for keeping of books of accounts by banker's in electronic form.**
  - **To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.**

- **The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime.**

- **The Act also sought to foster security practices within India that would serve the country in a global context.**

	· The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. **· The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals.** **· Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion.**
9.	What is the purpose of affidavit?
ANS:	– An affidavit is a written statement from an individual which is sworn to be true – it is essentially an oath that what they are saying is the truth. – An affidavit will be used along with witness statements to prove the truthfulness of a certain statement in court. – The contents of an affidavit reflect the personal knowledge of the individual making the statement. – This means that someone cannot be penalised for failing to include information which they were not aware of. – This personal knowledge can include personal opinion rather than fact; however, it must be stated that this is opinion not fact. – Any individual can offer an affidavit as long as they have the mental capacity to understand the seriousness of the oath. – Affidavit is a document, given under penalty of perjury, that investigators create to detail their findings.

	– This document is often used to justify issuing a warrant or to deal with abuse in a corporation – An affidavit is voluntarily made without any cross examination of the affiant and, therefore, is not the same as a deposition, arecord of an examination of a witness or a party made either voluntarily or pursuant to a subpoena, as if the party were testifying in court under cross-examination. – A request to a court to exercise its judicial power in favor of a party that contains allegations or conclusions of facts that are not necessarily verified differs from an affidavit, which states facts under oath. – An affidavit is based upon either the personal knowledge of the affiant or his or her information and belief. – Personal knowledge is the recognition of particular facts by either direct observation or experience. Information and belief are what the affiant feels he or she can state as true, although not based on firsthand knowledge.
10.	Explain the concept of conducting security investigations.
ANS:	- A security incident is: ● a violation, breach or infringement of protective security policy or procedure ● an approach from anybody seeking unauthorised access to official resources ● an attempt to gain unauthorised access to official resources ● any other event that harms, or may harm the security of the New Zealand government, its institutions or programmes. - Not all security incidents are significant enough to require investigation. Seek guidance from supporting agencies. ➔ *Your organisation's role* ● Your organisation must assess the harm from any security incident. Determine the impact of actual, potential, or suspected loss, compromise or disclosure. - You must: ● identify whether the incident is minor (an infringement or breach) or major (a violation, which you must report) ● report the incident to any other relevant agencies, - Always report these kinds of security incidents

- Your people and contractors must report:
  - crimes like theft or attempted theft, burglary, damage e.g. vandalism, fraud or assault
  - natural events like fire or storm damage which may compromise security
  - incorrect handling of information that is protectively marked.
- The people and tasks involved in reporting security incidents
- Your organisation must have a policy for security incident reporting. It should cover the roles and responsibilities of people who handle security incidents and run security investigations.

➔ *Chief Executives or Agency heads*

Your chief executive or agency head should ensure there are:

- processes for staff, contractors and contractor's employees to report security incidents
- records of the organisation's security performance and requirements.

➔ *Senior managers*

- Senior managers are responsible for the procedures for security incident reporting and recording — in their areas, and for the organisation overall.
- The Chief Security Officer (CSO), or their delegate, should help them.
- In security investigations, a senior manager, who is independent of the incident, should approve the terms of reference and objectives.
- They should also get regular reports on the investigation's progress.

➔ *Managers*

- Your managers should ensure security incidents are reported to the CSO, and work closely with them on any security concerns.
- If an incident involves your ICT system, you may also need to report to the Chief Information Security Officer (CISO).
- Managers have an important role to play. As they work closely with staff, they could be the first to detect a security incident or notice suspicious behaviour.

➔ *CSO*

- Your CSO, or their delegate, receives and actions information about security incidents.
- They should record security incidents and the outcome of investigations, and report regularly to senior management on security performance.

➔ *CISO / Information Technology Security Manager (ITSM)*

- Your CISO or ITSM receives and actions information about incidents involving ICT systems. These include denial of service attacks, targeted malicious email attacks, and loss of ICT assets or information.
- They should report major ICT security incidents to the National Cyber Security Centre (NCSC).
- They should tell your CSO about any ICT security incidents and the likely impacts. The CISO may have a role in investigating ICT security incidents.

