Security+ SY0-601

Module 4: Incident Response, Disaster Recovery, and Business Community.

aci LEARNING [HUBS]

Table of Contents.

ACI LEARNING

Learning objectives.

Upon completion of this module, you should be able to:

- Prepare, plan and understand the principles to keep your organization's operations fluid.
- Learn the fundamentals of Incident Response Planning.
- Understand Business Continuity and Disaster Recovery.
- Learn about basic digital forensics.

aci LEARNING

Incident response.

INCIDENT RESPONSE.

Key concepts.

In this section, we will cover the following key concepts:

- Cybersecurity tools.
- Incident response.
- Exercises.
- Disaster recovery.

aci LEARNING

Incident response.

Incident response sets the processes, guidelines, and resources for dealing with a security incident; it is a paramount activity in risk management.

NIST defines an incident as “the act of violating an explicit or implied security policy.”

Organizations must plan, train, and verify that their response plan is appropriate, works, and is compliant with the laws and regulations governing their organization.

There are a series of steps each Incident Response Plan must adhere to.

INCIDENT RESPONSE.

Incident Response Plans.

- Incident Response Plans (IRPs) should be created that map various categories of incidents. IRPs are considered part of the planning phase of incident response.
- Documentation should include procedures (playbook or runbook), internal, stakeholder and vendor contact information, lists of resources and inventory, and whatever other elements can assist with prioritizing, responding, and remediating the incident and the impacted systems.
- The IR team will require practice to be ready when the incident occurs and even to realistically assess response effectiveness and recovery time.

INCIDENT RESPONSE.

Incident Response Teams.

Incident response plans (IRPs) identify how a response should occur. An Incident Response Team (IRT) contains members who will train for and respond to an incident.

Different organizations call the IRT various terms: Cyber incident response team (CIRT), Computer emergency response team (CERT), etc.

IRT members must be available 7x24x365. This means you will need to train backup personnel. Team members will come from various departments:

- Legal.
- Communication.
- IT.
- HR.
- Sales/Marketing.

aci LEARNING

General notifications.

In an incident or disaster situation, various stakeholders need to be notified. At a company level, the incident response policy and disaster response policy provide guidance on notification procedures.

Generally, guidelines would address to whom updates should be communicated and in what format. Additionally, guidelines would distinguish what would warrant internal communication or public announcement. As such, marketing/public relations personnel and legal and HR staff may be involved.
Some companies specifically choose not to report on incidents and disasters, fearing reputational damage and loss of clientele.

CONTINUED ON NEXT SLIDE >

General notifications.

In instances where customers' information is exposed, concealing the attack exposes the customers to further losses that could have been limited. Through a notification, customers can react accordingly, canceling the compromised credit card or changing the account password. Companies who hide such attacks are held accountable by their users when knowledge of the attack inevitably surfaces later in the public forum.

INCIDENT RESPONSE.

Steps of IR

- Prepare response plans.
- Identify the nature of the incident.
- Limit the spread and impact of the incident.
- Find and remove the source.
- Restore from backups.
- Analyze the effectiveness of the response.

Preparation.

Preparation involves making the system resilient to attack in the first place.

- Preparation includes hardening systems, writing policies, training personnel, writing procedures for incident response (an IRP or incident response plan), creating lines of communication to all stakeholders, and identifying the proper resources and assets for incident response.
- Preparation is the key to defense in a potentially hostile environment, which is how we should begin to think of the internet, at least as security professionals.
- This starts with the design of your network -reduce the attack surface, prepare response plans, policies, and procedures, and ready your defensive and recovery mechanisms.

INCIDENT RESPONSE.

Identification.

Identification involves determining whether an incident has occurred, assessing the severity, and notifying stakeholders.

Identification is often accomplished using an attack framework; these frameworks can categorize adversary behaviors to make identifying indicators of an attack easier.

