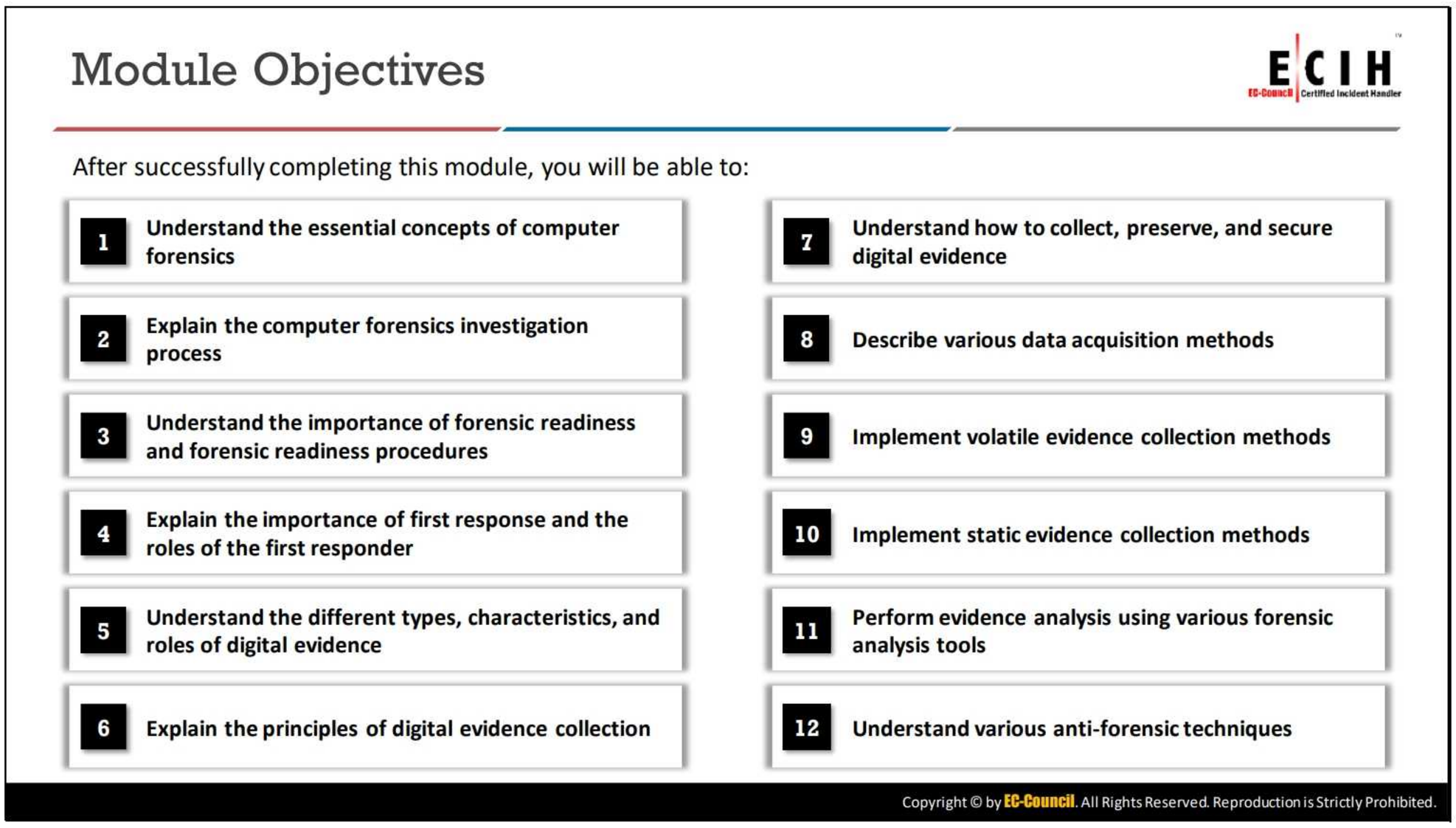
EC-Council Certified Incident Handler™

Module 03

Forensic Readiness and First Response

@UN5TABLE

This page is intentionally left blank.



Module Objectives

Ever-increasing cybercrime and the rise in computing technology have made an efficient and effective information security program essential for organizations. With the rapid change in technology and threat landscape, it is important for organizations to incorporate ongoing and proactive computer investigations into their current information security programs to thwart and prevent evolving threats. To implement these programs, organizations need to adapt current information security best practices to include certain aspects of digital forensic readiness into their current cybersecurity programs.

This module describes the basic concepts of computer forensics, including its role in incident handling, types of digital evidence, and various characteristics of digital evidence. It will also introduce you to the fundamental concepts of forensic readiness and first response. It not only explains different ways to secure and document the crime scene but also provides a brief overview on collecting and preserving digital evidence. The module also describes chain of custody forms, physical evidence collection from networked computers, powered on computers, powered off computers, etc. It also explains how to pack, store, and transport physical evidence from the crime scene. Besides covering data acquisition, data duplication, and image integrity verification, this module also explains volatile evidence collection and the methodology to collect volatile data such as system information, current system data, time, current system uptime, and running processes. Static evidence collection and evidence analysis are explained. This module also introduces forensic analysis tools, such as Forensic Explorer, EnCase Forensic, and FTK, and explains various anti-forensic techniques.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

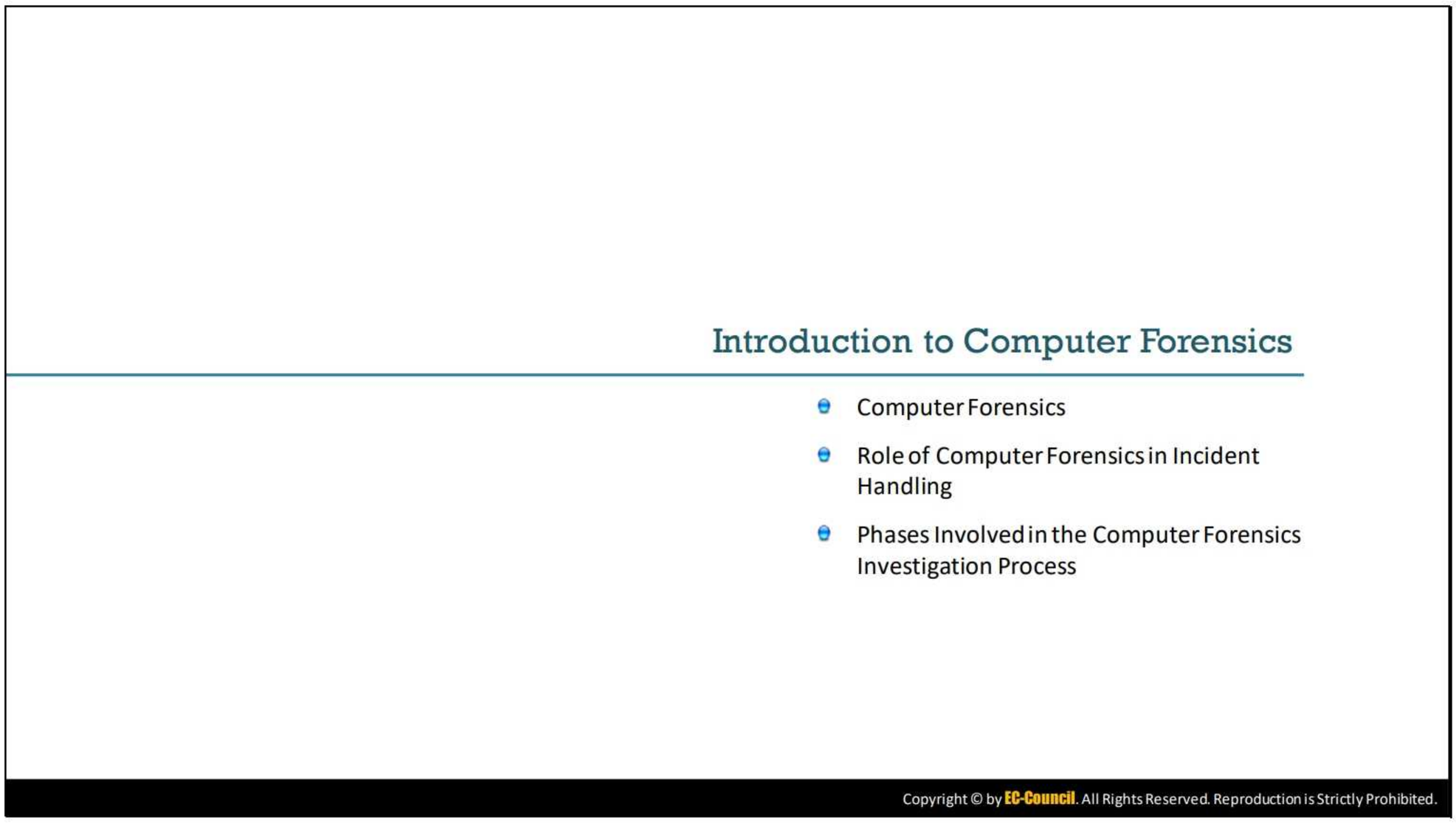
@UN5TABLE

At the end of this module, you will be able to:

- Understand the essential concepts of computer forensics
- Explain the role of computer forensics in incident handling
- Explain the computer forensics investigation process
- Understand the importance of forensic readiness and forensic readiness procedures
- Explain the importance of first response and the roles of the first responder
- Understand different types, characteristics, and role of digital evidence
- Explain the principles of digital evidence collection
- Understand how to collect, preserve, and secure digital evidence
- Describe various data acquisition methods
- Implement volatile and static evidence collection methods
- Perform evidence analysis using various forensic analysis tools
- Understand various anti-forensic techniques

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



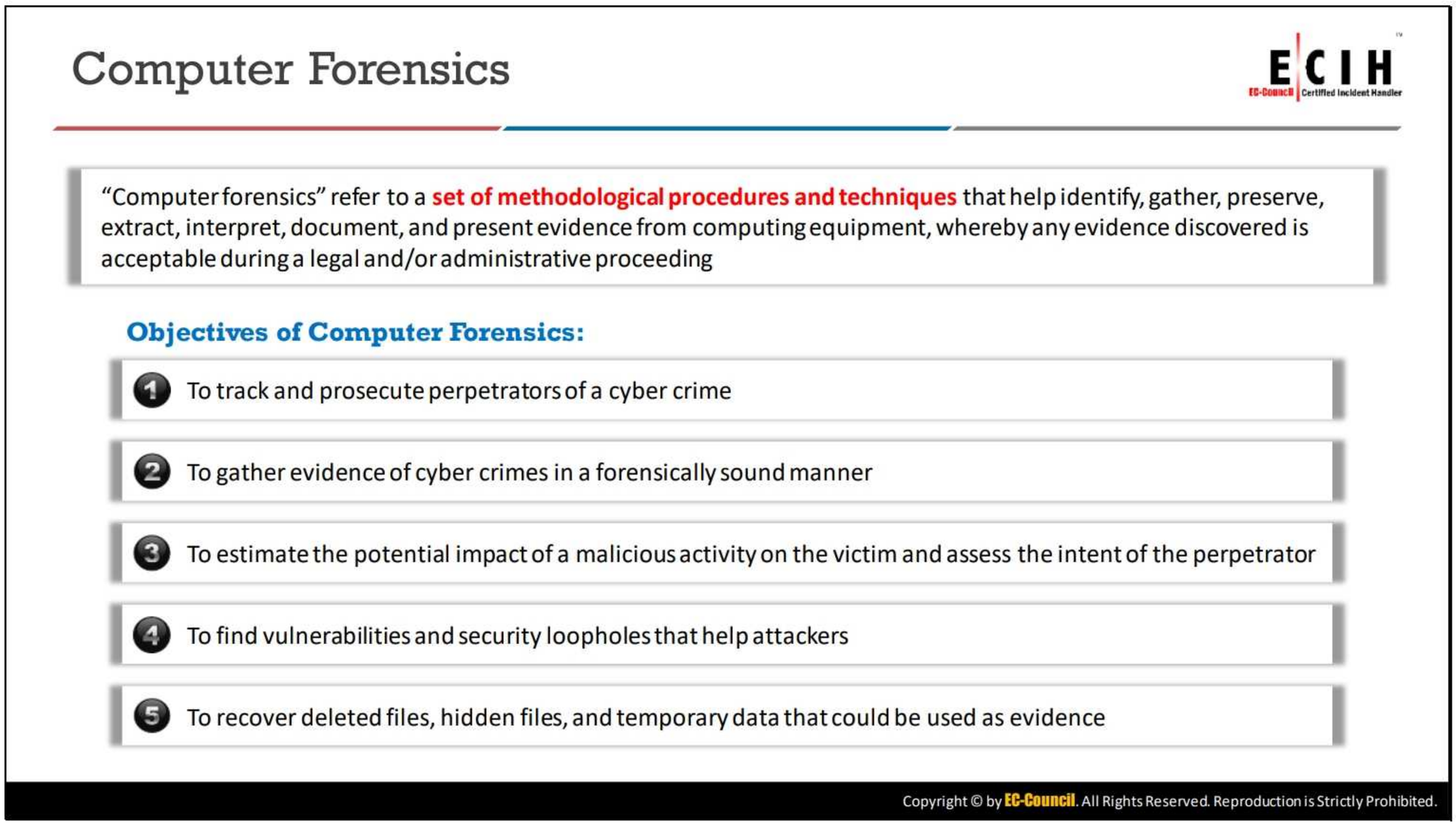
Introduction to Computer Forensics

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes the acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Incident responders must be professionally trained to extract, analyze, report, and investigate cases that involve cyber technology as the source or the victim of a crime.

This section discusses computer forensics and its role in incident handling, gives an overview of computer forensic process, and explains the phases involved in the computer forensics investigation process.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Computer Forensics

Computer forensics is a digital forensics division that deals with crimes committed across computing devices such as networks, computers, and digital storage media. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment in such a manner that the discovered evidence is acceptable during a legal and/or administrative proceeding in a court of law.

In short, computer forensics deals with the process of finding evidence related to a digital crime in order to trace the culprits and take legal action against them.

Listed below are the objectives of computer forensics:

- Identify, gather, and preserve the evidence of a cybercrime
- Track and prosecute the perpetrators in a court of law
- Gather evidence of cybercrimes in a forensically sound manner
- Interpret, document, and present the evidence in a manner admissible during prosecution
- Estimate the potential impact of a malicious activity on the victim, and assess the intent of the perpetrator
- Find vulnerabilities and security loopholes that help attackers
- Understand the techniques and methods attackers use to avoid prosecution and overcome them
- Recover deleted files, hidden files, and temporary data that could be used as evidence

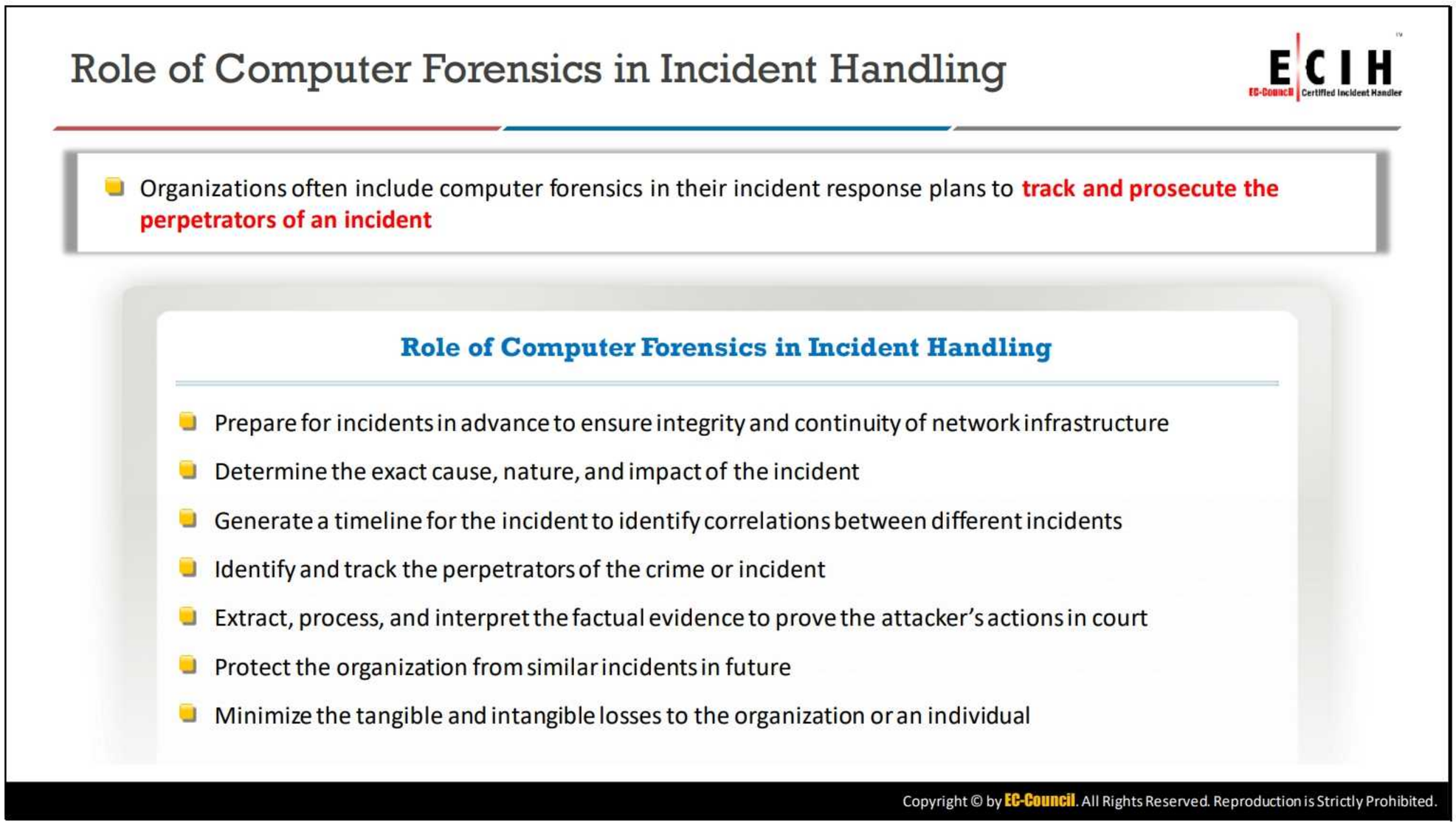
EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Perform incident response to prevent further loss of intellectual property, finances, and reputation during an attack
- Have knowledge about laws of various regions and areas, as digital crimes are omnipresent and remote in nature
- Know the process of handling multiple platforms, data types, and operating systems
- Understand the use of proper tools for various forensic applications

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Role of Computer Forensics in Incident Handling

Incident response is a process of developing a strategy to address the occurrence of any security breach in a system or network. The process includes formulating a security policy and identifying the goals of the incident response, creating an incident response team, analyzing threats, establishing methods for detecting a breach, and preparing to combat threats and mitigate damages in the event of a security breach.

Organizations create incident response plans to accomplish goals such as:

- Develop and implement a strong security policy
- Effectively monitor and analyze the systems and network traffic
- Ensure operational logs and logging mechanisms
- Handle incidents in a manner that minimizes the damage and reduces recovery time and costs
- Map the pathway for extracting evidence in a legally sound and acceptable manner
- Define the role of an incident response professional, such as identifying how the breach occurred, how to locate the method of the breach, and how to mitigate the breach

On the other hand, computer forensics is a legal process of finding, gathering, analyzing, and presenting the evidence in a court of law to determine the culprit behind the incident. Organizations often include computer forensics as part of the incident response plan to track and prosecute perpetrators of an incident.

There has been an exponential increase in the number of cybercrimes and litigations involving large organizations. This has highlighted the need for computer forensics. Organizations need

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

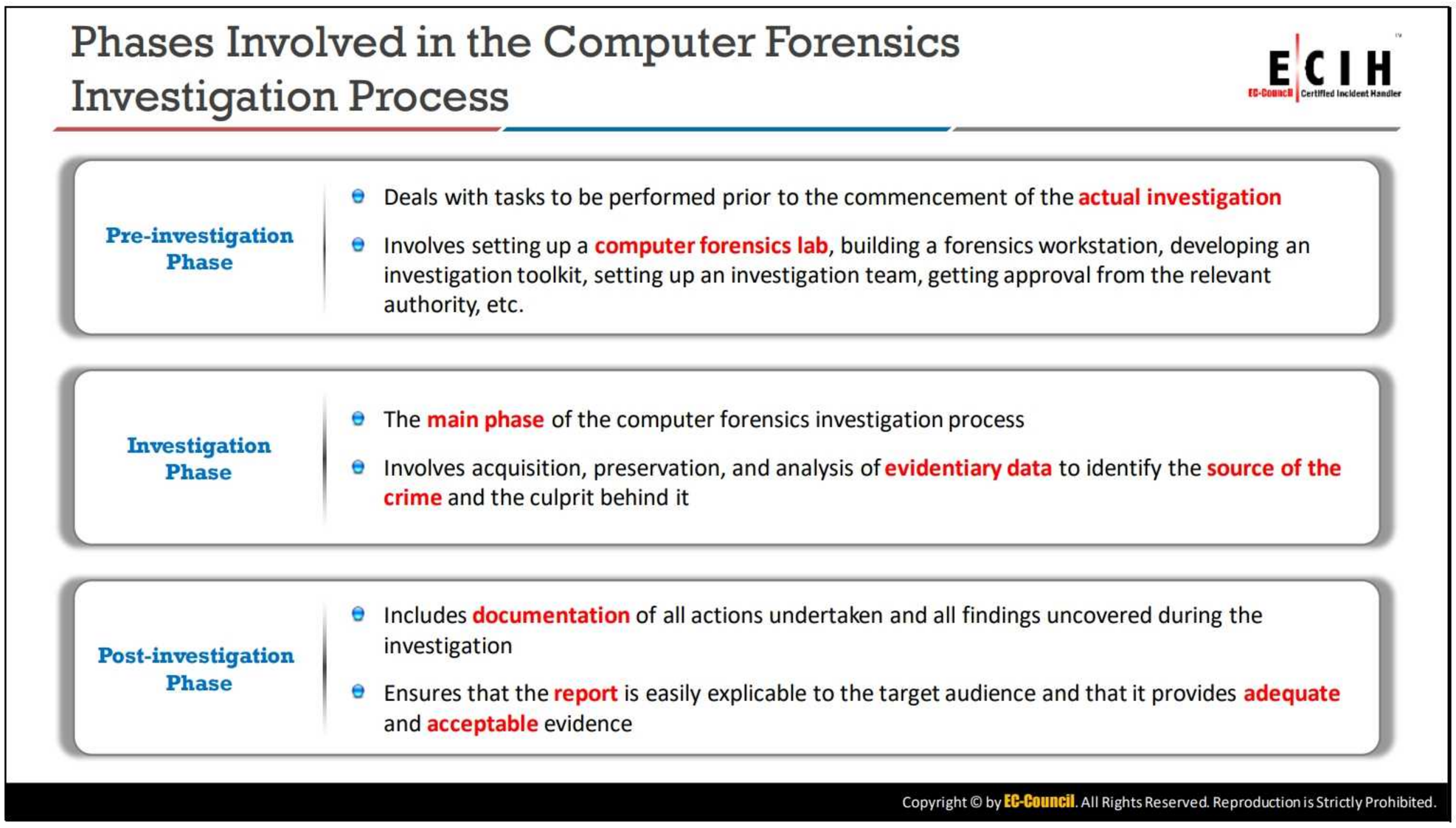
to employ the services of a computer forensics agency or hire a computer forensics expert to guard against computer incidents or solve crimes that involve the use of computers and related technologies. The staggering financial losses caused by computer crimes have also contributed to the renewed interest in computer forensics.

Computer forensics plays an important role in tracking cyber criminals. The main role of computer forensics in incident handling is to:

- Prepare for incidents in advance to ensure integrity and continuity of network infrastructure
- Identify and gather evidence of computer crimes in a forensically sound manner
- Determine the exact cause, nature, and impact of the incident
- Generate a timeline for the incident which helps in correlating different incidents
- Conduct a forensic analysis of the affected system which helps in determining the nature and impact of the incident
- Identify and track the perpetrators of the crime or incident
- Extract, process, and interpret the factual evidence so that it provides proof of the attacker's actions to the court
- Offer ample protection for data resources and ensure regulatory compliance
- Protect organizations from similar incidents that may occur in the future
- Counteract online crimes such as abuse, bullying, and reputation damage
- Minimize the tangible and intangible losses to an organization or an individual
- Support prosecution of the perpetrator of an incident
- Save an organizations' money and time by conducting a damage assessment of the victimized network
- Save organizations from legal liabilities and lawsuits

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Phases Involved in the Computer Forensics Investigation Process

Discussed below are different phases of the computer forensics investigation process:

- **Pre-investigation Phase**

  This phase involves all the tasks performed prior to the commencement of the actual investigation. It involves setting up a computer forensics lab, building a forensics workstation, developing an investigation toolkit, building an investigation team, getting approval from the relevant authority, etc.

  This phase also includes steps such as planning the process, defining mission goals, and securing the case perimeter and involved devices.

- **Investigation Phase**

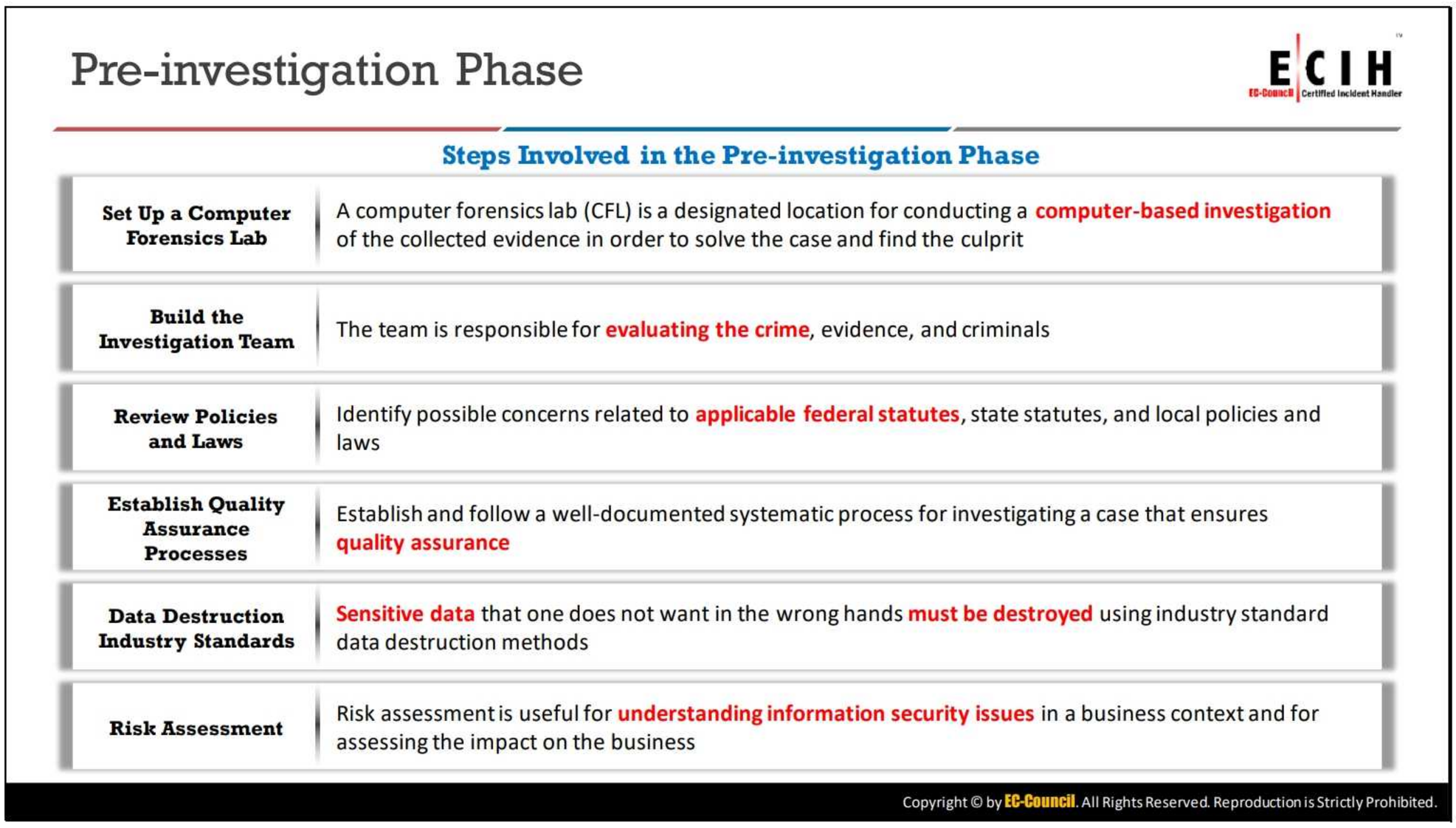
  Considered to be the main phase of the computer forensics investigation, the investigation phase involves acquisition, preservation, and analysis of the evidentiary data to identify the crime source and the culprit. This phase involves implementing the technical knowledge to locate the evidence and examine, document, and preserve the findings as well as the evidence. Trained professionals perform all the tasks involved in this phase to ensure the quality and integrity of the findings.

- **Post-investigation Phase**

  This phase involves the reporting and documenting of all actions undertaken, and the findings obtained during the course of an investigation. It ensures that the target audience can easily understand the report and that it provides adequate and acceptable evidence. Every jurisdiction has set standards for reporting the findings and evidence; the report should comply with all such standards as well as be legally sound and acceptable in a court of law.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Pre-investigation Phase

Incident responders cannot take action immediately after receiving a complaint or report of a security incident. They must follow a specific protocol that includes gathering plaintiff information, identifying the type of incident, and obtaining permission and warrants for taking further action. All of these processes combine to form the pre-investigation phase.

The pre-investigation phase includes the following steps:

- **Set Up a Computer Forensics Lab**

  A computer forensics lab (CFL) is a designated location for conducting computer-based investigation of the collected evidence to solve the case and find the culprit. The lab houses the instruments, software and hardware tools, suspect media, and the forensic workstations required to perform investigations of all types.

  Setting up a computer forensics lab includes:

  - Plans and budgets
  - Physical location and structural design considerations
  - Work area considerations
  - Human resource considerations
  - Physical security recommendations
  - Forensics lab licensing

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Build the Investigation Team**

  The investigation team plays a major role in solving a case. The team is responsible for evaluating the crime, evidence, and criminals. Every team member should be assigned specific tasks (roles and responsibilities) that facilitate the team in analyzing the incident.

- **Review Policies and Laws**

  It is essential that the investigation team is aware of the laws that will be applicable to the investigation, including the organization's internal policies, before starting the investigation process. The team should identify possible concerns related to applicable federal statutes, state statutes, and local policies and laws.

- **Establish Quality Assurance Processes**

  An investigator implements various tools and techniques to retrieve and analyze data of evidentiary value. However, the standalone procedure he/she follows may affect the resultant evidence and the case outcome. Thus, there is a need for a forensics unit to establish and follow a well-documented systematic process for investigating a case that ensures quality assurance.

- **Data Destruction Industry Standards**

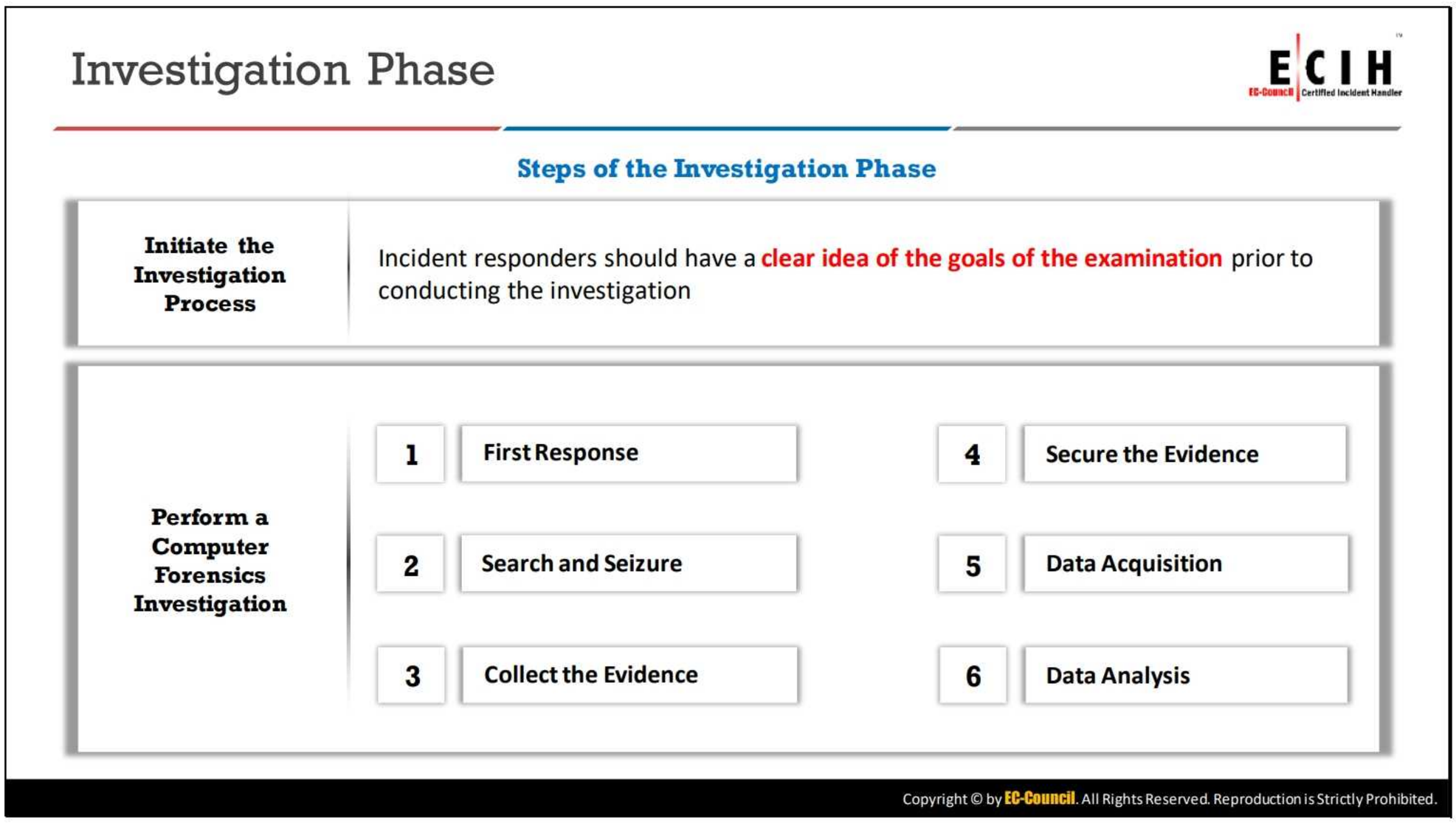
  Destruction of data using industry standard data destruction methods is essential to ensure sensitive data do not fall into the wrong hands. These standards depend on the levels of sensitivity. Data deletion on electronic devices is virtual. It physically remains on the device, posing a security threat if the device is not disposed of properly.