➔ *Employees*

- Everyone that works for your organisation must know about and follow your processes for reporting security incidents.
- Your organisation must provide security awareness training for employees, contractors, and contractors' employees.

11. Corporate investigations in detail.

ANS: **A corporate investigation is the thorough investigation of a corporation or business in order to uncover wrongdoing committed by management, employees, or third parties.**

There are many aspects of corporate investigations and they can vary significantly based on your needs. For example, corporate investigations can uncover if a business partner is legitimate, whether an employee is stealing from the company, or reveal fraud and embezzlement, just to name a few. A corporate investigator's main job, though, is ensuring a company is running smoothly and within the law.

Types of Corporate Investigation:

Depending on what you're looking to investigate within your business, an investigator will conduct one or multiple of these investigations:

Undercover Investigation: By blending in with the company, an investigator can look into employee misconduct like theft, substance abuse, or harassment. Investigators will often use covert surveillance as a part of their inspection.

Research Investigation: Investigators can conduct research in order to find information about companies that you do business with for acquisitions, mergers, joint ventures, venture capital, private equity, and investments. They can also perform in-depth employee background checks.

Financial Investigation: An investigator conducting a financial investigation can discover embezzlement, money laundering, fraud, and other white-collar crime.

E-Discovery / Electronic Investigation: With e-discovery, investigators can gather electronically stored information in order to collect necessary evidence. They can also potentially restore lost data.

Corruption Investigation: An investigator looking for corruption can uncover bribery, illegal foreign exchange, corporate fraud, and industrial espionage.

How does a corporate investigation work?

The methods of investigation with vary depending on what kind of investigation you are looking for and the individual investigator. Be specific about your needs and the information you are seeking so your investigator can use the right tools to resolve your situation. Some techniques an investigator might use include:

	● **Financial investigation** ● **Due diligence** ● **Computer forensics** ● **Security penetration checks** ● **Countermeasure sweeps** ● **Integrity testing** ● **Surveillance**
12.	Need of affidavit.
ANS:	***Affidavit*** **•Sworn statement of support of facts about or evidence of a crime** **–It is Submitted to a judge to request a search warrant** ● **Have the affidavit notarized under sworn oath to verify that the information in the affidavit is true** **–Judge must approve and sign a search warrant** ● **Before you can use it to collect evidence** **<u>Purpose of affidavit-</u>** **• An affidavit will be used along with witness statements to prove the truthfulness of a certain statement in court.** **•This means that someone cannot be penalised for failing to include information which they were not aware of.** **•An affidavit is based upon either the personalknowledge of the affiant or his or her information and belief.** **•Personal knowledge is the recognition of particular facts by either direct observation or experience.** **•Information and belief are what the affiant feels he or she can state as true, although not based on firsthand knowledge.** **•Submitted to a judge to request a search warrant**

13. Systematic approach for conducting the investigation.

ANS:

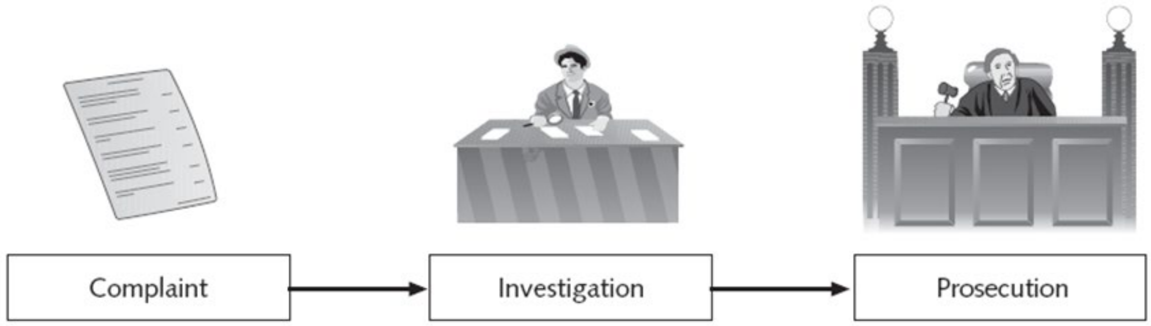


Figure 1-7 The public-sector case flow

–Criminal case follows three stages

The complaint, the investigation, and the prosecution

–A criminal case begins when someone finds evidence of an illegal act

–Complainant makes an allegation, an accusation or supposition of fact

–A police officer interviews the complainant and writes a report about the crime

•Police blotter provides a record of clues to crimes that have been committed previously

