Question 1: **The cyber forensics involves tough decisions and lot of planning. One of the first steps in planning includes the incident response planning? What planning is required by the forensic expert before approaching the forensics crime scene? Discuss 3 important planning points.  (6 Marks)**

**Ans :**

The incident response planning consists of all the activities necessary to accomplish the goals of incident response. The overall process and the activities should be well documented and understood by your response team, as well as by stakeholders throughout your organization. The process consists of three main activities, and we have found that it is ideal to have dedicated staff for each:  
  
1. Initial Response: The main objectives in this step include assembling the response team, reviewing network-based and other readily available data, determining the type of incident, and assessing the potential impact. The goal is to gather enough initial information to allow the team to determine the appropriate response. Typically, this step will not involve collecting data directly from the affected system. The data examined during this phase usually involves network, log, and other historical and contextual evidence. This information will provide you the context necessary to help decide the appropriate response. For example, if a banking trojan is found on the CFO’s laptop, your response will probably be quite different than if it is found on a receptionist’s system. Also, if a full investigation is required, this information will be part of the initial leads.

Some common tasks you may perform during this step are:

• Interview the person(s) who reported the incident. Gather all the relevant details they can provide.

• Interview IT staff who might have insight into the technical details of an incident.

• Interview business unit personnel who might have insight into business events that may provide a context for the incident.

• Review network and security logs to identify data that would support that an incident has occurred.

• Document all information collected from your sources.

2. Investigation: The goal of an investigation is to determine facts that describe what happened, how it happened, and in some cases, who was responsible. As a commercial IR team, the “who” element may not be attainable, but knowing when to engage external help or law enforcement is important. Without knowing facts such as how the attacker gained access to your network in the first place, or what the attacker did, you are not in a good position to remediate. It may feel comforting to simply pull the plug and rebuild a system that contains malware The five-step process, shown in attached figure, promotes an effective investigation.

Initial Leads: There are three common characteristics of good leads:

• Relevant: The lead pertains to the current incident. A common trap organizations fall into is categorizing anything that seems suspicious as part of the current incident. Also, an incident prompts many organizations to look at their environment in ways they never have before, uncovering many “suspicious activities” that are actually normal.

• Detailed: The lead has specifics regarding a potential course of investigation. For example, an external party may provide you with a lead that indicates a computer in your environment communicated with an external website that was hosting malware. Although it was nice of them to inform you, this lead is not very specific.

• Actionable: The lead contains information that you can use, and your organization possesses the means necessary to follow the lead.

a. Indicators of Compromise: IOC creation is the process of documenting characteristics and artifacts of an incident in a structured manner. This includes everything from both a host and network perspective—things beyond just malware.

b. IOC Deployment: Enabling IR teams to find evil in an automated fashion, either through an enterprise IR platform or through visual basic (VB) and Windows Management Instrumentation (WMI) scripting. The success of an investigation depends on your ability to search for IOCs across the enterprise and report on them in an automated way.

c. Identify systems of Interest:Hits are when an IOC tool finds a match for a given rule or IOC. Prior to taking action on a hit, you should review the matching information to determine if the hit is valid. This is normally required because some hits have a low confidence because they are very generic, or because of unexpected false positives.

d. Collect Evidence: Once systems are identified and have active indicators of compromise, the next step is to collect additional data for analysis. The primary goals when preserving evidence are to use a process that minimizes changes to a system, minimizes interaction time with a system, and creates the appropriate documentation. You may collect evidence from the running system or decide to take the system down for imaging.

e. Analyzing Data: Analyzing data is the process of taking the evidence preserved in the previous step and performing an examination that is focused on answering the investigative questions. The results of the analysis are normally documented in a formal report.

