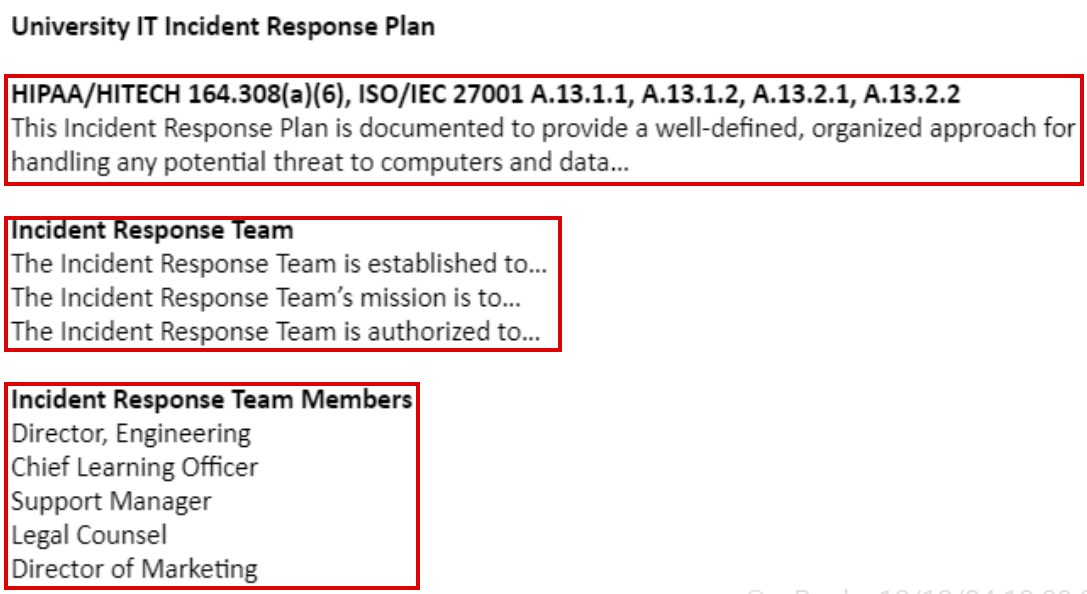
13.1 IR development

Preparation and identification

Incident response (IR) preparation begins with the formation of a cross-functional team responsible for developing an incident response plan known as the ***IR team***. An organization's IR team will often utilize existing plans, policies, and procedures during IR preparation. Ex: An IRP conducts stakeholder management using the organization's communication plan and conducts DLP using the organization's retention policy. The main output of IR preparation is an incident response plan. An ***incident response plan (IRP)*** is a set of processes an organization follows to recognize, respond, and recover from an incident.

IR identification follows preparation. However, identification only occurs when an incident is suspected. The goal of IR identification is to confirm whether or not an incident occurred.

PARTICIPATION ACTIVITY 13.1.1: IR preparation.



Animation content:

Static figure: A sample IRP document is shown with headers for applicable regulations, the IR team information, and the IR team members.
Step 1: The IR team includes any applicable regulations in the IRP. Ex: An IRP's compliance with HIPAA and ISO/IEC requirements. A red box highlights the applicable regulations section. HIPAA/HITECH 164.308(a)(6), ISO/IEC 27001 A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2 are listed as

example regulations applicable to the IRP.
Step 2: An IR team is established during IR preparation and the IR team's mission and authorizatior are detailed in an IRP. A red box highlights the IR team information section. The sample text for the section states the Incident Response Team is established to....
The Incident Response Team's mission is to.... The Incident Response Team is authorized to....
Step 3: IR team members are listed in an IRP. An IR team should be cross-functional and include members from across an organization. A red box highlights the IR team member section. The IR team members include the director of engineering, the chief learning officer, the support manager, the legal counsel, and the director of marketing.

Animation captions:

1. The IR team includes any applicable regulations in the IRP. Ex: An IRP's compliance with HIPA and ISO/IEC requirements.
2. An IR team is established during IR preparation and the IR team's mission and authorizations are detailed in an IRP.
3. IR team members are listed in an IRP. An IR team should be cross-functional and include members from across an organization.

PARTICIPATION ACTIVITY 13.1.2: IR preparation.

1) What is the main output of IR preparation?
   - Stakeholder management
   - Communication plan
   - IRP

2) Which team is responsible for executing an organization's IRP?
   - DR team
   - IR team
   - Purple team

3) Which event type does IR preparation address?
   - A disaster
   - An incident
   - A change

4) What information does an IRP include?

- Any applicable regulations
- A password policy
- An acceptable use policy

Containment and eradication

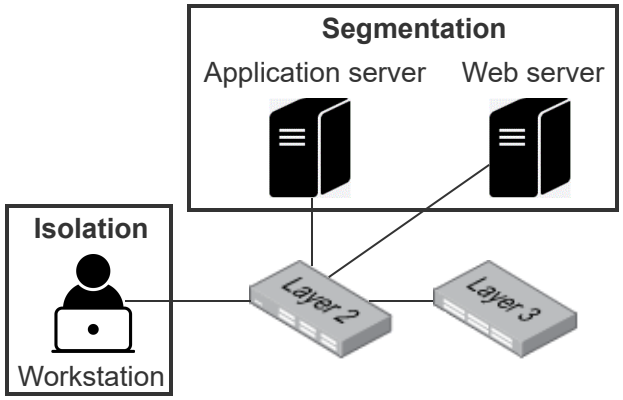
IR identification identifies an incident that must be contained and eradicated. IR containment strategies:

- ***Containment*** is an IR strategy used to prevent an incident from impacting other network resources.
- ***Isolation*** is an IR strategy used to limit an incident's impact to a single network resource.
- ***Segmentation*** is an IR strategy used to limit an incident's impact to a small group of network resources.

IR eradication follows IR containment by removing, or eradicating, an incident's impact on a network resource. Ex: Utilizing anti-malware software to remove malware from an infected computer.

Both IR containment and eradication may rely on a BCP to maintain BC if an impacted resource requires downtime. Ex: A BCP determines how to maintain network connectivity if IR eradication determines a router needs to be replaced.

PARTICIPATION ACTIVITY 13.1.3: IR containment.



Animation content:

Static figure: A basic network consisting of a workstation, two servers, a switch, and a router. A text box titled IR containment includes isolation and segmentation.
Step 1: Containment prevents an incident from impacting other network resources. Containment can be achieved through isolation or segmentation. The network appears with the IR containment text box.

Step 2: Isolation is intended for an individual network resource. An incident is contained by limiting or eliminating connections to other resources. The isolation text box moves over to the workstation and a box around the workstation indicates an isolation example.
Step 3: Segmentation is similar to isolation. However, segmentation is intended for a group of network resources. The segmentation text box moves over to the two servers and a box around the servers indicate a segmentation example.

Animation captions:

1. Containment prevents an incident from impacting other network resources. Containment can be achieved through isolation or segmentation.
2. Isolation is intended for an individual network resource. An incident is contained by limiting or eliminating connections to other resources.
3. Segmentation is similar to isolation. However, segmentation is intended for a group of network resources.

PARTICIPATION ACTIVITY 13.1.4: Containment and eradication.

1) Which IR process focuses on limiting an incident's ability to impact multiple resources?
   - ○ Preparation
   - ○ Identification
   - ○ Containment

2) Which incident containment technique is intended for an individual network resource?
   - ○ Isolation
   - ○ Segmentation
   - ○ Eradication

3) Which technique groups similar network resources together to minimize a potential incident's impact?
   - ○ Preparation
   - ○ Segmentation
   - ○ Eradication

4) Which IR process is focused on eliminating all traces of an incident?

- Eradication
- Preparation
- Identification

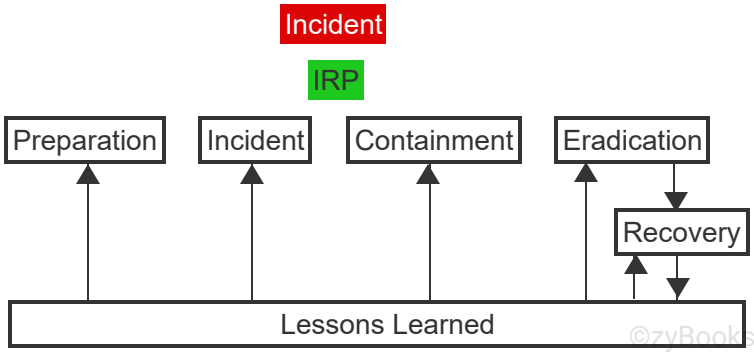
Recovery and lessons learned

The last two IR processes occur only if eradication is successful because an ineradicable incident wi continue to negatively impact a network resource. ***Incident recovery*** is a return to normal operation following an incident's eradication. An IRP's incident recovery process may reference an organizatior BCP. Ex: Incident recovery requiring a server backup uses the replication information in a BCP.

Lessons learned is the process of reviewing a recent task, incident, or event to identify an opportunit for improvement. Lessons learned is a process used in project management, incident response, and disaster recovery. Incident recovery typically produces lessons learned. Ex: A server requires more frequent backups to decrease incident recovery time.

The lessons learned process may include root cause analysis. ***Root cause analysis (RCA)*** is a systematic approach used to determine an incident's root causes. Understanding what caused an incident can lead to organizational changes designed to prevent future incidents. Ex: A breach due to stolen password leads an organization to implement two-factor authentication.

PARTICIPATION ACTIVITY 13.1.5: Recovery and lessons learned.