•Blotters now can be electronic files,databases

–Investigators delegate, collect, and process the information related to the complaint

–After that present the coll evidence to gov attorney.

–After you build a case, the information is turned over to the prosecutor

–Affidavit

•Sworn statement of support of facts about or evidence of a crime

–Submitted to a judge to request a search warrant

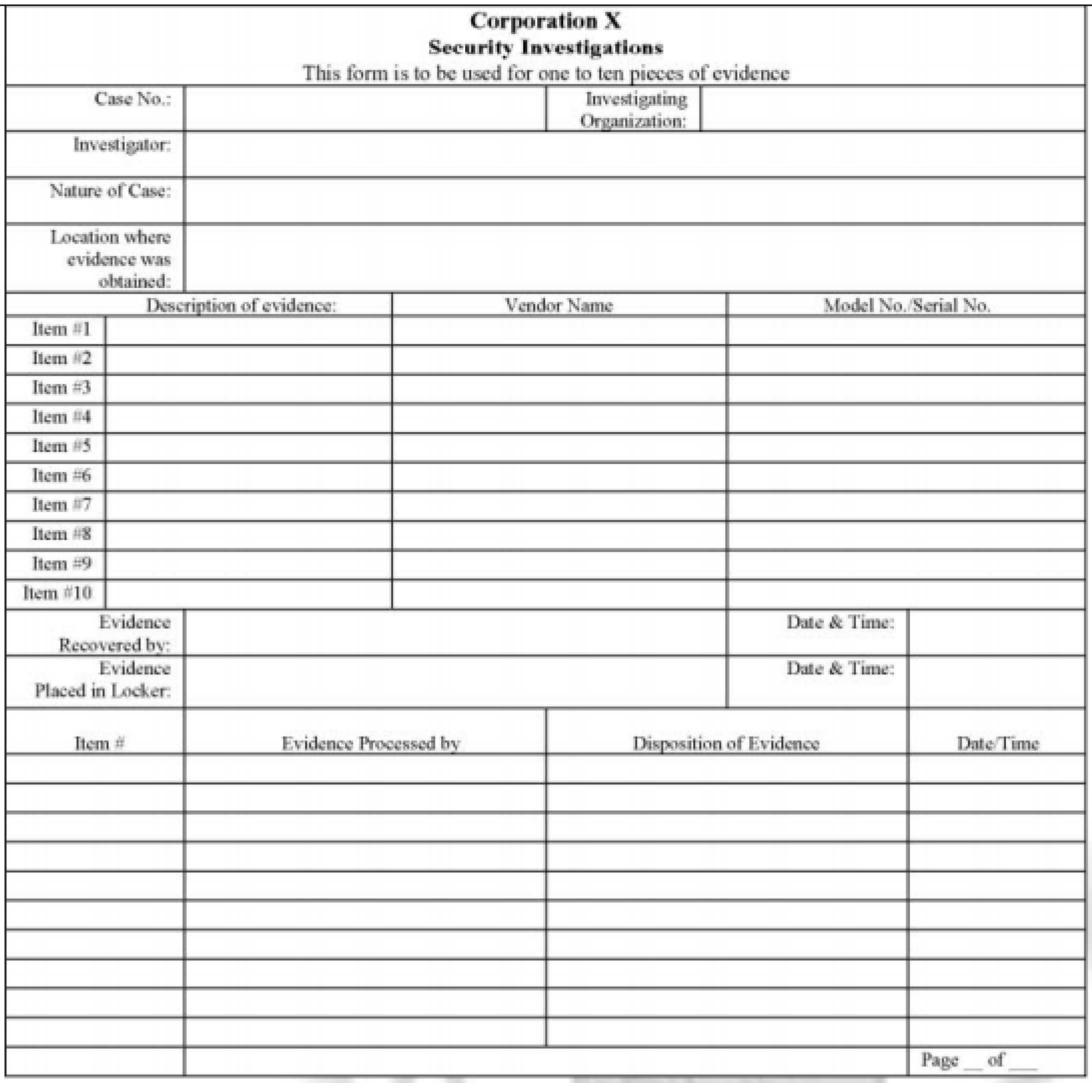
•Have the affidavit notarized under sworn oath to verify that the information in the affidavit is true