3. Remediation: Remediation plans will vary greatly, depending on the circumstances of the incident and the potential impact. The plan should take into account factors from all aspects of the situation, including legal, business, political, and technical. The plan should also include a communication protocol that defines who in the organization will say what, and when. Finally, the timing of remediation is critical. There are many moving parts to any organization, and undertaking the coordination of removing a threat is no easy task. The approach we take is to define the appropriate activities to perform for each of the following three areas:

• Posturing: Posturing is the process of taking steps that will help ensure the success of remediation. Activities such as establishing protocol, exchanging contact information, designating responsibilities, increasing visibility, scheduling resources, and coordinating timelines are all a part of the posturing step.

• Tactical (short term): Tactical consists of taking the actions deemed appropriate to address the current incident. Activities may include rebuilding compromised systems, changing passwords, blocking IP addresses, informing customers of a breach, making an internal or public announcement, and changing a business process.

• Strategic (long term): The Strategic portion of remediation addresses these areas, which are commonly long-term improvements that may require significant changes within an organization.

---------------------------------------------------------------------------------------------------------------------------------

Question 2: **Consider that you have approached the forensics crime scene. What are the necessary steps you need to follow while collecting evidence and taking it to forensics lab? Discuss the importance of three such important pillars/steps.   (6 Marks)**

**Ans :**

Identifying Digital Evidence:

Digital evidence can be any information stored or transmitted in digital form. Following are the general tasks I perform when working with digital evidence:

• Identify digital information or artifacts that can be used as evidence.

• Collect, preserve, and document evidence.

• Analyze, identify, and organize evidence.

• Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.

Collecting computers and processing a criminal or incident scene must be done systematically. To minimize confusion, I reduce the risk of losing evidence, and avoid damaging evidence, by being the only person to collect and catalog digital evidence at a crime scene or lab, if practical. If there’s too much evidence or too many systems to make it practical for one person to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloging evidence.

Identifying the nature of the case:

When I am assigned to a computing investigation case, I start by identifying the nature of the case, including whether it involves the private or public sector. The nature of the case dictates how you proceed and what types of assets or resources you need to use in the investigation.

Identifying the Type of Computing System

Next step is to determine the type of computing systems involved in the investigation. For law enforcement, this step might be difficult because the crime scene isn’t controlled. I might not know what kinds of computers were used to commit a crime or how or where they were used. In this case, I must draw on my skills, creativity, and sources of knowledge, such as the Uniform Crime Report

Determining Whether I Can Seize a Computer

Generally, the ideal situation for incident or crime scenes is seizing the computers and taking them to your lab for further processing. However, the type of case and location of the evidence determine whether you can remove computers from the scene. Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab. If removing the computers will irreparably harm a business, the computers should not be taken offsite, unless I have disclosed the effect of the seizure to the judge. An additional complication is files stored offsite that are accessed remotely. I will decide whether the drives containing those files need to be examined. Another consideration is the availability of online data storage services that rent space, which essentially can’t be located physically. The data is stored on drives where data from many other subscribers might be stored.

Obtaining a Detailed Description of the Location

The more information I have about the location of a computer crime, the more efficiently I can gather evidence from a crime scene. Environmental and safety issues are the primary concerns during this process. Before arriving at an incident or crime scene, identify potential hazards to my safety as well as that of other examiners. Some computer cases involve dangerous settings, such as a drug bust of a methamphetamine lab or a terrorist attack using biological, chemical, or nuclear contaminants. For these types of investigations, I must rely on the skills of hazardous materials (HAZMAT) teams to recover evidence from the scene. The recovery process might include decontaminating computing components needed for the investigation, if possible. If the decontamination procedure might destroy electronic evidence, a HAZMAT specialist or an investigator in HAZMAT gear should make an image of a suspect’s drive.

Determining who is in charge

Corporate computing investigations usually require only one person to respond to an incident or crime scene. Processing evidence involves acquiring an image of a subject’s drive. In law enforcement, however, many investigations require additional staff to collect all evidence quickly. For large-scale investigations, a crime or incident scene leader should be designated. Anyone assigned to a large-scale investigation scene should cooperate with the designated leader to ensure that the team addresses all details when collecting evidence.