Attack frameworks used in the identification phase include:

- Cyber Kill Framework.
- MITRE ATT&CK.
- Diamond Model of Intrusion Analysis.

IR prioritization.

If there are numerous incidents occurring at the same time, they must be prioritized.

The following are issues that need to be considered:

- Data integrity – The value of the data at risk is the most important element.
- Downtime – How has the organization quantified the cost of a system(s) being down?
- Economic/Publicity – Long-term costs could also include reputation and market standing.
- Scope – How many systems are affected? If a large number, is it masking an attack?
- Detection Time – The faster, the better.
- Recovery Time – How long before you can get the system back online.

Attack frameworks.

An attack framework is a set of comprehensive descriptions, examples, and definitions of the threat lifecycle from the initial access through exfiltration.

These frameworks are used to train individuals in incident response teams to identify potential attacks and attack vectors in their networks. Once trained using a specific framework, the CIRT can function and communicate more effectively since they all communicate using the same terms.

INCIDENT RESPONSE.

MITRE ATT&CK.

MITRE ATT&CK (Adversarial, Tactics, Techniques, and Common Knowledge) is a global database of documented attack types and TTPs. If a security analyst needs to further research the symptoms of an attack, MITRE ATT&CK is a well-known, trusted source of information.

MITRE ATT&CK can be very useful when mitigating or researching attacks or threats to a network; this library of attacks includes attack descriptions and possible responses to an attack.

You can read more at: https://attack.mitre.org/

aci LEARNING

MITRE ATT&CK matrices.

MITRE ATT&CK matrices include enterprise, mobile, and ICS. Each matrix provides insight into categories of attacks, listing various TTPs.

The enterprise matrix includes PRE (preparatory), Windows, macOS, Linux, cloud (with submatrices of its own), network, and containers, while the mobile matrix has submatrices for Android and iOS attacks.

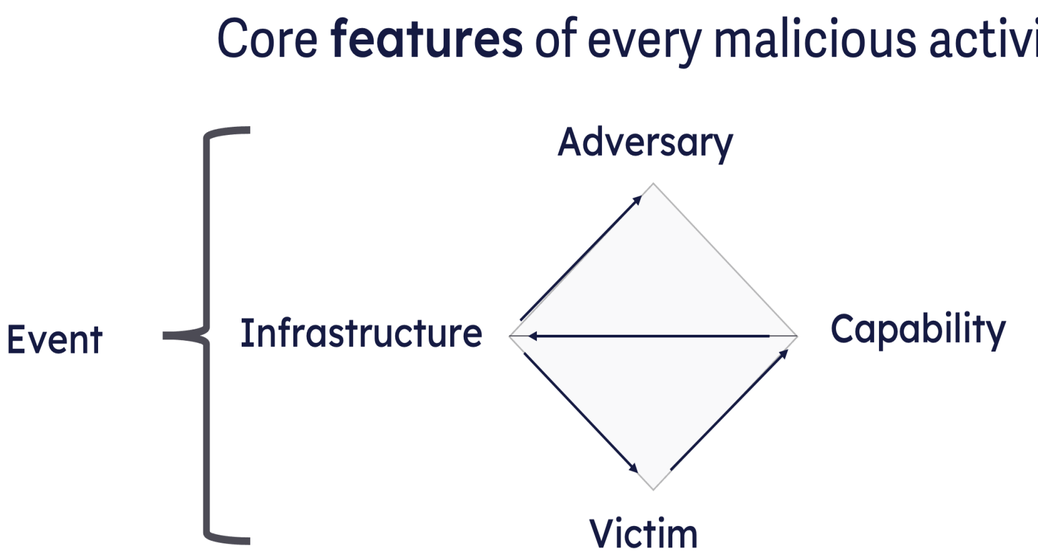
Categories under the enterprise matrix include reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact.

Tactics, Techniques, and Procedures (TTPs).

Tactics, Techniques, and Procedures (TTPs) are documented practices of known threats and attackers. Every major network should have documented TTPs on known threats.