Animation content:

Static figure: Text boxes represent the IR processes of preparation, identification, containment, eradication, recovery, and lessons learned.
Step 1: Prior IR processes can occur simultaneously. However, recovery can only occur if eradicatic is successful. A text box representing an incident appears followed by a text box representing an

IRP. The IR processes of preparation, identification, containment, and eradication appear under IRP. An arrow points down from eradication to recovery to indicate recovery depends on the completion of eradication.
Step 2: Recovery's completion leads into lessons learned. Lessons learned is the final IR process. Lessons learned examines effective and ineffective IRP processes. An arrow points down from recovery to lessons learned to indicate lessons learned begins when all IR processes are complete. Arrows pointing up from lessons learned to each IR process to indicate how lessons learned reviews all IR processes.

Animation captions:

1. Prior IR processes can occur simultaneously. However, recovery can only occur if eradication is successful.
2. Recovery's completion leads into lessons learned. Lessons learned is the final IR process. Lessons learned examines effective and ineffective IRP processes.

PARTICIPATION ACTIVITY 13.1.6: Recovery and lessons learned.

1) Which IR process must be successful before recovery can occur?
   - Identification
   - Containment
   - Eradication

2) Which lesson learned can be derived from a phishing incident?
   - User training is required.
   - A BCP is required.
   - A security policy is required.

3) What lesson can an organization learn from a malware incident?
   - A network firewall requires updating.
   - Anti-malware signatures require updating.
   - A content filter requires updating.

4) Which lesson learned could result from a MAC spoofing incident?

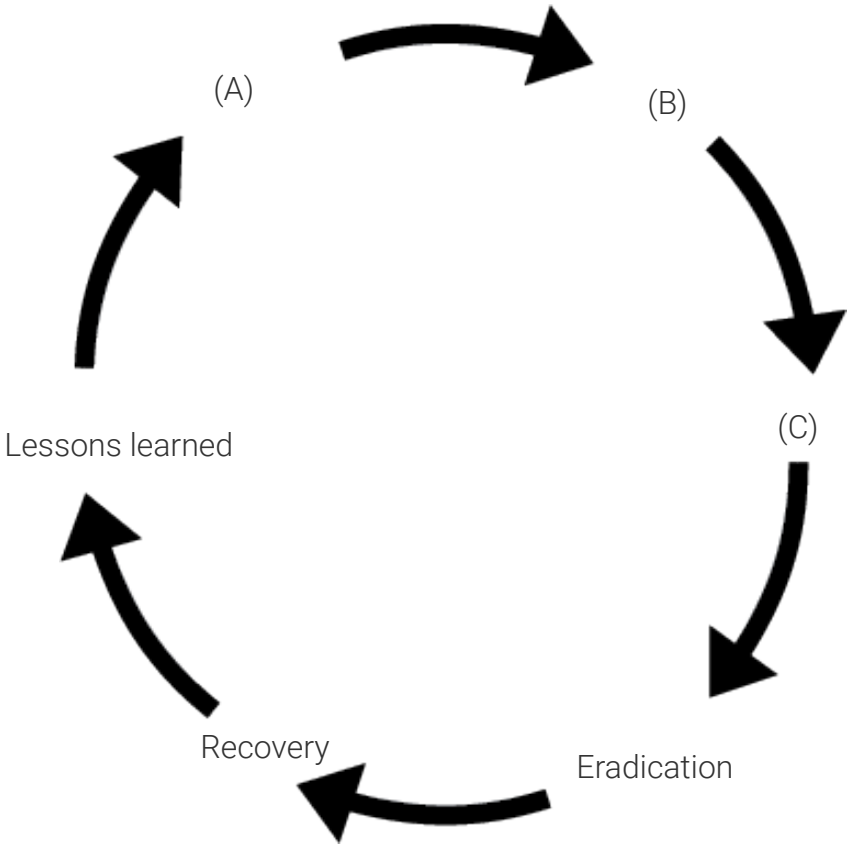
- A switch requires port security configuration.
- A router requires an SNMPv3 configuration.
- A WAP should switch from WPA2 to WPA3.

CHALLENGE ACTIVITY 13.1.1: IR development.

581480.4344582.qx3zqy7

Start

Select the missing steps in the incident response process.



(A) Pick

(B) Pick

(C) Pick

1 2 3

Check Next

13.2 IR identification resources

Software resources

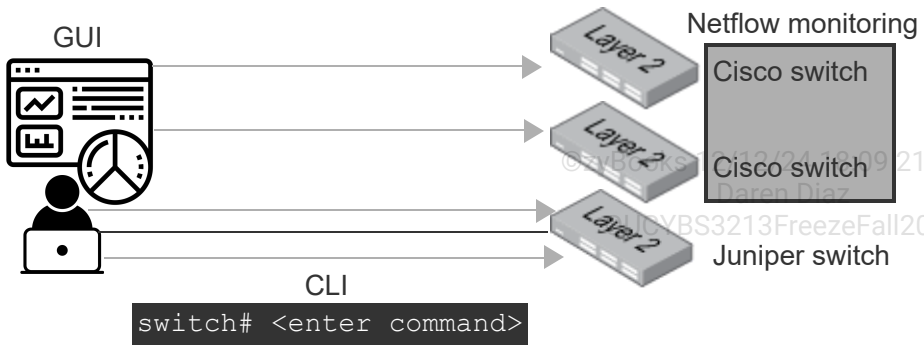
An incident can be identified by a software resource. Software is accessed using different interfaces:

- A ***command-line interface (CLI)*** is a text-based, or command-line interface used to execute commands via a keyboard.
- A ***graphical user interface (GUI)*** is a graphical interface used to interact with menus and icons via a pointing device.
- A ***network platform*** is a proprietary CLI or GUI used to execute a command or access software on a vendor-specific device.

Software resource examples:

- A ***vulnerability scan*** is completed by software to identify a device's vulnerabilities.
- A ***bandwidth monitor*** is monitoring software used to measure the amount of data a connection transfers.
- ***Netflow*** is a Cisco-proprietary protocol system that collects inbound and outbound traffic, or flow, on Cisco devices.
- ***Sampled flow (sFlow)*** randomly samples and collects a network's inbound and outbound traffic.
- ***IP flow information export (IPFIX)*** is an industry standard for collecting and visualizing IP flow.
- A ***protocol analyzer*** is monitoring software used to intercept and classify network traffic by protocol.

PARTICIPATION ACTIVITY 13.2.1: IR identification software.



Animation content:

Static figure: An administrator's workstation uses software resources to connect to different switches for incident identification. The software resources include a GUI tool, a CLI tool, and Netflow.
Step 1: IR identification software resources are available via a CLI or a GUI. Many software resources are non-proprietary. A GUI tool and a CLI tool establish a connection to a switch from the administrator's workstation.
Step 2: A software resource is typically installed on an administrator';s workstation and connects to multiple devices to streamline incident identification. The GUI and CLI tools on the administrator's workstation establish connections to three switches for incident identification.
Step 3: Netflow is a proprietary network platform and protocol system for Cisco devices. Netflow collects useful incident identification information. Two of the three switches are Cisco switches and are able to use Netflow. The third switch is a Juniper switch and cannot use Netflow.

Animation captions:

1. IR identification software resources are available via a CLI or a GUI. Many software resources are non-proprietary.
2. A software resource is typically installed on an administrator's workstation and connects to multiple devices to streamline incident identification.
3. Netflow is a proprietary network platform and protocol system for Cisco devices. Netflow collects useful incident identification information.

PARTICIPATION ACTIVITY 13.2.2: Software resources.

Select the IR identification resource described.

1) A data aggregating threat detection solution.
   - SIEM dashboard
   - Bandwidth monitor
   - Protocol analyzer

2) Cisco-proprietary monitoring software for networking devices.
   - sFlow
   - IPFIX
   - Netflow

3) Software to identify unusual amounts of network traffic.
   - Vulnerability scan

- Bandwidth monitor
- Protocol analyzer

4) Export IP flow for incident identification.

- IPFIX
- sFlow
- Netflow

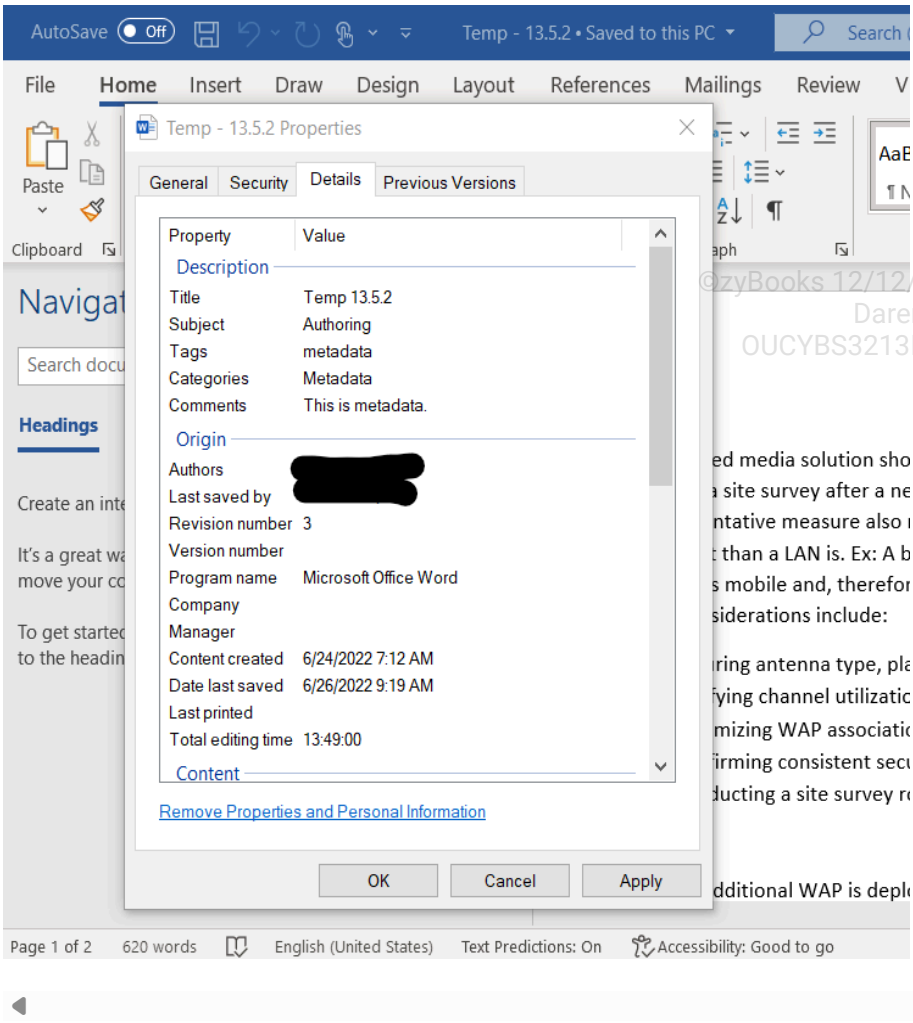
Metadata

Data is information stored in various forms. Ex: Data is stored in a file, on the internet, or on a mobile device. Data describing or identifying other data is known as ***metadata***. Metadata examples:

- A file's creation date and time, or timestamp.
- A sending email server's information.
- A hosting web server's information.
- A GPS coordinate for a picture taken with a mobile device.

Metadata is used for incident identification. Ex: An unauthorized file modification is identified by reviewing the file's metadata for a modification timestamp.

Figure 13.2.1: A Microsoft Word document's metadata.



PARTICIPATION ACTIVITY 13.2.3: Metadata.

Identify the metadata type used in IR identification.

1) A security professional determines a phishing incident's source by identifying the sending mail server.
   - ○ Email
   - ○ Mobile
   - ○ Web

2) An organization's IT department uncovers an attacker's physical location by reviewing a digital photograph's GPS coordinates.
   - ○ File

- Web
- Mobile

3) An attacker's IP address is discovered after an IR team member reviews an organization's web server events.
   - Web
   - Mobile
   - Email

4) A security professional discovers a file's author during IR identification.
   - Email
   - File
   - Web

Basic logs

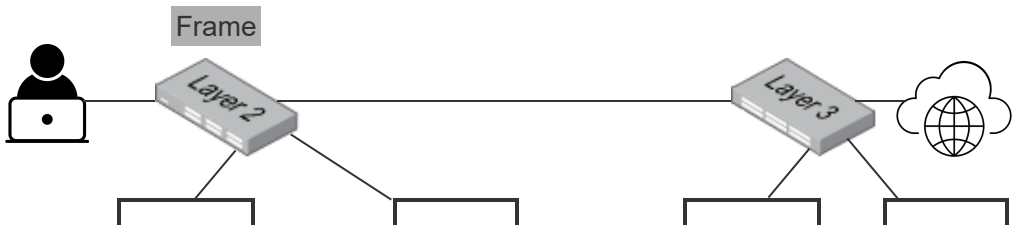
A device records, or logs, most activities in a device log. A device log is a text-based file containing various device events. A device log can identify when and how an incident occurred. Device logs remain on a local device by default. Two primary device log types exist:

- A ***traffic log*** is a device's recording of incoming and outgoing network traffic events.
- An ***audit log*** is a device's recording of system-related events such as failed and successful user login attempts.

Device log examples:

- A network device log for a switch or router's traffic-related events.
- A system device log for a server's application or security-related events.
- A web log containing client requests for a website.
- A DNS log recording DNS resolution requests and responses.

PARTICIPATION ACTIVITY 13.2.4: Networking device logs.



Animation content:

Static figure: A workstation is connected to a switch and a router. The router has a connection to the Internet. Text boxes representing traffic logs and audit logs appear beneath both networking devices. An incoming traffic log entry is shown as a traffic log example. A MAC address lookup log entry is shown as an audit log example.
Step 1: A networking device activity is recorded in a device log. Many networking devices have a traffic log and an audit log. A packet originates from the Internet and is recorded in the router's traffic log.
Step 2: A traffic log records all incoming and outgoing network traffic. Each networking device records a network traffic event. The packet is transmitted from the router to the switch and becomes a frame. The switch records the incoming frame as a traffic log entry.
Step 3: An audit log records system-related events. The switch needs to perform a MAC address table lookup to find the port for the destination MAC address in the frame. The switch performs a MAC address lookup based on the information contained in the frame. The MAC address lookup is recorded in the switch's audit log.

Animation captions:

1. A networking device activity is recorded in a device log. Many networking devices have a traffic log and an audit log.
2. A traffic log records all incoming and outgoing network traffic. Each networking device records a network traffic event.
3. An audit log records system-related events. The switch needs to perform a MAC address table lookup to find the port for the frame's destination MAC address.

PARTICIPATION ACTIVITY 13.2.5: Networking device logs.

Select the device log where each event is recorded.

1) A router receives an incoming packet.
   - ○ Traffic log
   - ○ Audit log

2) A router consults the routing table for an outgoing packet transmission.
   - ○ Traffic log

- Audit log

3) A switch forwards a frame to another switch after reviewing the MAC address table.
   - Traffic log
   - Audit log

4) A switch reviews the MAC address table before forwarding a frame to another switch.
   - Traffic log
   - Audit log

System logging protocol

System logging protocol, or ***syslog***, is a network protocol enabling a device or application to send log entries to a syslog server. A ***syslog server*** is a node configured to receive logs from syslog-configured devices and applications.

Syslog classifies log entries by descending severity levels. Eight syslog severity levels exist:

- ***Emergency***, or ***level 0***, is a syslog severity level indicating a system is unusable.
- ***Alert***, or ***level 1***, is a syslog severity level indicating an emergency event is likely to occur.
- ***Critical***, or ***level 2***, is a syslog severity level indicating an alert event is likely to occur.
- ***Error***, or ***level 3***, is a syslog severity level indicating a non-critical event occurred.
- ***Warning***, or ***level 4***, is a syslog severity level indicating an error event is likely to occur.
- ***Notification***, or ***level 5***, is a syslog severity level indicating a normal event requiring further attention occurred.
- ***Informational***, or ***level 6***, is a syslog severity level indicating a normal event not requiring further attention occurred.
- ***Debug***, or ***level 7***, is a syslog severity level recording a background event that is normally hidden.

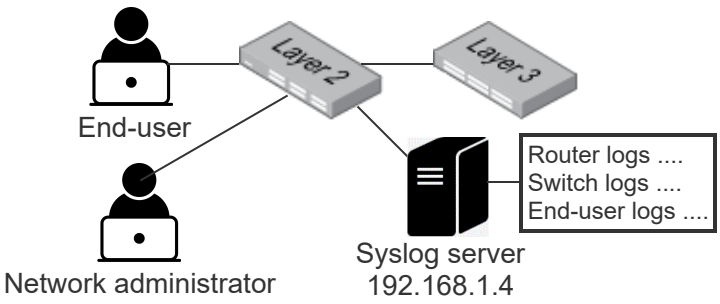
Table 13.2.1: Syslog severity levels with examples.

Level	Severity	Example
0	Emergency	Loss of primary ISP connectivity
1	Alert	Loss of backup ISP connectivity
2	Critical	Port failure

3	Error	Network interface down
4	Warning	Hard drive less than 1% of available storage
5	Notification	Software license expiring in 30 days
6	Informational	Word processing application opened
7	Debug	FTP download progress

PARTICIPATION ACTIVITY 13.2.6: Syslog.

```
#syslog configuration
0 = emergency
1 = alert
2 = critical
3 = error
4 = warning
5 = notification
6 = informational
7 = debug
```



Animation content:

Device logs remain on a local device by default. Syslog is a network protocol enabling a device or application to send log entries to a syslog server. A syslog server is a node configured to receive logs from syslog-configured devices and applications. Syslog classifies log entries by descending severity levels.

Animation captions:

1. Device logs remain on a local device by default. A syslog server is added to a network to centralize log collection.
2. A device requires a syslog server's IP address and severity level. Ex: Configuring severity level 3 sends levels 0 through 3 to a syslog server.
3. A common syslog configuration is severity level 4. Severity level 4 sends all warning, error, critical, alert, and emergency log entries to a syslog server.

PARTICIPATION ACTIVITY | 13.2.7: Syslog severity levels.

Select the syslog severity level required to capture the log entry described.