Using Additional Technical Expertise

After I collect evidence data, determine whether I need specialized help to process the incident or crime scene. For example, suppose I am assigned to process a crime scene at a data center running Microsoft Windows servers with several RAID drives and high-end UNIX servers. I must identify the additional skills needed to process the crime scene, such as enlisting help with a high-end server OS. Other concerns are how to acquire data from RAID servers and how much data I can acquire. RAID servers typically process several terabytes of data, and standard imaging tools might not be able to handle these large data sets.

Determining the Tools You Need

After I have gathered as much information as possible about the incident or crime scene, I can start listing what you need at the scene. Being overprepared is better than being underprepared, especially when I determine that I can’t transfer the computer to my lab for processing. To manage my tools, I use my initial-response field kit and an extensiveresponse field kit. Using the right kit makes processing an incident or crime scene much easier and minimizes how much I have to carry from your vehicle to the scene.

Storing and transferring Digital Evidence:

With digital evidence, I need to consider how and on what type of media to save it and what type of storage device is recommended to secure it. The media I use to store digital evidence usually depends on how long I need to keep it. If I investigate criminal matters, store the evidence as long as I can. The ideal media on which to store digital data are CDRs or DVDs. To help maintain the chain of custody for digital evidence so that it’s accepted in court or by arbitration, restrict access to my lab and evidence storage area. When my lab is open for operations, authorized personnel must keep these areas under constant supervision. When your lab is closed, at least two security workers should guard evidence storage cabinets and lab facilities and help in transferring them to secure locations.

----------------------------------------------------------------------------------------------------------------------------------

Question 3: **The following scenario where a company has filed a case against an employee for copyright violation and sharing the sensitive photographs with the competitors. After confiscating the laptop of that employee and necessary paper work, you are expected to find the evidence. What are the potential places inside the laptop where you need to search to do thorough analysis? Discuss at least 7 such places in the laptop where you would search for evidence. We have utilized the forensics tools and have done practice on them as well. Given that your experience, which tool would be best suitable for what purpose and what value addition doses that have for you.     (10 Marks)**

Ans :

Investigating Employee copyright violation

Would use Autopsy tool to analyze various data in the employee's laptop. Autopsy can analyze data from several sources including image files from other vendors. Autopsy can perform forensics analysis on the following file systems:

• Microsoft FAT, NTFS, ExFAT, UFS1, and UFS2

• ISO 9660 and YAFFS2

• Mac HFS+ and HFSX

• Linux Ext2fs, Ext3fs, and Ext4fs

The potential places inside the laptop that need to be analyzed are illustrated below:

* File Explorer
* NTFS and file system analysis
* The Master File Table (MFT)
* Windows prefetch

Prefetch files are stored in %SYSTEMROOT%\Prefetch. In this directory, you will find the following files:

NTOSBOOT-B00DFAAD.pf The system boot prefetch. This always has the same name. On Windows Servers, this is the only prefetch file that will exist by default.

Layout.ini Contains data used by the disk defragmenter.

AppName-########.pf Up to 128 application-specific prefetch files, each with the extension .pf, and each representing an executable file that ran at least once. These files are named by concatenating the executable name, a dash, and a 32-bit hexadecimal hash derived from the file’s path. That means that the same executable, if ran from two different paths, will have two different prefetch files.

* Event logs

Acquiring the Windows event logs is a straightforward file acquisition task. Each log is stored in a separate file in paths specified within registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog. On Windows XP, Windows Server 2003, and prior operating systems, the default event log paths are

Application %SYSTEMROOT%\System32\Config\AppEvent.Evt

System %SYSTEMROOT%\System32\Config\SysEvent.Evt

Security %SYSTEMROOT%\System32\Config\SecEvent.Evt

* Scheduled tasks

Attackers often use scheduled tasks to execute malware on a remote compromised system without the need for “helper” utilities such as PsExec, which may increase the likelihood of detection. This technique is especially common when the attacker’s access is limited to a command shell.