The purpose of TTPs is to identify and document the behaviors of possible attackers. If you know how and why an attacker may attack a network, that attack is far easier to mitigate.

The Diamond Model of Intrusion Analysis.



The Diamond Model of Intrusion Analysis is a standardized framework for how a company can classify and react to threats.

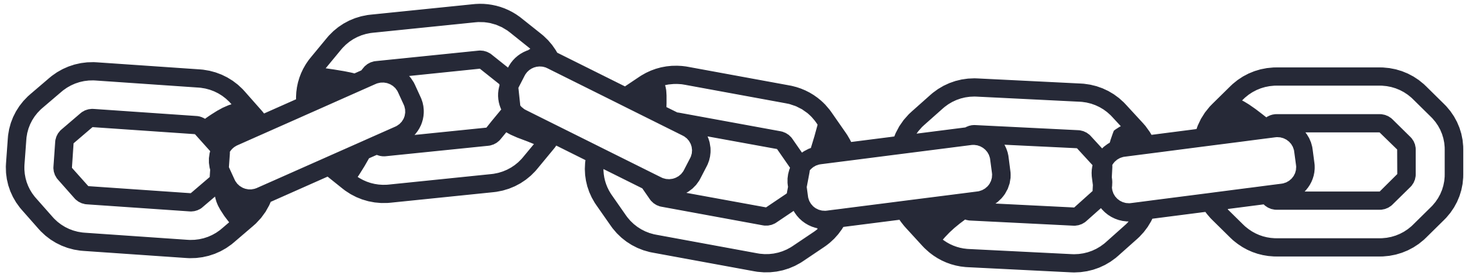
The diamond model is broken into four main categories:

- Adversary.
- Capability.
- Victim.
- Infrastructure.

Cyber Kill Chain.

The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions. The model identifies the stages an attacker must complete in order to achieve their objective. Any break in the chain will stop an attack in its' tracks and force the attacker to start over.

The Cyber Kill chain has seven steps; understanding these will help security professionals understand their adversary's tactics, techniques, and procedures (TTPs).



aci LEARNING

Cyber kill chain steps.

Reconnaissance	The attacker determines the best TTPs to use based on the information found.
Weaponization	Create a deliverable exploit.
Delivery	Put exploit into an email message, on a website, or in a USB.
Exploitation	Code is executed using the vulnerability identified in reconnaissance.

CONTINUED ON NEXT SLIDE >

Cyber kill chain steps.

Installation	Malware is installed on the system.
Command & Control (C2)	Create a backdoor so the adversary can re-engage and control the target system at will.
Actions on Objectives	Take the system down, deface websites, exfiltrate data, etc.

INCIDENT RESPONSE.

Containment.

Containment involves limiting the scope and magnitude of an incident.

The IRP (Incident Response Plan) should contain step-by-step procedures for containing an incident, thereby reducing the overall effect of the attack on the system.

aci LEARNING

INCIDENT RESPONSE.

Eradication.

Eradication is the process of removing the cause of the incident and restoring the affected systems; this involves removing the intrusion tools, malware, and unauthorized configuration changes made during the incident.

Recovery.

- Recovery involves reintegrating affected systems back into the business workflow.
- Recovery involves restoring systems from secure backup/images. You will want to re-audit the system to ensure it is no longer vulnerable to another attack.

aci LEARNING

INCIDENT RESPONSE.

Lessons learned.

Lessons learned involves analyzing the incident and your responses to it to determine what you can do better the next time.

IR exercises.

Walkthroughs, workshops, and orientation seminars: These are knowledge transfer events designed to train disaster recovery team members on their responsibilities and where they fit into the overall efforts.

Tabletop exercises: Team members meet in a conference and verbally walk through the process, with each team member demonstrating knowledge of their responsibilities, resources, and access.

CONTINUED ON NEXT SLIDE >

aci LEARNING

IR exercises.