1) The download progress of a FTP download.
   - Level 5
   - Level 6
   - Level 7

2) An application opening normally.
   - Level 4
   - Level 5
   - Level 6

3) A storage device with less than 1% of available storage space.
   - Level 2
   - Level 3
   - Level 4

4) Loss of ISP connectivity.
   - Emergency
   - Alert
   - Debug

Advanced logs

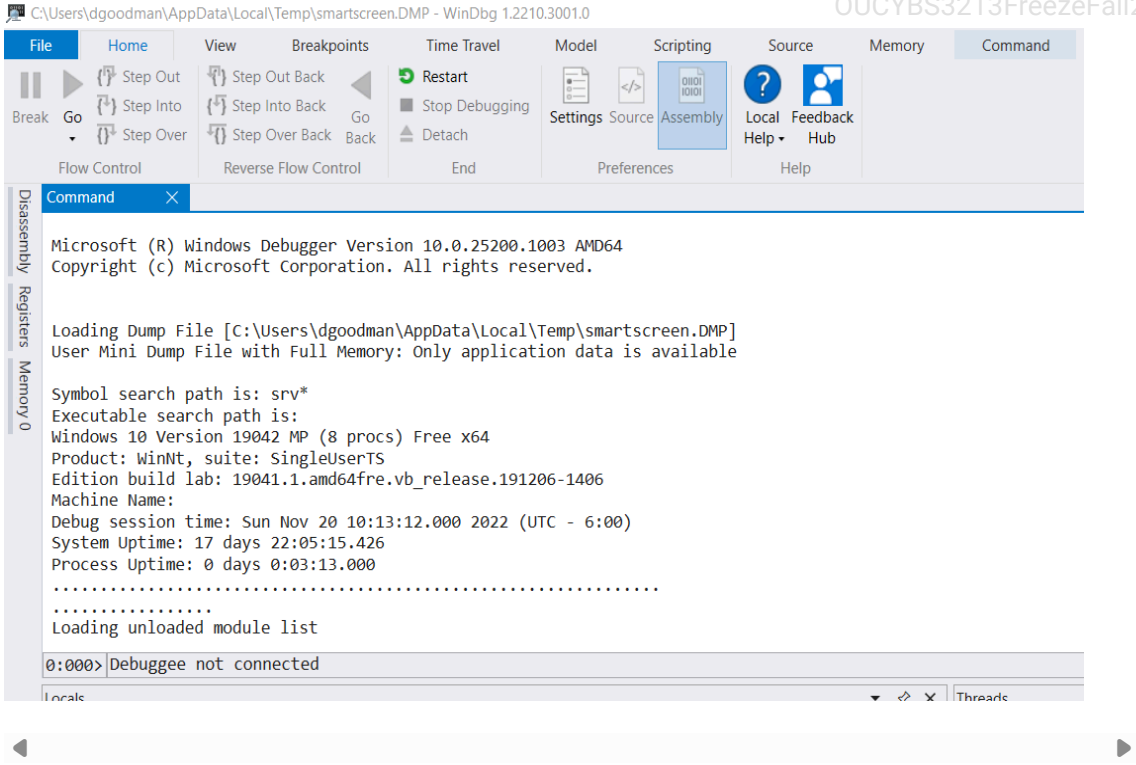
A basic log entry consists of a timestamp and a brief event description. An advanced log entry contains more event details that aid incident identification. Ex: An advanced log entry for a voice over IP (VoIP) application contains the authenticated user, protocol used, and session information. Syslog uses a service process running in the background, or ***daemon***, for advanced log collection. Syslog daemons:

- ***Syslogd*** is a legacy syslog daemon used on older Linux distributions.
- ***Syslog next generation (syslog-ng)*** is a syslog daemon providing advanced features and capabilities.
- ***Rsyslog*** is a syslog daemon used on most modern Linux distributions.

An advanced log focuses more on an OS or application than a basic log does. Advanced log examples:

- A ***journalctl log*** is the querying service for Linux's system manager known as systemd.
- A ***dump file*** is a point-in-time system or application status quickly captured in a text file.
- A ***session initiation protocol (SIP) log*** is a log containing events for voice, video, and messaging sessions.

Figure 13.2.2: Windows debugger.



PARTICIPATION ACTIVITY 13.2.8: Advanced logs.

1) Which daemon does syslog use on the most recent Linux distributions?
   - Journalctl
   - Syslogd
   - Rsyslog

2) Which utility logs systemd events?
   - Syslog
   - Journalctl
   - Rsyslog

3) Which log type quickly records a system's state?

- Metadata
- Traffic log
- Dump file

4) VoIP events are recorded in which log type?

- Journalctl
- SIP log
- Audit log

13.3 IR containment and eradication techniques

Reconfigure endpoint security

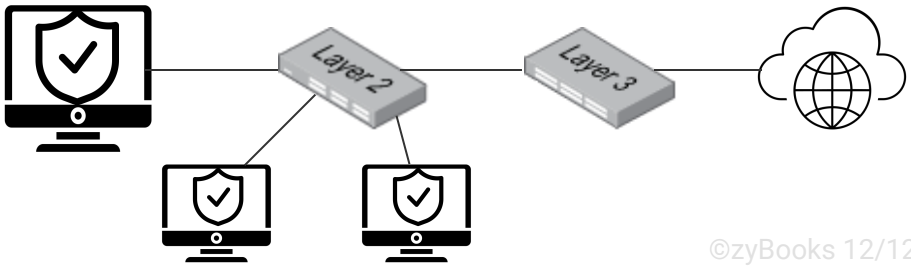
IR containment and eradication for an endpoint begins with quarantining the compromised endpoint. ***Quarantine*** is the process of isolating a compromised endpoint or data to prevent further compromise. A quarantined resource can be reintegrated into a network once the incident's source is eradicated.

A quarantined endpoint may require endpoint security reconfiguration before reintegration. Endpoint security reconfiguration examples:

- Installing all required security updates as part of patch management
- Installing all required anti-malware updates as part of malware protection
- Configuring a host-based firewall as part of host-based security
- Deploying EDR or ETDR as part of endpoint hardening
- Utilizing disk encryption as part of disk hardening

IR lessons learned may identify a compromised application as an incident's source. An ***application approved list*** is both a policy and a configuration of a list of allowed applications for an organization. An ***application deny list***, or ***application blocklist***, is both a policy and a configuration of a list of disallowed applications for an organization.

PARTICIPATION ACTIVITY 13.3.1: Reconfigure endpoint security.



Animation content:

Static figure: A basic network consisting of three personal computers connected to a switch. The switch is connected to the router. The router is connected to the internet.
Step 1: A malware-infected PC is quarantined from a network during the containment portion of IR containment and eradication. Malware originating from the internet infects one of the personal computers. The infected personal computer is quarantined by disconnecting the personal computer from the network.
Step 2: Anti-malware software removes the malware from the PC during the eradication portion of IR containment and eradication. The malware is removed from the infected personal computer by the anti-malware software.
Step 3: The endpoint security reconfigurations used on the individual PC are applied to all other endpoints to prevent any further incidents. Anti-malware software is deployed to the other two personal computers connected to the switch.
Step 4: The quarantined PC is reconnected to the network once the malware incident is resolved. The personal computer's network connection is reestablished.

Animation captions:

1. A malware-infected PC is quarantined from a network during the containment portion of IR containment and eradication.
2. Anti-malware software removes the malware from the PC during the eradication portion of IR containment and eradication.
3. The endpoint security reconfigurations used on the individual PC are applied to all other endpoints to prevent any further incidents.
4. The quarantined PC is reconnected to the network once the malware incident is resolved.

PARTICIPATION ACTIVITY 13.3.2: Reconfigure endpoint security.

1) Which endpoint security reconfiguration ensures an application's vulnerabilities are removed?

- Patch management
- Disk hardening
- Malware protection

2) IR containment and eradication uses which endpoint security reconfiguration to protect an endpoint from viruses?

- Host-based security
- Malware protection
- Disk hardening

3) Which endpoint security reconfiguration uses monitoring and analysis to detect and respond to an endpoint security incident?

- EDR
- DLP
- FDE

4) Which endpoint security reconfiguration disallows a compromised application's installation?

- Regular software audits
- Application denied list
- Host-based firewall

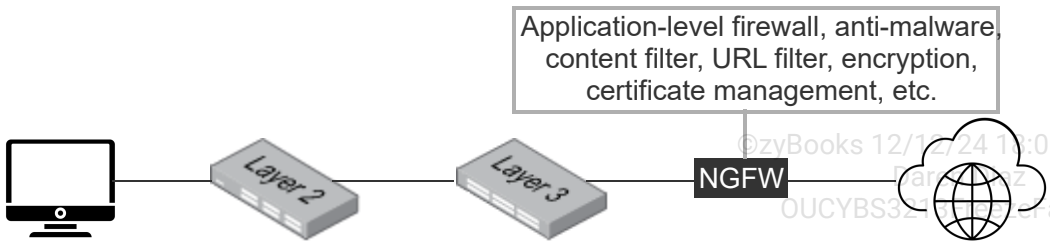
Configuration changes

A networking device configuration change focuses on stopping future incidents at the network level. Ex: Blocking a malicious IP address with a network firewall rule. Post-incident configuration changes include:

- Updating firewall rules
- Converting existing firewalls to NGFWs
- Enhancing DLP techniques
- Updating content or URL filters
- Updating current certificates and revoking other certificates

An incident involving a mobile device may justify the need for a mobile device management solution. ***Mobile device management (MDM)*** is hardware and software resources used to centralize the configuration, monitoring, and management of mobile devices.

PARTICIPATION ACTIVITY 13.3.3: Configuration changes.



Animation content:

Static figure: A basic network consisting of a personal computer connected to a switch. The switch is connected to the router. The router is connected to a firewall. The firewall is connected to the internet.
Step 1: A post-incident configuration change may result in replacing a traditional firewall with an NGFW. A red box appears around the traditional firewall to indicate the device targeted for a post-incident configuration change.
Step 2: A traditional firewall relies on simple rules to allow or block traffic using static traffic characteristics such as IP address, port number, or protocol. A text box appears above the traditional firewall to represent the firewall's rule configuration. The rules are examples of blocking an IP address, allowing a port number, and blocking a protocol.
Step 3: An NGFW can streamline other post-incident configuration changes such as enhancing DLP techniques, deploying a content filter, and improving certificate management. The traditional firewall fades away and is replaced by an NGFW. A text box appears above the NGFW to represent the NGFW's capabilities. The NGFW is an application-level firewall with anti-malware, content filtering, URL filtering, encryption, certificate management, and other capabilities.