- **Risk Assessment**

  Risk assessment is useful for understanding information security issues in a business context and to assess the impact to the business in the event of a security breach. Risk assessment helps senior management and decision makers in an organization to devise appropriate risk mitigation strategies according to the organization's goals and resources. A proper risk assessment also helps in minimizing the impact of an incident.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Investigation Phase

After obtaining the required permissions and assessing the case prerequisites, the investigator is ready to investigate the incident. The investigation phase includes various stages and processes that require careful and systematic execution to obtain better results.

The computer forensics investigation process is a collection of a wide variety of processes, starting from incident response to crime scene analysis, including evidence collection for the analysis, and from documenting actions and findings to reporting them. Each step in this process is equally crucial to ensure acceptance of the evidence in a court of law and prosecution of the perpetrators.

Steps involved in the investigation phase include:

- **Initiate the Investigation Process**

  Incident responders should have a clear idea about the goals of the examination prior to conducting the investigation. They should have an in-depth technical understanding about the inner workings of what is being examined. They should have the capability to take a systematic approach to examine evidence based on the nature of the request, e.g., a request made by an attorney.

- **Perform Computer Forensics Investigation**

  This step includes the following phases:

  - **First Response**

    First response refers to the first action performed after the occurrence of a security incident. Depending on the type of breach or attack, the first response can prevent further damage to the victim and assist incident responders in tracing the suspect.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Search and Seizure**

  The investigators should have keen knowledge of all the devices that could have played a part in transmitting the attack data to the victim device. They should be able to search for all the involved devices and seize them in a formal manner for evidentiary data analysis.

- **Collect the Evidence**

  Evidence is the crucial data that can help investigators in understanding the process of the attack and tracing the attacker. Therefore, the investigator should know where the evidence can be found and how to gather it.

- **Secure the Evidence**

  Evidence is fragile data that is easy to manipulate, alter, and destroy. Therefore, attackers are always looking for ways to damage it. Thus, it is important to store and secure the evidence in an efficient manner.

- **Data Acquisition**

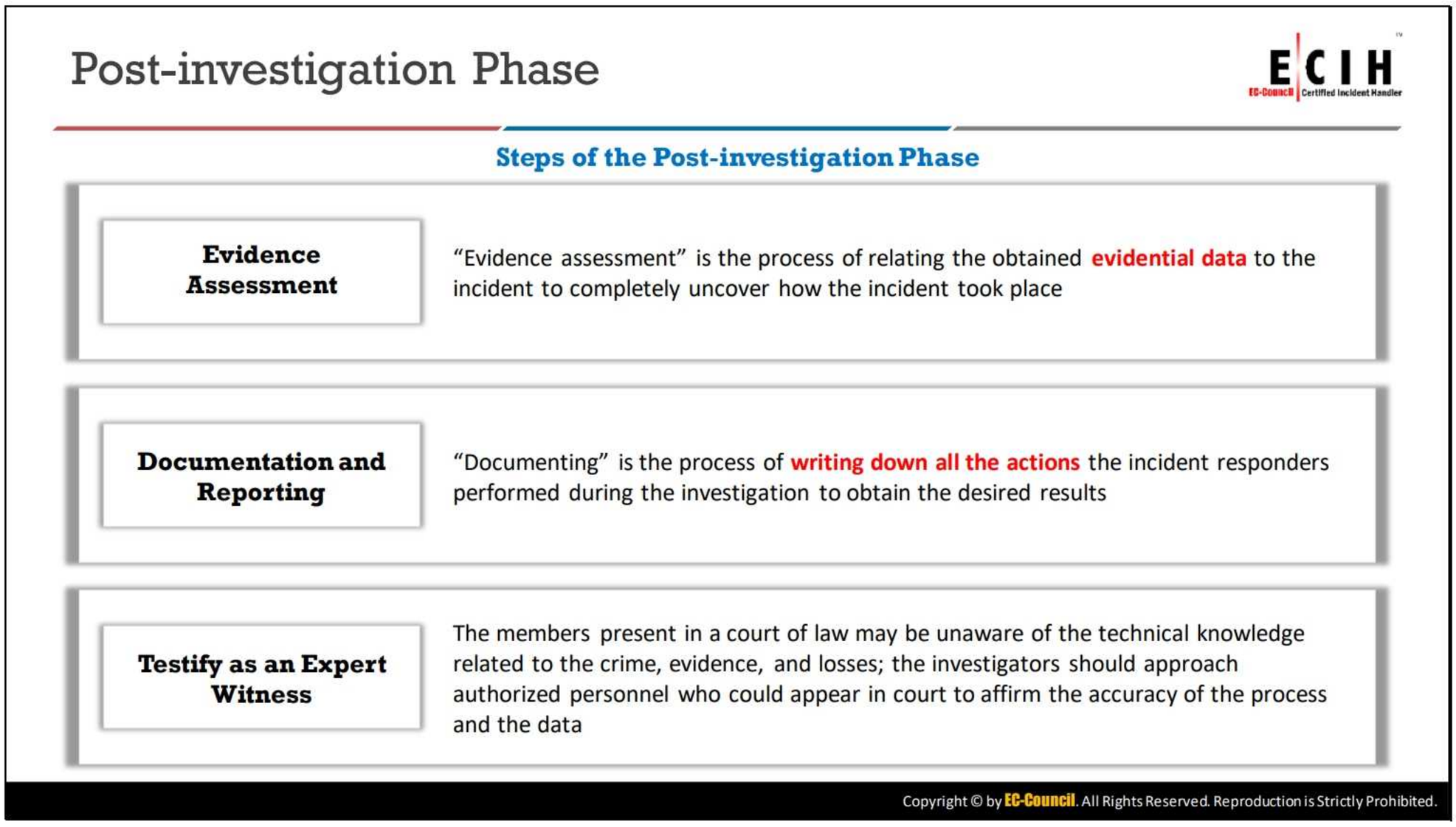
  During an investigation of digital devices, all the evidence may be present in the form of data. Therefore, the investigators should have expertise in acquiring different forms of data stored across various devices.

- **Data Analysis**

  Data analysis refers to the process of going through the data, finding the relevant evidential data, and connecting it to the crime. This analysis helps in tracing the crime and the perpetrator.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Post-investigation Phase

The responsibility of the investigators does not end with finding and analyzing the evidence data. They should also be able to explain how they arrived at the conclusion to prosecutors, attorneys, and judges.

Steps involved in the post-investigation phase include:

- **Evidence Assessment**

  Evidence assessment is the process of relating the obtained evidential data to the incident to understand how the complete incident took place. Evidence assessment is a crucial stage in the forensics process. The assessment depends on the type of incident, objectives required to perform the incident, loopholes present for incident occurrence, etc. During the assessment, it is important to assess the digital evidence in correlation with the scope of the case to decide the course of action.

- **Documentation and Reporting**

  Documenting is the process of writing all the actions the investigators have performed during the investigation to obtain the desired results. The investigators should meticulously organize and maintain the documentation, and submit it in court during trial. They need to document all the forensics processes applied to identify, gather, analyze, preserve, and report the evidence to present a well-founded report to a court of law and facilitate the prosecution.

- **Expert Witness Testimony**

  As the attorneys, prosecutors, and other parties present in a court of law may not be familiar with technical aspects regarding the crime, evidence, and losses, the

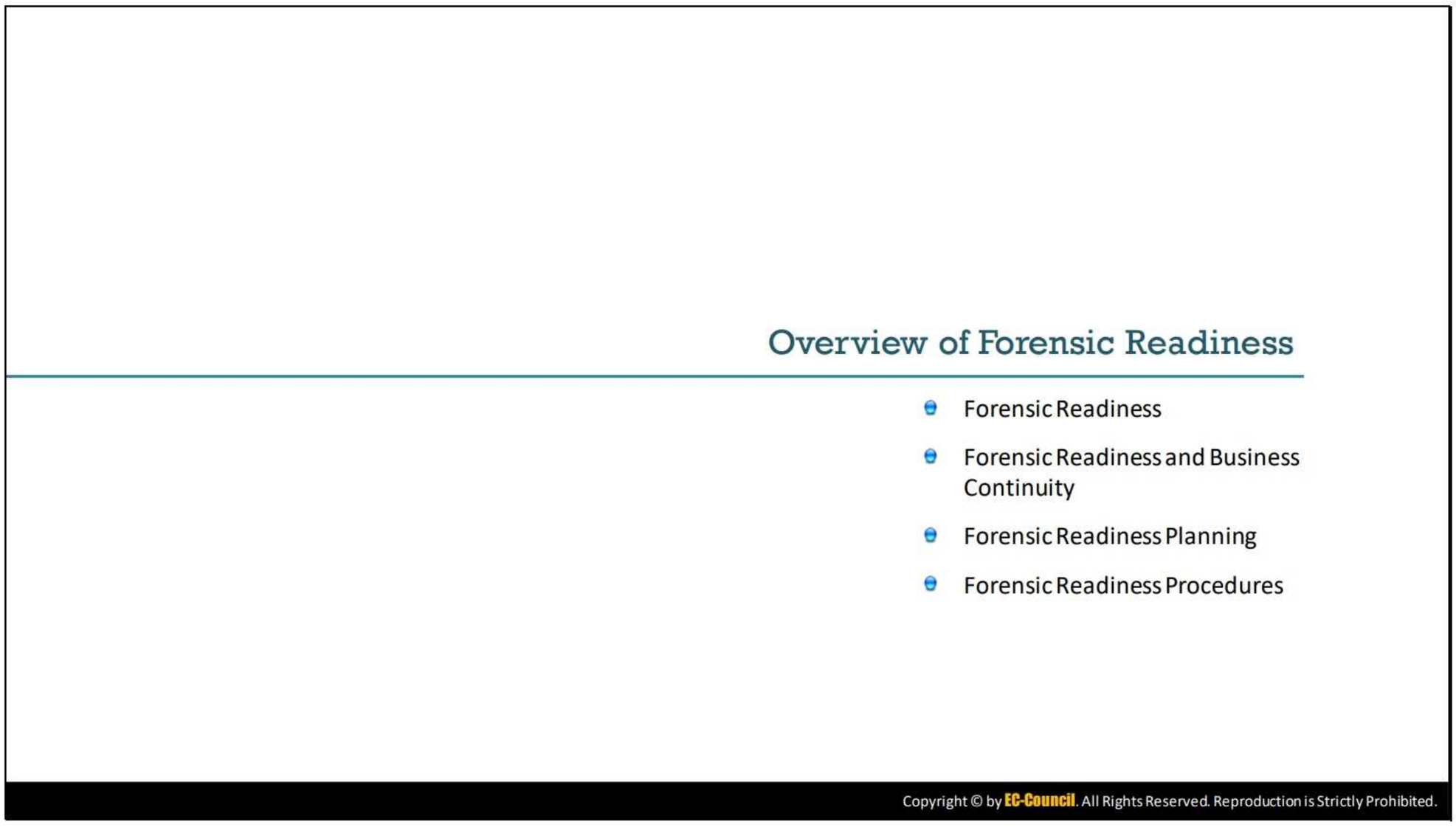
EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

investigators should approach authorized personnel who could appear in court to affirm the accuracy of the process and the data. An expert witness is a person who has a thorough knowledge of a subject and whose credentials can convince others to believe his or her opinions on that subject in a court of law.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



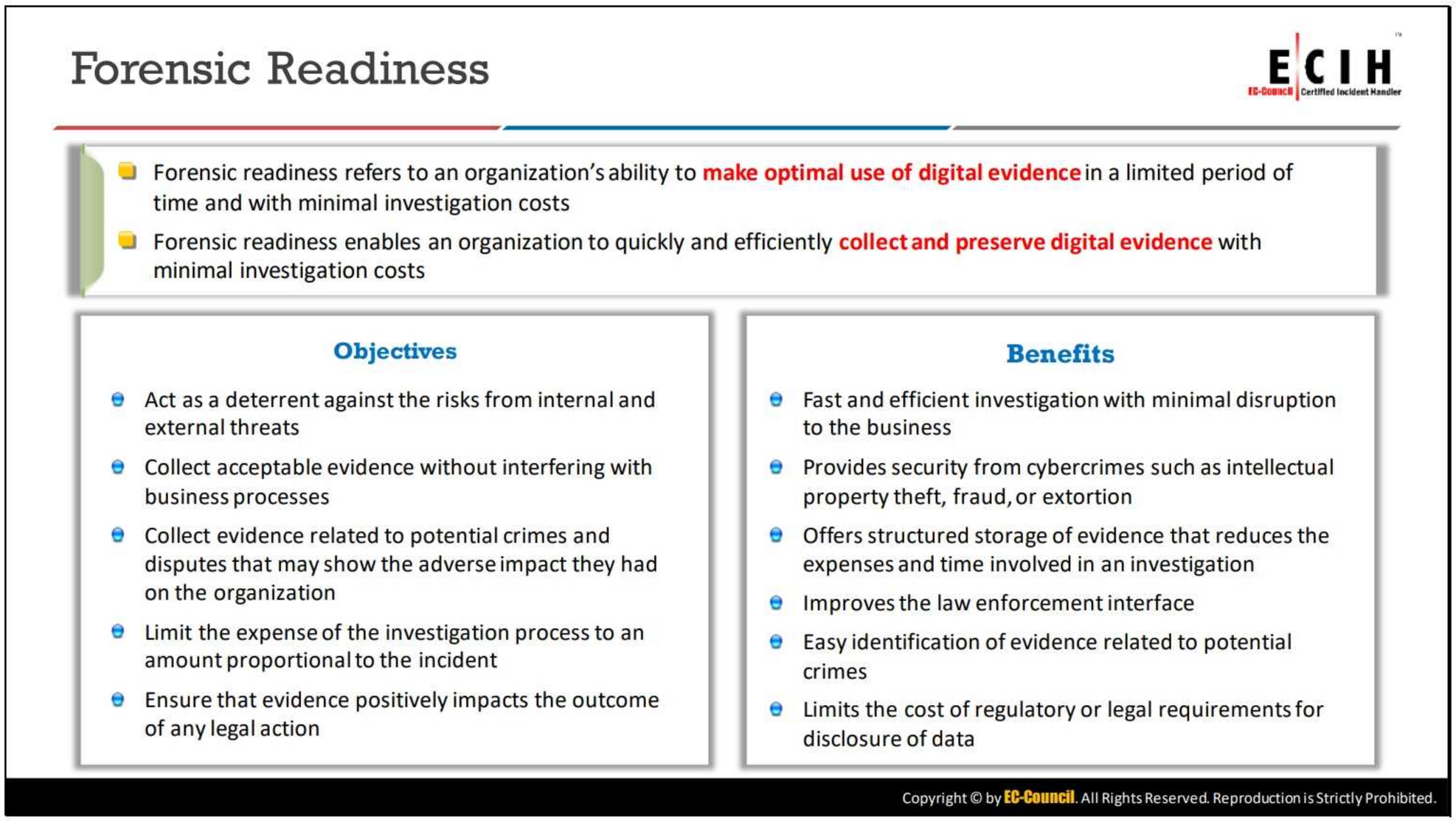
Overview of Forensic Readiness

In the current scenario, protecting critical IT assets from various cybersecurity attacks using different technical and security procedures is not sufficient. Organizations need to be well prepared to thwart the evolving cybersecurity threats. Forensic readiness helps organizations to improve their current cybersecurity posture, reduce the impact caused by security incidents, and assist security professionals in demonstrating that efficient and effective security measures have been taken to protect critical IT assets.

This section gives an overview of forensic readiness and business continuity, forensic readiness planning, and forensic readiness procedures.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness

Forensic readiness refers to an organization's ability to make optimal use of digital evidence in a limited period of time and with minimal investigation costs. It includes technical and nontechnical actions that maximize an organization's capability to use digital evidence.

Forensic readiness includes the establishment of specific incident response procedures and designated trained personnel to handle the procedures in case of a breach. It enables an organization to collect and preserve digital evidence quickly and efficiently with minimal investigation costs. Such a state of readiness along with an enforceable security policy helps the organization mitigate the risk of threat from employees and prepare preemptive measures. A forensically trained and well-prepared incident response team ensures proper reaction against any mishap and the ability to handle evidence according to proper legal procedures for possible use in a court of law.

An organization needs access to the actual digital evidence to support a proper forensics investigation process. The forensic readiness approach consists of those technical and nontechnical actions that maximize an organization's capability to use digital evidence. The focus of forensic readiness is to support the organization's need to use digital evidence.

Before discussing forensic readiness planning, it is important to understand the goals of forensic readiness, which are as follows:

- Act as a deterrent against the risks from internal and external threats
- Collect acceptable evidence in a forensically sound manner without interfering with the business processes
- Collect evidence focusing on potential crimes and disputes that may have an adverse impact on an organization

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

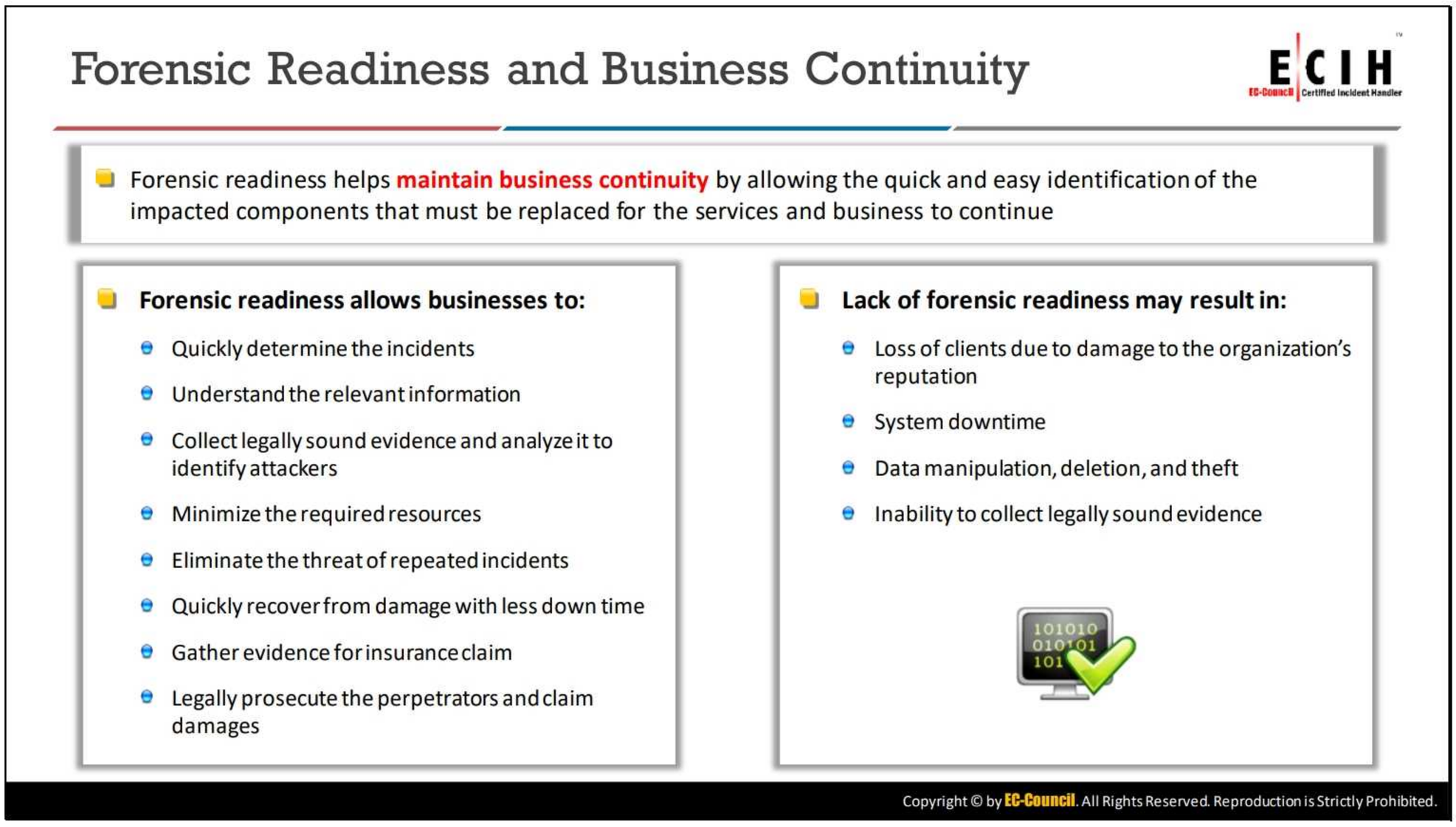
- Conduct an investigative process at a cost proportional to the incident
- Ensure that the evidence has a positive impact on the outcome of any legal action
- Extend the target of information security to the wider threats from cybercrime, such as intellectual property protection, fraud, or extortion

An incident response team that is forensically ready offers an organization the following benefits:

- Facilitates evidence gathering to act in the company's defense in case of a lawsuit
- Enables the use of comprehensive evidence collection to act as a deterrent to insider threat and processes all important evidence without fail
- Helps the organization conduct a fast and efficient investigation in the event of a major incident and take corresponding actions with minimal disruption to day-to-day business activities
- Facilitates a well-designed, fixed, and structured approach toward storage of evidence to reduce investigation expenses and time, and simultaneously preserve the all-important chain of custody
- Establishes a structured approach toward storage of all digital information, which not only reduces the cost of any court-ordered disclosure or regulatory/legal need to disclose data, but also fulfils requirements under federal law (for example, a response to a request for discovery under the Federal Rules of Civil Procedure)
- Extends the protection offered by an information security policy to cover wider threats of cybercrime, such as intellectual property protection, fraud, or extortion
- Demonstrates due diligence and good corporate governance of the company's information assets, as measured by the "Reasonable Man" standard
- Ensures that the investigation meets all regulatory requirements
- Improves upon and facilitates the interface with law enforcement
- Improves the prospects of successful legal action
- Provides evidence to resolve commercial or privacy disputes
- Supports employee sanctions up to and including termination based on digital evidence (for example, to prove violation of an acceptable-use policy)
- Helps prevent attackers from covering their tracks
- Limits the cost of regulatory or legal requirements for disclosure of data
- Helps avert similar attacks in the future

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness and Business Continuity

Incidents can impact and damage web servers, applications, systems, accounts, and networks critical for providing services to clients and customers, thus disrupting the business. Forensic readiness helps maintain business continuity by allowing quick and easy identification of the impacted components and replacing them to continue the services and business. It consists of technical and nontechnical actions that maximize an organization's capability to use digital evidence.

Forensic readiness allows businesses to:

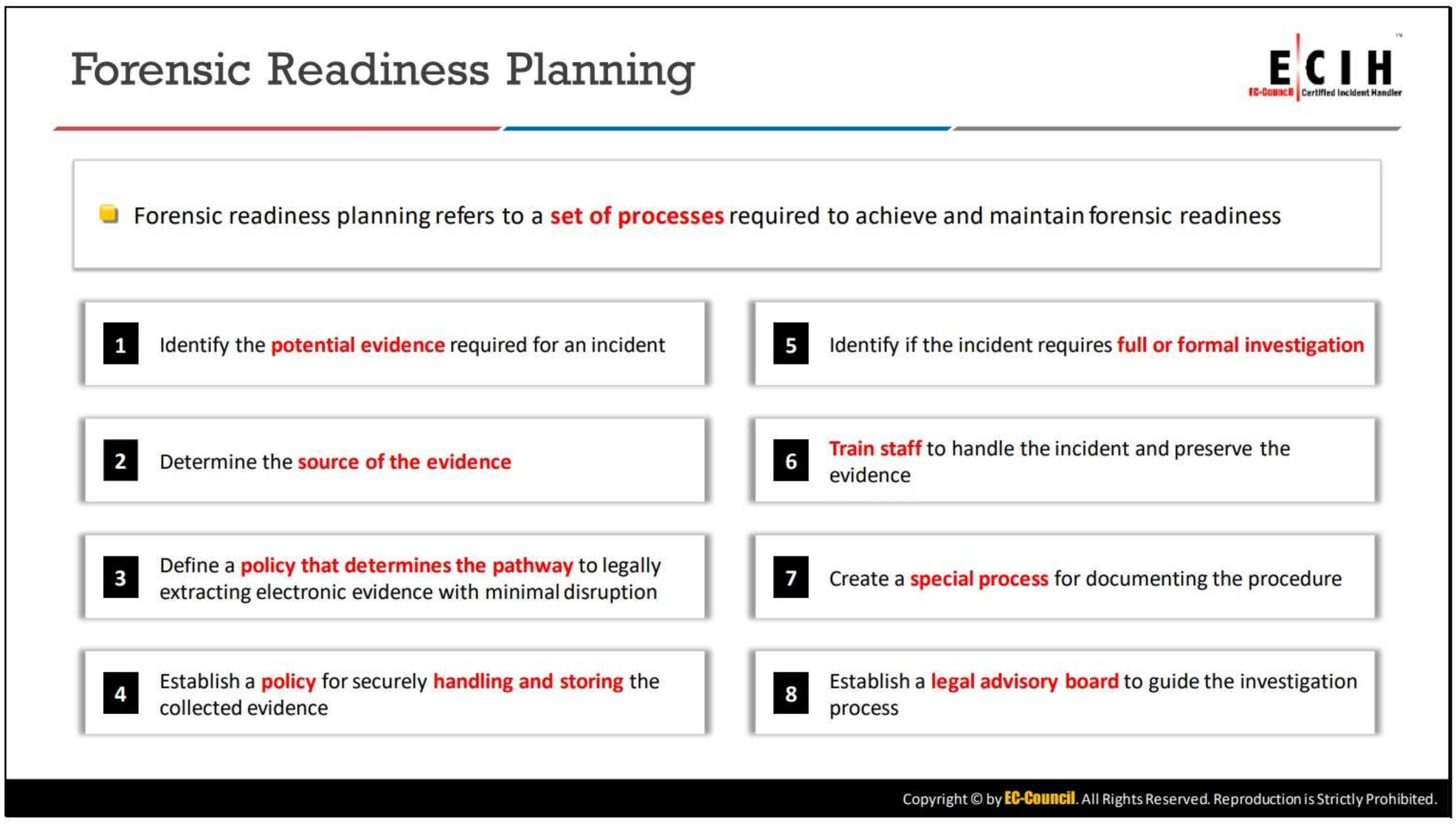
- Quickly determine the incidents
- Understand relevant information
- Collect legally sound evidence and analyze it to identify attackers
- Minimize the required resources
- Eliminate the threat of repeated incidents
- Quickly recover from damage with less down time
- Gather evidence required to claim insurance
- Legally prosecute the perpetrators and claim damages

Lack of forensic readiness causes:

- Loss of clients owing to the organization's damaged reputation
- System downtime
- Data manipulation, deletion, and theft
- Inability to collect legally sound evidence

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Planning

Forensic readiness planning refers to a set of processes required to achieve and maintain forensic readiness. It is the process of building a structure that enables an organization to deal with legal procedures following a criminal offense. This structure equips the organization to properly deal with incidents and evidence, while covering every aspect of the criminal procedure.

The following steps describe the key activities in forensic readiness planning:

- **Identify the potential evidence required for an incident**

  Define the purpose of evidence collection, gather information to determine evidence sources that can help deal with the crime, and design the best methods of collection. Produce an evidence requirement statement in collaboration with personnel responsible for managing the business risk and those operating and monitoring the information systems. Possible evidence files include IT audit and device logs, network logs, and system data.

- **Determine the source of the evidence**

  Forensic readiness should include knowledge of all the sources of potential evidence. Determine what currently happens to the potential evidence data and its impact on the business while retrieving the information.

- **Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption**

  Devise a strategy to collect evidence from all the relevant sources and preserve it in a legally sound manner, while causing minimal disruption to the work.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Establish a policy for securely handling and storing the collected evidence**

  Secure the collected evidence in such that it is available for retrieval whenever required in the future. Define a policy for safe storage and management of potential evidence as well as define security measures to protect data legitimacy and evidence integrity whenever someone tries to access, use, move, or store additional digital information. In the parlance of incident responders, this is the process of continuity of evidence in the United Kingdom and chain of custody in the United States. Document the records of those who had access to the evidence.

- **Identify if the incident requires full or formal investigation**

  Incidents are of different types. Evaluate the event to determine if it requires a full or formal investigation, or can be disregarded based on its impact on the business. Escalate an incident only if it has a major impact on business continuity.

  Therefore, any escalation to a full or formal investigation must be justified as it consumes resources as well as time.

- **Train the staff to handle the incident and preserve the evidence**

  Incident management requires a strong and well-qualified workforce; therefore, ensure that the staff has obtained the appropriate training required for fulfilling their roles. It is also necessary to ensure that staff members are competent to perform any role related to the handling and preservation of evidence.

- **Create a special process for documenting the procedure**

  A special documentation process is necessary to answer certain questions as well as support the findings. Documenting the complete process will also help in rechecking the investigation process if it yields false results and provide a backup for future reference. It will also help present the evidence in a court of law.

- **Establish a legal advisory board to guide the investigation process**

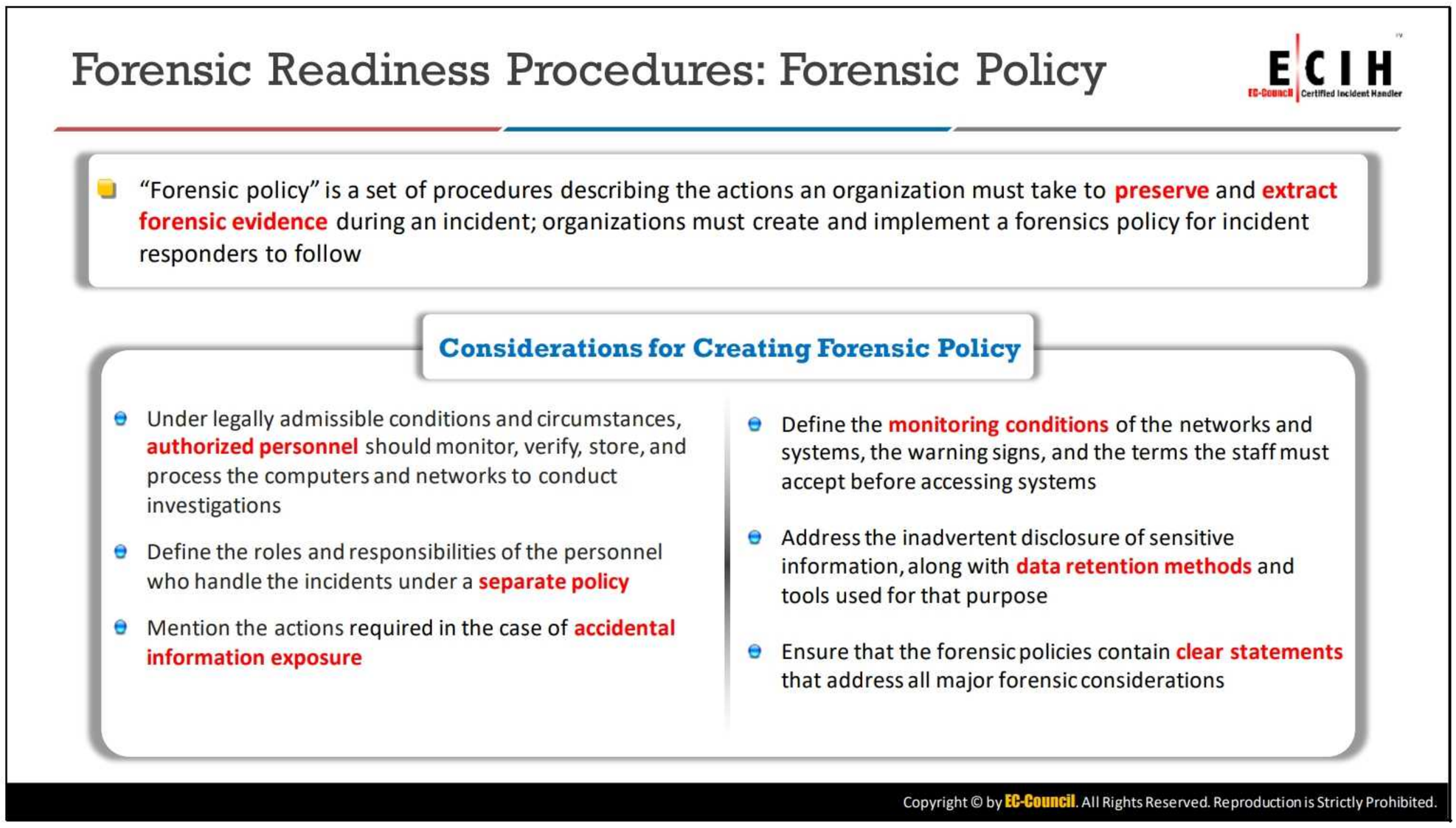
  All investigation processes should have a legal stance, and the organization should seek legal advice before taking any action on the incident. This is because some incidents may damage the company's reputation. Form a legal advisory board consisting of experienced personnel who understand the company's stance and can provide sound advice on the strength of the case and suggest further action.

  The legal advisory board will help the organization to:

  - Manage any dangers arising from the incident
  - File the incident legally and ensure proper prosecution
  - Understand legal and regulatory constraints, and suggest necessary action
  - Handle processes such as reputation protection and PR issues
  - Design legal agreements with partners, customers, investors, and employees
  - Investigate the company's commercial and civil disputes

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Procedures: Forensic Policy

A forensics policy will set guidelines for the employees, investigating personnel, and authorities to contribute to the forensics investigation process. It is a set of procedures describing the actions an organization must take to preserve and extract forensic evidence during an incident. Organizations must create a forensics policy and implement it for the incident responders to follow. In organizations, the Chief Information Security Officer (CISO) will be responsible for setting proper guidelines in association with other security and audit personnel.