Simulations: A team-based exercise where a red team simulates an attack on the organization's system. This is often done with Breach and Attack Simulation (BAS) software or Capture the Flag (CTF) simulations.

The blue team defends the network. A white team will referee the event. Should the white team bring the teams together during the exercise, the combined team is called the purple team.

These events are comprehensive but expensive.

INCIDENT RESPONSE.

Security, Orchestration, Automation, and Response (SOAR).

Security, Orchestration, Automation, and Response (SOAR) platforms are a collection of security software solutions and tools for browsing and collecting data from various sources. SOAR solutions use a combination of human and machine learning to analyze diverse data and prioritize incident response actions. A SOAR can identify an issue and begin incident response runbook steps with automation.

SOAR describes three software capabilities:

- Threat and vulnerability management.
- Security incident response.
- Security operations automation.

INCIDENT RESPONSE.

Knowledge check.

Let's apply what we have covered:

- List the Incident Response Plan steps.
- What is a tabletop exercise?
- Describe the seven steps of the Cyber Kill Chain.

Business continuity and disaster recovery.

BUSINESS CONTINUITY AND DISASTER RECOVERY.

Key concepts.

In this section, we will cover the following key concepts:

- Business continuity.
- Disaster recovery.

aci LEARNING

Business Continuity.

CONTINUED ON NEXT SLIDE >

Business Continuity (BC) is processes, procedures, and activities to ensure the business survives regardless of potential risk, threat, or disruptive event. ISO defines it as the ability of the organization to continue to deliver services or products at a predefined level following a disaster.

Business Continuity Planning (BCP) identifies controls and processes that enable an organization to maintain critical workflows in the face of some adverse events.

Business continuity.

- Business continuity planning prepares to continue critical operations when the normal means of doing so are disrupted. It may revolve around shifting operations to another branch, as a hot site, or temporarily outsourcing certain aspects of your business.
- Continuity of Operations Planning (COOP) is the term used mostly with government operations.

Business Impact Analysis (BIA).

A Business Impact Analysis (BIA) is a systematic process that determines and evaluates the potential effects of an interruption to critical business operations due to a disaster or disruptive event.

Business Process Analysis (BPA).

Business Process Analysis (BPA) identifies dependencies concerning Mission Essential Functions (MEFs).

Assets include people, tangible assets, intangible assets, and business practices, methods, and procedures.

Dependencies include inputs, hardware, outputs, and workflow.

Disaster recovery.

Disaster recovery is the ability of an organization to restore business data and applications; it is data-centric with an emphasis on IT infrastructure and data.

Objectives include:

- Reduce downtime.
- Reduce losses.
- Recover data.

BUSINESS CONTINUITY AND DISASTER RECOVERY.

Recovery sites.

A hot site has a network setup where network functions can be transferred in a very short time; it might be another branch of the company or a vendor that offers such services. Similarly, it might involve operations to the cloud and then point traffic to that site. A hot site has an up-to-date copy of production data.

A warm site typically has a network but is not up to speed on the functions needed; it might take hours to transfer services there as data is transferred via backups. A warm site does not have an up-to-date copy of production data.

A cold site is often little more than a building where a network could be set up; it has water, electricity, heat, air, and perhaps internet access, but everything else will need to be set up.

Key metrics.

Mission Essential Functions (MEF) represent a business function that cannot be deferred.

There are four main functions that help analyze a MEF:

- Maximum Tolerable Downtime (MTD).
- Recovery Time Objective (RTO).
- Work Recovery Time (WRT).
- Recovery Point Objective (RPO).

CONTINUED ON NEXT SLIDE >

Key metric-MTD.

Maximum tolerable downtime (MTD) represents the longest amount of downtime that a business function or system can undergo without causing a complete, unrecoverable failure of the overall organization.

Each individual process will likely have its own MTD, ranging from minutes to days for non-critical functions. The MTD sets the outer boundary for restoration of the function, with goals being somewhat shorter than that maximum.