Animation captions:

1. A post-incident configuration change may result in replacing a traditional firewall with an NGFW.
2. A traditional firewall relies on simple rules to allow or block traffic using static traffic characteristics such as IP address, port number, or protocol.
3. An NGFW can streamline other post-incident configuration changes such as enhancing DLP techniques, deploying a content filter, and improving certificate management.

PARTICIPATION ACTIVITY 13.3.4: Configuration changes.

1) Which post-incident configuration change results in blocking a malicious

IP address?

- Updating firewall rules
- Updating URL filters
- Utilizing certificate management

2) Which IR configuration change results in deploying an application layer firewall?

- Updating firewall rules
- Updating content filters
- Converting existing firewalls to NGFWs

3) Which post-incident configuration change prevents users from accessing malicious websites by domain name?

- Updating URL filters
- Updating content filters
- Enhancing DLP techniques

4) Which IR configuration change provides monitoring capabilities for an organization's mobile devices?

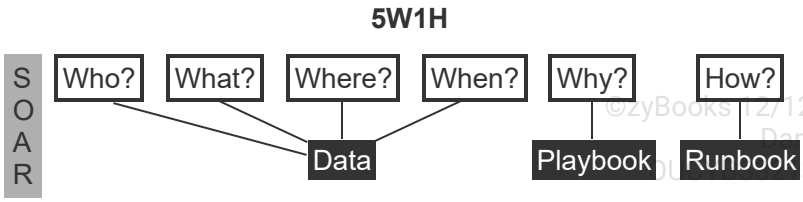
- UEM
- MDM
- MITM

Security orchestration, automation and response

Who, what, when, where, and why (5W) is an information gathering approach used in various scenarios. A "how" is added to the five W's (5W1H) to create a problem solving approach. An organization's security efforts should follow an information gathering and problem solving approach similar to 5W1H. ***Security orchestration, automation and response (SOAR)*** technology helps coordinate, execute and automate tasks in a single platform between people and tools. SOAR concepts are also applicable to IR. SOAR components:

- Security is an organization's commitment to secure data and operations.
- Orchestration is the coordination of all security efforts to achieve the same security goal.
- Automation is the use of automatic or automated processes to streamline security efforts.
- Response is the IR component of SOAR ensuring all incidents are responded to.

PARTICIPATION ACTIVITY | 13.3.5: SOAR.



Who, what, when, where, why, and how (5W1H) is an information gathering and problem solving approach. SOAR is comparable to 5W1H for security.

Animation content:

Static figure: Who, what, when, where, why, and how (5W1H) is an information gathering and problem solving approach. SOAR is comparable to 5W1H for security. Text boxes representing SOAR and 5W1H show the relationship between ingested data, a playbook, and a runbook.
Step 1: SOAR ingests security-related data for information gathering purposes. Ingested data provides "who, what, when, and where" information. The data text box moves under 5W1H and connections between the ingested data text box and the who, what, when, and where text boxes appear.
Step 2: A SOAR playbook contains security-related goals and objectives. A SOAR playbook provides "why" information. A text box representing a SOAR playbook appears and is connected to the why text box.
Step 3: A SOAR runbook includes step-by-step instructions for achieving a security-related goal. A SOAR runbook provides a "how" problem solving solution. A text box representing a SOAR runbook appears and is connected to the how text box.

Animation captions:

1. SOAR ingests security-related data for information gathering purposes. Ingested data provides "who, what, when, and where" information.
2. A SOAR playbook contains security-related goals and objectives. A SOAR playbook provides "why" information.
3. A SOAR runbook includes step-by-step instructions for achieving a security-related goal. A SOAR runbook provides a "how" problem solving solution.

PARTICIPATION ACTIVITY | 13.3.6: SOAR.

1) Which SOAR component contributes to threat and vulnerability management?

- Security
- Orchestration
- Automation

2) Which SOAR component contributes to security operations by eliminating dependence on manual responses?
   - Security
   - Orchestration
   - Automation

3) Which SOAR component is based on an organization's security goals?
   - Playbook
   - Runbook
   - CSC

4) Which SOAR component determines how an organization can achieve a security-related goal?
   - Playbook
   - Runbook
   - CSF

13.4 IR attack frameworks and exercises

Attack frameworks

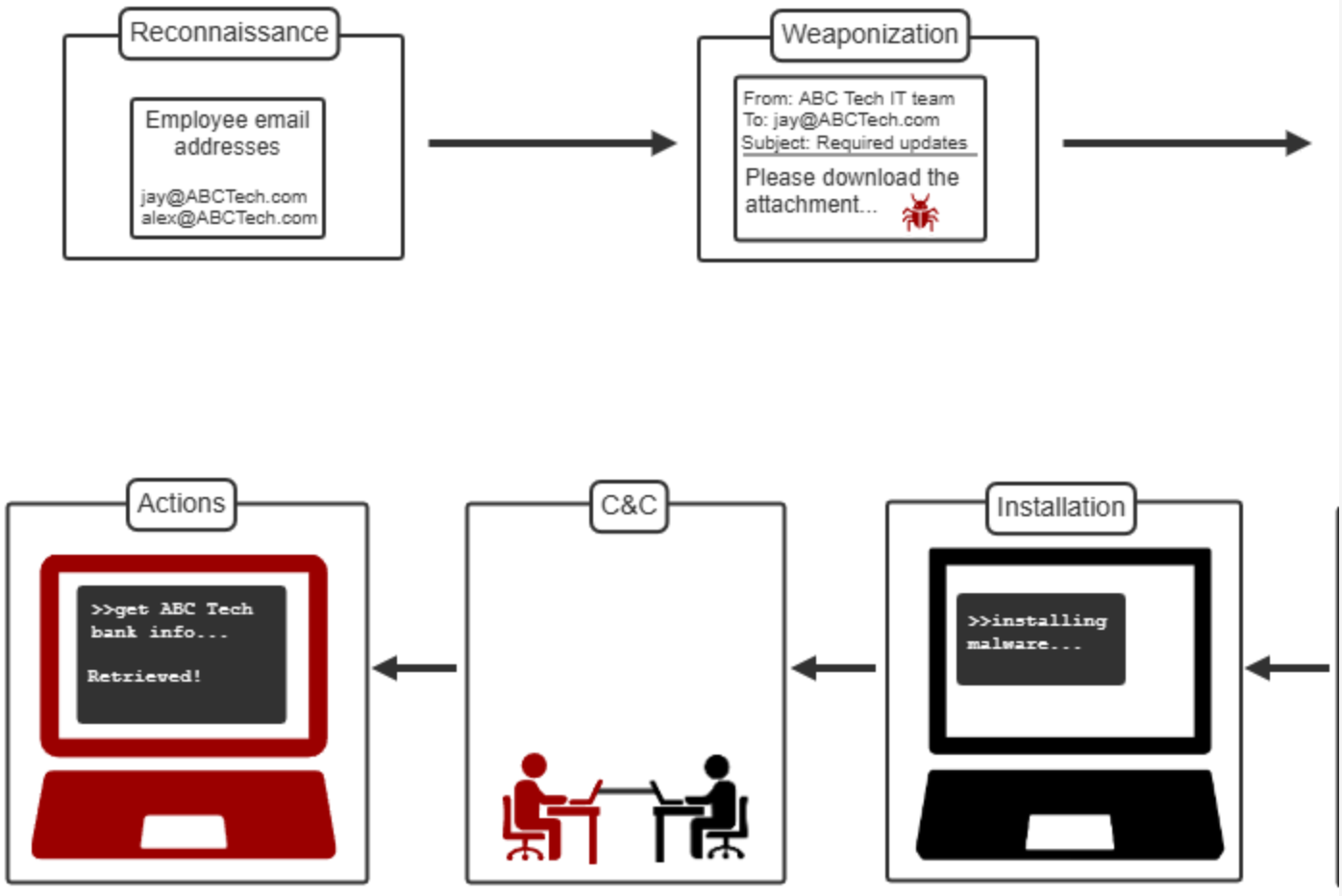
An attack framework is similar to a security framework in how an attack framework includes third-party developed guidelines, best practices, and/or policies for other organizations to use. An attack framework differs from a security framework in how an attack framework focuses on a specific attack type. Ex: An attack framework for an intrusion attack.

MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) is the MITRE corporation's attack framework that includes a database of attacks an organization can use for IR exercises. An organization uses MITRE ATT&CK to evaluate the effectiveness of the organization's IRP.

The ***Diamond Model of Intrusion Analysis*** is an attack framework focused on understanding the relationships among an incident's core components. The Diamond Model of Intrusion Analysis helps organizations understand how an adversary's traits, capabilities, and infrastructure target specific victims.

The ***Cyber Kill Chain*** is an attack framework focused on understanding the steps an attacker must take to be successful. Cyber Kill Chain's goal is to stop an attacker's progress as early as possible.

PARTICIPATION ACTIVITY 13.4.1: Cyber Kill Chain.



Animation captions:

1. During reconnaissance, an attacker searches for useful information about the target organization, such as a list of employee email addresses.
2. During weaponization, the attacker uses the information to craft a believable phishing email. The email is delivered to a target.

3. Exploitation happens when the employee opens the attachment and the malicious code executes.
4. During installation, the target's machine is installed with malware. Command and control (C&C) is established when the attacker creates a persistent channel that allows the attacker to control the target's machine.
5. The attacker can then carry out the actions on objectives, such as obtaining banking information.

PARTICIPATION ACTIVITY 13.4.2: Attack frameworks.