While creating a forensic policy, organizations must consider incorporating the following points:

- Under legally admissible conditions and circumstances, authorized personnel should monitor, verify, store, and process the computers and networks to conduct investigations.
- Define the roles and responsibilities of the personnel who handle the incidents under a separate policy. The personnel should be aware of the forensic policy.
- Outline roles and responsibilities, including the behavior and activities of every person involved in the process of computer forensics. The policy should contain the duties that individuals must perform and those to avoid. It must specify the use of tools and the extent to which they can be used.
- Define the actions required to be performed during accidental information exposure.
- Define the monitoring conditions of the networks and systems, the warning signs, and terms the staff must accept before accessing systems.
- Address the inadvertent disclosure of sensitive information, along with data retention methods and tools used for that purpose.

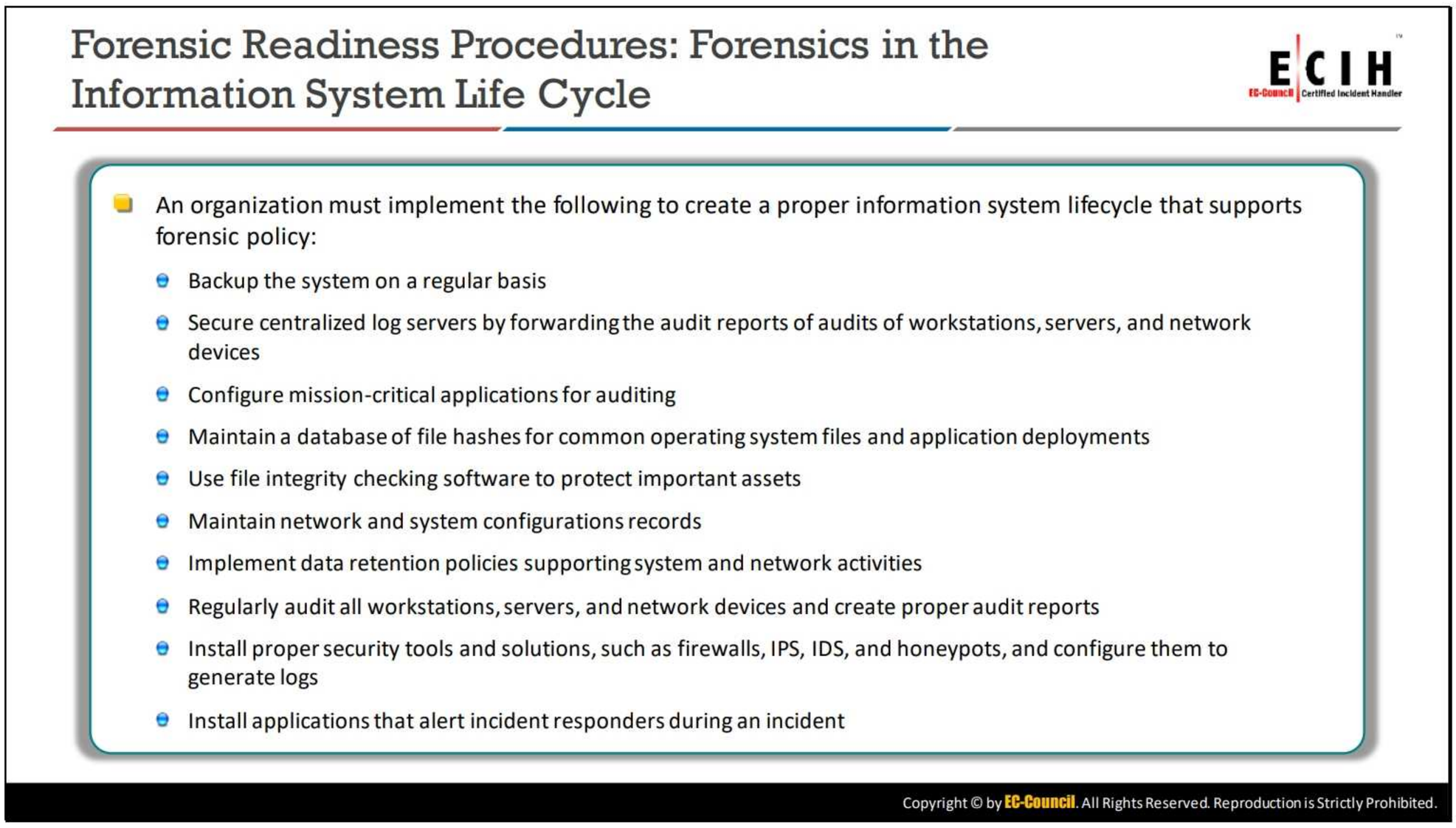
EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Define what actions should and should not be performed under normal and special conditions during incidents
- Ensure that forensic policies contain clear statements that address all major forensic considerations
- Determine the points of contact (POCs) during an incident
- Ensure that authorized personnel monitor systems and networks, perform forensic investigations, and assume custody of the physical and digital evidence
- Ensure that the forensic policy is consistent with other security policies in an organization

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Procedures: Forensics in the Information System Life Cycle

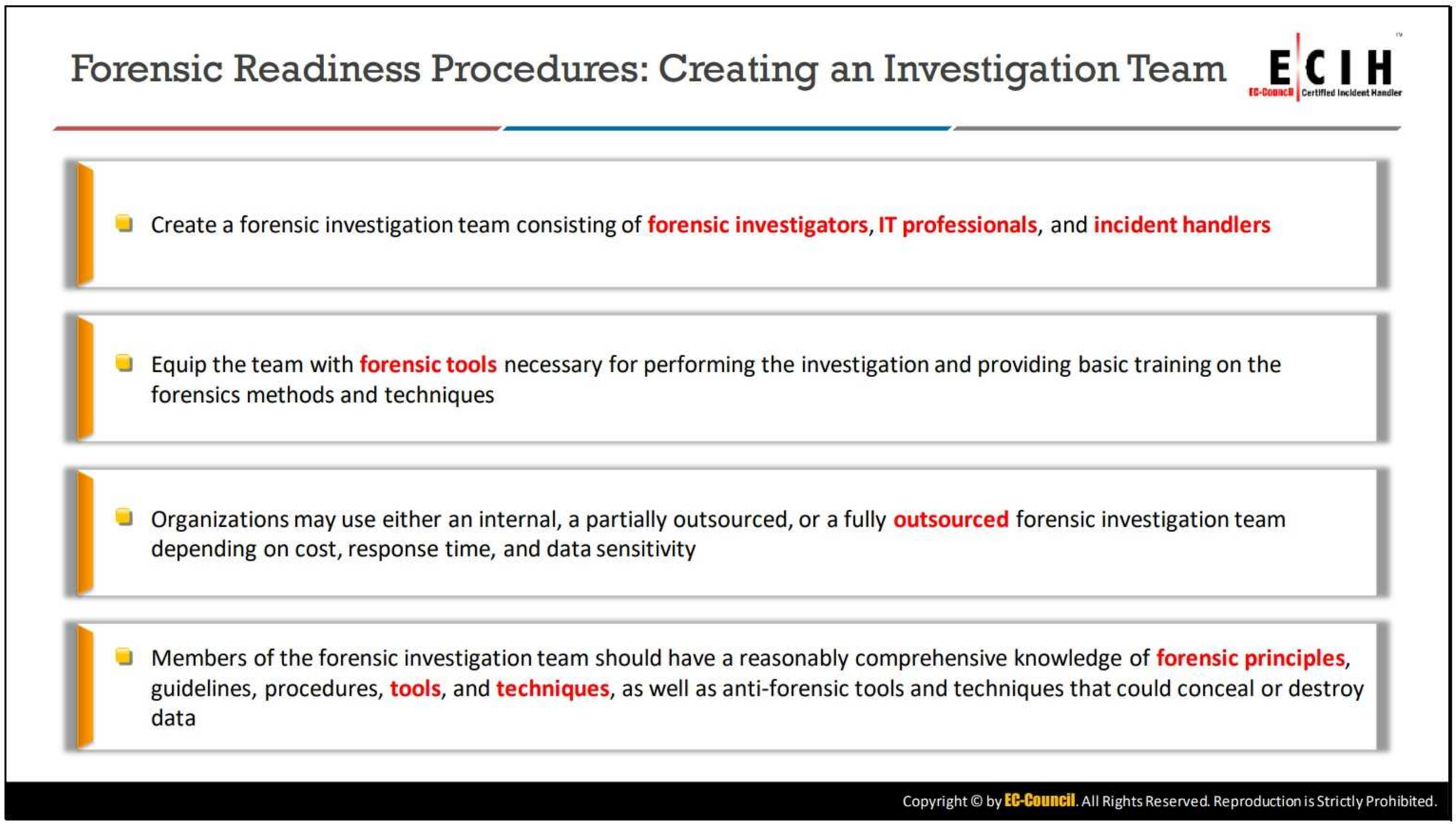
To efficiently handle the numerous incidents that an organization might encounter, it is essential that forensic considerations be incorporated into the existing information system life cycle. Some example considerations are provided below:

- Maintain a backup of the system on a regular basis
- To secure centralized log servers, forward audit reports by auditing the workstations, servers, and network devices
- Configure mission-critical applications for auditing
- Maintain a database of file hashes for the common operating system files and application deployments
- Use the file integrity checking software for protecting important assets
- Maintain network and system configurations records
- Implement data retention policies supporting system and network activities
- Regularly audit all workstations, servers, and network devices and create proper audit reports
- Install proper security tools and solutions, such as firewall, IPS, IDS, and honeypots, and configure them to generate logs
- Install applications that alert the incident responders during an incident

These considerations must be present in documents related to that specific domain, not in the overall centralized forensic policy, as they deal with the provisions for the existing policies and procedures in an organization.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Procedures: Creating an Investigation Team

The investigation team plays a major role in solving a case and is responsible for evaluating the crime, evidence, and criminals. The organization must assign specific tasks to every investigation team member based on their knowledge, skills, and abilities to make the process efficient.

The guidelines for building the investigation team are as follows:

- Create a forensic investigation team consisting of forensic investigators, IT professionals, and incident handlers
- Equip the team with forensic tools necessary for performing the investigation and provide basic training on forensic methods and techniques
- Use an internal, partially outsourced, or fully outsourced forensic investigation team considering cost, response time, and data sensitivity
- Ensure members of the forensic investigation team have a reasonably comprehensive knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as anti-forensic tools and techniques that could conceal or destroy data
- Ensure members of the forensic investigation team are trained on existing and emerging security threats
- Determine the person who should respond to an incident for a successful internal computer investigation
- Organize the team members and assign responsibilities to each member of the team
- Appoint a person as a technical lead among the team members

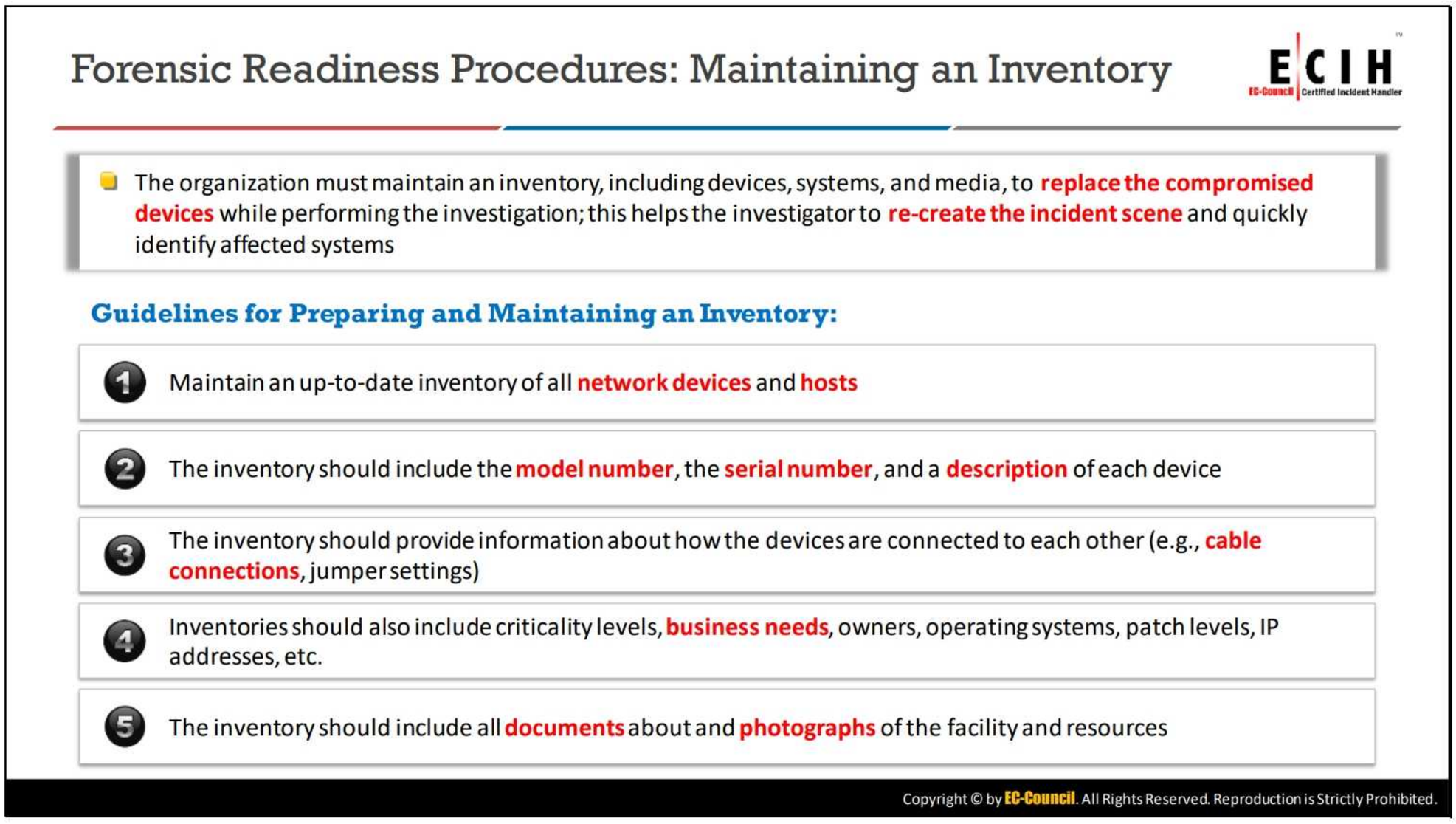
EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Limit the investigation team size to achieve confidentiality and avoid leakage of information
- Ensure each member of the team has the necessary clearance and authorization to complete assigned tasks
- Enlist help from a trusted external investigation team, if required

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Procedures: Maintaining an Inventory

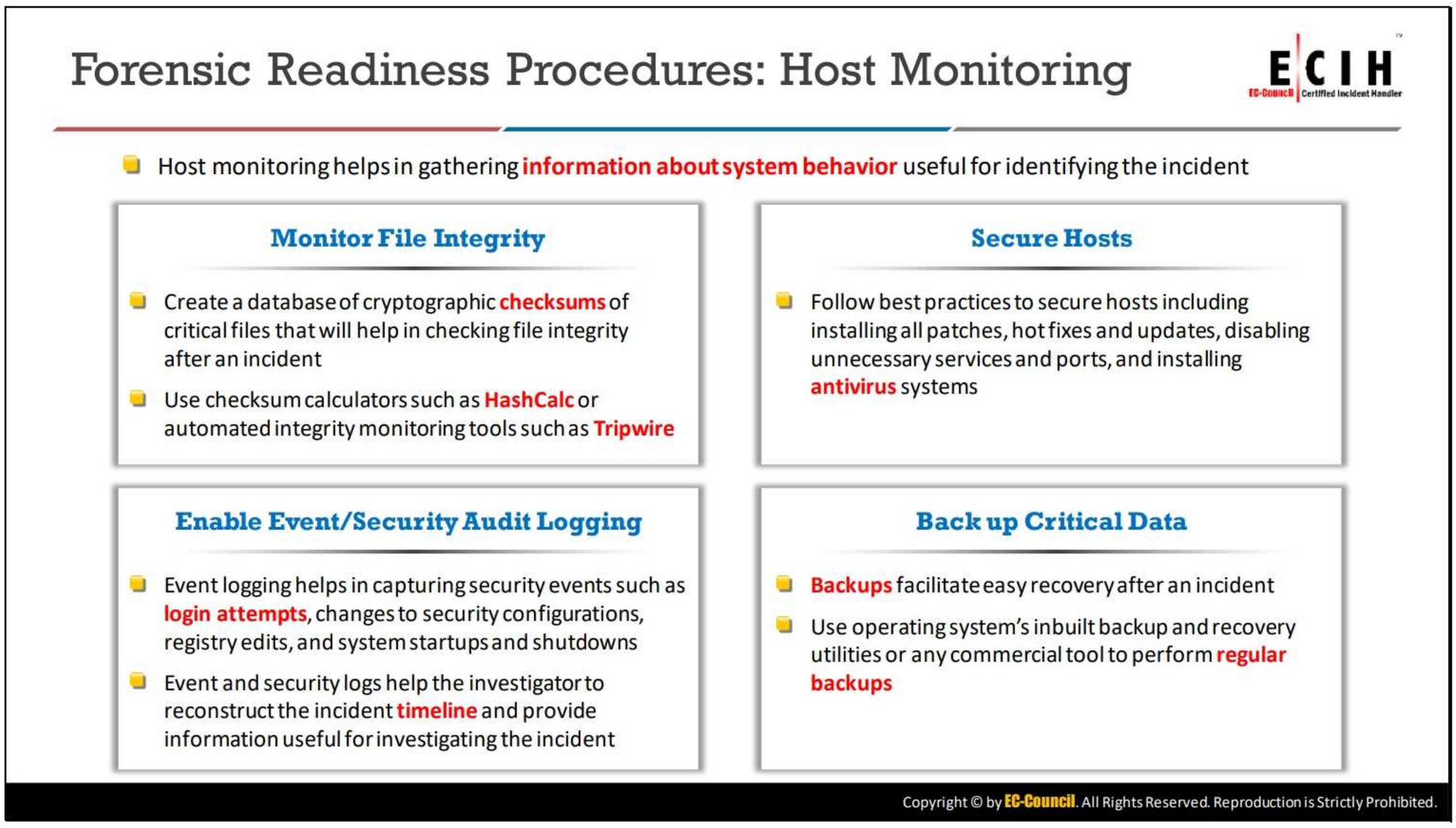
While the investigation is being performed, the organization must maintain an inventory, including devices, systems, and media, to replace the compromised devices. This helps investigators to recreate the incident scene and quickly identify the affected systems.

The guidelines for preparing and maintaining an inventory are as follows:

- Ensure that an up-to-date inventory of all network devices and hosts is maintained
- Ensure that the inventory should include the model number, serial number, and description of all the devices
- Provide information about how the devices are connected to each other (for example, cable connections, jumper settings)
- Ensure that inventories also include criticality levels, business needs, owners, operating systems, patch levels, IP addresses, etc.
- Include all the documents and photographs of the facility with all the resources in the inventory

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



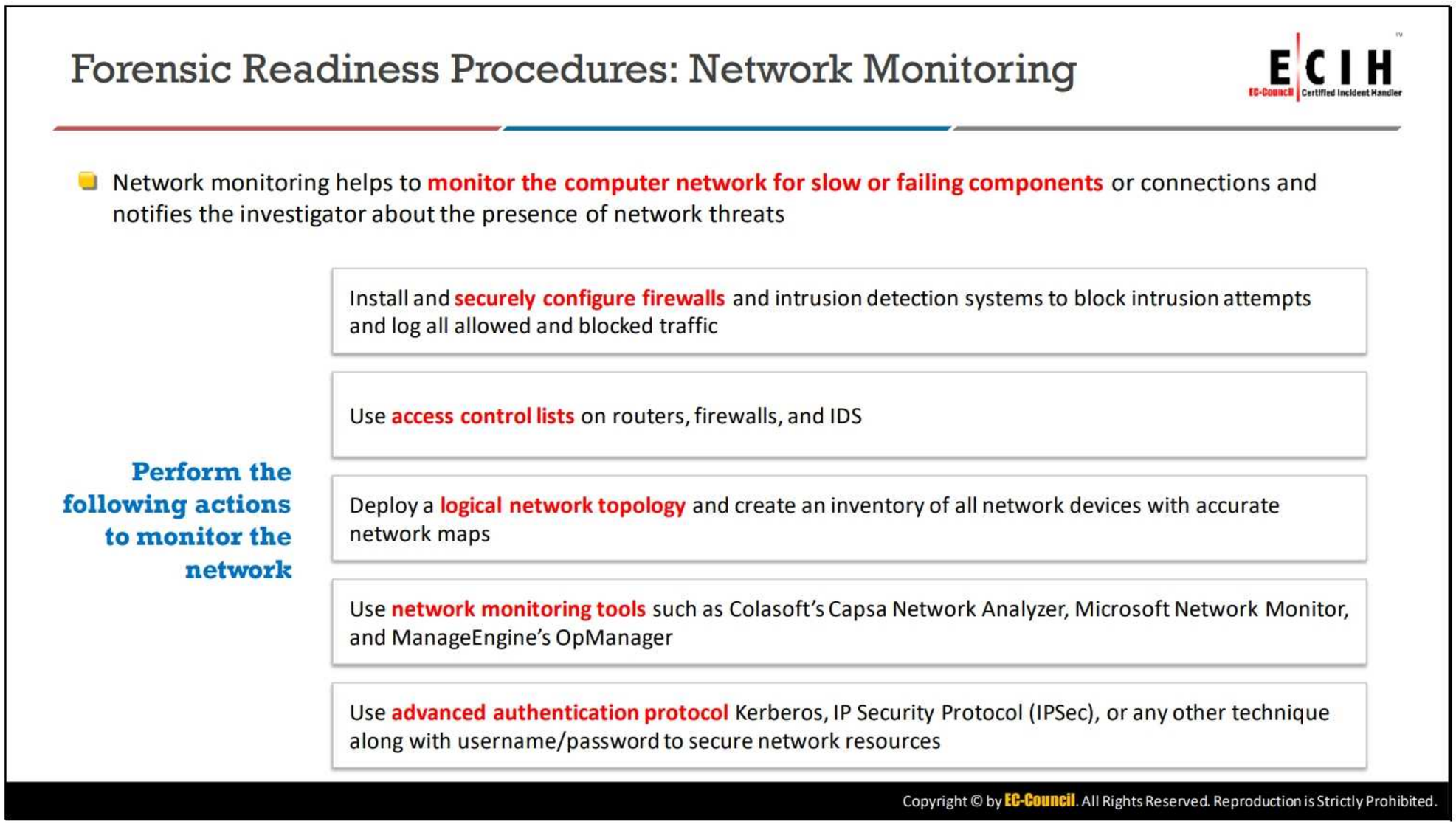
Forensic Readiness Procedures: Host Monitoring

Host monitoring helps in gathering useful information about the system behavior used to identify the incident. It includes the following tasks:

- **Monitor the integrity of critical files**
  - Create a database of cryptographic checksums of critical files that will help in checking the integrity of files after an incident
  - Incident responders can use checksum calculators such as HashCalc or automated integrity monitoring tools such as Tripwire
- **Increase or enable event and security audit logging**
  - Event logging helps in capturing security events such as login attempts, changes to security configurations, registry edits, system startups and shutdowns, and elevated privileges
  - Event and security logs help investigators to reconstruct the incident timeline and provide useful information to investigate the incident
- **Secure hosts**
  - Follow best practices to secure hosts, including installing all patches, hot fixes, and updates, disabling unnecessary services and ports, and installing antivirus systems
- **Back up critical data**
  - Backups facilitate an easy recovery after an incident
  - Organizations can use an operating system's built-in backup and recovery utilities or a commercial tool to perform regular backups

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensic Readiness Procedures: Network Monitoring

Network monitoring helps to monitor the computer network for slow or failing components or connections and notifies the investigator about the presence of network threats.

The investigator may perform the following actions to monitor the network for threats:

- Install and securely configure firewalls and IDSs to block intrusion attempts, and log all allowed and blocked traffic
- Use access control lists on routers, firewalls, and IDSs
- Deploy a logical network topology, and create an inventory of all network devices with accurate network maps
- Use network monitoring tools such as Colasoft's Capsa Network Analyzer, Microsoft Network Monitor, and ManageEngine's OpManager
- Use advanced authentication protocol Kerberos, IP Security Protocol (IPSec), or any other technique along with username/password to secure network resources
- Encrypt network traffic using Secure Sockets Layer (SSL) and Secure Shell (SSH) protocols

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

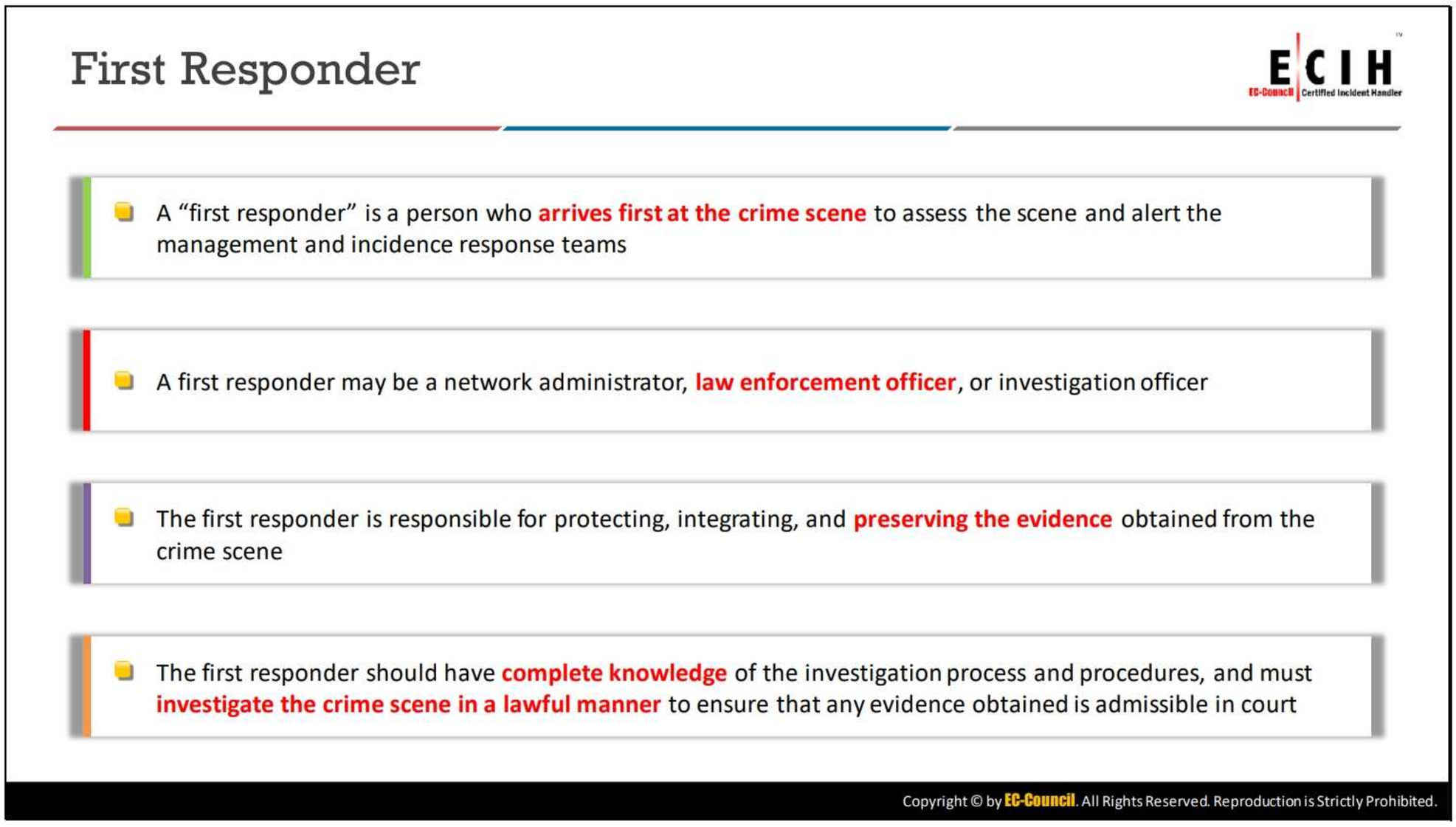
Overview of First Response

First response refers to the first action performed after the occurrence of a security incident. Depending on the type of breach or attack, the first response can prevent further damage to the victim and help incident responders to easily trace the suspect. It involves identifying victim systems and individuals to chart the next course of action.

This section discusses the first response, first response basics, roles of the first responder, first responder common mistakes, and incident response in different situations.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



First Responder

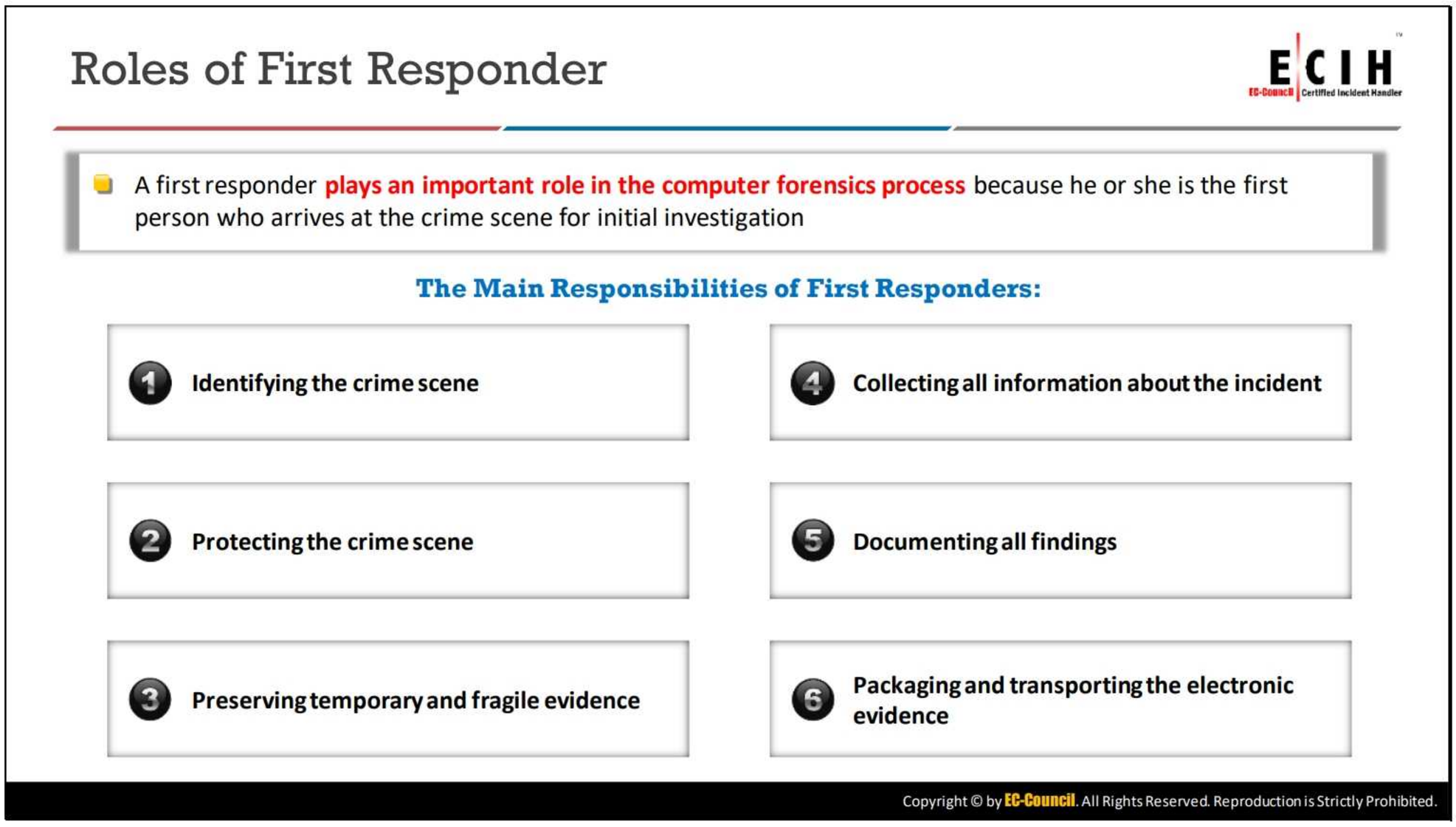
The term "first responder" refers to the person who is the first to arrive at the crime scene to assess the scene and alert the management and incident response teams. A first responder may be a network administrator, system administrator, law enforcement officer, or investigation officer. Generally, a first responder is a person who comes from the forensics laboratory or from the particular agency at the crime scene for the initial investigation.

If an incident occurs in a company or on individual computers, the victim first contacts the forensics laboratory or a particular agency for crime investigation. Next, the laboratory or agency sends the first responder to the crime scene for the initial investigation. The first responder is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene.

The first responder has complete knowledge of computer forensics investigation. He or she preserves all discovered evidence in a simple, protected, and forensically sound manner. First responders investigate the crime scene in a lawful manner so that the obtained evidence will be acceptable in a court of law.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Roles of First Responder

A first responder plays an important role in the computer forensics process because he or she is the first person who arrives at the crime scene for the initial investigation. The investigation process starts after all the evidence has been collected from the crime scene. If the evidence collected by the first responder is forensically sound, it is easier for the investigation team to find the actual cause of the crime. Therefore, it is important for the first responder to collect the proper evidence.

The main responsibilities of first responders are:

- **Identifying the crime scene**

  After arriving at the crime scene, the first responder identifies the scope of the crime scene and establishes a perimeter. Establishing a perimeter includes identifying a particular area, room, several rooms, or a building that is dependent on the networked computers. After that, the first responder begins listing the computer systems that are involved in the incident from which he or she can collect the evidence.