CONTINUED ON NEXT SLIDE >

Key metrics- RTO and WRT.

- The Recovery Time Objective (RTO) is the period following a disaster in which an individual IT system can remain offline — this includes identifying the incident and performing recovery.
- The RTO is one of the two factors that need to be considered when determining how you will attain your maximum tolerable downtime (MTD).
- Work Recovery Time (WRT) is the period after systems recovery to train users on any working practices that may have changed. Note: RTO + WRT cannot exceed MTD.

CONTINUED ON NEXT SLIDE >

Key metrics- RPO.

The Recovery Point Objective (RPO) is the amount of data loss you can sustain, measured in time, before not being able to recover.

The RPO helps identify your backup strategy. How often should you back up? The answer had better align with your RPO. Where do you store your backups? The answer had better align with your RPO.

MTTF.

$$\frac{\text{Total Hours of Operation}}{\text{Number of Units}}$$

Or

$$\frac{\text{THO}}{\text{TNU}}$$

- Meantime To failure (MTTF) is calculated as MTTF = THO/TNU. The total hours of operation (THO) of all the redundant devices are divided by the total number of units (TNU). MTTF is calculated for devices that are not repairable.
- For Example: If one system runs 250 hours, another runs 100 hours, and a third runs 130 hours, for a combined total of 480 hours, divided by three machines for a value of 160 hours MTBF.

MTBF.

$$\frac{\text{Total Operational Time}}{\text{Number of Failures}}$$

Or

$$\frac{\text{TOT}}{\text{TNF}}$$

Mean time between failures (MTBF) is calculated as MTBF = TOT/TNF. The total operational time (TOT) of all the redundant devices is divided by the total number of failures (TNF). MTBF is calculated for devices/systems that are repairable.

For Example: If you have 5 machines running collectively for a total of 860 hours, during which time 2 failures occurred, then the MTBF is 860/2, or 430 hours between failures on average.

Mean Time To Repair (MTTR).

- The Mean Time To Repair (MTTR) is the average time it takes to replace a device, component, or system to recover from a failure.
- The mean time to repair (MTTR) is important in determining the overall recovery time objective (RTO).
- Ticketing systems must be in place to track this time, and industry/vendor best practices must be used to know where to start with the metrics. Training systems must be implemented to ensure the MTTR is either maintained.

Order of restoration.

A mission-essential function (MEF) cannot be delayed; in other words, this function is one the organization cannot afford to be without beyond what is unavoidable, such as scheduled maintenance.

The order of restoration is the process of delegating the order to bring systems back up. In general, restore power, bring the layer 1 systems online, then the layer 2 and 3 devices, bring security devices online, then bring services back online and finally (and last) bring clients back online.

DRP exercises.

- Functional Exercises: Activities are performed in scenario-based situations that allow members to practice/demonstrate the actual skills needed for the recovery.
- Full-Scale Exercises: These are simulations that reflect/simulate real disasters, with members performing recovery activities as they would in actual disasters.

BUSINESS CONTINUITY AND DISASTER RECOVERY.

Knowledge check.

Let's apply what we have covered:

- List and describe RTO, MTD, and RPO.
- What is the difference between MTTF and MTBF?
- What is a Business Continuity Plan?
- Describe the order of restoration.
- Describe a hot, warm, and cold site.

Digital forensics.

DIGITAL FORENSICS.

Key concepts.

In this section, we will cover the following key concepts:

- Digital forensics.
- Secure the scene.
- Latent data and admissibility.
- E-discovery.
- Acquisition.
- Order of volatility.

aci LEARNING

DIGITAL FORENSICS.

Key concepts.

In this section, we will also cover the following key concepts:

- Write blockers.
- Time.
- Documentation.
- Forensic software.
- Evidence.

ACI LEARNING

Digital forensics.