.job Files: Configuration data for scheduled tasks is stored in .job files—one per task—within the %SYSTEMROOT%\Tasks directory. The Windows Task Scheduler service logs the start time and completion of previously executed tasks to a plain-text file named SchedLgU.txt.

This file grows to a maximum of 32KB before rolling. %SYSTEMROOT%\SchedLgU.txt Windows 2000, Server 2003, and XP %SYSTEMROOT%\Tasks\SchedLgU.txt Windows Vista, 2008, and later

* The registry

The registry serves as the primary database of configuration data for the Windows operating system and the applications that run on it. It was initially designed to do away with the multitude of .ini and other text-based configuration files that programs would maintain (often in inconsistent formats and locations) and scatter throughout a system.

As the operating system and applications have grown in complexity, so too has the scope of information tracked in the registry—as well as the forensic evidence that can be gleaned from it.

Two user hives, NTUSER.DAT and USRCLASS.DAT, are stored in different locations, depending on the version of Windows, as listed next. Windows XP and Server 2003 \Documents and Settings\<user>\NTUSER.DAT \Documents and Settings\<user>\Local Settings\Application Data\Microsoft\Windows\USRCLASS.DAT Windows Vista, 7, and Server 2008 \Users\<user>\NTUSER.DAT \Users\<user>\AppData\Local\Microsoft\Windows\USRCLASS.DAT

* Other artifacts of interactive sessions

LNK Files: Windows shortcut files, also known as “link files” due to their extension (.lnk), act as pointers to other files or folders on a system. Link files differ from symbolic links insofar as they only serve as extensions for Windows Explorer, whereas a symbolic link can be transparently acted upon as if it were its target file by any program.

* The Recycle Bin
* Memory forensics:

What kinds of evidence can you obtain from memory? The list is extensive and evergrowing as memory forensics toolkits continue to evolve, but it includes the following:

* Running processes and the system objects/resources with which, they interact
* Active network connections
* Loaded drivers
* User credentials (which may be hashed, obfuscated, or even appear in clear text)
* Portions of nonvolatile sources of evidence such as the registry, event log, and Master File Table

Question 4: **A Cyber stalking and intimidation case has come for you to investigate where the person is accused of sending threating emails. You as a forensic expert has to prove that the crime has happened. And do necessary investigation to either acquit the accused or collect enough evidence for his/her conviction. What will be your steps of action once you take charge of all the electronic devices of the accused. Discuss the tools that would help you. (10 Marks)**

Ans:

* Examining Email Messages:

Since the crime is committed via e-mail, I would first access the victim’s computer to recover the evidence. Using the victim’s e-mail client, I would find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. If I can’t actually sit down at the victim’s computer, I will guide the victim on the phone to open and print a copy of an offending message, including the header. The header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps me trace the e-mail to the suspect.

* Copying an Email Message:

Before I start an e-mail investigation, I will copy and print the e-mail involved in the crime or policy violation. I will also want to forward the message as an attachment to another e-mail address, depending on my organization’s guidelines. The following activity shows how to use Outlook 2007, included with Microsoft Office, to copy an e-mail message to a USB drive.

1. Insert a USB drive into a USB port.

2. Open Windows Explorer or the Computer window, navigate to the USB drive, and leave this window open.

3. Start Outlook by clicking Start, pointing to All Programs, pointing to Microsoft Office, and clicking Microsoft Office Outlook 2007.

4. In the Mail Folders pane, click the folder containing the message I want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message I want to copy.

5. Resize the Outlook window so that I can see the message I need to copy and the USB drive icon in Windows Explorer or the Computer window.

6. Drag the message from the Outlook window to the USB drive icon in Windows Explorer or the Computer window.

7. Click File, Print from the Outlook menu to open the Print dialog box. After printing the e-mail so that I have a copy to include in my final report, exit Outlook.

* Viewing Email Headers:

After I copy and print a message, I will use the e-mail program that created it to find the e-mail header. After I open e-mail headers, copy and paste them into a text document so that I can read them with a text editor such as a Notepad.