- **Protecting the crime scene**

  In a cybercrime case, a search warrant is required for searching and seizing digital/electronic evidence. Therefore, a first responder protects all the computers and electronic devices and waits for the case officer in charge.

- **Preserving temporary and fragile evidence**

  In the case of temporary and fragile evidence that could change or disappear, such as monitor/screen information or a running program, the first responder does not wait for the case officer in charge. He or she takes photographs of all the evidence.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Collecting complete information about the incident**

  In collecting the complete information about the incident, the first responder conducts preliminary interviews of all persons present at the crime scene and asks questions about the incident.

- **Documenting all findings**

  The first responder documents all information about the collected evidence in the chain of custody document sheet. The chain of custody document sheet contains information such as case number, name of the person who reported the case, address and telephone number, location of the evidence, date/time of evidence collection, and a complete description of the evidence.

- **Packaging and transporting the electronic evidence**

  After collecting the evidence, the first responder labels all the evidence and places it in evidence storage bags, which protect the evidence from sunlight and high temperature. These bags also block wireless signals so that wireless devices cannot acquire data from the evidence. Next, the first responder transports these packed bags to the forensics laboratory.

- **Gathering preliminary information at the scene**

  At the time of an incident, the first responder secures the crime scene and the surrounding area to avoid any tampering of the evidence. Preliminary information at the crime scene provides the basis for the forensics investigation and facilitates in finding the evidence if there is no third-party interference at the incident scene.

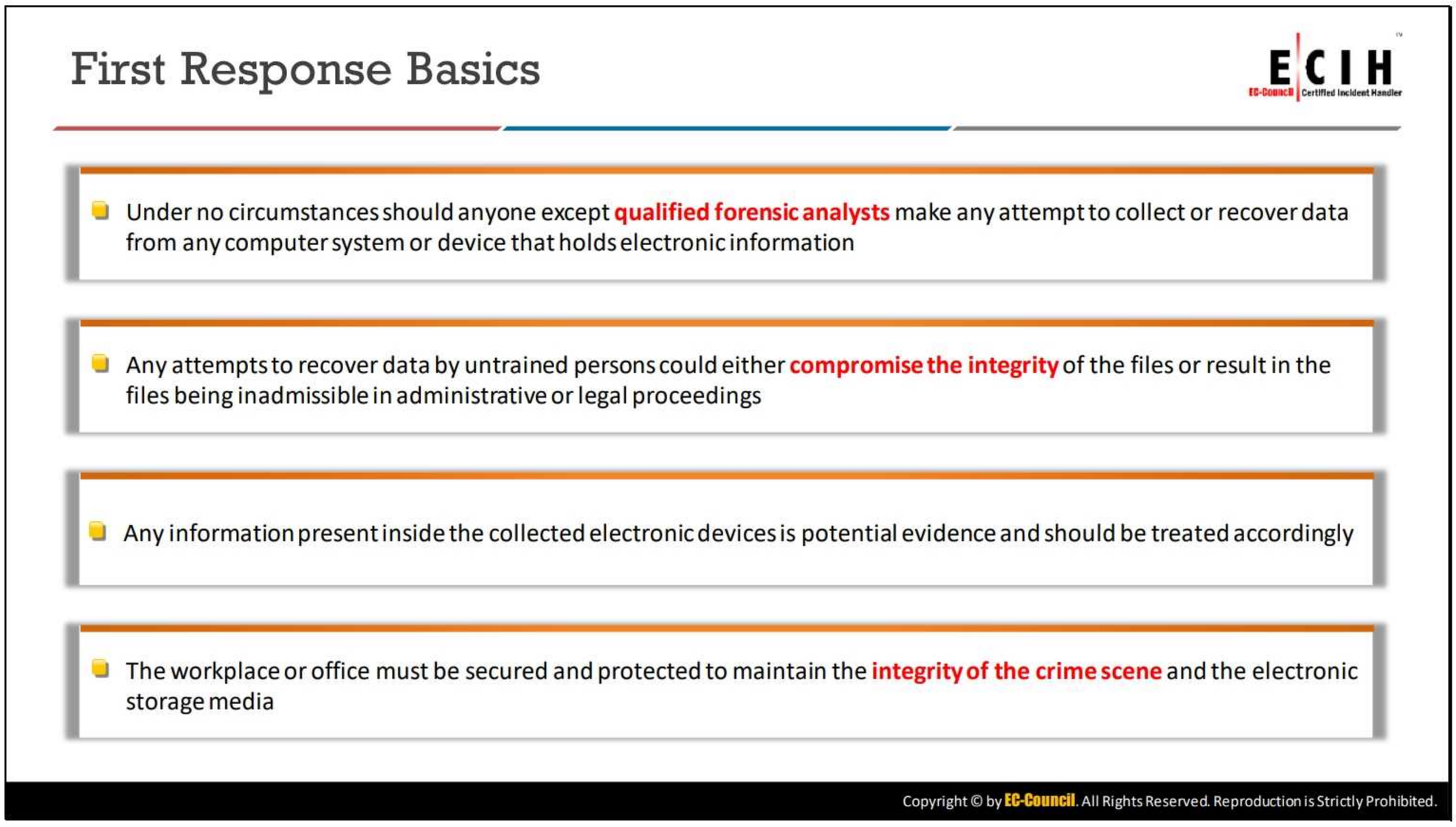
Preliminary information helps the incident responders/investigators to verify if the crime had occurred, nature of the incident, mark the perimeter, estimate the case process and expenditure, as well as gather knowledge of the plaintiff.

The preliminary information at the incident scene offers the following details:

- Type of incident
- Reason for the occurrence of the incident
- Potential damage caused by the incident
- Potential evidence from scattered objects outside the attacked system
- Details of the person who last used the system before the incident
- People who first knew about the incident's occurrence

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



First Response Basics

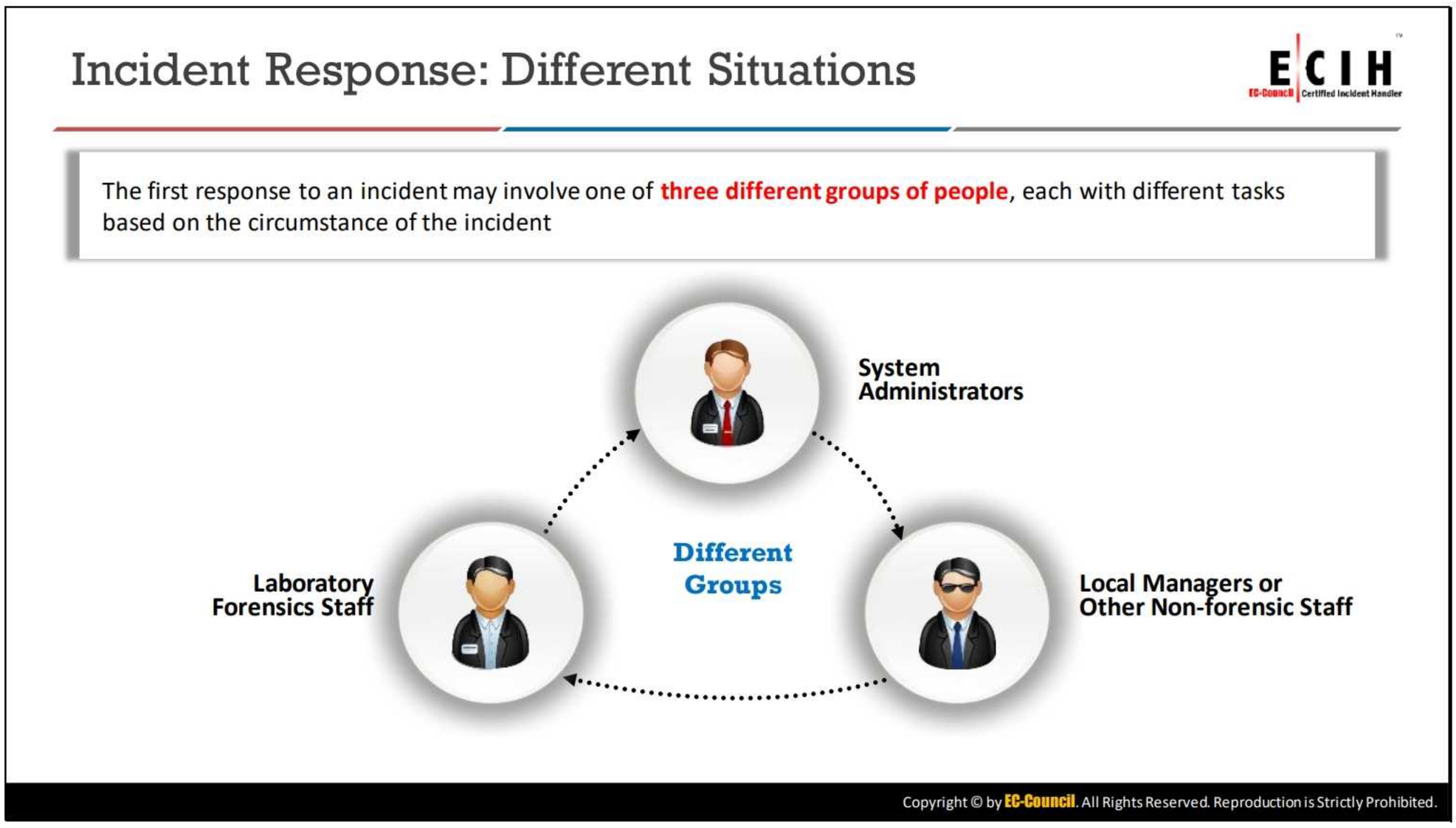
The success of any incident response investigation depends upon how an on-site first responder handles the situation. He/she must act quickly and make appropriate decisions based on the severity of the impact that the incident has on the organization's assets and various other information.

Some rules that the first responders must follow during a computer incident, are as follows:

- Under no circumstances should anyone except qualified forensic analysts attempt to collect or recover data from any computer system or device that holds electronic information
- Any attempts to recover data by untrained persons could either compromise the integrity of the files or result in the files being inadmissible in administrative or legal proceedings
- Any information present inside the collected electronic devices is potential evidence and should be treated accordingly
- The workplace or office must be secured and protected to maintain the integrity of the crime scene and the electronic storage media

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Incident Response: Different Situations

The activity the first responder performs at the incident location has a great impact on the investigation process and can influence the accuracy or the success of the investigation procedure. Therefore, investigation firms must be careful when selecting the first response team for an incident.

The first response to an incident may involve one of three different groups of people, each having different tasks based on the circumstances of the incident:

- **System Administrators**

  The system administrator's role is very important in ensuring network security and maintenance as well as investigating the security breach. The admin is responsible for monitoring and maintenance of the system, and these activities can become the basis for the investigation during the forensic evaluation and administrative actions.

  Once a system administrator discovers an incident, he or she must report it according to the current organizational incident reporting procedures. He or she should then not touch the system, unless directed to by either the incident response team or duty manager or one of the forensic analysts assigned to the case.

  The system administrator should explain to the incident responder/investigator the security protocols and procedures followed for using the systems and storage media. The admin might have to appear for the legal proceedings to explain the measures taken during the initial shutdown or isolation of the subject computer.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Non-forensics Staff**

  Non-forensics staff is responsible for securing the crime scene and ensuring that it remains in a secure state until the forensics team advises otherwise. They should also take notes about the scene and those present to hand over to the attending forensics team. The surrounding area of a suspect computer should be secured, not just the computer itself.

- **Laboratory Forensics Staff**

  First response by laboratory forensics staff involves six stages:

  1. **Securing and evaluating the electronic crime scene**

     The process protects the crime scene from unauthorized access and keeps the evidence safe. First response by laboratory forensic staff in this stage involves the following considerations:

     - Obtaining a search warrant for search and seizure
     - Planning the search and seizure
     - Conducting the initial search of the scene
     - Addressing health and safety issues

  2. **Conducting preliminary interviews**

     This activity helps incident responders to identify all personnel, subjects, or others at the crime scene, along with their position at the time of entry and their reason for being at the crime scene. This stage involves:

     - Asking questions
     - Checking the consent issues
     - Witnessing signatures
     - Initialing interviews

  3. **Documenting the electronic crime scene**

     Documentation of the electronic crime scene is a continuous process during the investigation, resulting in a permanent record of the scene. Documentation includes:

     - Photographing the scene
     - Sketching the scene

  4. **Collecting and preserving electronic evidence**

     Electronic evidence is fragile in nature and easily lost or damaged. The staff should be cautious when:

     - Collecting evidence
     - Dealing with powered OFF/ON computers at the time of seizure

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Seizing portable computers
- Preserving electronic evidence

5. **Packaging electronic evidence**

   While packaging the collected electronic evidence, the staff must document and list all the evidence, and all containers should be properly labeled to seize the evidence. During packaging:

   - Follow exhibit numbering
   - Fill the panel on the front of evidence bags with the proper details
   - Avoid folding and scratching storage devices
   - Label the containers that hold the evidence in an appropriate manner

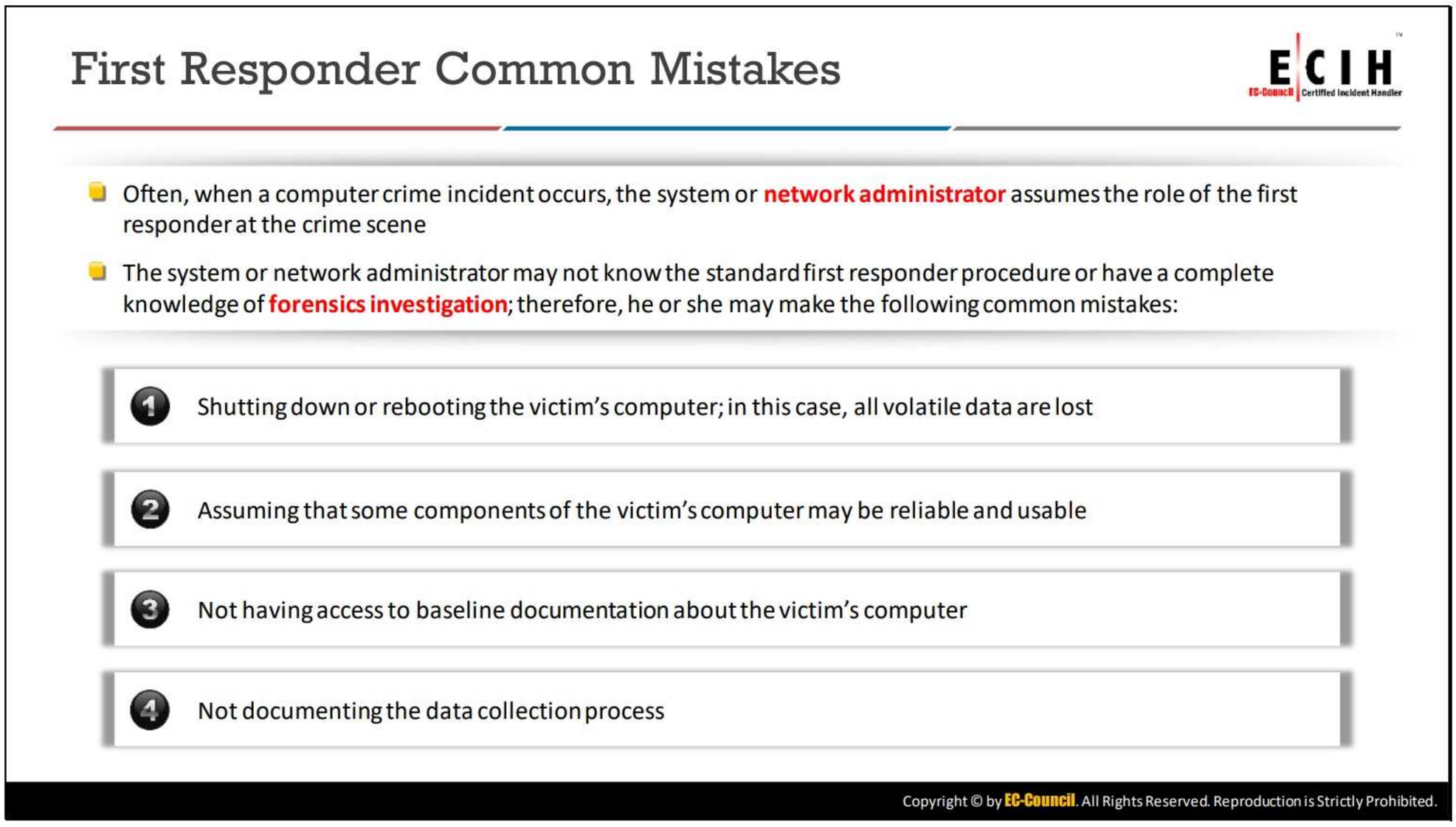
6. **Transporting electronic evidence**

   Incident responders/investigators should take special precautions for transporting the electronic evidence. Ensure proper transporting procedures are followed to avoid physical damage:

   - Ensure proper handling and transportation to the forensics laboratory
   - Have a strict chain of custody and keep track of all the forensics processes applied

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



First Responder Common Mistakes

Usually, when a computer crime incident occurs in an organization, a system or network administrator takes charge as a first responder at the crime scene because many organizations do not appoint a special forensic investigator for such types of incidents. The system or network administrator cannot properly handle computer crime security incidents because they do not know first responder procedures, or they do not have a complete knowledge of the forensic investigation process. In such cases, they make the following common mistakes:

- **Shutting down or rebooting the victim's computer**

  In this case, the system loses all volatile data, such as modified, accessed, or changed (MAC) time and log files, shuts down the running processes when shutting down and rebooting.

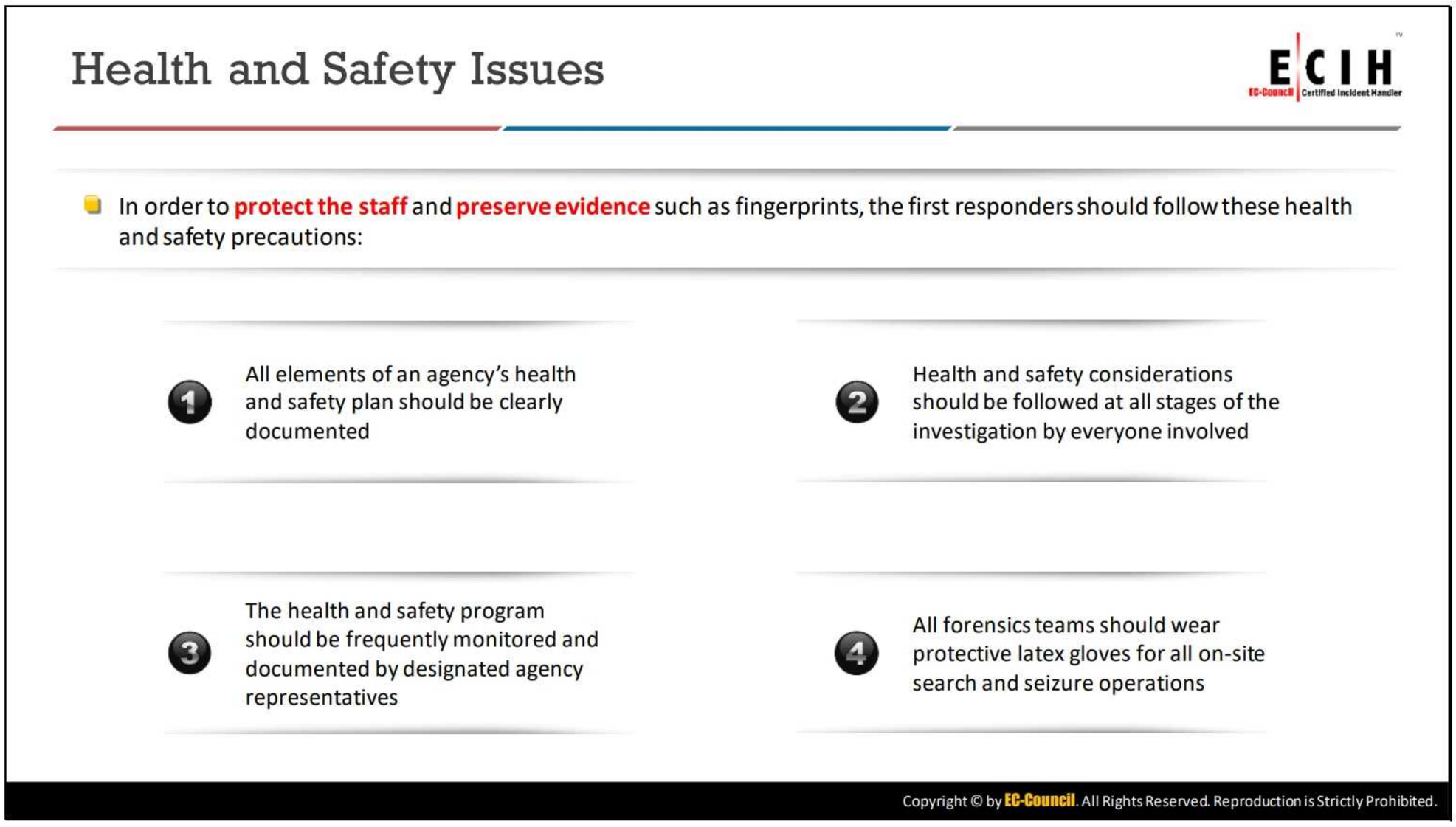
- **Assuming that some components of the victim's computer are reliable and usable**

  In this case, using certain commands on the victim's computer may activate Trojans, malware, and time bombs that delete vital volatile data.

- **Lacking access to baseline documentation about the victim's computer**
- **Failing to document the data collection process**

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Health and Safety Issues

To protect the staff and preserve evidence such as fingerprints, the first responders should follow these health and safety precautions:

- All elements of an agency's health and safety plan should be clearly documented
- Designated agency representatives should frequently monitor and document the health and safety program
- Everyone involved in the investigation of an incident must follow all health and safety considerations during the performance of all phases of incident handling, response, and forensic procedures
- Persons engaged in the inspection of different types of digital evidence should work according to the rules and policies of the agency
- Forensic teams should wear protective gloves for all on-site search and seize operations. This precaution protects the staff and preserves any fingerprints

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Securing the Crime Scene

- First responders must ensure the safety of all the individuals at the crime scene and protect the **integrity of the evidence**
- After arriving at the location, first responders must move to the **scene of the incident** and identify the victim devices, networks, etc. and mark the perimeter around them
- Some best practices for securing a crime scene include:
  1. Follow the standard procedures and policies of the legal authority while securing the scene
  2. Make sure the scene is safe for the responders
  3. Verify the type of incident
  4. Secure all electronic devices, including personal or portable devices
  5. Verify any data related to the offense
  6. Remove all persons from the crime scene or the area containing evidence

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Securing the Crime Scene (Cont'd)

7	Do not allow any individual to access the scene or electronic devices	14	Protect and preserve the evidence that is at risk of being easily lost
8	Deny any offer of help or technical assistance	15	Physically and electronically protect perishable data (e.g., pagers and caller ID boxes)
9	Isolate other persons who are present at the scene	16	Make sure that the devices that contain perishable data are secured, documented, and photographed
10	Locate and help the victim	17	Find telephone lines that are connected to devices such as modems and caller ID boxes
11	Transmit additional flash messages to other responding units	18	Document, disconnect, and label telephone lines and network cables
12	Request additional help at the scene if needed	19	Observe the current situation at the scene, and record observations
13	Establish a security perimeter to see if the offenders are still present at the crime scene area	20	Protect physical evidence or hidden fingerprints that may be found on keyboards, mice, diskettes, and DVDs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Securing the Crime Scene

First responders must ensure the safety of all the individuals at the crime scene as well as protect the integrity of the evidence. After arriving at the location, the first responders must move to the scene of the incident and identify the victim devices, networks, etc. and mark a perimeter.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Some best practices to secure the crime scene are as follows:

- Follow standard procedures and policies of the legal authority while securing the scene
- Make sure that the scene is safe for the responders
- Verify the type of incident
- Secure all electronic devices, including personal or portable devices
- Verify any data that are related to the offense
- Remove all persons from the crime scene or the area containing evidence
- Do not allow any individual to access the scene or electronic devices
- Refuse any offer of help or technical assistance
- Isolate other persons who are present at the scene
- Locate and help the victim
- Transmit additional flash messages to other responding units
- Request additional help at the scene, if needed
- Establish a security perimeter to see if the offenders are still present at the crime scene area
- Protect and preserve the evidence that is at risk of being easily lost
- Protect perishable data (e.g., pagers and caller ID boxes) physically and electronically
- Ensure that devices containing perishable data are secured, documented, and photographed
- Locate telephone lines that are connected to devices, such as modems and caller ID boxes
- Document, disconnect, and label telephone lines and network cables
- Observe the current situation at the scene and record observations
- Protect physical evidence or hidden fingerprints that may be found on keyboards, mice, diskettes, and DVDs

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Collecting Incident Information

- Adhering to departmental policies and applicable laws, first responders must gather the following information about the victim devices and connected systems:
  - Actual holders and/or users of any electronic devices present at the crime scene
  - Web mail and social networking website account information
  - Usernames and Internet service providers
  - Passwords required to access the system, software, or data
  - Purpose of using the system
  - Automatic applications in use
  - Documents explaining the hardware or software installed on the system
  - Any off-site data storage
  - Unique security schemes or destructive devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Incident Information (Cont'd)

Conducting Preliminary Interviews

- The first responders must perform the following steps to gather information about the persons present at the crime scene:
  - Identify the persons present at the crime scene, conduct individual interviews, and note everyone's physical position and reason for being there
  - As part of the investigation process, determine if the incident was a criminal act, policy violation, or accident
  - If the suspect is present, ask questions that are compliant with the relevant human resources or **legislative guidelines** of the jurisdiction
  - During an initial interview, suspects are often taken off guard, having been given little time to create a false story. This means that they will often answer truthfully questions such as, "What are the passwords for the account?"
  - If the system administrator is present at the time of the initial interview, gather important information such as the number of systems involved, persons associated with a particular account, and relevant passwords
  - The first responders must take complete custody of the **physical evidence** to ensure its safety and security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Incident Information

While adhering to departmental policies and applicable laws, the first responders must collect the following information about the victim devices and connected systems:

- Identity of actual holders or users of any electronic devices present at the crime scene
- Web mail and social networking website account information

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

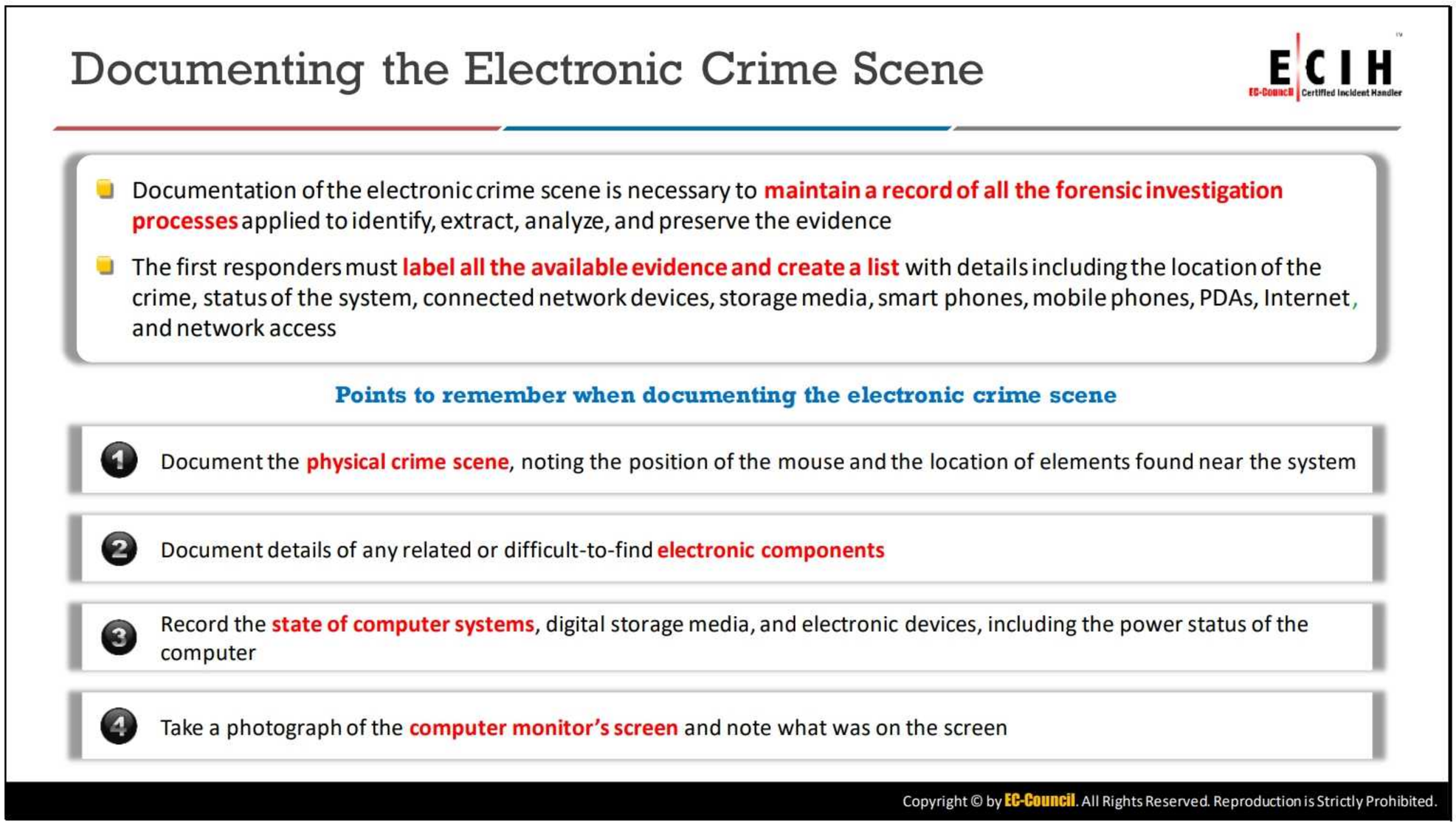
- Usernames and internet service providers
- Passwords required to access the system, software, or data
- Purpose of using the system
- Automatic applications in use
- Any offsite data storage
- Unique security schemes or destructive devices
- Documentation detailing installation of hardware or software on the system

The forensic team must conduct preliminary interviews to gather more evidence. As a part of their preliminary investigation, the first responders must perform the following steps to gather information about the persons present at the crime scene:

- Identify the persons present at the crime scene, conduct individual interviews, and note everyone's physical position and his or her reason for being there
- As part of the investigation process, determine if the incident was a criminal act, violation of policies, or accident
- If the suspect is present, ask questions that are compliant with the relevant human resources or legislative guidelines, with regard to the jurisdiction
- During an initial interview, suspects are often surprised, having been given little time to create a false story. This means that they will often answer questions such as, "What are the passwords for the account?" truthfully
- If the system administrator is present at the time of the initial interview, gather important information such as the number of systems involved, persons associated with an account, and the relevant passwords
- First responder must take complete custody of the physical evidence for its safety and security
- Whenever possible, evidence must be secured in such a way that only a person with complete authority is allowed access

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Documenting the Electronic Crime Scene

Documentation of the electronic crime scene is a continuous process during the investigation, resulting in a permanent record of the scene. Documenting the electronic crime scene is necessary to maintain a record of all the forensic investigation processes applied to identify, extract, analyze, and preserve the evidence. The first responders must comprehensively document the scene in detail. They must label all the available evidence and create a list with details, including crime location, system status, connected network devices, storage media, smartphones, mobile phones, PDAs, internet, and network access.

The document will help to trace the serial numbers or other identifiers of procured devices. Documenting also includes taking photographs, video, notes, and sketches of the scene to recreate it later.

The points to consider while documenting the electronic crime scene are:

- Document the physical crime scene, noting the position of the mouse and the location of the elements found near the system
- Document details of any related, difficult to find electronic components
- Record the state of the computer system, digital storage media, electronic devices, and predictable evidence, including power status of the computer
- Take a photograph of the computer monitor's screen and write notes on what was observed on the screen

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

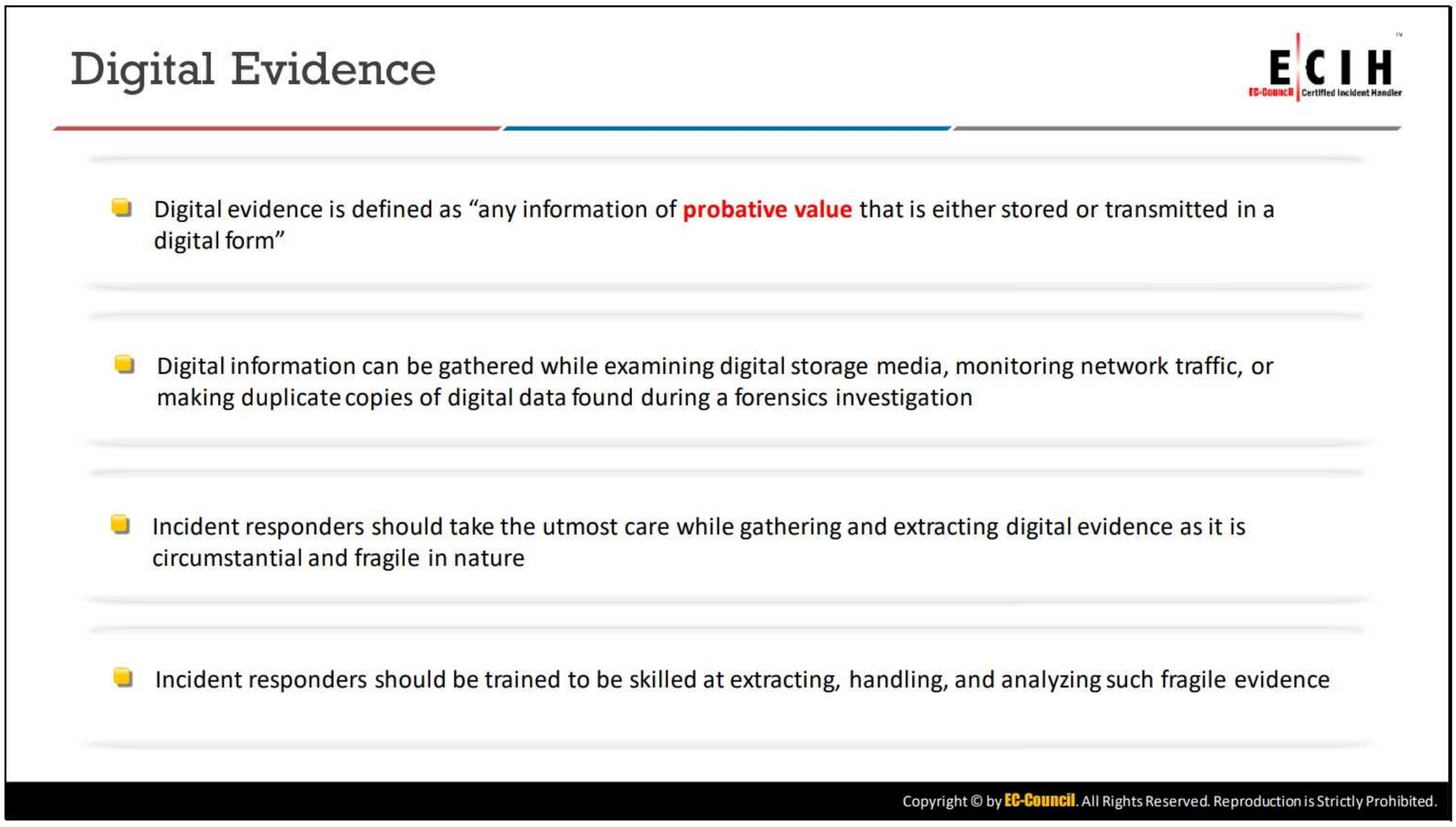
Overview of Digital Evidence

Incident responders face many challenges during the investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence. Digital evidence plays an essential role in cybercrime investigations. Digital evidence helps incident responders track the perpetrator.