Digital forensics is the practice of collecting evidence from computer systems and networks to a standard that will keep accepted in a court of law. There are two basic motives for forensics in computers following an attack. The first is to gather admissible evidence in court, while the second is to gather information for internal use.

If you pursue only the internal use, you are free to do things however you desire, though elements like bias should still be avoided to ensure your conclusions are evidence-based.

CONTINUED ON NEXT SLIDE >

Digital forensics.

Pursuing the first does not preclude using the evidence for internal purposes such as strengthening defenses, but in some cases, companies have no intention of going to court. Those companies may wish to keep the fact that they suffered an attack as a private matter to be dealt with internally. There are strict guidelines regulating how evidence must be gathered, preserved, analyzed, and submitted to the court, whether the proceeding is criminal or civil.

DIGITAL FORENSICS.

Secure the scene.

Securing the scene involves closing off an area and documenting everything seen on the scene when you get there.

CSIRT teams are the primary response force to incidents; they are responsible for securing the scene, which aids in procuring the resources necessary to facilitate a good discovery.

aci LEARNING

DIGITAL FORENSICS.

Latent data and admissibility.

Digital evidence is latent. Latent means that the data is not directly perceivable by the human eye. At its most basic level, this is because the data is all binary and thus not human-readable; we require the computer to present it to us in a readable form.

In gathering evidence for use in court, the driving factor behind the controls on how it must be collected, preserved, processed, and presented is the principle of due process, which ensures fairness in prosecutions by instituting a set of safeguards against abuse.

DIGITAL FORENSICS.

E-discovery.

E-discovery software filters data down to what is needed, storing it in a database in an admissible format. It can assist in identifying and deduplicating, minimizing the data that must be analyzed. E-discovery software also assists with searches and tagging information that is determined to be relevant.

aci LEARNING

DIGITAL FORENSICS.

Acquisition.

Evidence acquisition is taking and copying e-data to be utilized throughout the forensics process.

The acquisition is gathering a “forensically clean” bit-for-bit image of the hard drive. Several images will be needed. Additionally, hashes will be taken off the hard drive and each image to validate that they are identical.

CONTINUED ON NEXT SLIDE >

DIGITAL FORENSICS.

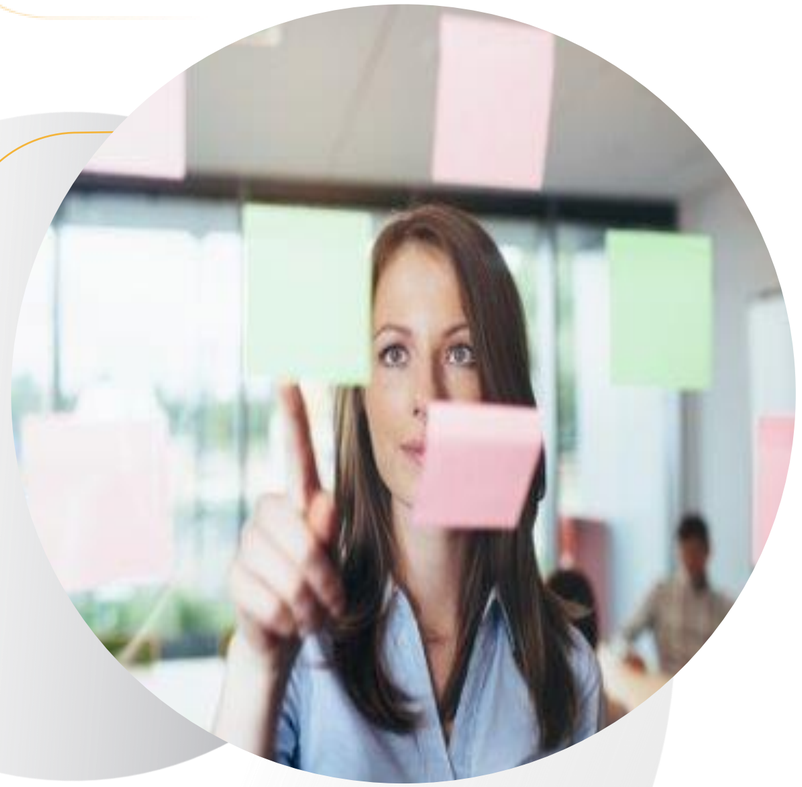
Acquisition.