To retrieve an Outlook e-mail header, I would follow these steps:

Start Outlook, and then select the original of the message I copied as mentioned above.

Right-click the message and click Message Options to open the Message Options dialog box. The Internet headers text box at the bottom contains the message header

Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.

Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.

Save the document as Outlook Header.txt in my work folder. Then close the document and exit Outlook.

* Examining Email Headers:

The next step is examining the e-mail header I saved to gather information about the e-mail and track the suspect to the e-mail’s originating location. The primary piece of information looking for is the originating e-mail’s domain address or an IP address. Other helpful information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it’s supplied.

To open and examine an e-mail header, follow these steps:

1. Open the Computer window or Windows Explorer and navigate to my work folder.

2. Double-click a .txt file containing message header text, such as Outlook Header.txt. The message header opens in Notepad.

The e-mail header provides a lot of information. Lines 1 to 5 show the e-mail servers through which the message traveled. Line 1 shows the return path, which is the address an e-mail program uses for sending a reply, usually indicated as the “Reply to” field in an e-mail. Do not rely on the return path to reveal the e-mail’s source account, however. Spoofing (faking) an e-mail address in the Return-

* Examining Additional Email Files

E-mail programs save messages on the client computer or leave them on the server. How e-mails are stored depends on settings on the client and server. On the client computer, you could save all your e-mail in a separate folder for record-keeping purposes. For example, in Outlook, you can save sent, draft, deleted, and received e-mails in a .pst file, or you can save offline files in an .ost file. With these client files (.pst and .ost), users can access and read their e-mail offline (when their computers aren’t connected to the central e-mail server).

In Web-based e-mail, messages are displayed and saved as Web pages in the browser’s cache folders. Many Web-based e-mail providers also offer instant messaging (IM) services that can save message contents in proprietary and nonproprietary file formats. These files are usually stored in different folders than Internet data files are. For example, in Windows, you can scan IM files and folders under Documents and Settings\username\Application Data or under Program Files.

* Tracing an email message:

As part of the investigation, I will determine an e-mail’s origin by further examining the header with one of many free Internet tools. Determining message origin is referred to as “tracing.” I would several sources such as DNS Registry, ARIN to find out the domain thats hosting the email server and try trace the email to a specific end-point.

Using Network Email Logs:

Network administrators maintain logs of the inbound and outbound traffic routers handle. Routers have rules to allow or deny traffic based on source or destination IP address. In most cases, a router is set up to track all traffic flowing through its ports. Using these logs, one can determine the path a transmitted e-mail has taken. The network administrator who manages routers can supply the log files you need. Review the router logs to find the victim’s (recipient’s) e-mail, and look for the unique ID number

Network administrators also maintain logs for firewalls that filter Internet traffic; these logs can help verify whether an e-mail message passed through the firewall. Firewalls, such as WatchGuard, Cisco Pix, and Check Point, maintain log files that track Internet traffic destined for other networks or the network the firewall is protecting. When the network administrator provides firewall log files, you can open them in a text editor, such as Notepad in Windows or vi in UNIX.

Examining Email Server Logs:

The files that provide helpful information are log files and configuration files. Sendmail creates a number of files on the server to track and maintain the e-mail service. The first one to check is /etc/sendmail.cf, which contains configuration information for Sendmail, so you can determine where log files are stored. Sendmail refers to the sendmail.cf file to find out what to do with an e-mail after it’s received. For example, if the server receives an e-mail from an unsolicited site, a line in the sendmail.cf file can tell the Sendmail server to discard it.

Similar to the sendmail.cf file, the syslogd file includes e-mail logging instructions. By viewing this file, you can determine how Sendmail is set up to log e-mail events and which events are logged. The syslogd file’s configuration is located in /etc/syslog.conf, which contains three pieces of information that tell you what happened to an e-mail when it was logged: the event, the priority level of concern, and the action taken when it was logged. By default, Sendmail can display an event message, log the event message to a log file, or send an event message to a remote log host.