This section provides an overview of digital evidence, types of digital evidence, characteristics of digital evidence, roles of digital evidence, and types of evidence.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Digital Evidence

Digital evidence is defined as "any information of probative value that is either stored or transmitted in a digital form" and helps incident responders/investigators trace the perpetrator. Digital devices are frequently used in cyberattacks and other security breaches that store data about the session, such as login user, time, type of connection, and IP addresses. Therefore, these devices, like servers and routers, act as a source of digital evidence that can be used by incident responders to prosecute the attacker.

Digital evidence is present across computing devices, servers, routers, etc. It is revealed during forensic investigations while responders/investigators are examining digital storage media, monitoring the network traffic, or making duplicate copies of digital data.

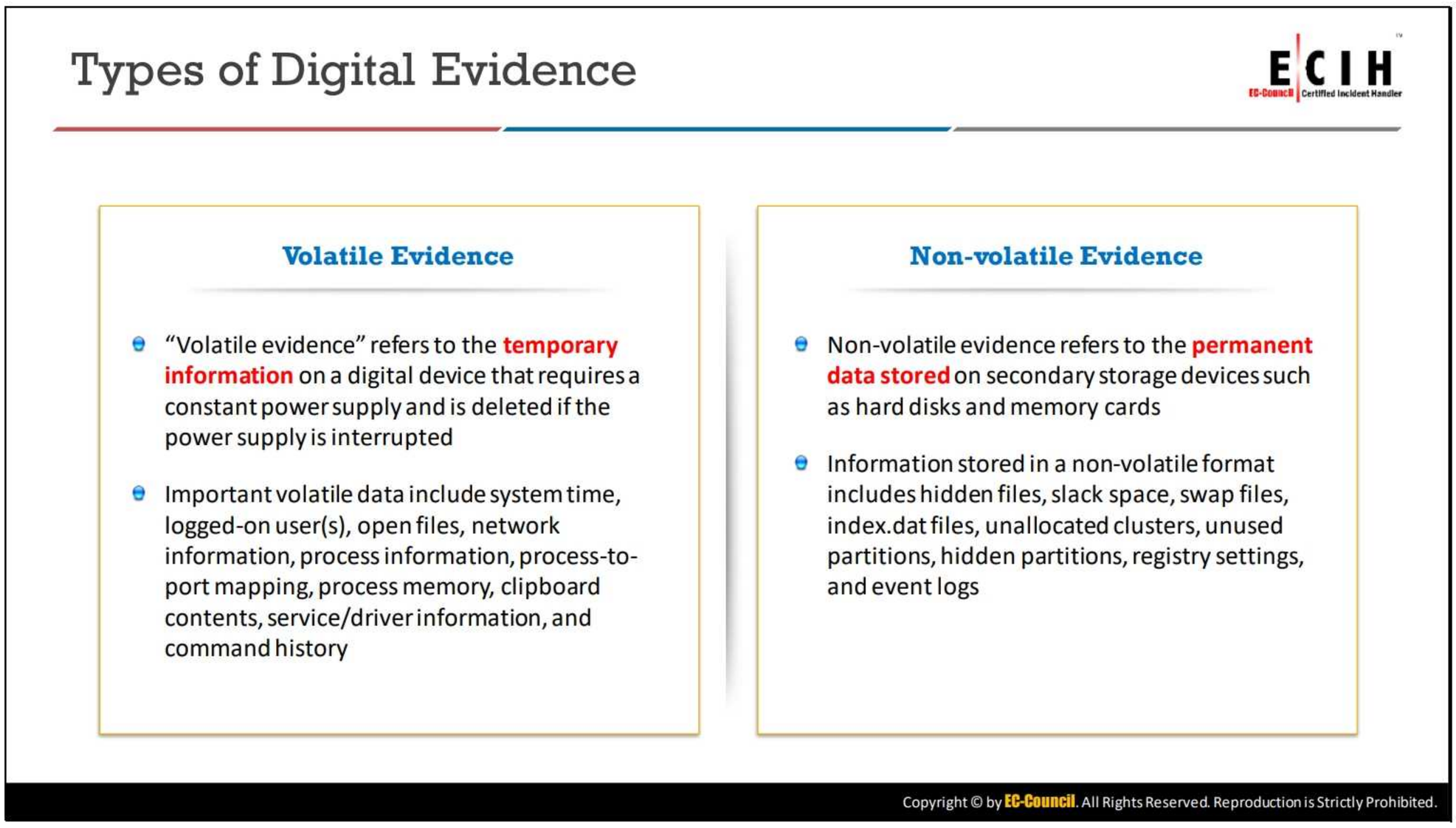
Incident responders/investigators should take utmost care while gathering and extracting the digital evidence as it is circumstantial and fragile in nature. This makes it difficult for an incident responder/investigator to trace the criminal activities. Incident responders/investigators should be trained and skilled to extract, handle, and analyze such fragile evidence.

Listed below are the different sources of digital evidence:

- Desktop computers, laptops, network storage devices, and servers
- DVDs, ports such as USB, Firewire, and PCMCIA
- Thumb drives, flash disks, memory disks, magnetic disks, optical disks
- Portable devices such as PDAs, digital cameras, audio/video players, and cell phones
- Various types of computer and network logs

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Types of Digital Evidence

Cyber criminals directly depend on technology and digital devices to engage with the targeted system or network. Therefore, most of the evidence is present in the devices used by an attacker to connect to a network or to the computing devices of the victim. Digital evidence can be any type of file stored on a device, including a text file, image, document, executable file, and application data. Most of this evidence is in the storage media of the devices.

Based on its fragility and lifespan, digital evidence is of two types:

- **Volatile Evidence:** Volatile evidence refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. For example, the RAM stores most volatile data and discards it when the device is switched off.

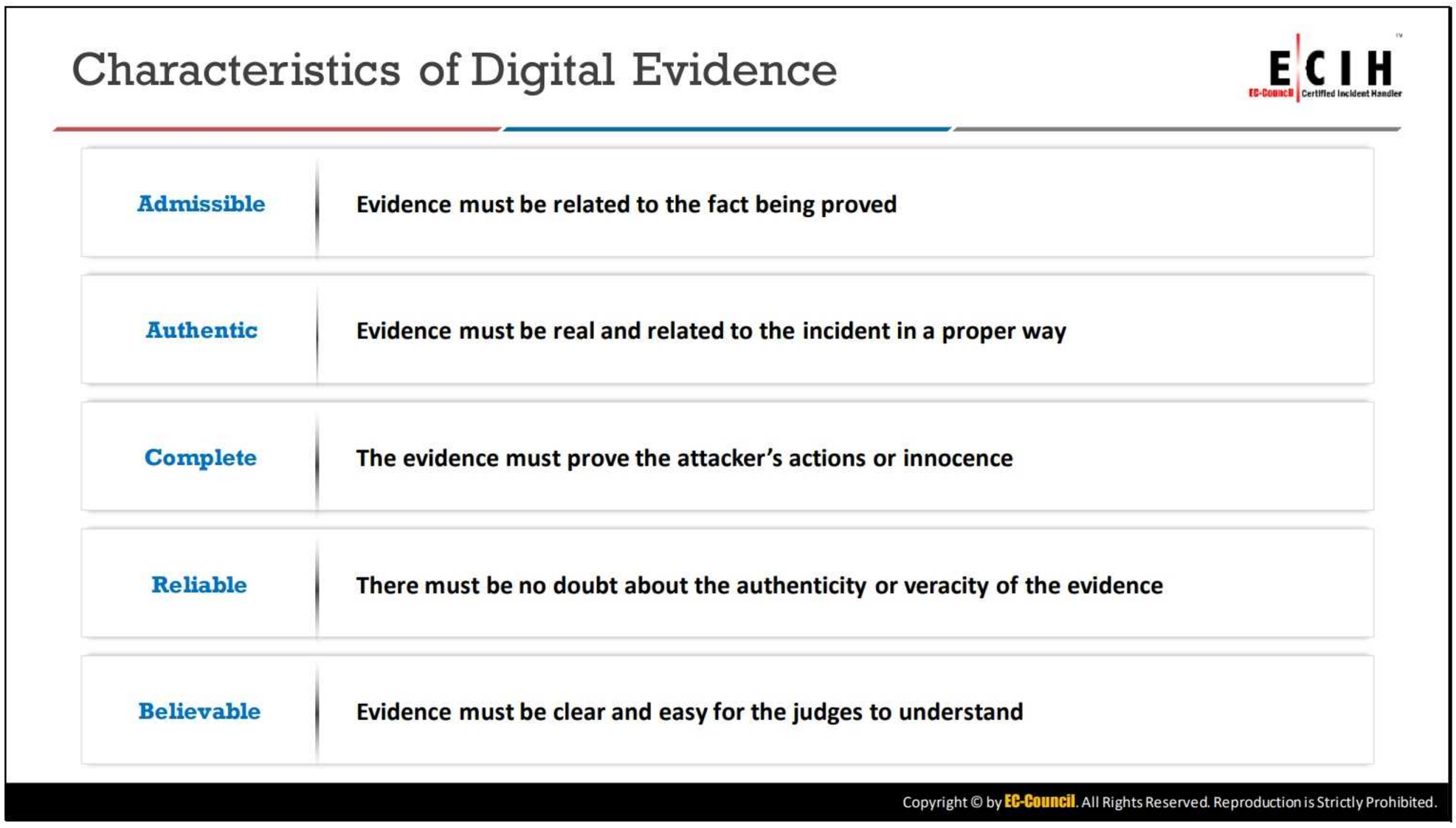
  Important volatile data include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, and command history.

- **Nonvolatile Evidence:** Nonvolatile evidence refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Nonvolatile data does not depend on a power supply and remains intact even when the device is switched off.

  Information stored in nonvolatile form includes hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Characteristics of Digital Evidence

The digital evidence must have certain characteristics to be disclosed in the court of law. The main characteristic of digital evidence is its relevance and weight (influence). The term "relevance" refers to the connection between digital evidence and the fact that is to be proved. The digital evidence is accepted in a court of law when it is relevant. If the collected digital evidence does not change the probability of the fact, the evidence is irrelevant. The term "weight of the digital evidence" refers to how much the digital evidence changes the probability of the fact.

The digital evidence must have certain characteristics to be acceptable in a court of law

- **Admissible**

  Incident responders must present evidence in an admissible manner, which means that it should be relevant to the case, act in support of the client presenting it, and be well communicated and non-prejudiced.

- **Authentic**

  It is extremely easy to manipulate digital evidence, which raises questions of ownership. Therefore, incident responders must provide supporting documents regarding the authenticity of the evidence with details such as its source and relevance to the case. If necessary, they must also furnish details such as the author of the evidence or path of transmission.

- **Complete**

  The evidence must be complete, which means it must either prove or disprove the consensual fact in the litigation. If the evidence fails to do so, the court is liable to dismiss the case citing lack of strong evidence.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Reliable**

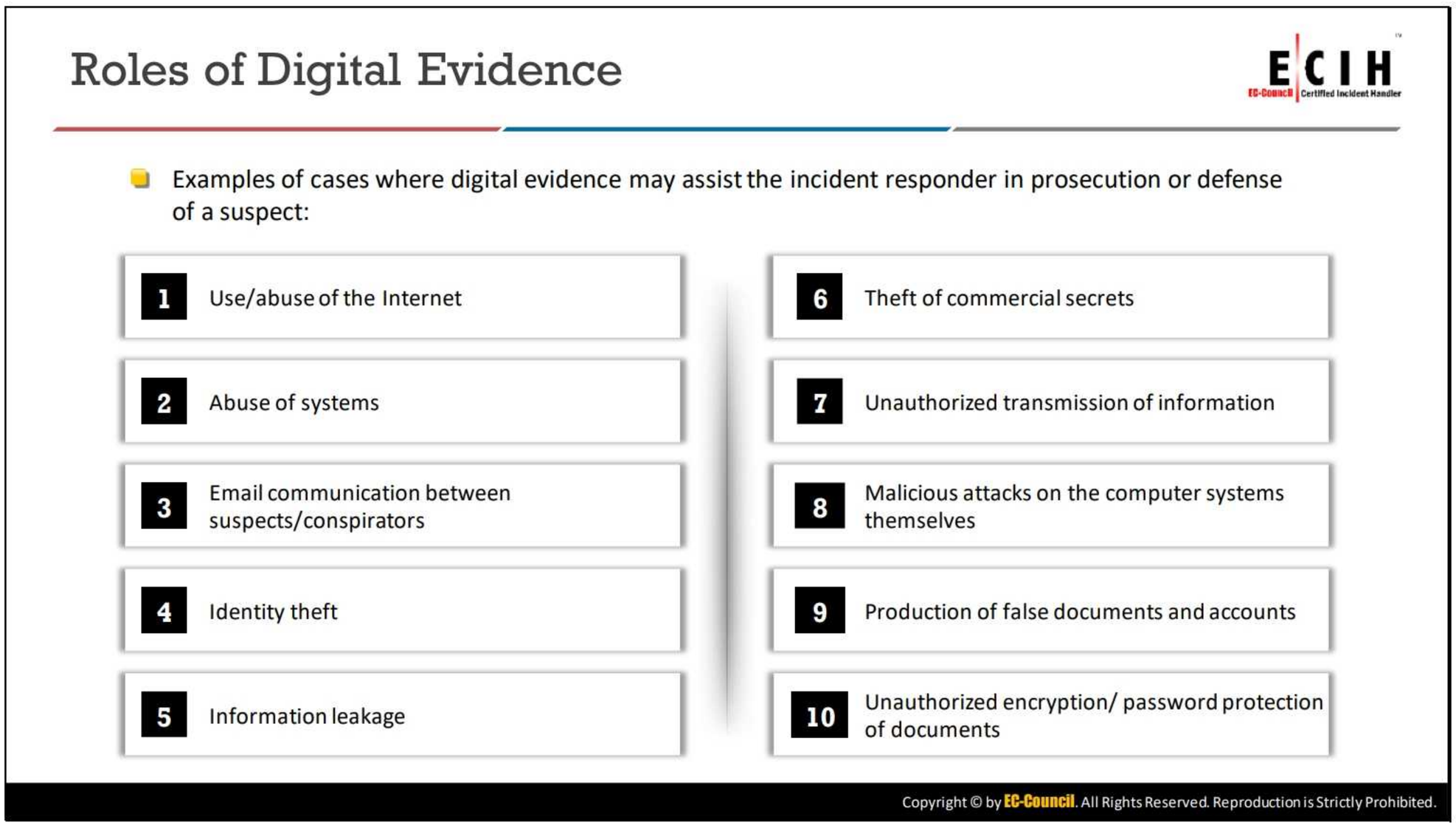
  The forensic experts should extract and handle the evidence while maintaining a record of the tasks performed during the process to prove that the evidence is reliable. Forensic investigations must be conducted only on copies of the evidence because the court requires the original evidence for future reference.

- **Believable**

  Incident responders and prosecutors must present the evidence in a clear and comprehensible manner to members of the jury. They must explain the facts clearly and obtain an expert's opinion to confirm the investigation process.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



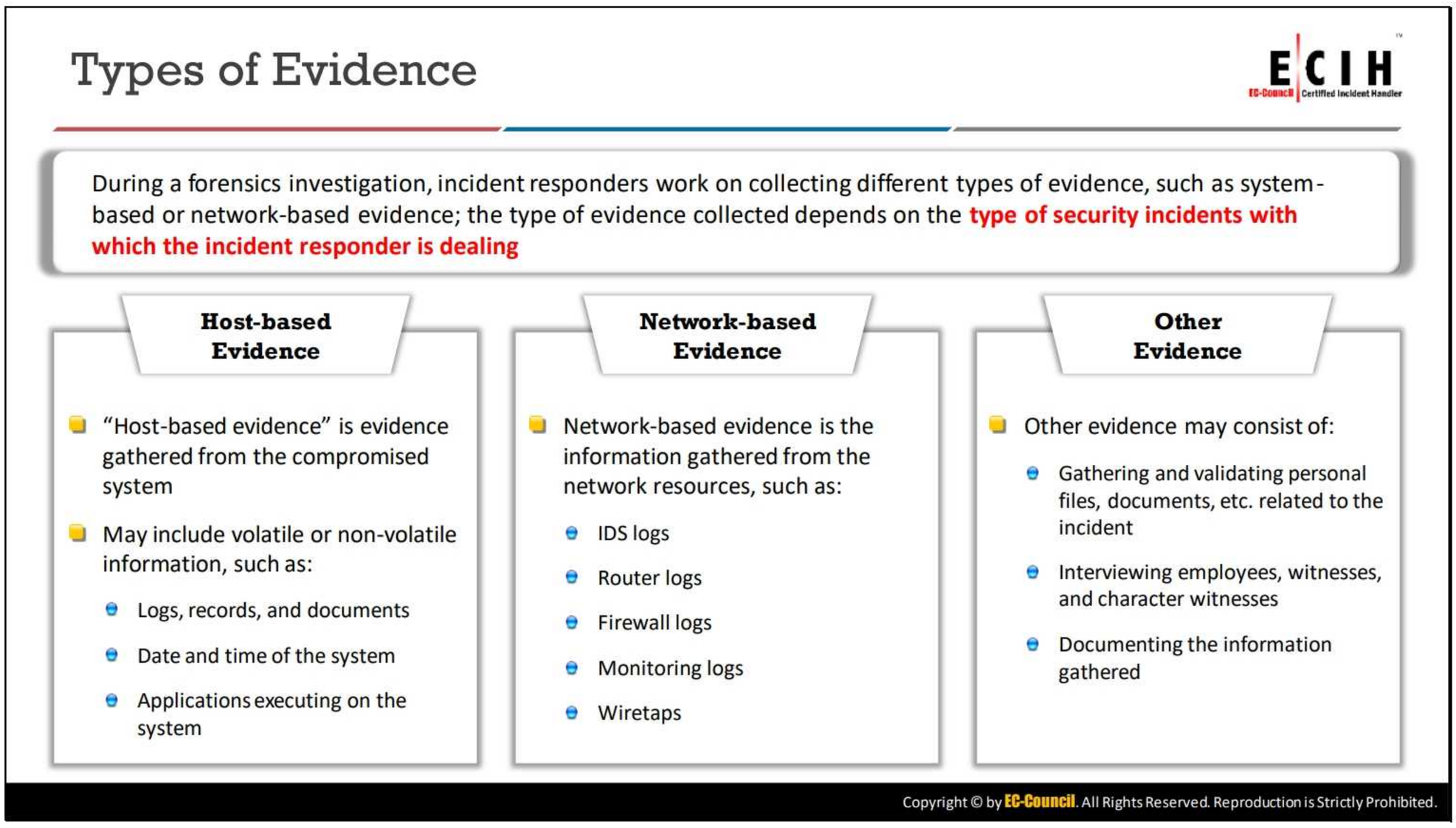
Roles of Digital Evidence

When an intruder bypasses the victim's computer or network, he or she leaves evidence, which can serve as clues to unravel the attack. Examples of cases where digital evidence may assist the forensic incident responder in the prosecution or defense of a suspect:

- Use/abuse of the internet
- Abuse of systems
- Email communication between suspects/conspirators
- Identity theft
- Information leakage
- Theft of commercial secrets
- Unauthorized transmission of information
- Malicious attacks on the computer systems themselves
- Production of false documents and accounts
- Unauthorized encryption/password protection of documents

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Types of Evidence

Forensic evidence plays an essential role in the investigation of cybercrimes in organizations. Incident responders extract, process, and interpret the factual evidence so that it proves the attacker's actions in court. During a forensics investigation, incident responders work on collecting different types of evidence, such as host based or network based. It depends on what type of security incident the incident responder is dealing with.

Organizations deal with the following types of evidence:

- **Host-based Evidence**

  Host-based evidence is the evidence gathered from the compromised system. It may include collected volatile or nonvolatile information such as:

  - Logs, records, documents, and any other information stored in a computer system
  - Date and time of the system
  - Applications executing on the system
  - Network connections
  - Open sockets or ports
  - Applications listening on open ports
  - State of the network interface

- **Network-based Evidence**

  Network-based evidence is the information gathered from network resources, such as:

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **IDS logs**: Intrusion detection system (IDS) logs help to identify unusual levels of attacks, concerted attacks, and unusual protocols and port combinations.
- **Router logs**: Router logs help to identify the number of systems connected to a specific router.
- **Firewall logs**: Firewall logs display the active and inactive sessions of a host machine.
- **Monitoring logs**: Monitoring logs collect the information of the systems in a network. Any suspected activity of a host machine can be analyzed through monitoring logs.
- **Wiretaps**: Wiretaps gather metadata of a device located where the monitoring device is placed.
- **Pen-register/trap and traces**: Pen-register/trap and trace logs record device routing information.
- **Authentication servers**: Logs generated in authentication servers help the administrators to identify any unknown entity attempting to access the network.

▪ **Other Evidence**

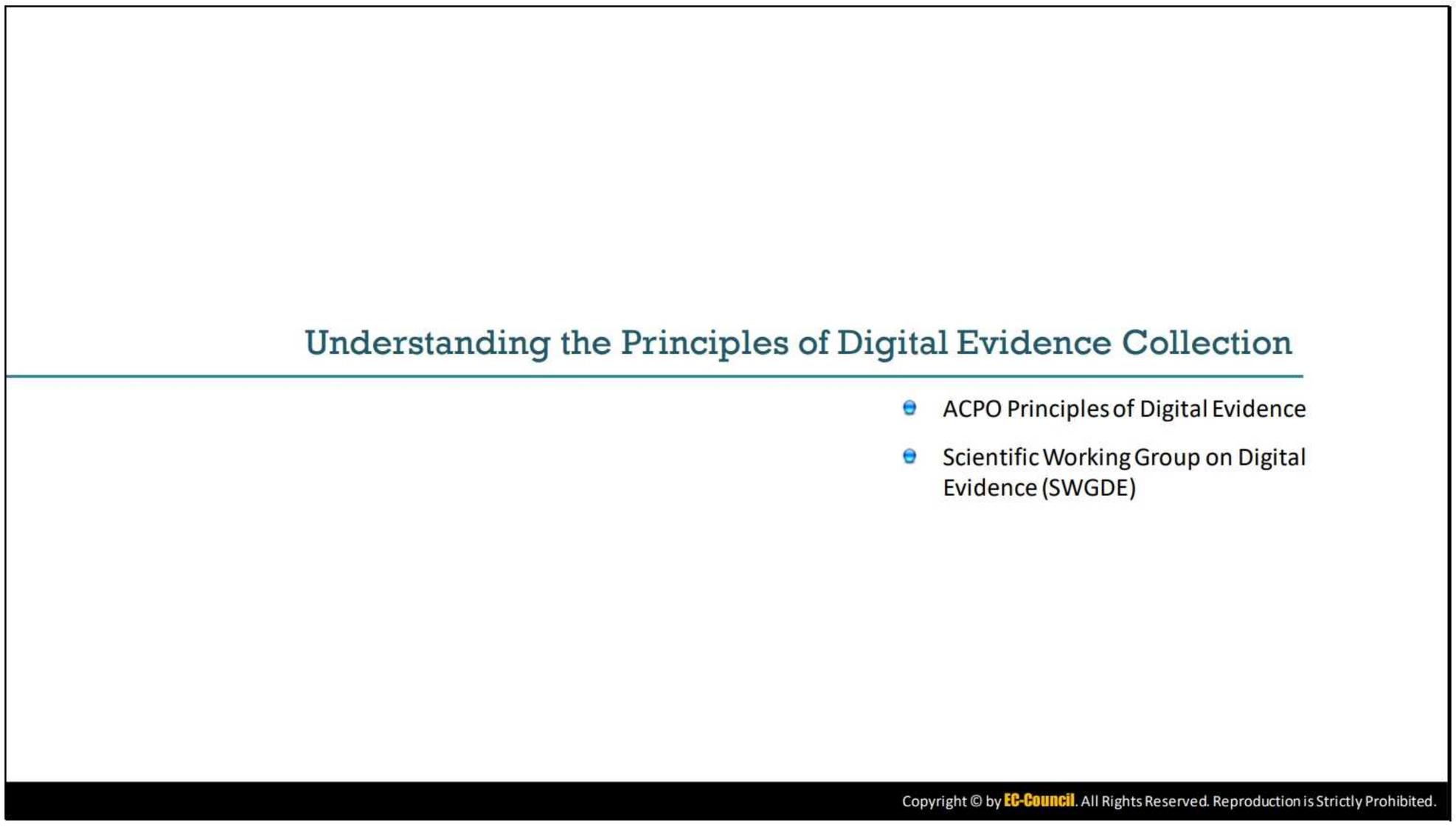
Other evidence may consist of:

- Validated personal files, documents, etc. related to the incident
- Employee, witness, and character witness interviews
- Documentation of gathered information related to the incident

The incident handler creates a chain of custody document which includes detailed information about the evidence, such as the model number, serial number, IP address, and time of collection, and information about all the people involved in collection or evidence handling, such as their name, designation, and contact number.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



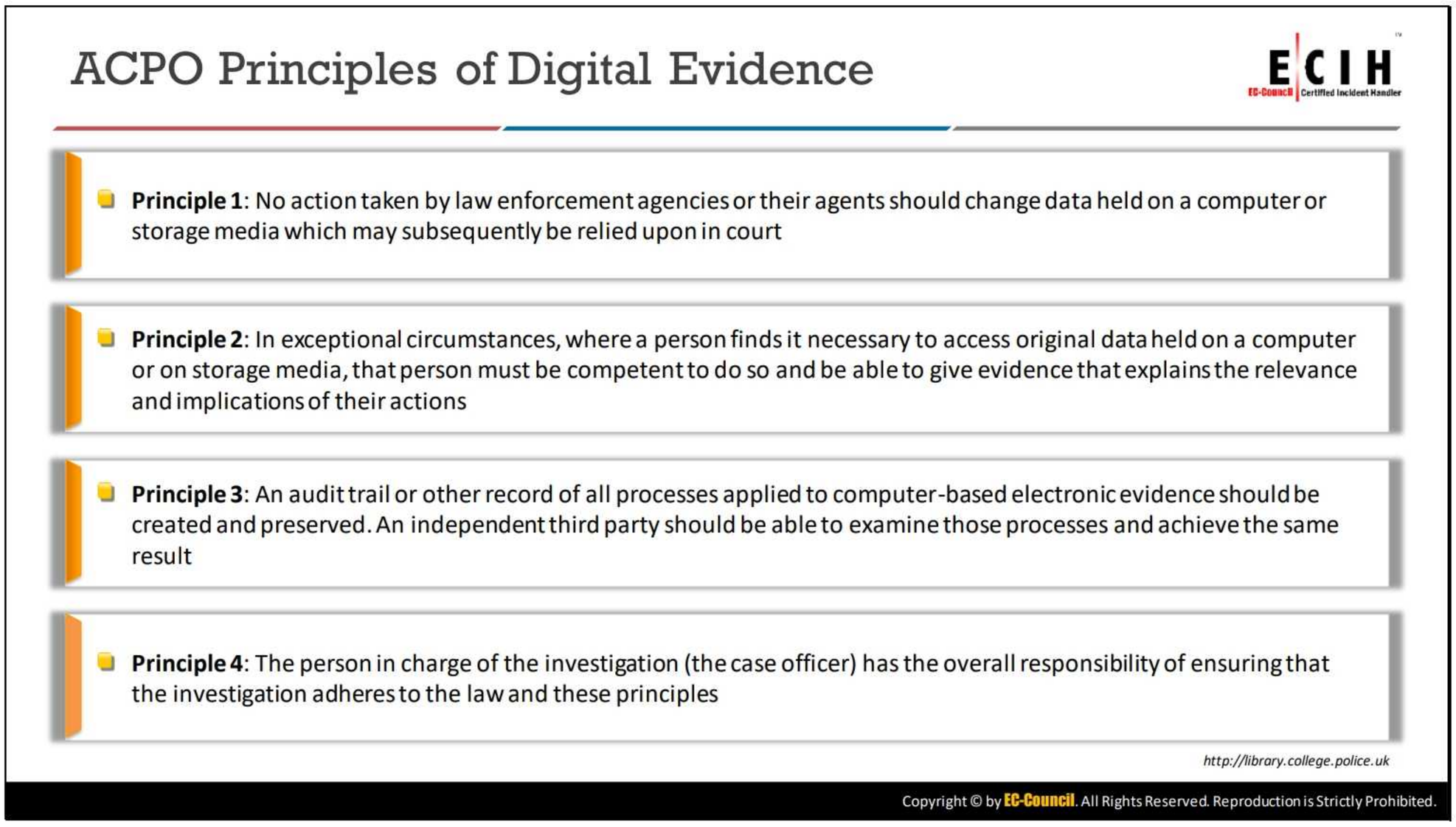
Understanding the Principles of Digital Evidence Collection

Prior to the investigation, it is important for the incident responder to understand the principles of digital evidence. The submission of evidence in a legal proceeding, especially in computer crime cases, can have major challenges. Specific knowledge is required to collect, preserve, and transport the evidence because the evidence obtained from a cybercrime case might vary from the traditional forms of evidence. Often, evidence associated with computer crimes is in the form of an electronic pulse, that is, in digital form. The principles of digital evidence collection ensure that the evidence is stored, examined, preserved, and examined in a way that protects the reliability and correctness of the evidence.

This section discusses about Association of Chief Police Officers (ACPO) principles of digital evidence and Scientific Working Group on Digital Evidence (SWGDE).

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



ACPO Principles of Digital Evidence

Source: *http://library.college.police.uk*

- **Principle 1**

  No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

- **Principle 2**

  In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

- **Principle 3**

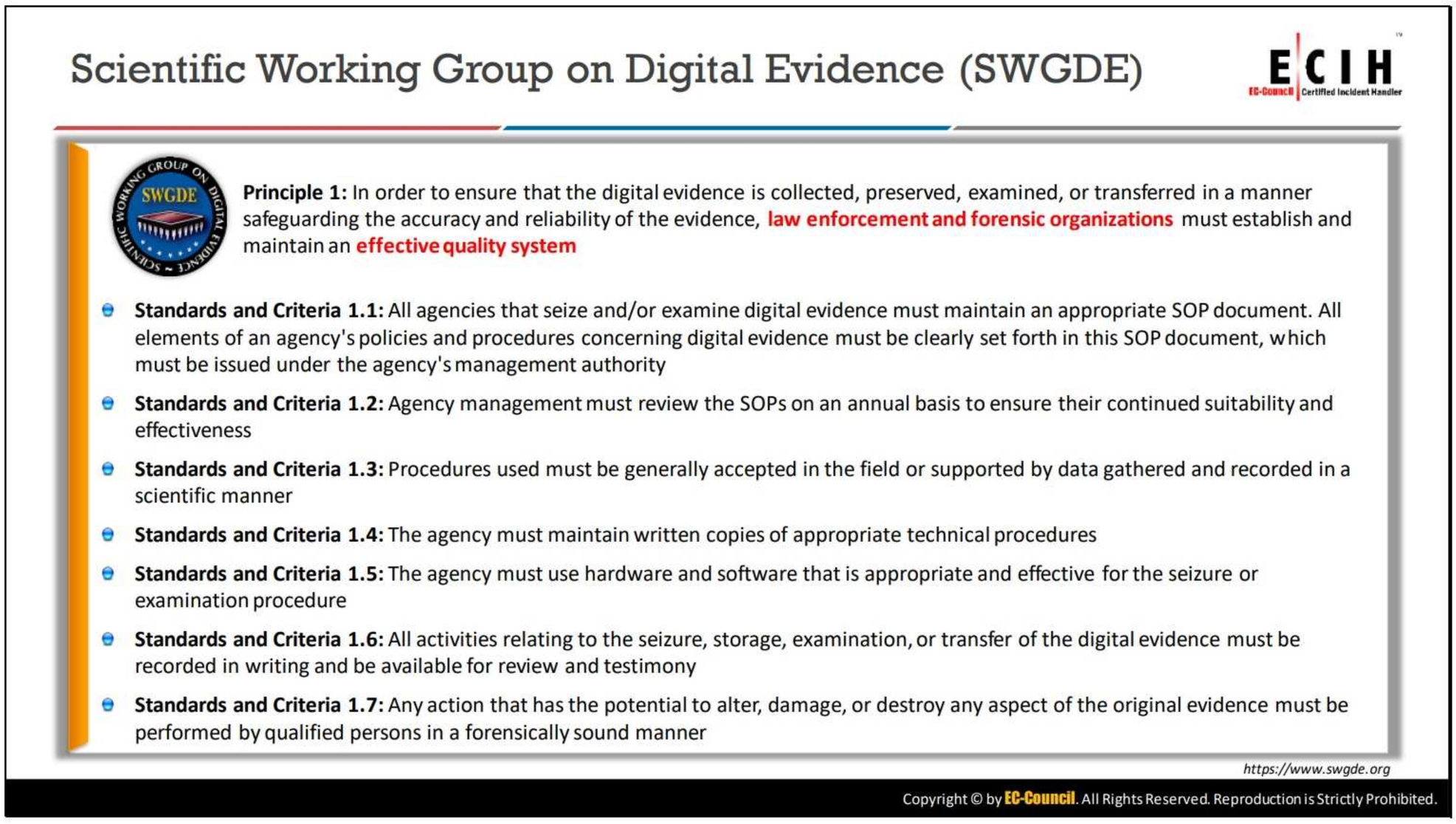
  An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

- **Principle 4**

  The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Scientific Working Group on Digital Evidence (SWGDE)

Source: *https://www.swgde.org*

- **Principle 1**

  To ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective system for quality control.