1) Which attack framework consists of several specific attacks an organization can use for an IR exercise?
   - Cyber Kill Chain
   - MITRE ATT&CK
   - The Diamond Model of Intrusion Analysis

2) Which MITRE ATT&CK attack prepares an organization for an attacker's attempt to gain account capabilities beyond those assigned to an account?
   - Privilege escalation
   - DoS
   - DNS poisoning

3) Which link in the Cyber Kill Chain helps an organization understand an attacker's information gathering techniques?
   - Reconnaissance
   - Infrastructure
   - Capability

4) Which Diamond Model of Intrusion Analysis components have a dependency?
   - Capability and victim
   - Adversary and victim

- Capability and infrastructure

IR exercises

Evaluating an organization's IR and IRP effectiveness is accomplished by using an attack framework with an IR exercise. An ***IR exercise*** is the use of an attack framework and an organization's IRP to evaluate an organization's IR efforts. IR exercises:

- A ***tabletop exercise*** is an IR exercise type where the IR team talks through each IRP step.
- A ***walkthrough exercise*** is an IR exercise type where the IR team walks through each IRP step without taking action.
- A ***simulation exercise*** is an IR exercise type where the IR team executes the IRP on a simulated incident.

Additionally, incident response may involve:

- ***Failover*** is the process of automatically switching to redundant systems or resources to maintain uninterrupted operation in case of a primary system failure. Failover mechanisms ensure seamless transition to backup systems in case of failure, which could be tested and evaluated during simulation exercises.
- ***Parallel processing*** involves simultaneously using multiple computing resources to perform tasks. Parallel processing increases efficiency and speeds up execution times, which is valuable in scenarios simulated during tabletop or walkthrough exercises.

PARTICIPATION ACTIVITY 13.4.3: IR exercises.

Animation content:

Static figure: A tabletop, walkthrough, and simulation exercise are represented by text boxes. Text boxes also represent an IR team, IRP, and attack framework. Each IR exercise type includes different procedures and requires different IR resources.

Step 1: A tabletop exercise requires the IR team to sit around a table and talk through each IR step in an IRP. The IR team and IRP text boxes move to the tabletop box. A text box within the tabletop box appears to state a tabletop exercise involves an IRP readthrough and talkthrough.
Step 2: A walkthrough exercise is more thorough than a tabletop exercise because the IR team acts out, or walks through, each IR step in an IRP. The IR team and IRP text boxes move to the walkthrough box. A text box within the walkthrough box appears to state a walkthrough exercise involves acting out IRP processes.
Step 3: A simulation exercise is the most thorough IR exercise because an attack framework scenario is presented to the IR team for IRP execution. The IR team and IRP text boxes move to the simulation box. The attack framework text box also moves to the simulation box. A text box within the simulation box appears to state a simulation exercise involves executing an IRP.

Animation captions:

1. A tabletop exercise requires the IR team to sit around a table and talk through each IR step in an IRP.
2. A walkthrough exercise is more thorough than a tabletop exercise because the IR team acts out, or walks through, each IR step in an IRP.
3. A simulation exercise is the most thorough IR exercise because an attack framework scenario is presented to the IR team for IRP execution.

PARTICIPATION ACTIVITY 13.4.4: IR exercises.

1) What can an organization use to determine IR effectiveness?
   - Gamification
   - IR exercise
   - Phishing campaign

2) Which IR exercise requires an IR team to only talk through processes in an organization's IRP?
   - Tabletop
   - Walkthrough
   - Simulation

3) Which IR exercise type requires an IR team to act out IRP processes?
   - Tabletop
   - Walkthrough

- Simulation

4) Which IR exercise type attempts to replicate a real-world incident response scenario?

- Tabletop
- Walkthrough
- Simulation

5) How does parallel processing differ from failover mechanisms in the context of incident response exercises?

- Failover mechanisms prioritize task execution over system redundancy
- Parallel processing focuses on redundant system configuration
- Parallel processing emphasizes task efficiency through resource utilization

CHALLENGE ACTIVITY 13.4.1: IR attack frameworks.

581480.4344582.qx3zqy7

Start

The Diamond Model of Intrusion Analysis identifies an incident's adversary, capability, infrastructure, and victim. Which of the following are classified as infrastructure? Select all that apply.

- [ ] Gray hat hacker
- [ ] PowerShell
- [ ] Online forum
- [ ] USB drive
- [ ] Online dating profile

13.5 Digital forensics

Digital forensics

Digital forensics is a branch of forensic science that focuses on collection, examination, analysis, and reporting on electronically stored and/or processed data. Digital forensics is used in tasks such as investigating digital crimes, identifying internal policy violations, recovering from system damage or data loss, and reconstructing security incidents. Ex: Digital forensics is used in the investigation of unauthorized access to a computer, or a distributed denial-of-service (DDoS) attack against a web server.

Digital forensics has several sub-branches, including computer forensics, network forensics, database forensics, and cloud forensics. Each digital forensics sub-branch focuses on investigating a specific electronic device or computing environment. Ex: Computer forensics focuses on data residing on a computer, including data in the computer's volatile memory, registers, and storage media.

Table 13.5.1: Digital forensics.

Digital forensic stages	Activities
Collection	Identifying, labeling, recording, and acquiring data from all relevant data sources.
Examination	Processing collected data using a combination of automated and manual methods, and assessing and extracting data of interest.
Analysis	Analyzing the results of the examination to derive useful information that addresses the questions that motivated the collection and examination of the data.

Reporting	Reporting the results of the analysis, including describing the actions taken and explaining how tools and procedures were selected.

PARTICIPATION ACTIVITY 13.5.1: Digital forensics.

Select the data source that is relevant to each digital forensics sub-branch

How to use this tool

IP packets **Instance memory** **Transaction logs** **USB flash drive**

	Network forensics
	Computer forensics
	Database forensics
	Cloud forensics

Reset

Digital evidence

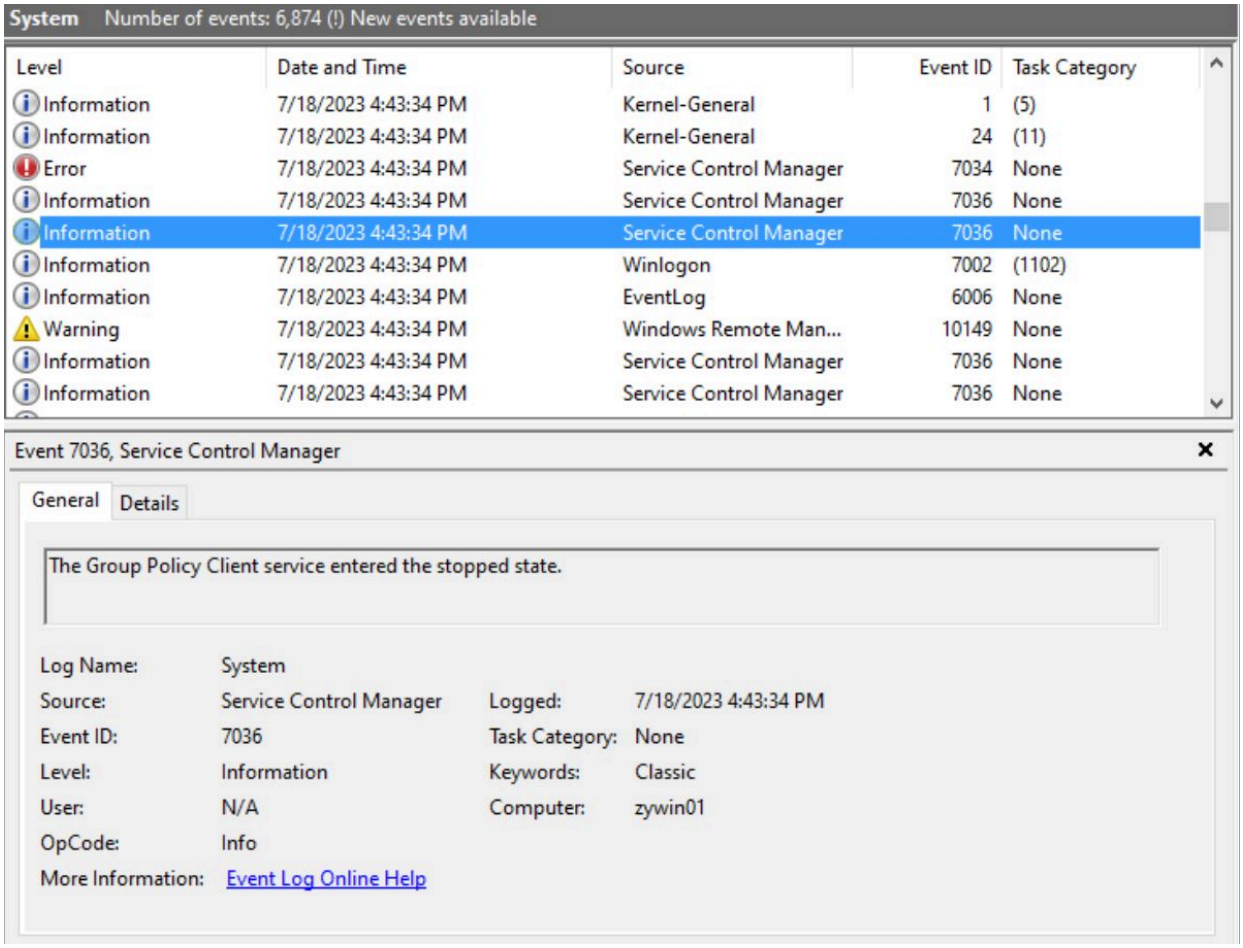
Digital evidence is electronic data of value to an investigation that is stored on, processed, received, or transmitted by an electronic device. Ex: A video file on a mobile device is digital evidence if the file contains information relevant to an intellectual property theft case. Digital evidence can be part of investigating any crime where crime-relevant data is present in digital form.