The syslog.conf file simply specifies where to save different types of e-mail log files. The first log file it configures is /var/log/maillog, which usually contains a record of Simple Mail Transfer Protocol (SMTP) communication between servers. Typically, UNIX systems are set to store log files in the /var/log directory. However, an administrator can change the log location, especially when an e-mail service specifies a different location. If you’re examining a UNIX computer and don’t find the e-mail logs in /var/log, you can use the find or locate command to find them.

* Email Forensics Tools

For many e-mail investigations, I can rely on e-mail message files, e-mail headers, and e-mail server log files. However, if I can’t find an e-mail administrator willing to help with the investigation, or if I encounter a highly customized e-mail environment, I can use data recovery tools and forensics tools designed to recover e-mail files. The following tools are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

• DataNumen for Outlook and Outlook Express

• FINALeMAIL for Outlook Express and Eudora

• Sawmill-GroupWise for log analysis

• DBXtract for Outlook Express

• Fookes Aid4Mail and MailBag Assistant for Outlook, Thunderbird, and Eudora

• Paraben E-Mail Examiner, configured to recover several e-mail formats

• AccessData FTK for Outlook and Outlook Express

• Ontrack Easy Recovery EmailRepair for Outlook and Outlook Express

• R-Tools R-Mail for Outlook and Outlook Express

• OfficeRecovery’s MailRecovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM LotusNotes

Few vendors have products for analyzing e-mail in systems other than Microsoft, such as Apple Mail or Novell Evolution. In this section, you learn about a method for acquiring Evolution e-mail directories and extracting messages with Hex Workshop. These techniques can be used with all e-mail systems that create flat plaintext files, known as an mbox format, to store messages. Vendor-unique e-mail file systems, such as Microsoft .pst or .ost, typically use Multipurpose Internet Mail Extensions (MIME) formatting, which can be difficult to read with a text or hexadecimal editor.

To carve e-mail messages from Evolution, you need to copy the .evolution directory, its subdirectories, and content to another storage medium that can be transported to your forensic workstation. One way is to export the .evolution directory and subdirectories from an image file to a target directory by using a forensics tool, such as FTK, EnCase, X-Ways Forensics, or Sleuth Kit and Autopsy. These tools export the directory with all subdirectories to the target drive path you designate. For an e-mail recovery that requires extracting only e-mail data from a litigant’s computer, the UNIX/Linux tar command is an easy tool to use. You can create a tarball of the entire .evolution directory and uncompress it so that a hexadecimal editor on any OS can read it. For other e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually. This technique requires perseverance because it’s tedious and time consuming.

* Recovering Outlook Files:

I might need to reconstruct .pst files and messages. With many advanced computer forensics tools, such as X-Ways Forensics, AccessData FTK, and Guidance Software EnCase, deleted .pst files can be partially or completely recovered. Typically, additional effort is required to reconstruct these recovered files so that their content can be extracted as part of a data recovery or forensics examination. The Scanpst.exe recovery tool comes with Microsoft Office and can repair .ost files as well as .pst files. Several other recovery tools are designed to reconstruct e-mail data in Outlook and other e-mail formats. One tool that has been well tested is Advanced Outlook Repair

* Action taken:

One advantage of using data recovery tools is that I don’t need to know how the e-mail server or e-mail client operates to extract data from these computers. Data recovery tools do the work and allow me to view evidence on the computer. After I compare e-mail logs with the messages, I should verify the e-mail account, message ID, IP address, and date and time stamp to determine whether there’s enough evidence for a warrant. If so, I can obtain and serve a warrant for the suspect’s computer equipment.

Question 5: **The cyber-attack has happened in the bank where malware was installed and lot of sensitive data got leaked.  As a forensic expert you are expected to propose the remediation steps for the bank so that system can be improved. How do you proceed with the remediation steps? Discuss the steps in brief. [You are not expected to do cyber forensic evidence gathering in this case Knowing them, how do they help you?].              (10 Marks)**

**Ans:**

1. Form the remediation team. Remediation teams are formed only when an incident is declared and incident ownership is assigned. The remediation team is similarly structured, with representatives from legal, IT (both infrastructure and helpdesk), security, and business line managers.