- **Standard Operating Procedures (SOPs)**

  Standard operating procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and broadly accepted procedures, equipment, and materials. Implementation of SOPs ensures that company-compliant policies and plans are followed. It is important that no modifications are made to SOPs before implementation to achieve the desired outputs. However, if any modifications are required, they must be communicated before starting an investigation.

  - **Standards and Criteria 1.1**

    All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

    Discussion: The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

The development and implementation of these SOPs must be under an agency's management authority.

- **Standards and Criteria 1.2**

  Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

  Discussion: Rapid technological changes are the hallmark of digital evidence, wherein the types, formats, and methods for seizing and examining digital evidence change quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, management must review and update SOP documents annually.

- **Standards and Criteria 1.3**

  SOPs must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

  Discussion: As a variety of scientific procedures may be validly applied to a given problem, standards, and criteria for assessing procedures need to be flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

- **Standards and Criteria 1.4**

  The agency must maintain written copies of the appropriate technical procedures.

  Discussion: Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed, and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

- **Standards and Criteria 1.5**

  The agency must use hardware and software that are appropriate and effective for the seizure or examination procedure.

  Discussion: Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem.

  Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and tested to ensure that it operates correctly. Software must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Standards and Criteria 1.6**

  All activities related to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

  Discussion: In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person can evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.

  The requirement for evidence reliability necessitates a chain of custody for all items of evidence. This implies that proper documentation must be maintained in chronological order for all digital evidence.

  Case notes and records of observations must be of a permanent nature. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Authenticate notes and records by handwritten signatures, initials, digital signatures, or other marking methods.

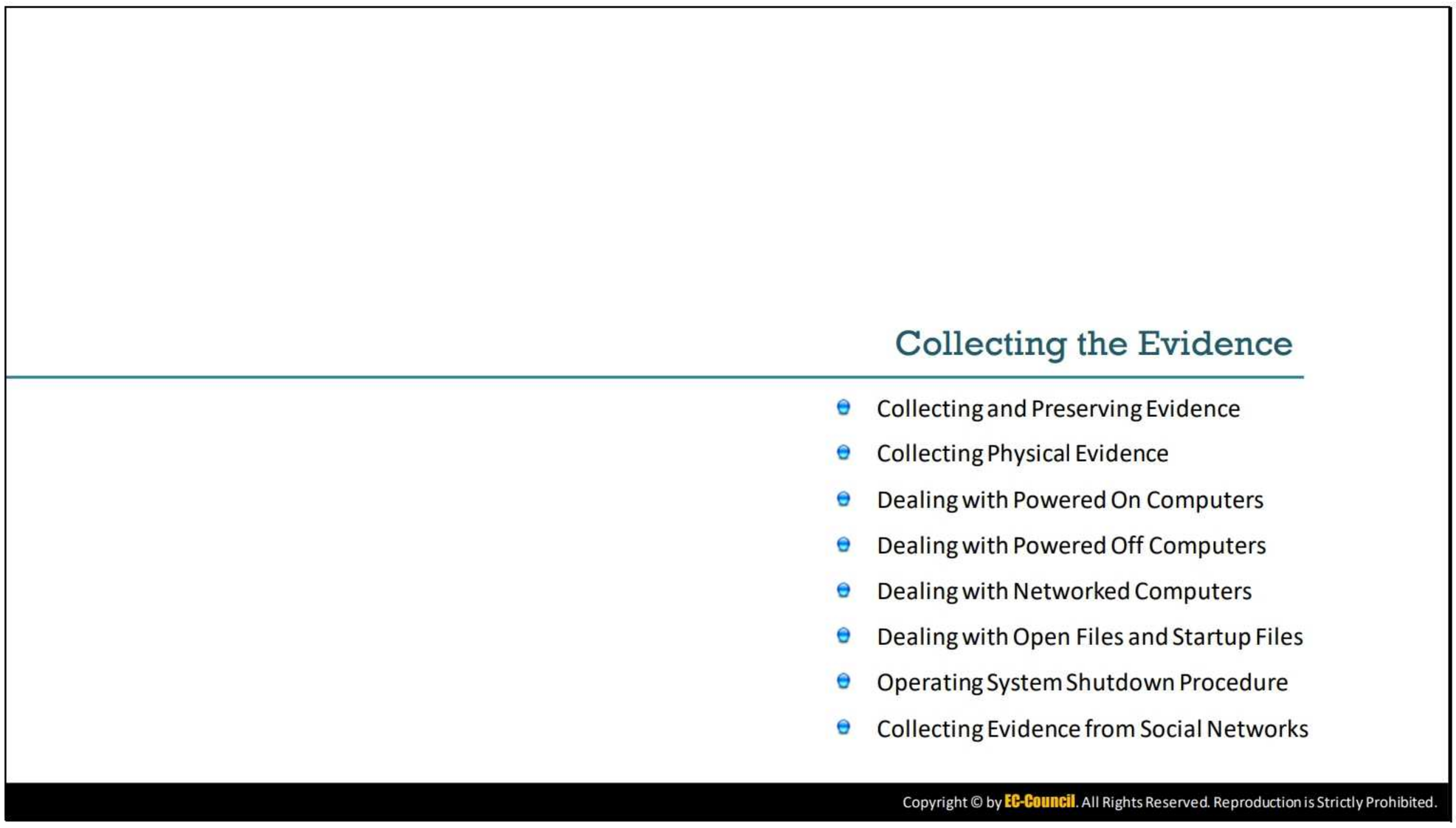
- **Standards and Criteria 1.7**

  Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

  Discussion: As outlined in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A high-quality forensic program consists of professionally trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



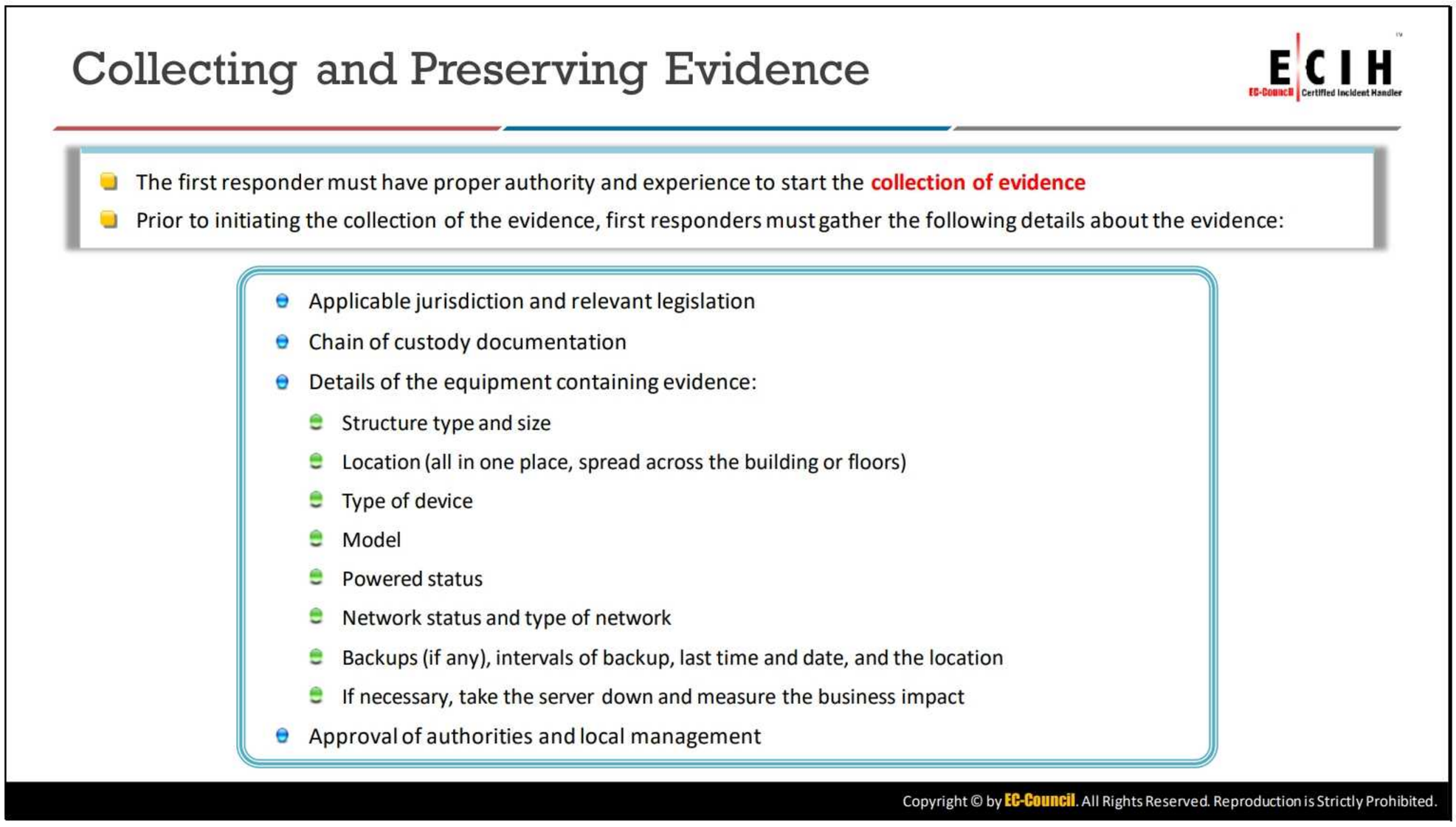
Collecting the Evidence

Evidence is the crucial data that can help incident responders in understanding the nature of the attack and trace the attacker. Therefore, the incident responders should know where they can find the evidence and how to gather it.

This section discusses collecting and preserving evidence, collecting physical evidence, dealing with powered on computers, dealing with powered off computers, dealing with networked computers, dealing with open files and startup files, operating system shutdown procedure, and collecting evidence from social networks.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting and Preserving Evidence

Any individuals acting as a first responder must secure the crime and document scene, must have proper authority, training, and experience to start collection of evidence. Prior to initiating the collection of evidence, first responders must gather the following details about the evidence:

- When an incident is reported and where a computer is assumed to be a part of the incident, it is often the case that this is the first and only item seized
- The crime scene should be investigated in a way that covers the entire area, keeping in mind the concept of the computer being at the middle of the circle
- Pieces of evidence found at the crime scene should be first photographed, identified within documents, and then properly gathered
- All collected evidence should be marked clearly so that it can be easily identified later
- Markings on the evidence should, at the very least, include date and time of collection and the initials of the collecting person
- Evidence should be identified, recorded, seized, bagged, and tagged on-site, with no attempts to determine contents or status
- Applicable jurisdiction and relevant legislation
- Create a chain of custody document
- Details of the equipment containing evidence:
  - Structure type and size

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

  - Location (all in one place, spread across the building or floors)
  - Type of device
  - Model
  - Powered status
  - Network status and type of network
  - Backups (if any), intervals of backup, last time and date, and the location
  - If it is necessary to take the server down and the business impact
- Approval of authorities and local management

The points to remember while preserving the electronic evidence are:

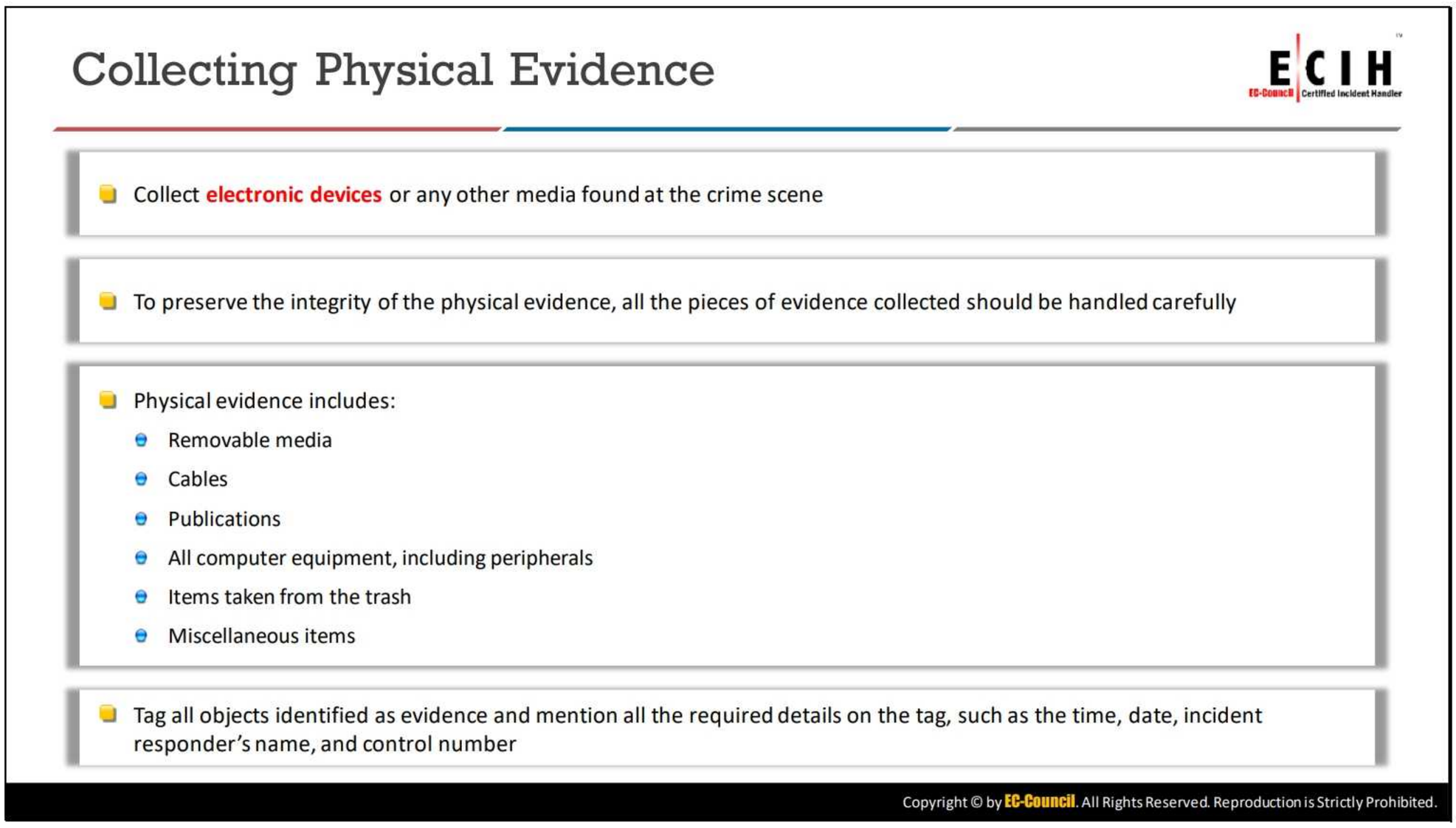
- Document the actions and changes that you observe on the monitor, system, printer, or other electronic devices
- Verify that the monitor is ON, OFF, or in sleep mode
- Remove the power cable, depending on the power state of the computer, that is, ON, OFF, or in sleep mode
- Do not turn ON the computer if it is in the OFF state
- Take a photo of the monitor screen if the computer is in the ON state
- Check the connections of the telephone modem, cable, ISDN, and DSL
- Remove the power plug from the router or modem
- Remove any portable disks that are available at the scene to safeguard potential evidence
- Keep the tape on drive slots and the power connector
- Photograph the connections between the computer system and the related cables, and label them individually
- Label every connector and cable connected to the peripheral devices

For handheld devices such as cell phones, tablets, and digital cameras:

- Do not turn the device ON if it is OFF
- Leave the device as it is if it is ON
- Photograph the screen display of the device
- Label and collect all cables and transport them along with the device
- Make sure that the device is charged

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Physical Evidence

The victim computer and its elements are vital evidence sources in a computer forensic investigation. Collect all the electronic devices or any other media found at the crime scene. Seize storage devices like hard drives, memory cards, and removable media as they can have stored information. Handheld devices like smartphones, mobile phones, PDAs, digital multimedia devices, and GPS receivers can have valuable evidence information like internet browsing history, emails, chat logs and friend lists, pictures and image files, and financial records.

The peripheral devices themselves are potential evidence. Information stored in the device such as scanned or printed documents, incoming and outgoing phone and fax numbers, and information about device usage can all contain valuable evidence.

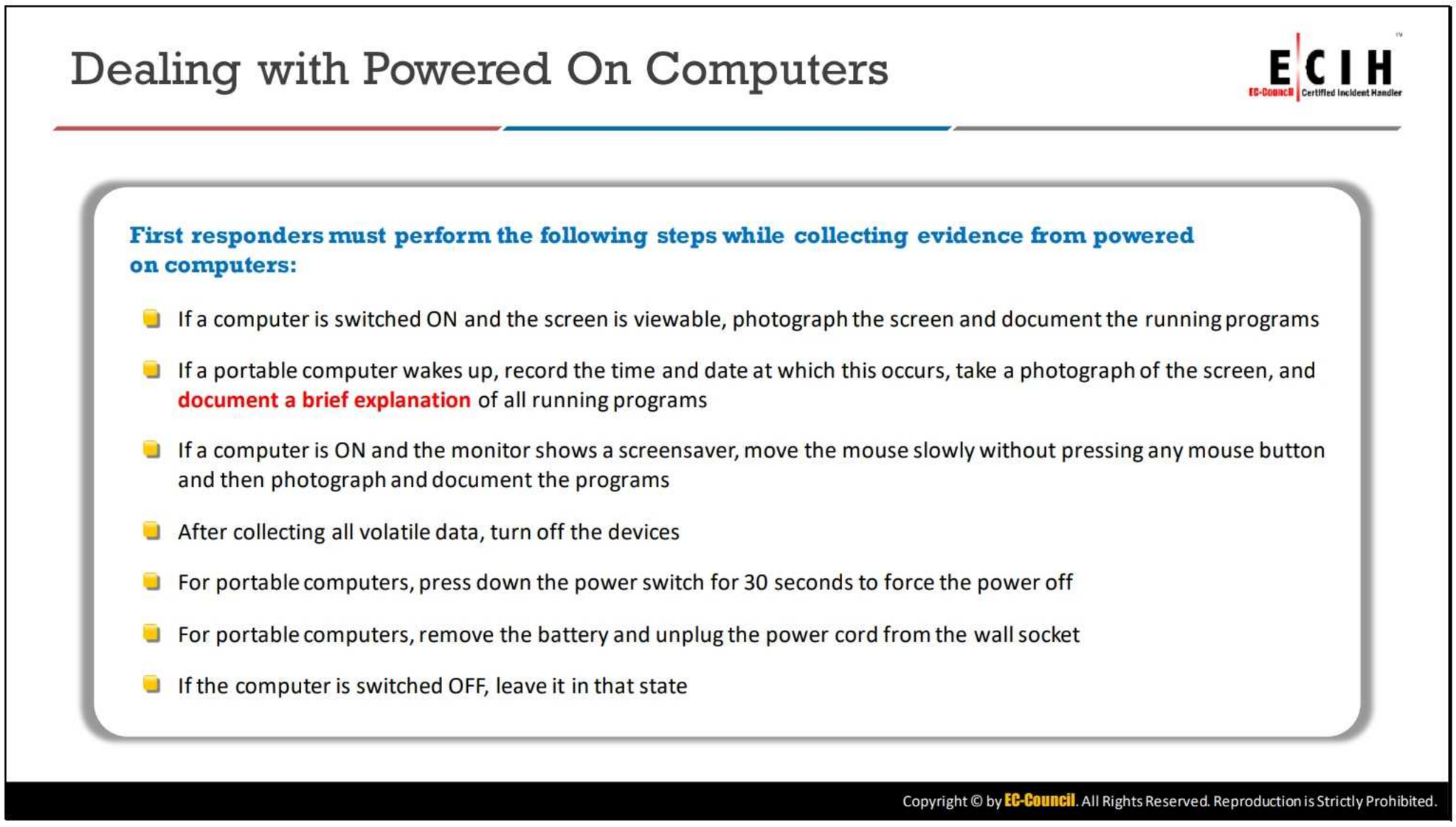
To preserve the integrity of the physical evidence, handle all the pieces of evidence collected carefully. Tag all the objects identified as evidence, and mention all the required details on the tag, such as the date, time, incident responder's name, and control number.

The physical evidence should include:

- Removable media
- Cables
- Publications
- All computer equipment, including peripherals
- Items taken from the trash
- Miscellaneous items

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Dealing with Powered On Computers

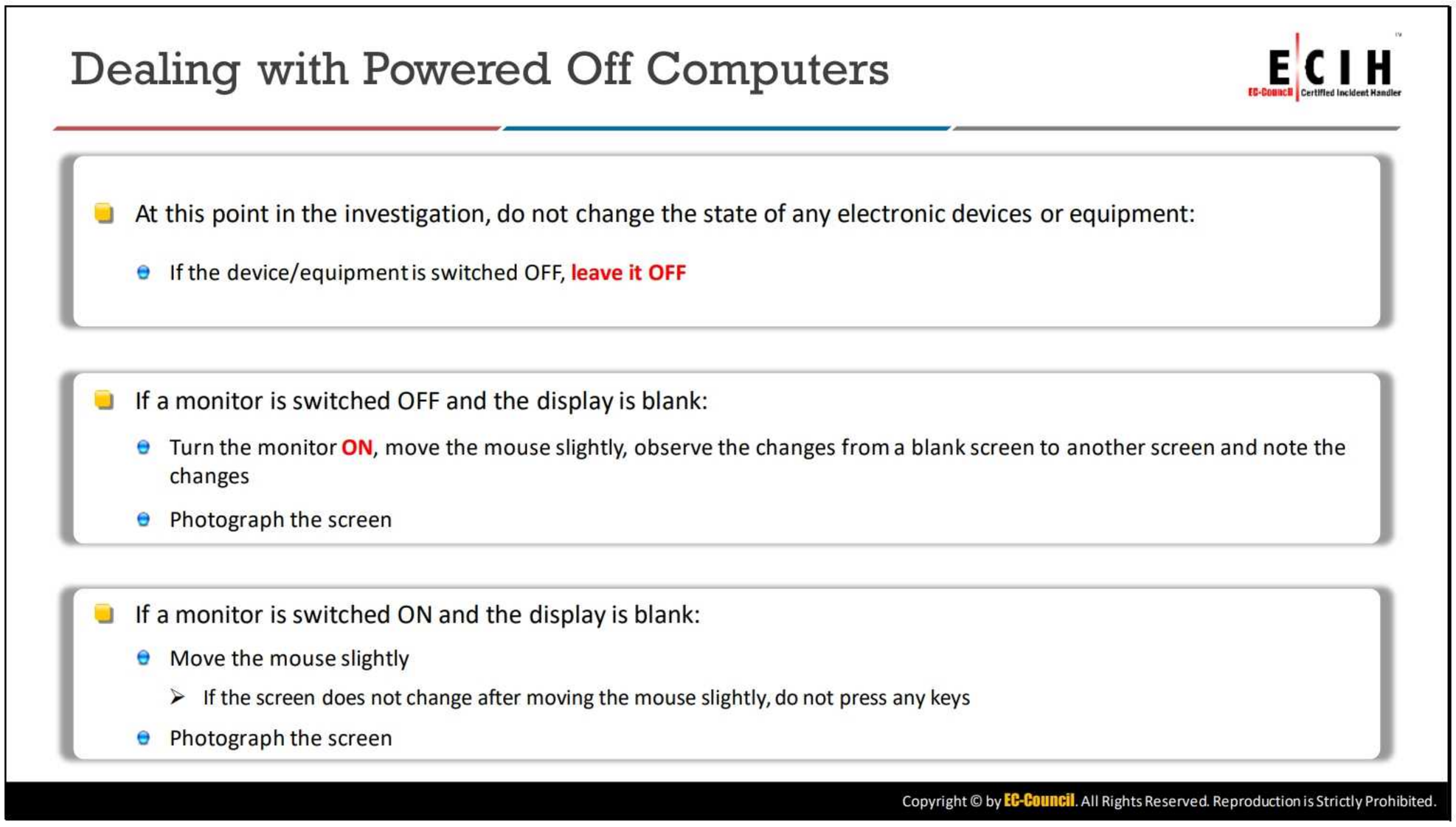
Electronic evidence is versatile in nature and easily broken during collection, preservation, and analysis. Therefore, first responders must act with caution while dealing with powered-on computers to prevent any damage to the evidence residing on them. In a powered-on computer system, both portable and desktop, the RAM contains crucial vital information, which is volatile in nature. Removing or shutting down the power supply will lead to deletion of this vital information. First responders must collect the volatile data from the powered-on device only if they have the skills, ability, and proper authorization, else they must wait for the arrival of the incident response team.

First responders must perform the following steps while collecting electronic evidence from powered-on computers:

- If a computer is switched ON and the screen is viewable, photograph the screen and document the running programs
- If a portable computer wakes up, record the time and date at which this occurs, photograph the screen, and give brief explanation of all the programs running
- If a computer is ON and the monitor shows a screensaver, move the mouse slowly without pressing any mouse button and then photograph and document the programs
- After collection of the complete volatile data, turn off the devices
- In portable computers, press down the power switch for 30 seconds to force the power off
- In portable computers, remove the battery and unplug the power cord from the wall socket
- If the computer is switched OFF, leave it in that state

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Dealing with Powered Off Computers

At this point of the investigation, do not change the state of any electronic devices or equipment:

- If it is switched OFF, leave it OFF

If a monitor is switched OFF and the display is blank:

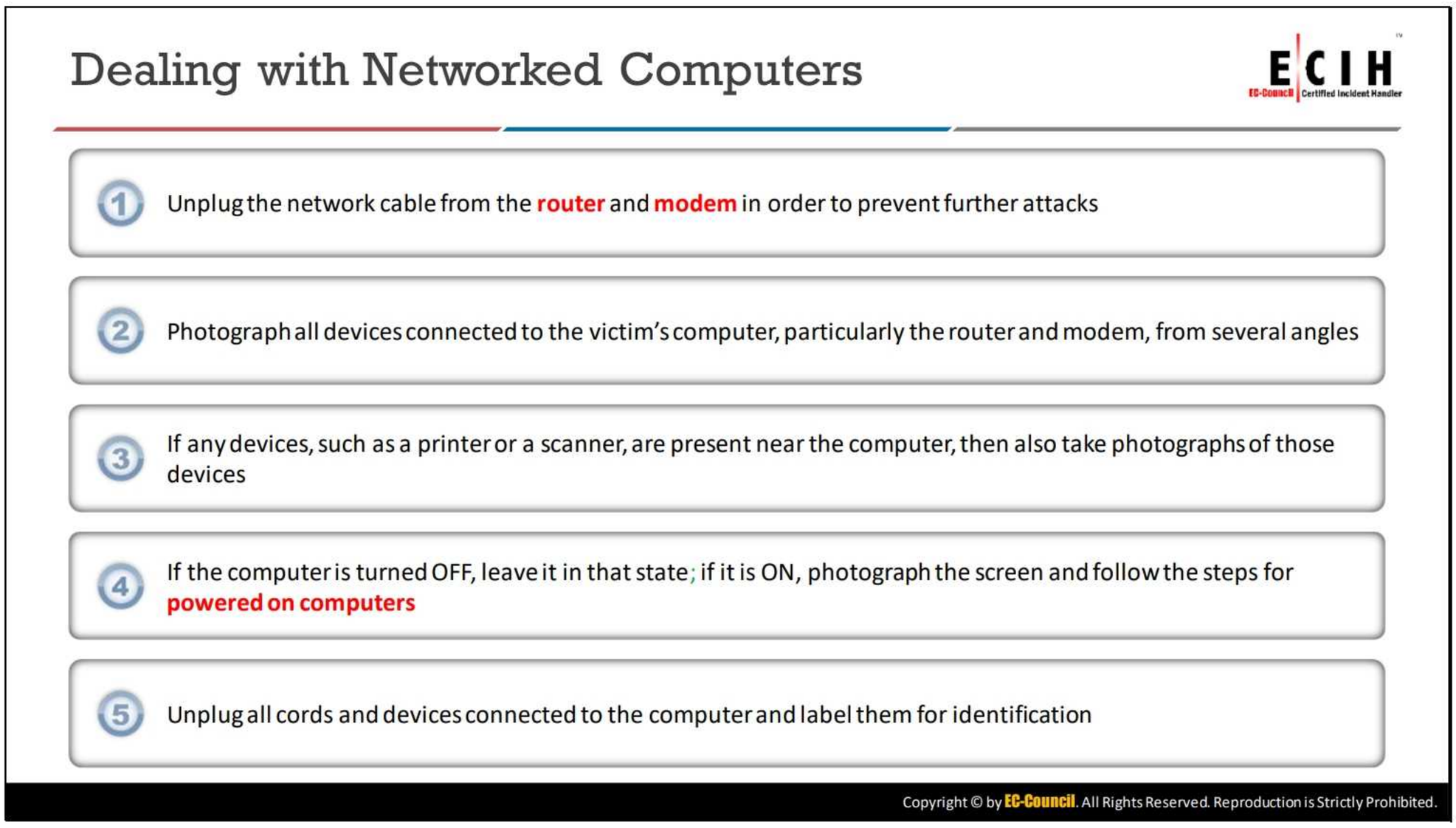
- Turn the monitor ON, move the mouse slightly, observe the changes from a blank screen to another screen, and note the changes
- Photograph the screen

If a monitor is switched ON and the display is blank:

- Move the mouse slightly
  - If the screen does not change on moving the mouse slightly, do not press any keys
- Photograph the screen

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



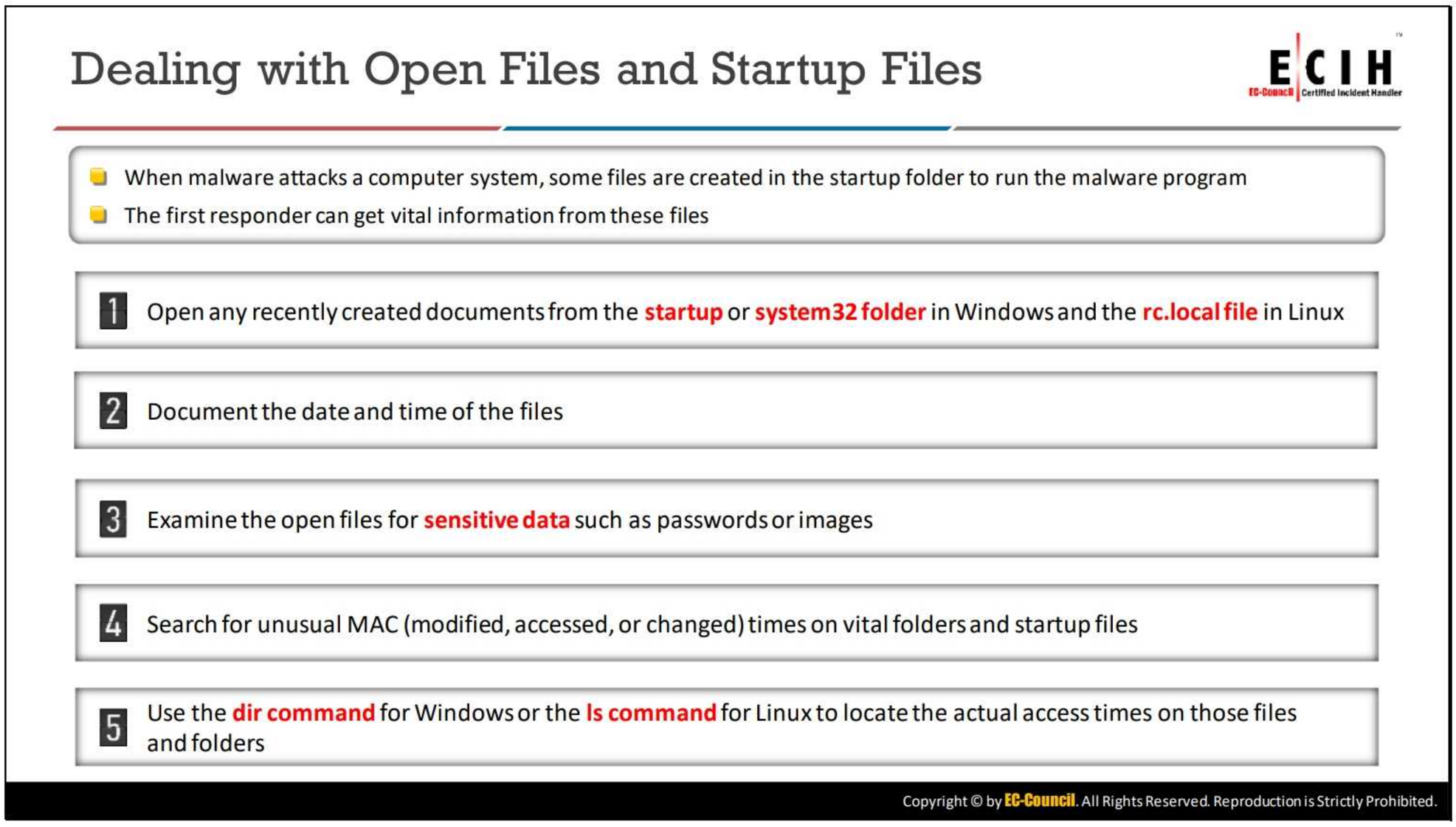
Dealing with Networked Computers

If the victim computer has an internet connection, the first responder must adhere to the following procedures to protect the evidence:

- Unplug the network cable from the router and modem, because the internet connection can make it vulnerable to further attacks
- Do not use the computer for evidence search because it may alter or change the integrity of the existing evidence
- Photograph all the devices connected to the victim's computer, especially the router and modem, and take photographs of the computer from different angles
- If any devices are present near the victim computer, such as a printer or scanner, take photographs of those devices
- If the computer is turned OFF, leave it in that state, and if it is ON, photograph the screen and follow the steps for powered on computers
- Unplug all cords and devices connected to the computer and label them for identification
- Unplug the main power cord from the wall socket
- Pack the collected electronic evidence properly and place it in a static-free bag
- Keep the collected evidence away from magnets, high temperature, radio transmitters, and other elements that may damage the integrity of the evidence
- Document all the steps that are involved in searching and seizing the victim's computer for later investigation.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Dealing with Open Files and Startup Files

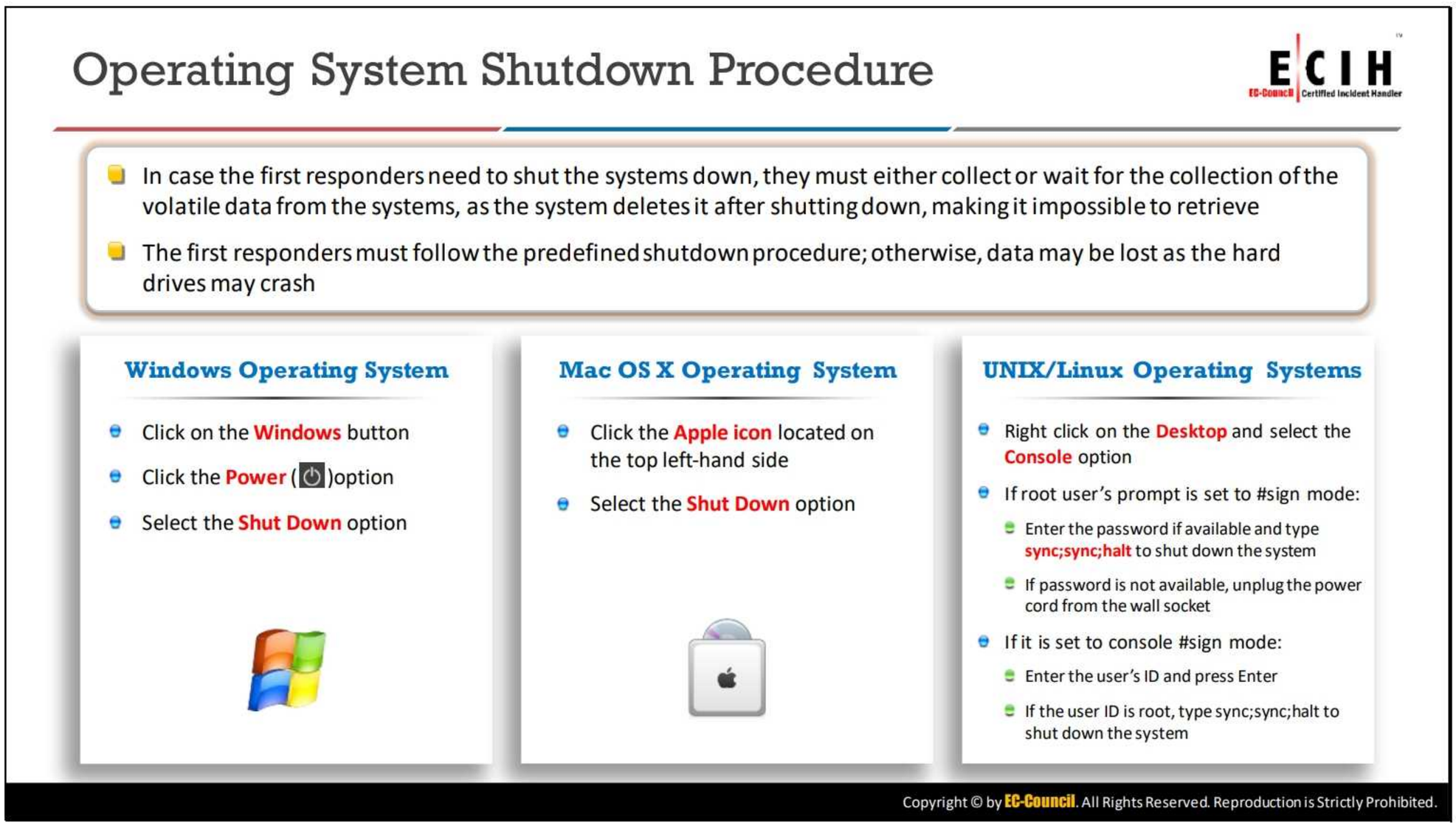
When a malware attack occurs, the malicious software infiltrates the computer and creates files. The malicious code is run by executing malware created files in the startup folders for Windows operating systems and in the rc.local file folder for the Linux operating systems. First responders can obtain vital information from these files. Use the ls command for the Linux operating system.