Digital evidence is presented in a digital forensic report along with timelines of events and timestamps for each digital evidence piece. A ***timestamp*** is a digital record of the date and time an event occurred. Timestamps are used to track when data was created, accessed, or modified. An operating system, application, or firmware may use different time zones when creating timestamps. A ***time offset*** is the time difference between a system's local time and Greenwich Mean Time (GMT). Ex: The Eastern Standard Time (EST) is 5 hours behind GMT. The timestamps on a system using EST have an offset of -5 hours.

Physical devices and hardware components containing digital evidence are tagged, labeled, and photographed for forensic reports. Ex: A photo of a tagged SSD. Forensic reports also include

summaries of interviews conducted with involved parties. Ex: An interview with an individual who witnessed an unauthorized person entering a company's premises.

Example 13.5.1: Event logs for system events on Windows Server. Each system event has a timestamp that may be used in a timeline of forensic events.



PARTICIPATION ACTIVITY 13.5.2: Digital evidence.

1) Data stored in a server's memory may be used as evidence in a digital forensic investigation of a network intrusion only when the data _____.

   - ○ is copied from the server's memory to a storage device

- is relevant to the network intrusion
- is deleted from the server's memory

2) The timestamp of a blocked malicious IP packet in a firewall log file using a time offset of 2 hours is 3:00 PM. The packet was blocked at _____ GMT.

- 1:00 PM
- 3:00 PM
- 5:00 PM

3) Physical devices containing digital evidence are tagged and labeled so that _____.

- new evidence can be added to the devices
- evidence is identifiable during the forensic investigation
- ensure the integrity of the digital evidence

Chain of custody and provenance

Since forensic data may be used as evidence in a criminal case, the handling of data should be documented to ensure the data's integrity. The ***chain of custody*** is the process of tracking the movement of evidence through the evidence's collection, preservation, and analysis. The chain of custody documents each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer. The chain of custody ensures the integrity of the evidence and holds the individuals involved accountable for the actions taken on the evidence. Maintaining an evidence's chain of custody is a necessary requirement for the evidence's admissibility in a court of law.

Provenance is a record describing the origin and historical information about a piece of data. Provenance includes information on the origin of the data, how data has changed, and how the data has moved over time. Ex. A file's provenance includes details about how and where the file was created and all the actions performed on the file over the file's life span. Maintaining accurate provenance ensures evidence credibility, authenticity, and integrity.

Both the chain of custody and provenance involve documenting the history of evidence. However, chain of custody is mainly concerned with the physical handling of evidence in investigative settings,

while provenance is used for establishing the complete history of data.

Example 13.5.2: A chain of custody form containing fields such as name of the receiving organization, person from whom the item was received, location and date/time the item was obtained, item number, quantity, and signature lines for all parties involved.

©zyBooks 12/12/24 18:09 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

Chain of Custody Document		Sequence Number:	
Receiving Organization:		Location:	
Name of Person From Whom Received:		Address:	
Location from Where Obtained:		Reason:	Date/Time Obtained:

Item Number	Quantity	Description

Item Number	Date	Released By:	Received By:	Reason for Change:
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	

Credit: The American Society of Digital Forensics & eDiscovery, Inc.[1]

PARTICIPATION ACTIVITY 13.5.3: Chain of custody.

1) What is the main objective of maintaining the chain of custody?

- To document all modifications to evidence after evidence collection
- To remove inadmissible evidence which is not relevant to a forensic investigation
- To ensure the integrity of digital evidence

2) Why would a piece of digital evidence not be admissible in a court of law even if the evidence's chain of custody is maintained?

- Because discrepancies may exist among the evidence's chain of custody forms maintained by different investigators
- Because the digital evidence was moved to a new location during the forensic investigation
- Because a judge may decide the evidence is not relevant to the case

3) An investigator intends to transport an SSD from a victim's computer to a digital forensic lab for examination. Which one of the following actions can make the digital evidence on the SSD inadmissible in a court of law?

- Connecting a write blocker to the SSD
- Removing the SSD from the victim's computer
- Not updating the SSD's chain of custody form

Legal holds

*Digital forensics may be used to ensure an organization's compliance with laws and regulations, as well as response to legal inquiries. Ex: Digital forensics may be conducted in response to legal holds. A **legal hold** is the practice of ensuring all forms of potentially relevant data to an anticipated litigation against an organization is identified and preserved.Typically, a legal hold takes the form of a notification sent by an organization's legal team to the organization's employees, instructing employees to not delete information relevant to a legal case.*

(*1) The American Society of Digital Forensics & eDiscovery, Inc. "Chain of Custody form". https://https://asdfed.com/.

13.6 Digital evidence acquisition

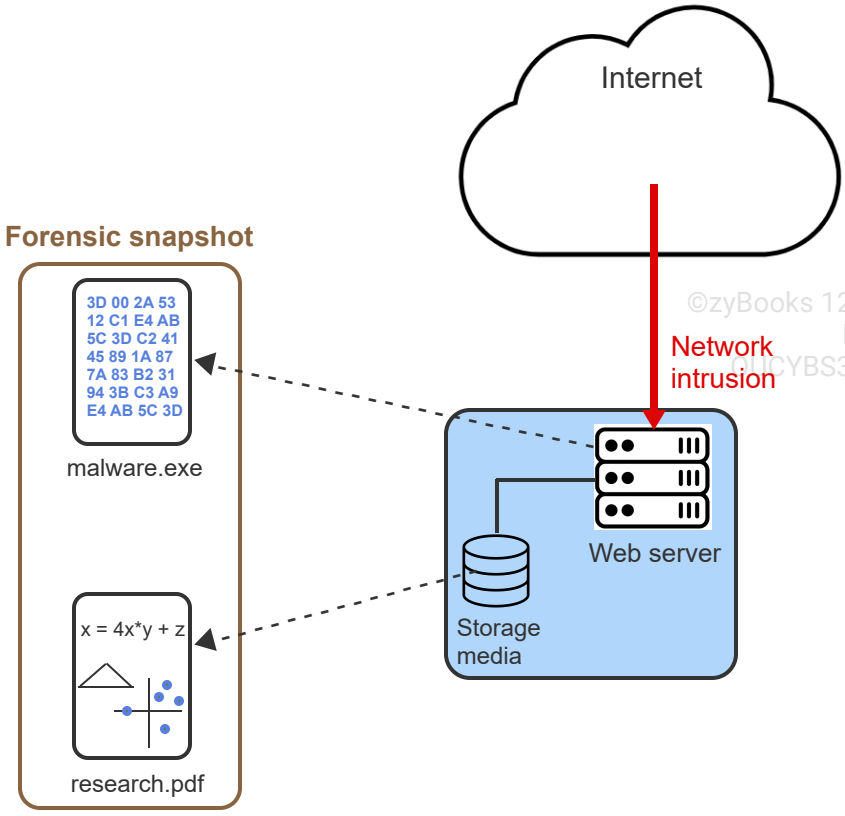
Digital evidence acquisition

Digital evidence acquisition is the process of collecting relevant data to a forensic investigation, while preserving data integrity. Ex: Acquiring data residing in a server's memory without modifying the data.

Digital evidence may reside on hardware and software components, including memory, storage media, operating system logs, and network devices. A ***forensic artifact*** is any data that may potentially be used as digital evidence. Ex: Logs, registry keys, and file timestamps. A forensic artifact is digital evidence only if the artifact is relevant to a forensic investigation. Ex: A file timestamp is a forensic artifact. However, the file timestamp is digital evidence if the timestamp helps establish the timeline of a network intrusion.

A forensic snapshot captures a system's data at a specific point in time, thus preserving the data for evidence acquisition in a forensic investigation. Ex: A forensic snapshot of a web server after a network intrusion resulting in intellectual property theft.

PARTICIPATION ACTIVITY 13.6.1: Digital evidence acquisition.



Animation content:

Static image: A cloud representing the internet on the top. A web server is connected to the internet. The web server is attached to storage media. A box titled forensic snapshot encloses two files named malware.exe and research.pdf.
Step 1: A company's web server makes company information available to authorized users, including information considered intellectual property.
Step 2: If a web server is compromised via a network intrusion, forensic artifacts may exist on the web server's hardware and software components.
Step 3: Digital evidence acquisition involves collecting all relevant data to the network intrusion and the potential loss of company's intellectual property.
Step 4: Forensic artifacts include programs running in the web server's memory (Ex: malware.exe) and files stored on the web server's storage media (Ex: research.pdf)..
Step 5: A forensic snapshot saves the web server's artifacts (Ex: malware.exe and research.pdf).

Animation captions:

1. A company's web server makes company information available to authorized users, including information considered intellectual property.
2. If a web server is compromised via a network intrusion, forensic artifacts may exist on the web server's hardware and software components.

3. Digital evidence acquisition involves collecting all relevant data to the network intrusion and the potential loss of company's intellectual property.
4. Forensic artifacts includes programs running in the web server's memory (Ex: malware.exe) and files stored on the web server's storage media (Ex: research.pdf).
5. A forensic snapshot saves the web server's artifacts (Ex: malware.exe and research.pdf).

PARTICIPATION ACTIVITY 13.6.2: Digital evidence acquisition.