There are four steps to the data acquisition process using hashes to prove the integrity of the data:

- Hash the original disk media.
- Bit-by-bit copy using an imaging utility.
- Hash the image (must match the hash of the original disk media).
- Make another copy and verify with a hash again. Work from this copy.

DIGITAL FORENSICS.

Order of volatility.



The order of volatility is the order in which data must be collected, starting with the most at-risk data and proceeding to the lowest-risk data.

It’s easy to accidentally destroy latent evidence if these procedures are not followed. Data stored in memory is volatile and can be lost by simply writing other things into RAM that push it out.

aci LEARNING

DIGITAL FORENSICS.

Order of volatility – most to least.

- CPU registers and cache memory.
- Data are currently written to RAM, including the system's routing table, ARP cache, process table, and kernel statistics.
- Temporary file systems.
- Non-volatile storage devices (HDDs, SSDs, flash memory devices such as thumb drives).
- Remote logging and monitoring data.
- Physical Configuration and network topology.
- Archival media, such as backup tapes, CDs, and DVDs.

aci LEARNING

DIGITAL FORENSICS.

Write blockers.

A write blocker is a device that can be used between the target system and the system receiving the image to prevent write commands from causing any such changes.

- It's important to ensure that nothing done in the collection process alters the data in the target system.
- They prevent a user from creating, writing, or generating new data, generally in conjunction with a database.
- Write blockers can be used to protect the chain of custody by protecting the drive. Write blockers still provide read access to the data without manipulating the information.

DIGITAL FORENSICS.

Timestamps and offsets.

- Timestamps are very useful because they designate when something happened or occurred. Timestamps appear on emails, messages, and access logs. In auditing practices, timestamps are used to confirm or deny actions and activities.
- If a timestamp is inaccurate because a real-time clock is running fast or slow, the timeline of events would be skewed as well. When branches of an organization span multiple time zones, a time offset is required to reflect simultaneous events occurring in separate time zones.

aci LEARNING

DIGITAL FORENSICS.

Documentation.

Documentation is integral to the digital forensics field. Each piece of evidence must go through a chain of custody. The documentation will help prove that no evidence has been tampered with; it will also assist in finding the appropriate piece of evidence when needed.

Digital forensics software offers a secure way to preserve and document evidence and the process.

aci LEARNING

DIGITAL FORENSICS.

Chain of custody.

Chain of custody is the entire process of tracking and documenting evidence gathered during an investigation. A chain of custody is often heavily documented to confirm the validity of the evidence.

Legal hold refers to the legal controls in place to force the preservation of data that may be relevant to a future court proceeding.

In short, evidence cannot be destroyed. Whether some specific data is subject to a legal hold can be determined by regulations, industry standards and best practices, or more narrowly, by notice of litigation or lawsuit to an enterprise by law enforcement or lawyers.

DIGITAL FORENSICS.

E-discovery software.

Autopsy is the GUI front-end for The Sleuth Kit. It is an example of open-source E-Discovery software.

EnCase Forensic is a digital forensics case management toolset from Guidance Software designed to guide a forensics investigation through the steps.

The Forensic Toolkit (FTK) offers a forensics software package designed for use on Windows servers.

WinHex allows recovery and manipulation of hexadecimal data with varying levels of functionality, depending on the license type.

aci LEARNING

Additional evidence.

Memory dumps. A system memory dump produces an image file of the contents of RAM, which includes the running processes, temporary file systems, registry data, network connections, etc.

Another useful option is a crash dump, created when a Windows system has a bluescreen level error or unrecoverable error.