–Judge must approve and sign a search warrant

•Before you can use it to collect evidence

14. Sample of multi-evidence form used in corporate environment.

ANS:



Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

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 evidence was collected. If you’re using multi-evidence forms, a new form should be created for each location.

• Description of evidence—A list of the evidence items, such as “hard drive, 20 GB” or “one USB drive, 128 MB.” On a multi-evidence form, write a description for each item of evidence you acquire.

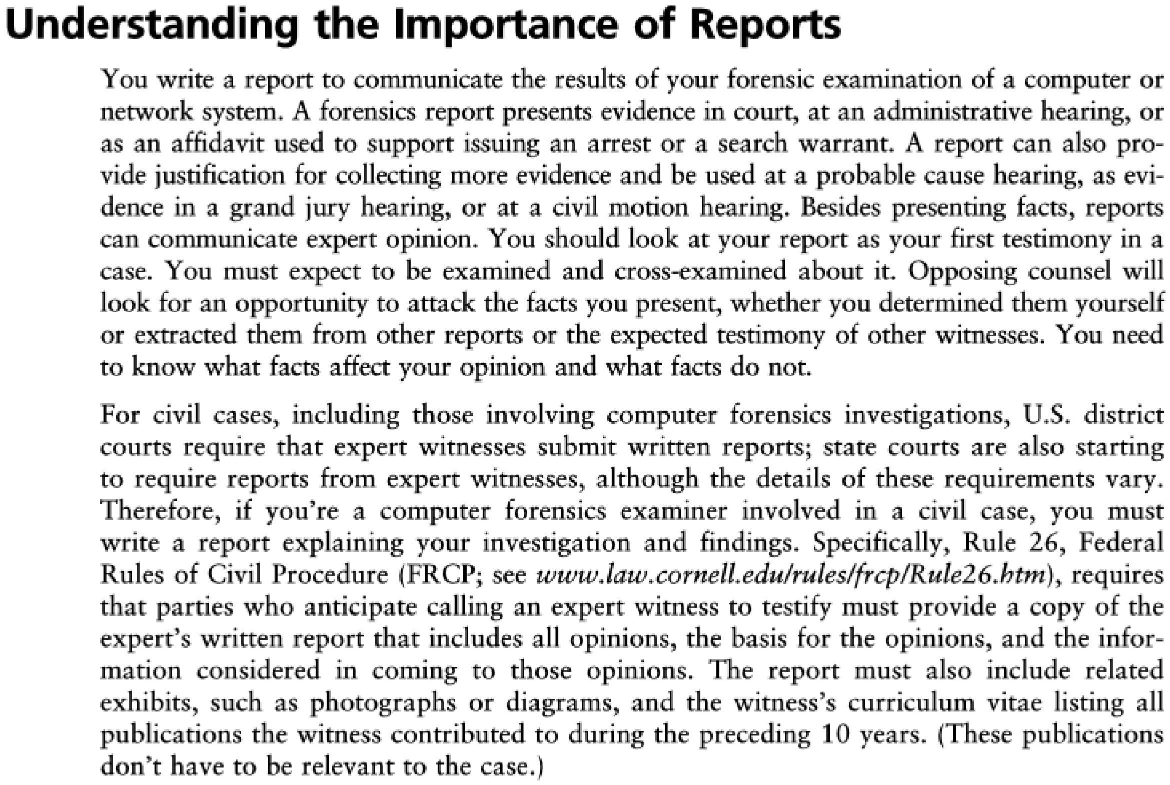
• Vendor name—The name of the manufacturer of the computer evidence. List a 20 GB hard drive, for example, as a Maxtor 20 GB hard drive, or describe a USB drive as an Attache 1 GB PNY Technologies drive. In later chapters, you see how differences among manufacturers can affect data recovery.