2. Determine the timing of the remediation actions. Business leaders, in coordination with the legal, remediation, and investigation teams, must decide what actions begin immediately and what is delayed until the investigation is over. This step is started by meeting with the investigation team to learn about the attacker activity to date. Conduct a meeting with business stakeholders and key executives. The business stakeholders and key executives can understand that this would disrupt business operations, but containment was critical to stop the continued loss of cardholder data. This approach is an example of a combined action remediation; the remediation team will implement immediate containment actions in the restricted financial environment, but delay action to the rest of the environment.

3. Develop and implement remediation posturing actions. Posturing actions are implemented while the incident is ongoing and often include enhancements to system and network monitoring, mitigating critical vulnerabilities, and preparing support teams for enterprise-wide changes, such as password resets or twofactor deployments. Most posturing actions are nearly indiscernible from normal maintenance by an attacker. With the containment plan in place, the remediation team concentrated on developing posturing actions, which are actions that enhance the security of the environment while the investigation is ongoing. First, enhancing visibility is one of the objectives of posturing actions, which assists both the current investigation and future detection efforts. Second, the investigation team has not yet fully scoped the compromise, so the remediation team has time to focus on these activities before concentrating on the eradication event.

4. Develop and implement incident containment actions. Containment actions are designed to deny the attacker access to specific environments or sensitive data during an investigation. Containment actions are often disruptive short-term solutions that are implemented in a very short amount of time.

5. Develop the eradication action plan. The goal of the eradication plan is to remove the attacker’s access to the environment and to mitigate the vulnerabilities the attacker used to gain and maintain access. These actions are clearly documented, and the team should spend time rehearsing them in a way that does not disrupt the investigation. This step of the remediation process is typically executed at or near the conclusion of the investigation, once the attacker’s tools, tactics, and procedures are well understood.

6. Determine eradication event timing and implement the eradication plan. There is a point in the investigation where a “steady state” is reached. At this point, while additional system compromises may be discovered, after analysis, no new tools or techniques are discovered. It is important to understand that the eradication event must be well planned and executed at the right time in order to be successful. When the investigative team has a good grasp of the tools, techniques, and processes being used, the eradication step is executed. This step also includes the post-monitoring and verification of eradication activities.

7. Develop strategic recommendations. Throughout the investigation and remediation process, you should document areas for improvement. These notes are the basis for strategic recommendations, which will help improve the security of your environment. Strategic recommendations often consist of remedial actions that cannot be implemented prior to, or during, the investigation. Quite often, strategic recommendations align directly with welldocumented information security best practices. Furthermore, strategic recommendations typically require significant cross-functional working groups to implement. These activities may disrupt business and are often expensive to implement. Strategic actions typically occur months to years following an eradication event.

8. Document the lessons learned from the investigation. Documentation that is generated as a result of an investigation should be stored in a central location. This location should be restricted to incident responders only, given the potential sensitivity of the documentation. This information will be invaluable to help your organization improve over time. Examples of the expected documentation are reports developed and notes about the environment

The remediation effort should be concise and effective. If your remediation team attempts to enact significant changes in a tactical situation, there is a real risk that the result will be rushed and incomplete. The seven most common factors critical to the remediation effort are as follows:

• Incident severity The incident severity will dictate the type of remediation implemented. The severity of an incident is something each organization needs to decide for itself. The type of incident can also change the severity. Remediation of a breached external web server that only contains public information is much less severe than remediation of an incident where an attacker obtained domain administrator credentials An organization with a mature incident response process will have documented various incident severity levels so an incident responders can determine the proper severity and approach quickly.

• Remediation timing Stakeholders should agree on the tentative timing of the remediation actions at the beginning of the planning process. Some efforts are designed to immediately remove the attacker’s access to sensitive systems or data, whereas others are designed to allow the investigative team time to gather enough information to comprehensively remove the attacker from the environment while simultaneously strengthening defenses.