Disk images. There are three device states from which disk images can be acquired.

CONTINUED ON NEXT SLIDE >

Additional evidence.

Live acquisition occurs while the host is running, which may provide additional information but may also be inadmissible in court as the data will have changed.

Static acquisitions are run against a shutdown machine, though there are two main variations:

- Properly shutting down the host can give malware on the system an opportunity to respond to the shutdown event and try to remove evidence of its existence.
- Pulling the plug to shut the system down is a way to avoid that risk, but it has the potential to corrupt data.

CONTINUED ON NEXT SLIDE >

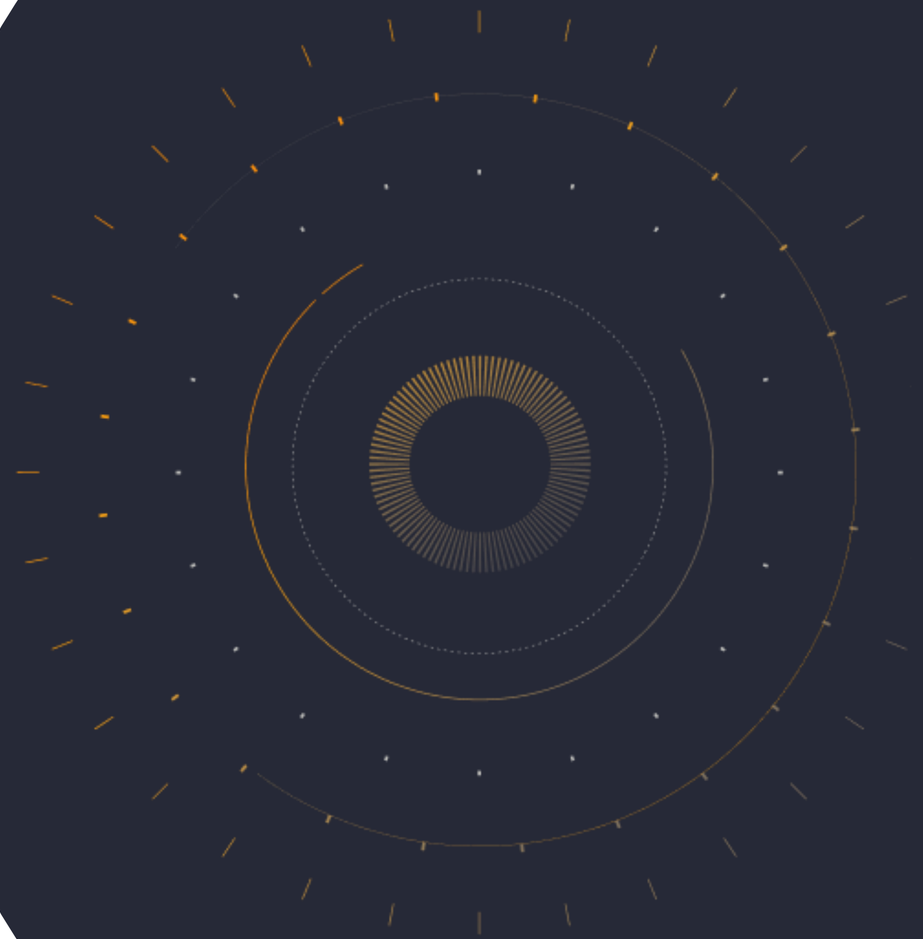
Additional evidence.

Artifacts. Other important potential sources of evidence include network packet captures, analysis, and artifacts. Artifacts are any data not found in the main data structures of an OS.

Recovering data remnants, the remains of data deleted from the file system but still physically present on the hard drive, in whole or in part, is known as carving.

DIGITAL FORENSICS.

Knowledge check.



Let's apply what we have covered:

- What are the two methods of static acquisition of a disk?
- Describe, from most to least, the Order of Volatility.

End of Module.

For additional practice, please complete all associated self-study activities and labs.