Steps for dealing with open files and startup files:

- Open any recently created documents from the startup or system32 folder in Windows and the rc.local file in Linux
- Document the date and time of the files
- Examine the open files for sensitive data such as passwords or images
- Search for unusual MAC times on vital folders and startup files
- Use the `dir` command for Windows or the ls command for Linux to locate the actual access times on those files and folders

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Operating System Shutdown Procedure

First responders have to make a crucial decision when shutting down the computer system, because it is important to shut down the operating system in a proper manner so that it will not damage the integrity of the files.

In case the first responders need to shut the systems down, they must either collect or wait for collection of the volatile data from the systems, as the systems delete this data after shutting down and it is impossible to retrieve.

First responders must shut down the systems in a proper manner so that it will not damage the integrity of the files. Different operating systems have different shutdown procedures. The first responders must follow the predefined shutdown procedure; otherwise, data may be lost as the hard drives may crash.

For Windows operating system:

- Click on the **Windows** button from the bottom left of the screen
- Click the **Power** ( ) option from the menu
- Then, select **Shut down** option
- Wait until the system shuts down completely and unplug the power cord from socket

MAC OS X Operating System:

- Click the **Apple** icon located on the top left-hand side of the Mac OS taskbar
- Select **Shut Down** near the bottom
- Unplug the power cord from the wall socket

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

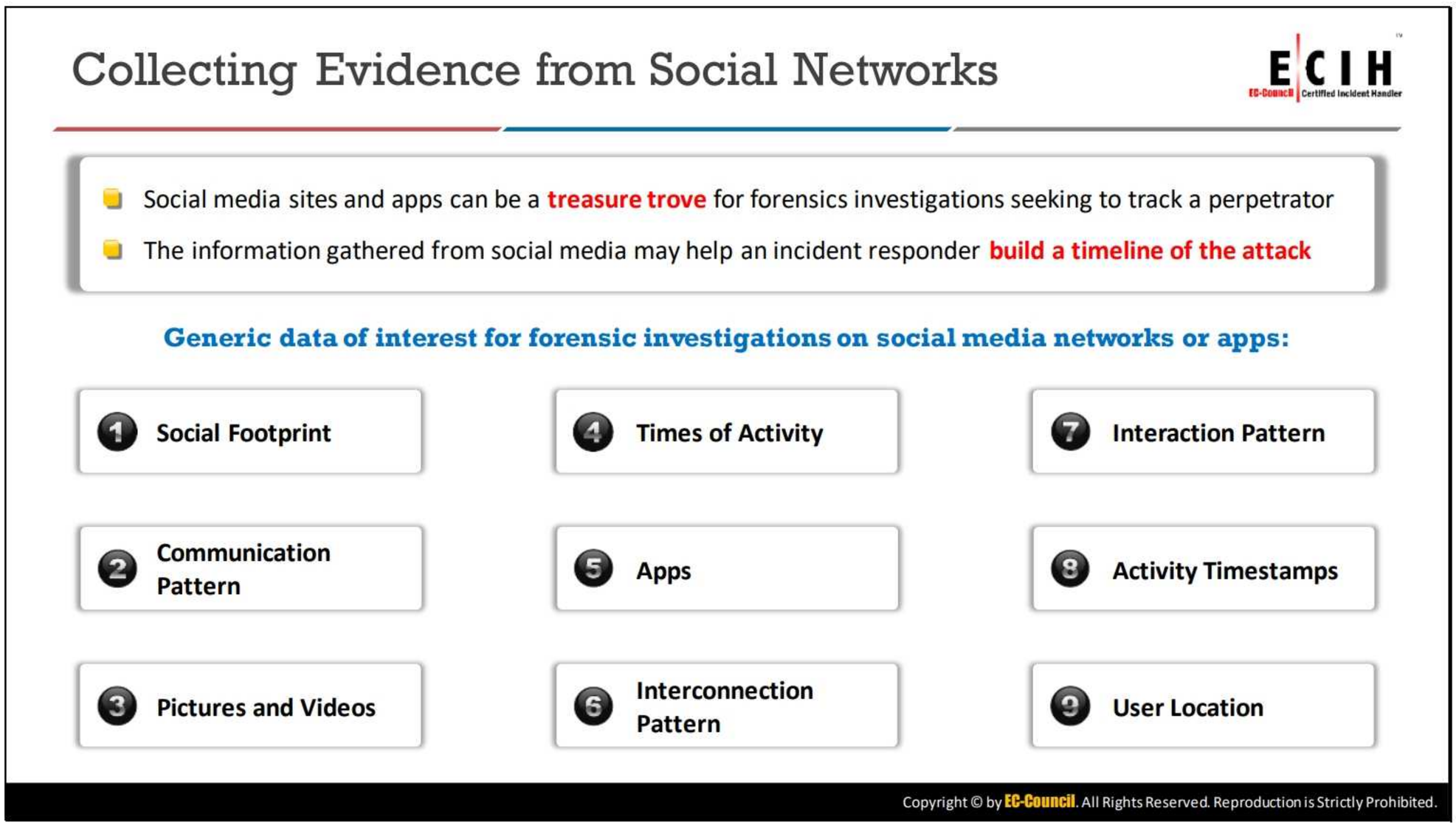
@UN5TABLE

UNIX/Linux Operating Systems:

- Right click on the **Desktop** and select the **Console** option
- If root user's prompt is set to #sign mode:
  - Enter the password if available and type **sync;sync;halt** to shut down the system
  - If the password is not available, unplug the power cord from the wall socket
- If it is set to console #sign mode:
  - Enter the user's ID and press **Enter**
  - If the user ID is root, type **sync;sync;halt** to shut down the system
  - If user's ID is not root, unplug the power cord from the wall socket

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Evidence from Social Networks

The number of people using social networking sites is increasing rapidly. Such sites have become one of the easiest ways to communicate and share data. This has led to cyber criminals finding various ways to commit crimes via social networking. Owing to the use of social media for illegal and criminal purposes, it has become a crucial source of evidence in the field of computer forensics. Some popular social networking sites are Facebook, WhatsApp, Twitter, LinkedIn, Google+, Snapchat, and so on.

Thus, social media sites and apps can be a treasure trove for forensic investigations to track a perpetrator. The information gathered from social media might help an incident responder to build a timeline of attack.

Social media forensics depend on a limited set of data sources as acquiring the server's hard drives is not possible and acquiring data needs the service operator's cooperation.

Generic data of interest for forensic investigations on social media networks or apps:

- **Social Footprint**: Social graph of the user and with whom the user is connected.
- **Communication Pattern**: Network used for communicating, method of communication, and with whom the user has communicated.
- **Pictures and Videos**: Pictures and videos uploaded by the user and on which other people's pictures is the user tagged.
- **Times of Activity**: The time the user has connected to the social network and the exact time a specific activity of interest has taken place.
- **Apps**: Apps used by the user and their purpose. Information that can be inferred in the social context.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Interconnection Pattern**: Includes user data such as user's friend list, chat messages, and group chats. This data helps the incident responder know about the user's friends, groups, connections added, and so on.
- **Interaction Pattern**: The interaction pattern helps a user interact with another user via messages and the interaction frequency.
- **Activity Timestamps**: The timeline of the activities of a user on a social networking platform can provide vital information for investigation. The timestamp of user communication and details about data sharing such as posting of photos and status updates reveal vital information about the activities of the user.
- **User Location**: Social networking sites have a geo-tagging or location update feature where the users can mention their precise location at a certain time.

The above mentioned information is stored only with the social network operator.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

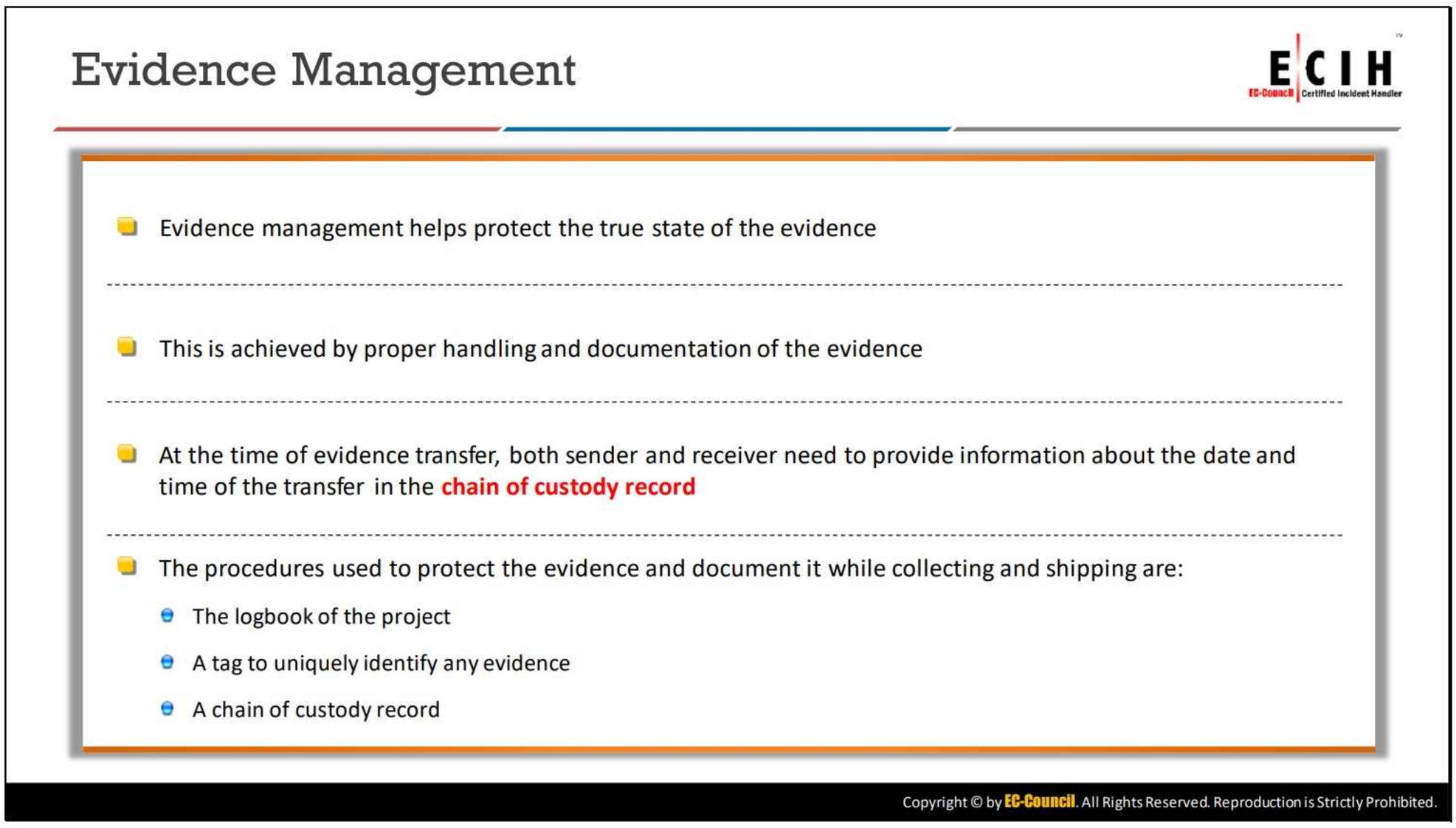
Securing the Evidence

Understanding the importance of securing the evidence is essential as forensic evidence are fragile and can be altered, damaged, or destroyed by improper handling or examination. It is essential to safeguard the integrity of the evidence and render it acceptable in a court of law.

This section discusses evidence management, chain of custody, simple format of the chain of custody document and chain of custody form. It also outlines the evidence bag contents list. It then discusses about how packaging, transporting, and storing of electronic evidence must be performed in a secure manner.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Evidence Management

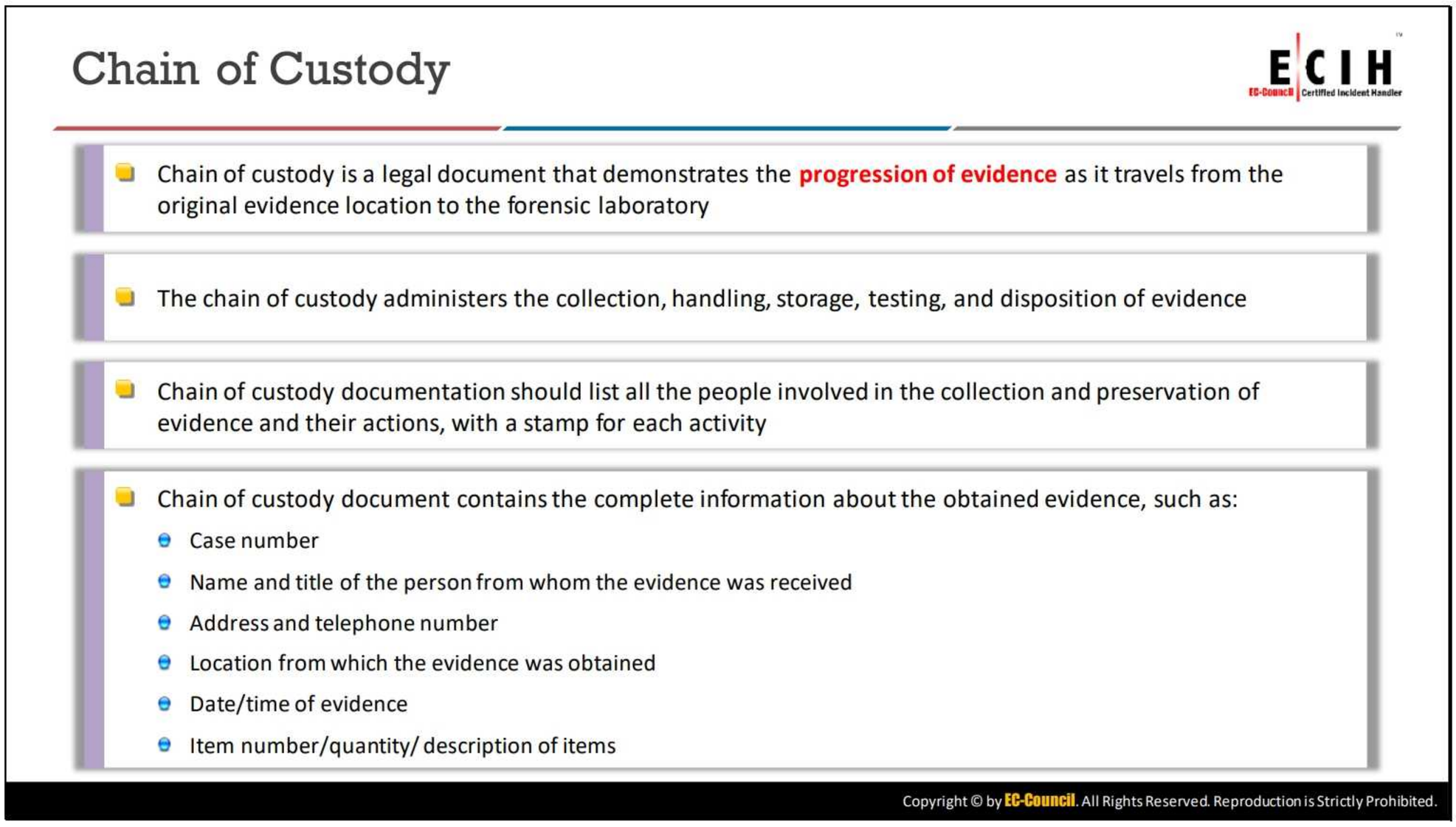
Evidence management helps in effectively protecting the true state of an evidence. This is achieved by the proper handling and documentation of the evidence. At the time of evidence transfer, both sender and receiver are required to provide the information about the date and time of transfer in a chain of custody record.

The procedures used to protect the evidence and document it while collecting and shipping are as follows:

- The logbook of the project to record observations related to the evidence
- A tag to uniquely identify any evidence
- A chain of custody record

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Chain of Custody

Chain of custody is a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory. It is a roadmap that shows how first responders and investigators collected, analyzed, and preserved the evidence. The first responders/investigators need to present this document in the court. It ensures accurate auditing of the original data evidence, imaging of the source media, tracking of the logs, and so on. The chain of custody shows the technology used and the methodology adopted in the forensic phases as well as the persons involved in it.

The chain of custody administers the collection, handling, storage, testing, and disposition of evidence. It helps to ensure the protection of evidence against tampering or substitution of evidence. Chain of custody documentation should list all the people involved in the collection and preservation of evidence and their actions, with a stamp for each activity.

The chain of custody form should identify:

- Sample collector
- Sample description, type, and number
- Sampling data and location
- Any custodians of the sample

Submission of the digital evidence in court requires a multi-dimensional approach. From this point of view, the chain of custody assumes significance. The first responder needs to document each step taken during the period of collecting the evidence. Moreover, the document should also include the detailed notes of procedures performed on the evidence. It is crucial that the first responders clarify the source, date of recovery, method of recovery, and

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

nature of the digital evidence. Any individual possessing a piece of evidence must handle it in a manner such that it is capable of standing legal scrutiny in case of an evidence tampering claim.

The chain of custody document contains all the information about the obtained evidence, which include the following:

- **Case number**

  It is a unique number allocated by the forensics laboratory or agency to the crime case.

- **Name and title from whom received**

  This field contains information about the individual releasing or forwarding the evidence item to inquiry personnel.

- **Address and telephone number**

  This field contains the complete address and telephone number of the individuals who handled the electronic evidence.

- **Location of the evidence**

  This field contains information about the physical location of the evidence during its extraction or acquisition.

- **Date/time of evidence**

  This field contains information about the data and time of acquiring the evidence.

- **Reason and process of obtaining the evidence**

  This field contains the information about why the first responders had obtained the evidence item and the process they followed for acquiring it.

- **Item number/quantity/description of items**

  This field contains the complete information about the obtained evidence. It contains information such as:

  - Name of the evidence
  - Color
  - Manufacturing company name
  - Marking information
  - Packaging information

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Simple Format of the Chain of Custody Document

Chain of Custody Document		
Laboratory or Agency Name:	Case Number:	
Received From (Name and Title):	Address and Telephone Number:	
Location From Which Evidence Was Obtained:	Reason Evidence Was Obtained:	Date and Time Evidence Was Obtained:

Item Number	Quantity	Description of Item

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Chain of Custody Form

Computer System Worksheet		
GSI File #		
Date:	Agency:	Agency Case #:
Site #:	Site Address #:	
Examiner:		
Notes:	Room/Location ID:	
Computer Description (Fill–in or check all that apply)		
Make: ☐ None	Case Type ☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ Laptop ☐ Desktop ☐ All in one ☐ Rack Mount	
Model: ☐ None	System Date:	Local Date:
Serial #: ☐ None	System Time:	Local Time: ☐ PSD ☐ PDT
OAN: ☐ None	System Status: ☐ On ☐ Active ☐ Suspended/Stand-by ☐ Screen Saver Active ☐ Off ☐ No Power/Not Connected ☐ Other	
Apparent OS ☐ Unk	Active/Open Programs: ☐ None ☐ N/A	
From ☐ N/A ☐ Screen ☐ Start Button ☐ Other	1.	
Shutdown Method ☐ Hard ☐ Soft ☐ Unknown ☐ N/A ☐ Other	2.	
Shutdown Date and Time	3.	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Chain of Custody Form (Cont'd)

Peripherals and Connections				
✓	INTERFACE	DESCRIPTION	NOTES	
☐	RJ-45	NIC Interface		
☐	RJ-11	Telephone Modem		
☐	☐ EGA ☐ VGA	Monitor	Media Model	Serial No
☐	☐ PS/2 ☐ AT	Keyboard	Media Model	Serial No
☐	☐ PS/2 ☐ AT	Mouse	Media Model	Serial No
☐	☐ LPT ☐ USB	Printer	Media Model	Serial No
☐	☐ A/V	Speaker	Media Model	Serial No
☐			Media Model	Serial No
☐	PASSWORD INFO:			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

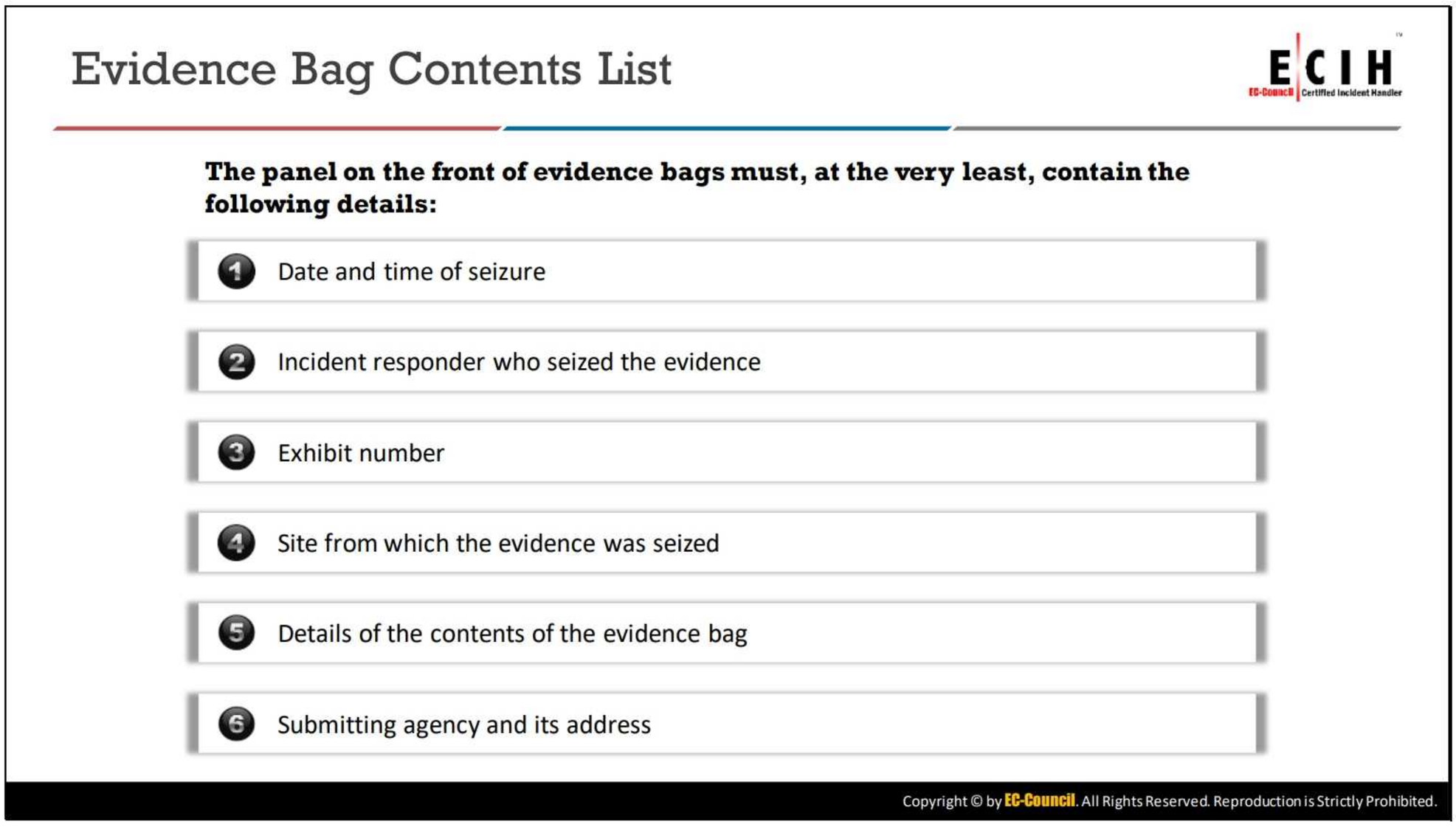
Chain of Custody Form (Cont'd)

Chain of Custody Form				
Package #' s	Date/Time	Released By	Received By	Reason
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	
	Date Time	Name/Agency Signature	Name/Agency Signature	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Evidence Bag Contents List

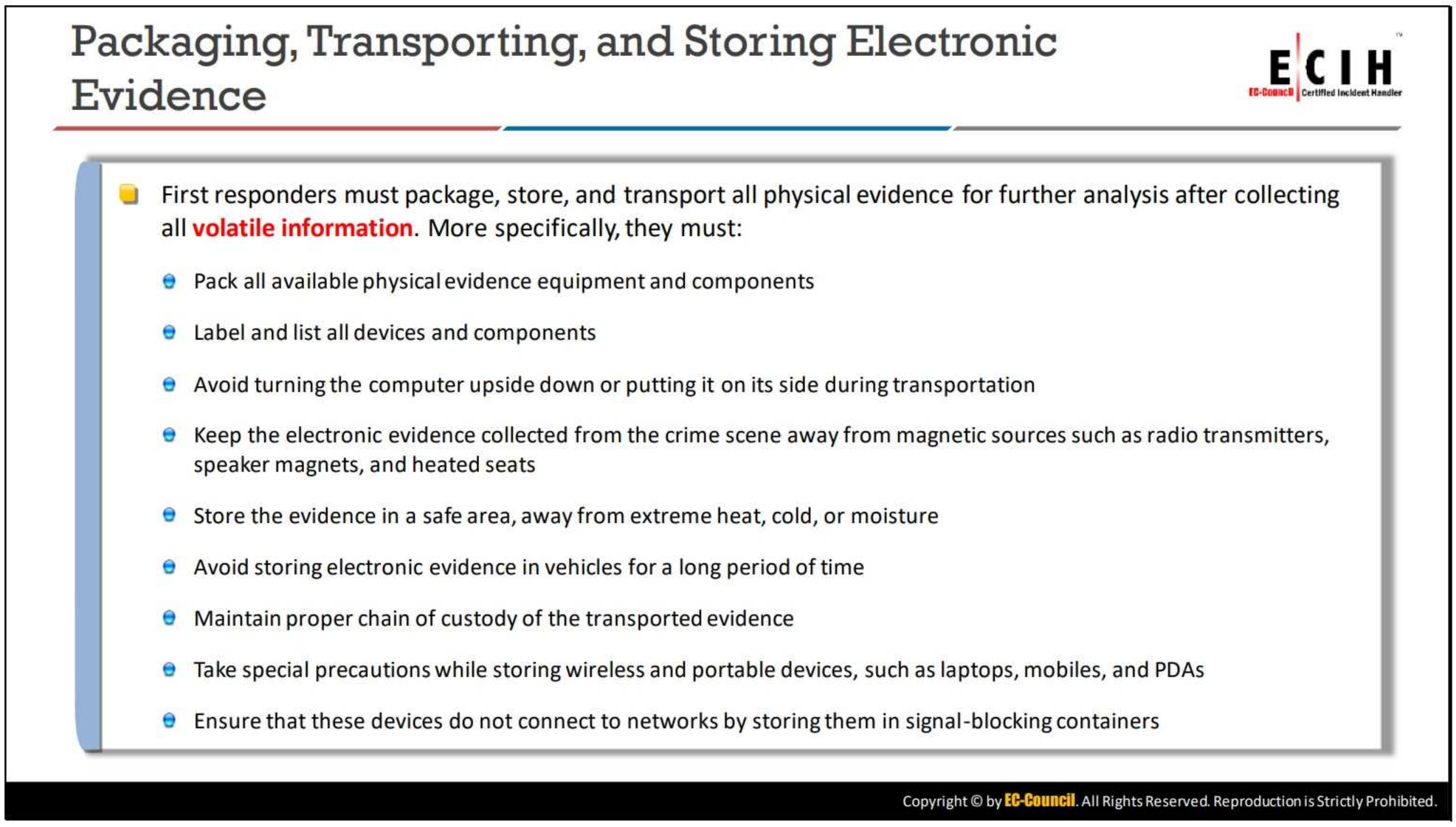
The panel on the front of evidence bags must contain the following details:

- Date and time of seizure
- Incident responder who seized the evidence
- Exhibit number
- Where the evidence was seized from
- Details of the contents of the evidence bag
- Submitting agency and its address

Additional details required on the panel of the evidence bags include the name of the officers who took photographs or prepared the scene sketch, sites where individual items were found, and names of the suspects, if any.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Packaging, Transporting, and Storing Electronic Evidence

First responders need special equipment to analyze the devices, extract the evidence, and analyze it. Therefore, they need to transport it to the laboratory for investigation and also to the court. Digital evidence is generally stored in computers and electronic devices, which are sensitive to extreme weather conditions, physical shock, static electricity, humidity, magnetic fields. First responders must therefore package, store, and transport all the physical evidence for further analysis after collection of volatile information.