• The remediation team There are three primary concerns with incident remediation teams—the size of the team, the skill level, and management support. The size of the team may affect the team’s ability to coordinate and ensure proper execution of simultaneous actions. The team’s skill level will dictate how thorough the remediation effort can be. An experienced remediation team will be more comfortable taking customized approaches, whereas a less skilled team may want to keep the remediation effort within their comfort zone.

• Technology: The type of technology in place will affect how you implement remediation actions. This includes security technology as well as enterprise management technology. For example, your organization may have software to assist with changing local administrator account passwords throughout an enterprise. An organization that does not have this software may have to develop a script to change the local administrator account password on every system.

• Budget An organization with a large IT and security budget can purchase and implement best-of-breed technology, whereas an organization without a large budget may have to implement less expensive compensating controls.

• Management support Most comprehensive remediation efforts require an organization to implement changes that affect day-to-day operations. For example, implementing a unique local administrator or root account password on all systems may require system administrators to change how they interact with systems. Securing management support will help ensure that even the most painful remediation actions are implemented and supported throughout the organization.

• Public scrutiny Your legal or PR team may be required to disclose information about an incident due to regulatory requirements. In some cases, information is made public due to an information leak or third-party discovery. In other cases, the attacker may try to extort the victim company by threatening to make the compromise or stolen information public.

Question 6: **What are the major challenges in the cyber-forensics investigation that are different from the civil or criminal cases. What are the similarities in cyber-forensics investigation with civil and/or criminal investigation? Discuss at least 2 similarities and 2 differences.  Knowing them how do they help you.  (8 Marks)**

**Ans:** Digital forensics has been defined as the use of scientifically derived and proven methods towards identification, collection, preservation, validation, analysis, interpretation and presentation of digital evidence from digital sources to facilitate the reconstruction of events found to be criminal.

Following are the major challenges in the cyber forensics investigation that are different from the general civil and criminal investigations:

1. Technical Challenges:

- Forensic techniques such as encryption, data hiding in storage space and covert channels.

- Data center operations

- Cloud deployments and operations

- Time to archive data

- Skills gap between employees, management and invetigators.

- Steganography

2. Legal Challenges:

- Privacy issues in examining data

- Absence of guidelines and standards for cyber investigations

- Limitation of laws in various countries pertaining to loopholes

- Analyzing a running computer deemed illegal in many countries

- Preservation of electronic evidence

- Not enough legal validity to digital evidence

3. Resource Challenges

- Volume of data obtained can be very large and difficult to store/transfer

- Change in technology versions and tools all the time makes it difficult for forensics to match data patterns.

Similarities/Differences between Cyber-forensic investigations with civil/criminal investigations:

In a civil case, there tends to be a lot of negotiation over what computers and what data can be inspected, as well as where and when. There is not likely to be any seizing of computers, and quite a long time may take place between the time the request to inspect a computer is made and the time the computer is made available to be inspected. It is common for one party to have access to a very limited area of data from the other party’s computer. During this time, a defendant may take the opportunity to attempt to hide or destroy data.

When law enforcement has a case involving computer forensics, the intention is to locate enough data to find the defendant guilty in court, where the standard for information presented tends to be fairly high. From the time digital data or hardware is seized and acquired, Rules of Evidence must be kept in mind. Law enforcement personnel must follow accepted procedures or evidence could be thrown out. Acquisition of data and discovery in criminal cases often must follow sometimes strict and differing procedures depending upon whether the jurisdiction is federal, state, or municipality and at times depending upon a judge’s preferences.

In a civil case, the initial processes of electronic discovery may be just to find enough data to show one or the other party whether they are likely to prevail, should the case go all the way to court. As such, the initial presentation of data may be fairly informal, and be just enough to induce the parties to settle the case. On the other hand, the data found may be so minimal the line of inquiry into electronic evidence is dropped.