• Model number or serial number—List the model number or serial number (if available) of the computer component. Many computer components, including hard drives, memory chips, and expansion slot cards, have model numbers but not serial numbers.

• Evidence recovered by—The name of the investigator who recovered the evidence.

The chain of custody for evidence starts with this information. If you insert your name, for example, you’re declaring that you have taken control of the evidence. It’s now your responsibility to ensure that nothing damages the evidence and no one tampers with it. The person placing his or her name on this line is responsible for preserving, transporting, and securing the evidence.

- Date and time—The date and time the evidence was taken into custody. This information establishes exactly when the chain of custody starts.
- Evidence placed in locker—Specifies which approved secure container is used to store evidence and when the evidence was placed in the container.
- Item #/Evidence processed by/Disposition of evidence/Date/Time—When you or another authorized investigator retrieves evidence from the evidence locker for processing and analysis, list the item number and your name, and then describe what was done to the evidence.
- Page—The forms used to catalog all evidence for each location should have page numbers. List the page number, and indicate the total number of pages for this group of evidence. For example, if you collected 15 pieces of evidence at one location and your form has only 10 lines, you need to fill out two multi-evidence forms. The first form is noted as “Page 1 of 2,” and the second page is noted as “Page 2 of 2.”

15.	Explain significance of reports in forensics investigations.
ANS:	 **Understanding the Importance of Reports** You write a report to communicate the results of your forensic examination of a computer or network system. A forensics report presents evidence in court, at an administrative hearing, or as an affidavit used to support issuing an arrest or a search warrant. A report can also provide justification for collecting more evidence and be used at a probable cause hearing, as evidence in a grand jury hearing, or at a civil motion hearing. Besides presenting facts, reports can communicate expert opinion. You should look at your report as your first testimony in a case. You must expect to be examined and cross-examined about it. Opposing counsel will look for an opportunity to attack the facts you present, whether you determined them yourself or extracted them from other reports or the expected testimony of other witnesses. You need to know what facts affect your opinion and what facts do not. For civil cases, including those involving computer forensics investigations, U.S. district courts require that expert witnesses submit written reports; state courts are also starting to require reports from expert witnesses, although the details of these requirements vary. Therefore, if you're a computer forensics examiner involved in a civil case, you must write a report explaining your investigation and findings. Specifically, Rule 26, Federal Rules of Civil Procedure (FRCP; see *www.law.cornell.edu/rules/frcp/Rule26.htm*), requires that parties who anticipate calling an expert witness to testify must provide a copy of the expert's written report that includes all opinions, the basis for the opinions, and the information considered in coming to those opinions. The report must also include related exhibits, such as photographs or diagrams, and the witness's curriculum vitae listing all publications the witness contributed to during the preceding 10 years. (These publications don't have to be relevant to the case.)
16.	What is the Evidence collection process in private sector?
ANS:	Private-sector organizations include businesses and government agencies that aren't involved in law enforcement. ISPs can investigate computer abuse committed by their employees, but not by customers. ISPs and other communication companies now can investigate customers' activities that are deemed to create an emergency situation. An emergency situation under the Patriot Act is the immediate risk of death or personal injury, such as finding a bomb threat in an e-mail message. In the private sector, the incident scene is often a workplace, such as a contained office or manufacturing area, where a policy violation is being investigated. Everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority —that is, company management. Businesses have inventory databases of computer hardware and software. Having access to this database and knowing what applications are on suspected computers help identify the computer forensics tools needed to analyze a policy violation and the best way to conduct the analysis.