1) The _____ security property should be maintained during evidence acquisition to ensure the evidence is not modified and admissible in a court of law.
   - confidentiality
   - integrity
   - availability

2) A deleted file in the Recycle Bin of a Windows system is a forensic artifact, but not forensic evidence unless the _____.
   - file's authenticity can be ensured by a forensic investigator
   - file contains information relevant to a forensic investigation
   - file was not deleted by a forensic investigator

3) The _____ forensic artifact(s) may contain a list of visited websites by a user on a Windows system.
   - event logs
   - cookies
   - Recycle Bin

©zyBooks 12/12/24 18:09 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

4) A forensic investigator may take a forensic snapshot of a computer's pagefile to find out whether malware existed on the computer's _____ .
   - network drive

- memory
- network interface card (NIC)

5) A forensic investigation of a ransomware attack may include the analysis of a computer's _____ forensic artifact to identify polymorphic malware.
   - authentication log
   - kernel cache
   - memory

Order of volatility

Data volatility is the measure of how long data is retained on an electronic component in absence of power. The ***order of volatility*** is the sequence of data acquisition in a forensic investigation based on data volatility. Data is acquired starting with the most volatile (most likely to disappear) and ending with the least volatile. Ex: Random access memory (RAM) requires power for data retention, but a hard disk drive (HDD) retains data even when no power is supplied to the device. In a forensic investigation of a laptop, data in the laptop's RAM is acquired before data on the laptop's HDD.

Volatile data often contains time-sensitive information relevant to an ongoing security incident. Ex: Active network connections, running processes, and volatile artifacts can provide immediate clues about malicious activities or unauthorized access. Following the order of volatility helps ensure critical data is captured before the data is lost, increasing the effectiveness of digital forensic investigations.

Table 13.6.1: The order of volatility according to Internet Engineering Task Force (IETF) RFC 3227.

Order of volatility	Data source
1	Registers, cache
2	Routing tables, ARP cache, process tables, kernel statistics, memory
3	Temporary file systems
4	Disks

5	Remote logging, monitoring data
6	Physical configurations, network topologies
7	Archival media

PARTICIPATION ACTIVITY 13.6.3: Order of volatility.

1) Why should the order of volatility be followed in a forensic investigation?

- To ensure non-volatile data is acquired before an electronic component's power is disrupted
- To ensure volatile data is acquired before an electronic component's power is disrupted
- To ensure evidence is admissible in court of law

2) The disk, memory, and logs of a Windows system may contain data relevant to a forensic investigation. Which of the following options identifies the correct order of volatility?

- Disk, memory, logs
- Memory, disk, logs
- Logs, disk, memory

3) Why should data in ARP cache be acquired before data on archival media?

- Because archival media does not contain any relevant data
- Because ARP cache is stored on disk
- Because ARP cache is stored in RAM

4) In a scenario where multiple computers are suspected to be involved in a network intrusion, what should be prioritized first for volatile data collection?

- Servers handling network traffic
- Offline workstations
- Workstations with active users

5) In which of the following scenarios would ignoring the order of volatility be justified in a forensic investigation?

- The least volatile data is time-sensitive
- The critical data is stored on an external device
- Encrypted data is found on a device

Strategic Intelligence/Counterintelligence

Strategic Intelligence and counterintelligence help digital forensic investigators gain insight into the latest tactics, techniques, and procedures (TTP) used by attackers. Information provided by threat intelligence sources enable investigators to focus on relevant data and limit forensic investigations to manageable levels. Strategic intelligence also helps organizations prepare for potential attacks and expedites organizations' security incident response and recovery efforts.

13.7 Digital forensic investigations

On-premises vs. cloud environments

A digital forensic investigation is guided by where data is stored and processed. In an on-premises environment, organizations have direct control over the organizations' data which enables forensic investigations without the need for a cloud provider's involvement. When digital evidence exists in the cloud, access to and analysis of cloud data is subject to agreements between an organization and a cloud provider.

Right-to-audit is a legal contract that grants one party the right to perform an audit of the records, operations, or processes of another party. Right-to-audit is often included in service level agreements (SLAs) and is intended to provide transparency and verification of a party's business activities. An organization which stores data in the cloud includes right-to-audit clauses in SLAs to ensure the organization's customer data is securely processed by the cloud provider.

Data jurisdiction is the legal and regulatory framework that determines which laws have jurisdiction over data. Cloud data is often stored in data centers across the world and are subject to laws in different jurisdictions. Data jurisdiction impacts data privacy since data may exist in countries with varying data privacy laws.

Data breach notification is the process of informing individuals, organizations, or authorities when a data breach has occurred, possibly exposing sensitive or personal information. Data breach notification is a component of privacy regulations and data protection in many jurisdictions. The location of data impacts the legal responsibilities of organizations and cloud providers when a data breach occurs.

Table 13.7.1: The responsibilities of organizations and cloud providers.

	On-premises	Cloud
Right-to-audit	Organizations have direct access to systems and data and can perform regular audits	Organizations' data is stored on cloud servers which may delay and limit audits
Data jurisdiction	Organizations select geographic location of data to comply with data regulations	Data may exist in multiple geographic regions with cloud providers responsible for regional regulatory compliance
Data breach notification	Organizations are responsible for compliance with data breach notification laws	Responsibilities are shared between organizations and cloud providers with SLAs outlining notification responsibilities

PARTICIPATION ACTIVITY 13.7.1: On-premises vs. cloud environments.

How to use this tool

Data breach notification **Data jurisdiction** **Right-to-audit**

	A legal contract that grants one party the right to perform an audit of the records, operations, or processes of another party
	A legal framework that determines which laws have jurisdiction over data
	The process of informing individuals or organizations when a data breach has occurred that may have exposed sensitive or personal information.

Reset

Evidence integrity

Both cryptographic hash functions and checksums are used to ensure the integrity of digital evidence. A ***checksum*** is a string of letters and numbers derived from a data block for the purpose of detecting accidental errors and intentional modifications of data during the data's storage or transmission. Unlike hashing, checksums cannot be used to verify data authenticity because checksums are not collision resistant. Ex: A piece of digital evidence can be modified in a way that the modified data has the same checksum as the original data. Since checksums are commonly used in network protocols to detect errors in data transmission, checksums should be fast to calculate. Ex: TCP checksums are used for detecting data transmission errors.

Digital signatures, timestamps, and chain of custody help establish evidence integrity by non-repudiation. Non-repudiation ensures that an individual involved in a communication cannot later deny involvement in the communication. Accountability for actions taken on digital evidence is also established with non-repudiation by identifying and attributing activities to specific individuals or entities. Non-repudiation prevents individuals from denying involvement in action taken on digital evidence and ensures that the evidence has not been modified and can be attributed to a specific entity.

Table 13.7.2: Comparison between cryptographic hash functions and checksums.

	Cryptographic hash functions	Checksums
Purpose	Data integrity verification, digital signatures, password storage	Error detection in data transmission and storage
Collision resistance	Yes	No
Output length	Variable depending on the hash algorithm	Fixed
Computation speed	Slow	Fast
Verification process	Data recipient compares the hash of received data with the hash calculated by data sender	Data recipient calculates the checksum of received data and compares the checksum with the transmitted checksum

PARTICIPATION ACTIVITY 13.7.2: Evidence integrity.

1) Crytographic hash functions are fast to compute compared to checksums
   - True
   - False

2) Checksums are not collision resistant
   - True
   - False

3) Checksums are used in digital signatures
   - True
   - False

4) All crytographic hash functions produce output of the same length

- True
- False

Evidence recovery

Digital forensic techniques can be used for data recovery when files are damaged or deleted. ***File carving*** is the process of identifying and recovering files in the absence of filesystem metadata by analyzing file formats in a storage media's unallocated space. Deleted files can be identified by searching for header and footer values associated with different file types.

A ***file signature***, also known as ***magic number***, is a sequence of bytes at the beginning of a file that uniquely identifies the file type. Ex: The file signature of a Java class file is the hexadecimal value 'ca fe ba be' because the four bytes of every Java class file begins with 'ca fe ba be'. Since deleted files are placed in unallocated space, a deleted Java class file can be located by searching for 'ca fe ba be' in unallocated space.

Example 13.7.1: An image file named computer.jpg opened in a hex editor. The first four bytes of every jpg file begins with the hexadecimal number 'ff d8 ff e0'.

computer.jpg

0000038f	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	01	00	d8
00000010	00	d8	00	00	ff	e1	10	d0	45	78	69	66	00	00	4d	4d
00000020	00	2a	00	00	00	08	00	04	01	3b	00	02	00	00	00	03
00000030	42	53	00	00	87	69	00	04	00	00	00	01	00	00	08	4a
00000040	9c	9d	00	01	00	00	00	06	00	00	10	c2	ea	1c	00	07
00000050	00	00	08	0c	00	00	00	3e	00	00	00	00	1c	ea	00	00
00000060	00	08	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

PARTICIPATION ACTIVITY 13.7.3: Evidence recovery techniques.

1) File carving identifies a deleted file in unallocated space by searching for the file _____.

- name

- signatures
- size and permissions

2) File carving may fail to recover a deleted file because _____.

- filesystem metadata may no longer exist for the file
- the deleted file was not large enough to be recovered
- the space occupied by the file's data may have been used to store other files

3) File signatures can be used to search for a deleted file in unallocated space because the file signatures are _____.

- not deleted with the file
- unique to each file type
- never overwritten by new data

E-discovery

***E-discovery**, or **electronic discovery**, is the process of identifying, preserving, collecting, and producing electronically stored information (ESI) in legal proceedings or investigations. Ex: E-discovery is conducted in response to a lawsuit involving the theft of intellectual property, or an investigation into non-compliance to a regulatory standard. ESI can include a wide range of digital data such as emails, documents, audio and video files, social media content, and instant messages.*

13.8 LAB: Digital forensics (Walkthrough)

IT-Labs are not printable at this time.

13.9 LAB: Digital forensics evidence acquisition (Walkthrough)

IT-Labs are not printable at this time.

13.10 LAB: Analyzing data breaches through USB forensics (Scenario)

IT-Labs are not printable at this time.