To investigate employees suspected of improper use of company computing assets, a corporate policy statement about misuse of computing assets allows corporate investigators to conduct covert surveillance with little or no cause and access company computer systems without a warrant, which is an advantage for corporate investigators.

A well-defined corporate policy should state that an employer has the right to examine, inspect, or access any company-owned computing assets.

As a standard practice, companies should use both warning banners and policy statements. With a policy statement, an employer can freely initiate any inquiry necessary to protect the company or organization.

If a corporate investigator finds that an employee is committing or has committed a crime, the employer can file a criminal complaint with the police.

If you discover evidence of a crime during a company policy investigation, first determine whether the incident meets the elements of criminal law.

You might have to consult with your corporate attorney to determine whether the situation is a potential crime.

Next, inform management of the incident; they might have other concerns, such as protecting confidential business data that might be included with the criminal evidence.

In this case, coordinate with management and the corporate attorney to determine the best way to protect commingled data.

After you submit evidence containing sensitive information to the police, it becomes public record.

Public record laws do include exceptions for protecting sensitive corporate information; ultimately, however, a judge decides what to protect.

After you discover illegal activity and document and report the crime, stop your investigation to make sure you don’t violate Fourth Amendment restrictions on obtaining evidence.

If you follow police instructions to gather additional evidence without a search warrant after you have reported the crime, you run the risk of becoming an agent of law enforcement.

Your next step is to work with the corporate attorney to write an affidavit confirming your findings.

The attorney should indicate in the affidavit that the evidence is commingled with company secrets and releasing the information will be detrimental to the company’s financial health.

When the affidavit is completed, you sign it before a notary, and then deliver the affidavit and the recovered evidence with log files to the police, where you make a criminal complaint.

At the same time, the corporate attorney goes to court and requests that all evidence recovered from the hard disk that’s not related to the complaint and is a company trade

	secret be protected from public viewing. You and the corporate attorney have reported the crime and taken steps to protect the sensitive data. In the evidence you’ve turned over to the police, the detective notices that the suspect is collecting most of his contra-band from e-mail attachments. The prosecutor instructed the detective to ask you to collect more evidence to determine whether the suspect is transmitting contraband pictures to other potential suspects. In this case, you should immediately inform the detective that collecting more evidence might make you an agent of law enforcement and violate the employee’s Fourth Amendment rights.
17.	Describe procedures for **preparing forensics evidence** for testimony.
ANS:	•Document your steps –To prove them repeatable •Preserve evidence and document it •Do not use formal checklist –Do not include checklist in final report –Opposing attorneys can challenge them •Collect evidence and document employed tools •Maintain chain of custody •Collect the right amount of information –Collect only what was asked for •Note the date and time of your forensic workstation when starting your analysis –Check your clock with time.gov •Keep only successful output –Do not keep previous runs •Search for keywords using well-defined parameters •Keep your notes simple •List only relevant evidence on your report •Define any procedures you use to conduct your analysis as scientific

	–And conforming to your profession’s standards •Monitor, preserve, and validate your work •Validate your evidence using hash algorithms
18.	Describe the fourth amendment to the United States constitution.
ANS:	**fourth amendment :** The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The ultimate goal of this provision is to protect people’s right to privacy and freedom from unreasonable intrusions by the government. However, the Fourth Amendment does not guarantee protection from all searches and seizures, but only those done by the government and deemed unreasonable under the law. To claim violation of Fourth Amendment as the basis for suppressing a relevant evidence, the court had long required that the claimant must prove that he himself was the victim of an invasion of privacy to have a valid standing to claim protection under the Fourth Amendment. However, the Supreme Court has departed from such requirement, issue of exclusion is to be determined solely upon a resolution of the substantive question whether the claimant's Fourth Amendment rights have been violated, which in turn requires that the claimant demonstrates a justifiable expectation of privacy, which was arbitrarily violated by the government.
	Explain Laws & regulations related to Digital forensics
	Explains, Information Technology Act in detail

Note:-

- One case study is expected as the unit 2 /unit4/unit1 each in the syllabus.