They must perform the following steps:

- Pack all the available physical evidence equipment with its components
- Ensure the labelling of all devices and their components and create a list
- Pay special attention to hidden or trace evidence, and take necessary actions to safeguard it
- Pack magnetic media in antistatic packaging
- Avoid the use of materials such as plastic bags for packaging because they may produce static electricity
- Avoid the folding and scratching of storage devices such as diskettes, DVDs, and tapes
- Avoid turning the computer upside down or putting it on its side during transportation
- Keep the electronic evidence collected from the crime scene away from magnetic sources such as radio transmitters, speaker magnets, and heated seats
- Store the evidence in a safe area, away from extreme heat, cold, or moisture

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

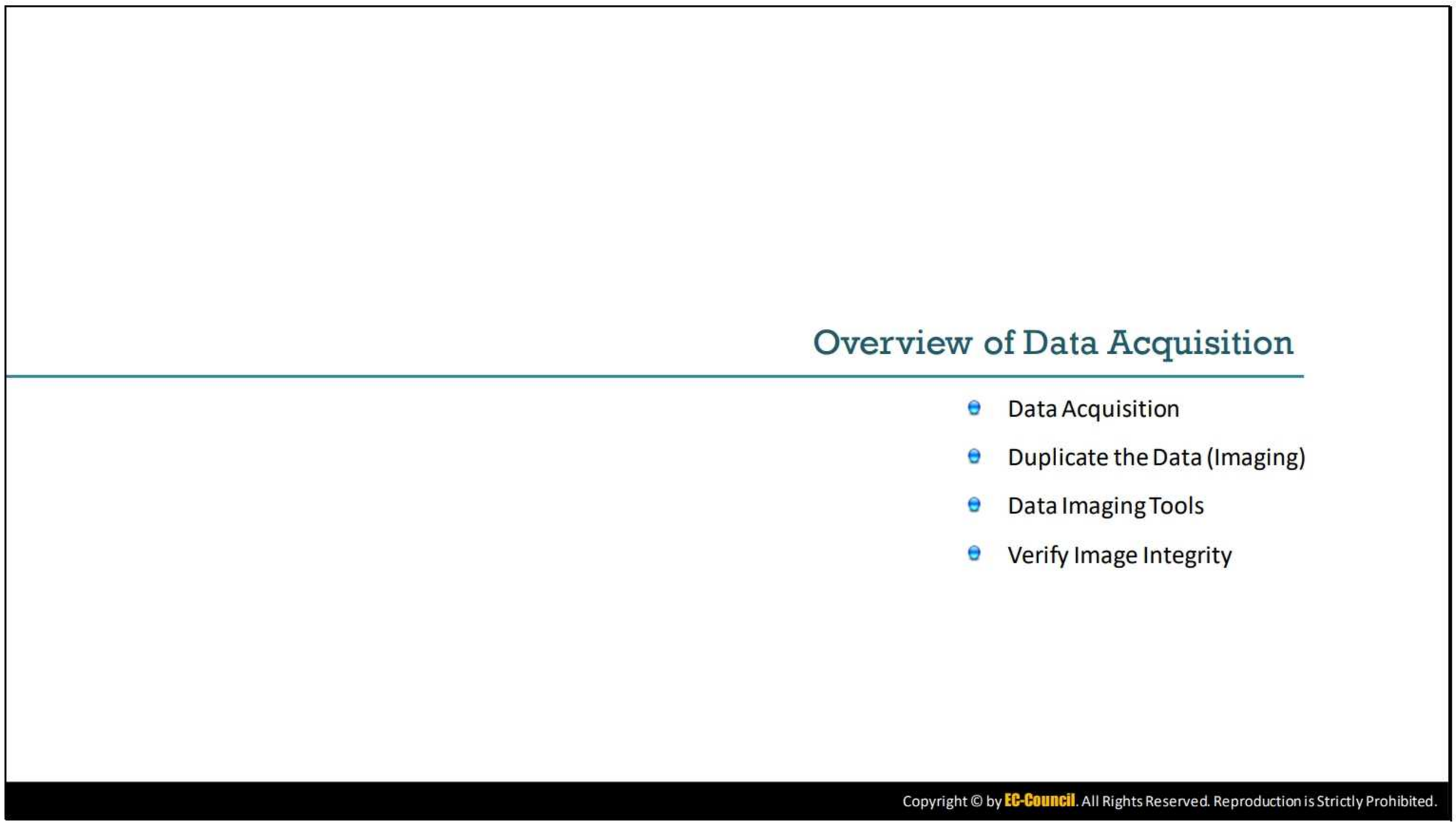
- Avoid storing electronic evidence in vehicles for a long period of time
- Maintain proper chain of custody of the transported evidence
- Take special precautions while storing wireless and portable devices, such as laptops, mobiles, and PDAs
- Ensure that these devices do not connect to the networks by storing them in signal blocking containers

Electronic devices contain digital information that may be potential evidence such as system date, time, and configuration. They lose this potential evidence because of improper and prolonged storage. Digital/electronic evidence is fragile in nature. Therefore, first responders should follow the practices mentioned below:

- Ensure the electronic evidence is listed in accordance with departmental policies
- Store the electronic evidence in a secure and weather-controlled environment
- Protect the electronic evidence from magnetic fields, dust, vibrations, and other factors that may damage its integrity

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



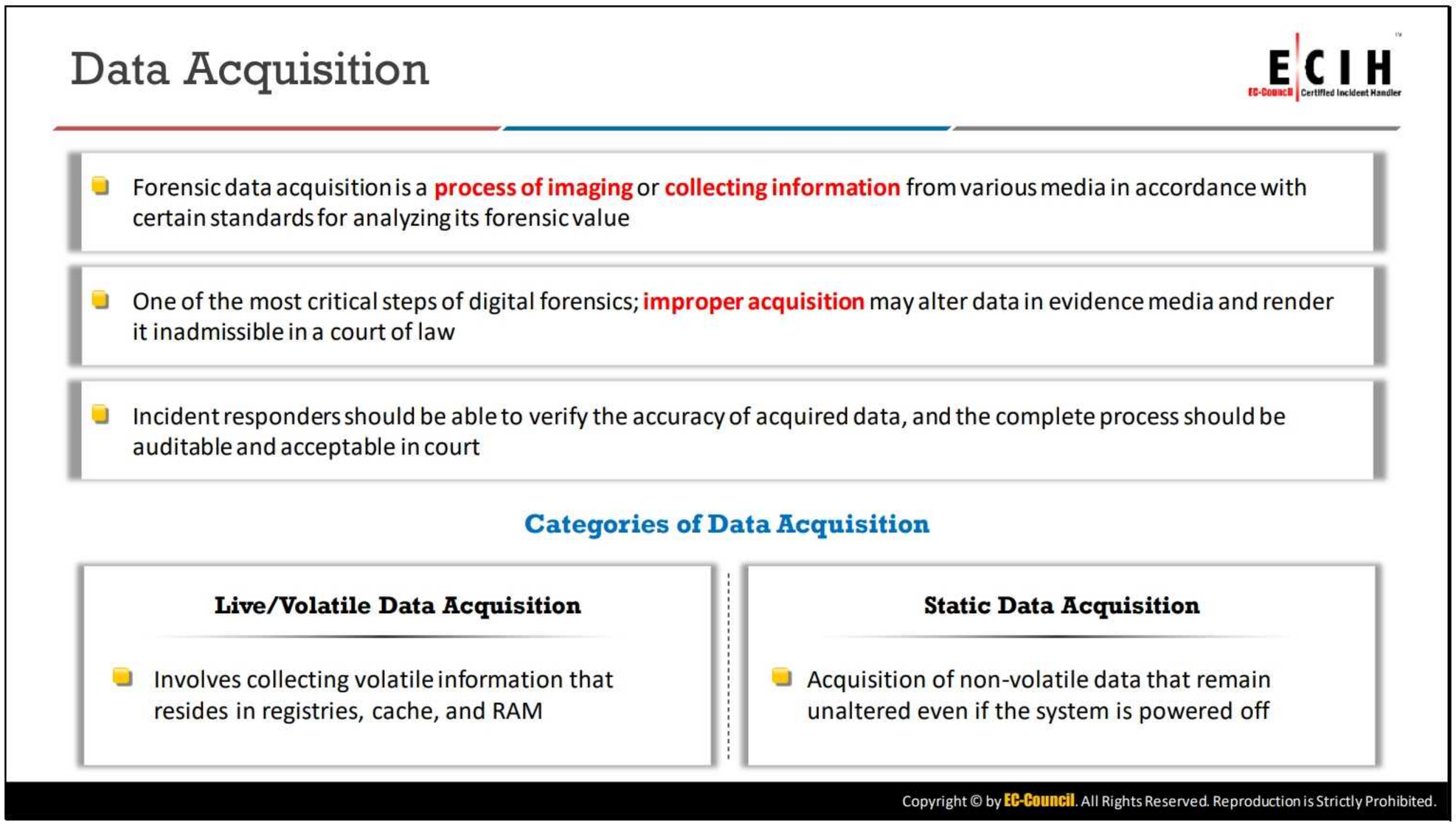
Overview of Data Acquisition

Data acquisition is the first pro-active step in the process of forensic investigation. The aim of forensic data acquisition is to extract every bit of information present on the victim's hard disk and create a forensic copy to use it as evidence in the court. In some cases, data duplication is preferable instead of data acquisition to collect the data. First responders/investigators can also present the duplicated data in court.

This section discusses about data acquisition, how to duplicate the data (imaging) and verify image integrity.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Data Acquisition

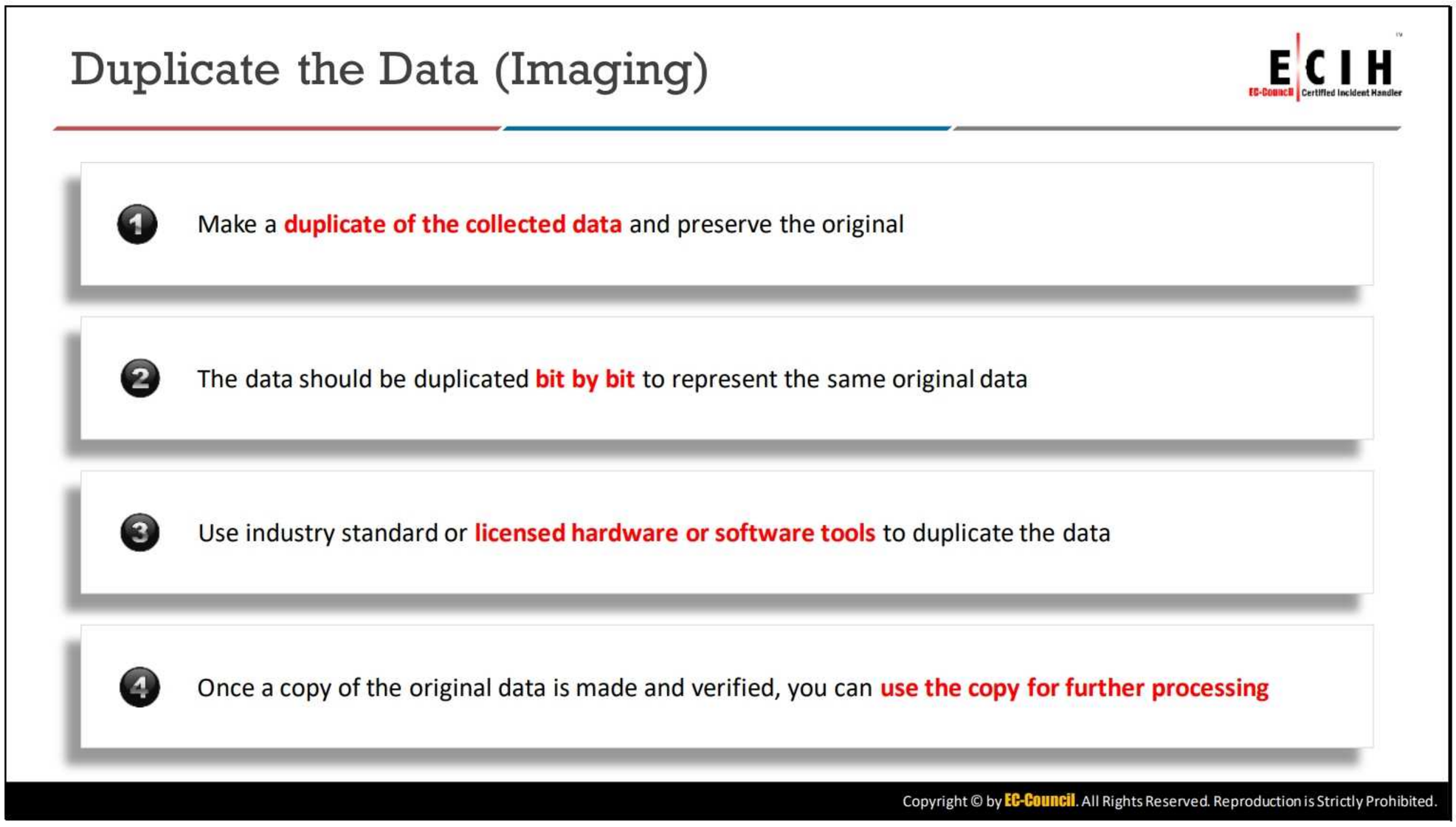
Data acquisition is the use of established methods to extract the Electronically Stored Information (ESI) from suspect computer or storage media to gain insight into a crime or an incident. Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value. It is one of the most critical steps of digital forensics as improper acquisition may alter data in evidence media and render it inadmissible in the court of law. Incident responders should be able to verify the accuracy of acquired data, and the complete process should be auditable and acceptable to the court. With the progress of technology, the process of data acquisition has become more accurate, simple, and versatile. It uses several types of electronic equipment, ranging from small sensors to sophisticated computers.

Following are the two categories of data acquisition:

- **Live/Volatile Data Acquisition:** It is the process of acquiring volatile data from a working computer (either locked or in sleep condition) that is already powered on. Volatile data are fragile and can be lost when the system loses power or the user switches it off. Such data are contained in registries, cache, and RAM. Since RAM and other volatile data are dynamic in nature, collection of this information should occur in real time.
- **Static Data Acquisition:** It is the process of acquiring nonvolatile or unaltered data remaining in the system after the system has been shut down. Incident responders can recover such data from hard drives and from slack space, swap files, and unallocated drive space. Other sources of nonvolatile data include DVD-ROMs, USB thumb drives, smartphones, and PDAs. Static acquisition is usually applicable for those computers that the police seize during a raid and include encrypted drives.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Duplicate the Data (Imaging)

Performing investigation on the original evidence can misdirect it to different results and could make the original evidence vulnerable. Data duplication is an important step in securing the original evidence. Investigating the original evidence can cause damage to the identity of the evidence that would make it no longer useful to the case.

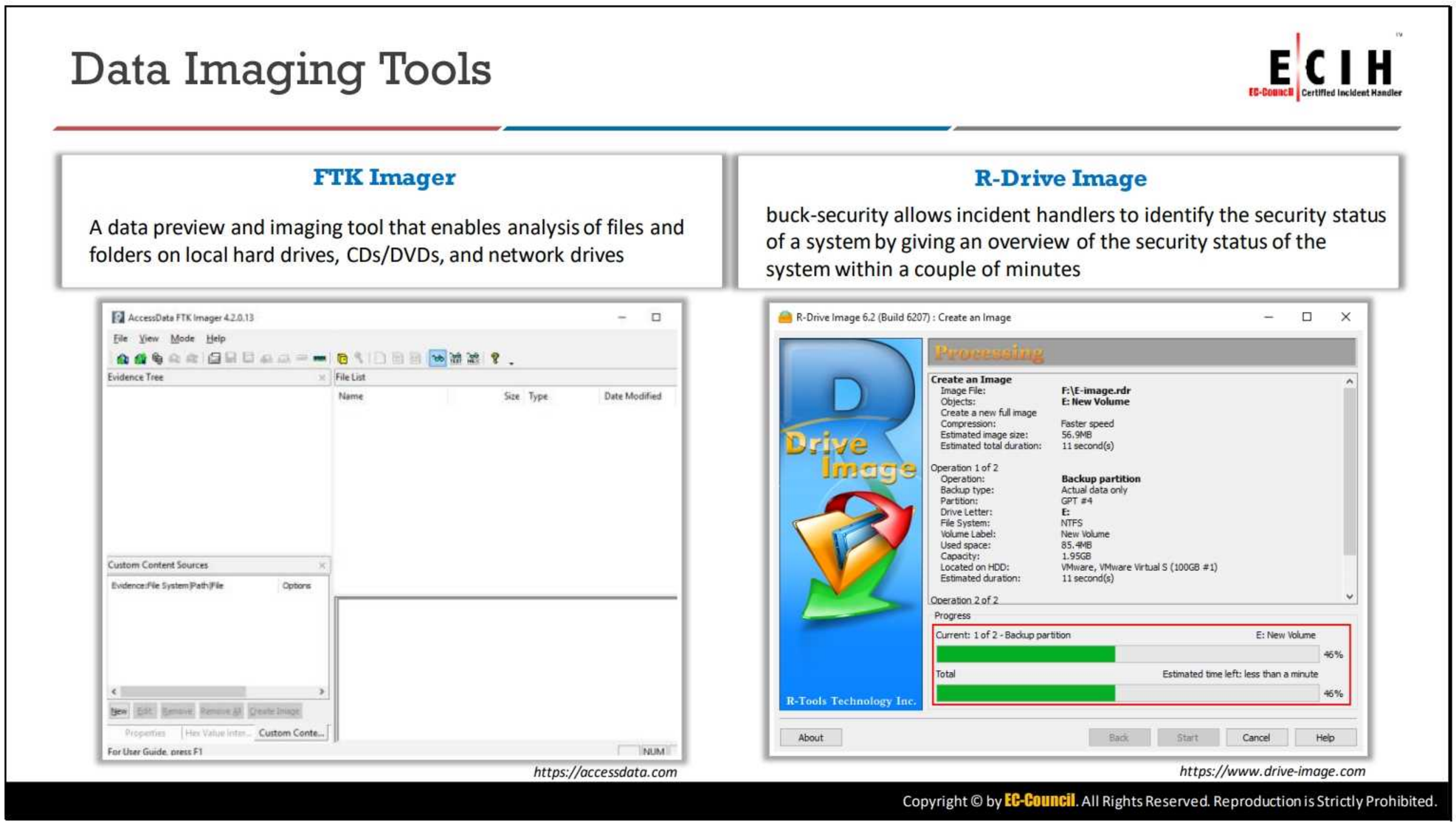
Data duplication includes bit-by-bit copying of the original data using a software or hardware tool. The duplicated data should be an exact blueprint of the original evidence and make two or more copies to perform different investigations. The copies can also help if one copy is damaged. Send the duplicated data to the forensics lab for investigation and further analysis.

The points to remember while duplicating the data:

- Make a duplicate of the collected data so as to preserve the original
- The data should be duplicated bit by bit to represent the same original data
- Use industry standard or licensed hardware or software tools to duplicate the data
- Once a copy of the original data is made and verified, you can use the copy for further processing

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Data Imaging Tools

Some important tools used for creating a duplicated bit by bit image are discussed as follows:

- **FTK Imager**

  Source: *https://accessdata.com*

  FTK Imager is a data previewing and imaging tool that enables the analysis of files and folders on local hard drives, CDs/DVDs, network drives, and examination of the content of forensic images or memory dumps. FTK Imager can also create MD5 or SHA1 hashes of files, review and recover files deleted from the Recycle Bin, export files and folders from forensic images to disk and mount a forensic image to view its contents in Windows Explorer.

- **R-Drive Image**

  Source: *https://www.drive-image.com*

  R-Drive Image is a potent utility that allows for the creation of disk image files for backup or duplication purposes. The R-Drive Image restores the images on the original disks, on any other partitions, or even on a hard drive's free space. Using the R-Drive Image, one can restore the system after heavy data loss has been caused by an operating system crash, virus attack, or hardware failure.

  Features:

  - A simple wizard interface
  - Image file compression
  - Removable media support

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

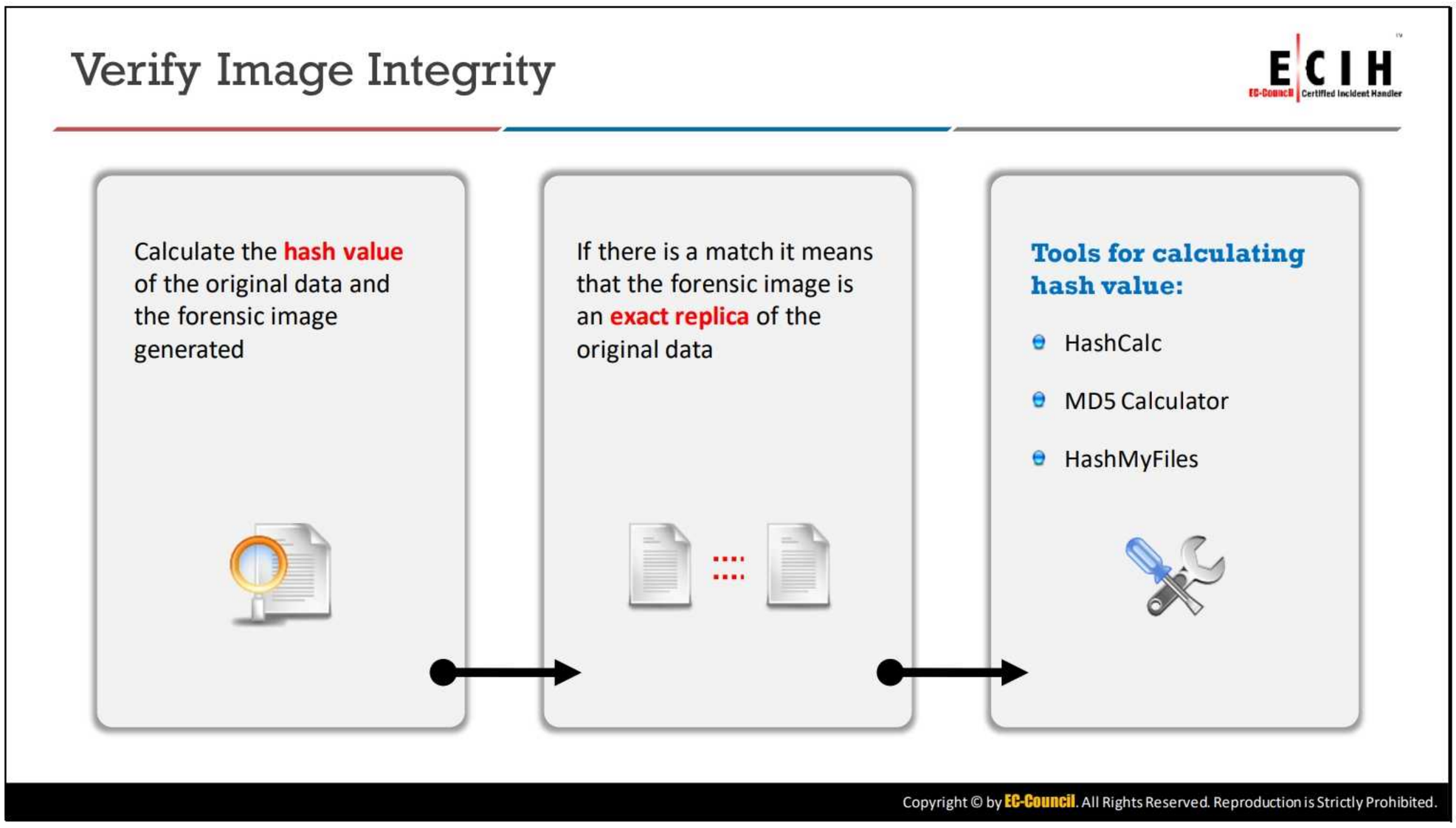
- Image files splitting
- Image Protection

Some data imaging tools are listed below:

- EnCase Forensic (*https://www.guidancesoftware.com*)
- Data Acquisition Toolbox (*https://in.mathworks.com*)
- RAID Recovery for Windows (*https://www.runtime.org*)
- R-Tools R-Studio (*https://www.r-studio.com*)
- F-Response Imager (*https://www.f-response.com*)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Verify Image Integrity

Hash values are equivalent to data fingerprints. No two files can contain the same hash values. MD5 and SHA are the two hash algorithms used in forensics, where the MD5 hash for the original evidence and the forensic image are calculated and compared. Same hash values indicate that the image is the same as the evidence.

The following steps can be performed to verify image integrity:

- Calculate the hash value of the original data and the forensic image generated
- If there is a match between the two, it means that the forensic image is an exact replica of the original data

Some tools used to calculate the hash value are discussed below:

- **HashCalc**

  Source: *https://www.slavasoft.com*

  The free calculator is used to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It allows for the calculation of hash (message digest), checksum and HMAC values based on the most popular algorithms, which include MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey (eDonkey2000,ed2k) and eMule tools.

- **MD5 Calculator**

  Source: *http://www.bullzip.com*

  This calculator helps in calculating the MD5 hash value of the selected file. By right clicking on the file, the "MD5 Calculator" can be chosen, and the program will then

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

calculate the MD5 hash. The MD5 Digest field contains the calculated value. To compare this MD5 digest to another, one can paste the other value into the Compare To field. Subsequently, an equal sign ("=") will appear between the two values if they are equal; otherwise, the less than ("<") or greater than (">") sign will appear, which implies that the values are different.

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles is a small utility that allows for the calculation of the MD5 and SHA1 hashes of one or more files in the system. It allows the copying of the MD5/SHA1 hashes list into the clipboard or save them into text/html/xml file. One can launch HashMyFiles from the context menu of Windows Explorer and display MD5/SHA1 hashes of the selected file or folder.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Understanding the Volatile Evidence Collection

- Why Are Volatile Data Important?
- Order of Volatility
- Volatile Data Collection Methodology
- Collecting Volatile Information
  - System Information
  - Current System Date and Time/Command History
  - Current System Uptime
  - Running Processes
  - Open Files, Clipboard Data, and Service/Driver Information
  - Logged-On Users
  - DLLs or Shared Libraries
  - Network Information
  - Network Connections

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

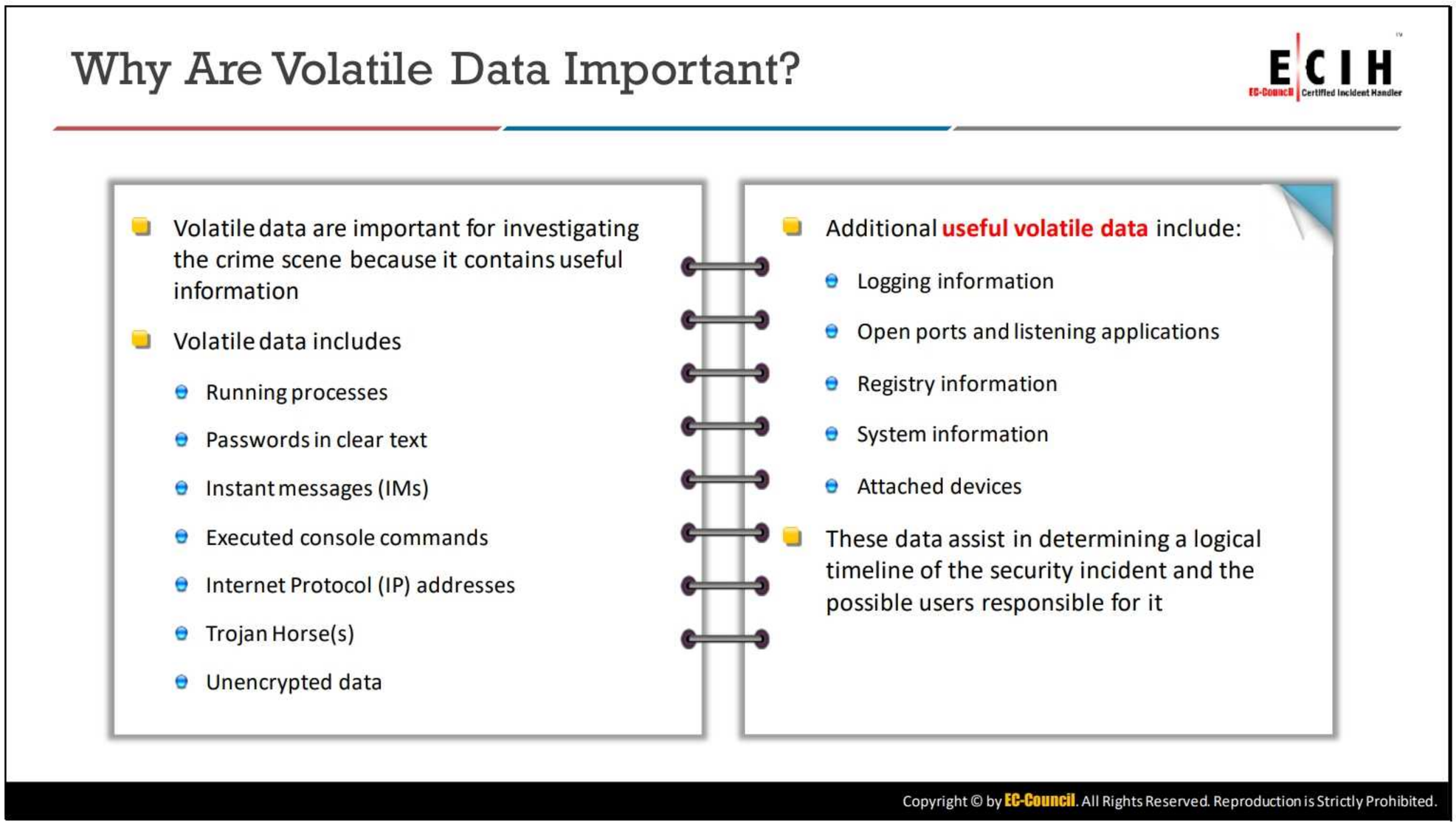
Understanding the Volatile Evidence Collection

Most systems store data related to the current session in temporary form across registries, cache, and RAM. These data are easily lost when the user switches the system off, thereby resulting in the loss of the session information. Therefore, first responders need to extract it as a priority.

This section explains the significance of volatile data, order of volatility, volatile data collection methodology, and collecting volatile information along with tools.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Why Are Volatile Data Important?

Volatile Information refers to the data stored in registries, cache, and RAM of digital devices. These data are lost or erased when the system is shut down or rebooted. The volatile information is dynamic in nature and time-variant; therefore, incident responders/investigators should be able to collect the data in real time.

Volatile data exists in the physical memory or RAM and consists of process information, process-to-port mapping, process memory, network connections, clipboard contents, state of the system, and so on. The incident responders/investigators must collect this data during the live data acquisition process.

The first step to take after finding the security incident report is to acquire the volatile data. Volatile data is crucial for investigating the crime scene because it contains useful information.

Volatile data includes:

- Running processes
- Passwords in cleartext
- Instant messages (IMs)
- Executed console commands
- Internet Protocol (IP) addresses
- Trojan horse(s)
- Unencrypted data

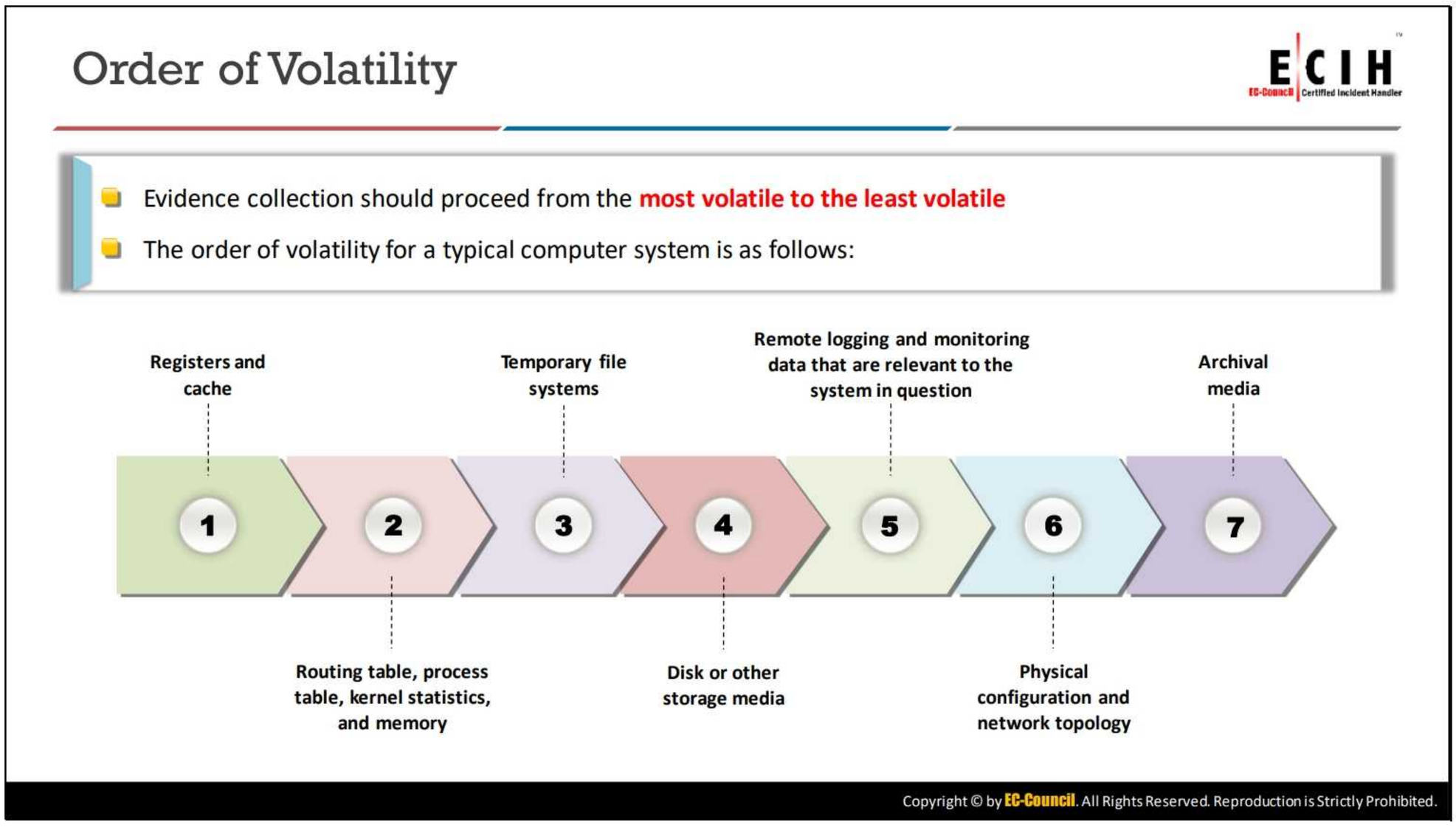
Additional useful volatile data includes:

- Logging information
- Open ports and listening applications
- Registry information
- System information
- Attached devices

This data assists in determining a logical timeline of the security incident and the possible users responsible.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Order of Volatility

Incident responders/investigators should always remember that the entire data do not have the same level of volatility and collect the most volatile data first during live acquisitions.

The order of volatility for a typical computer system is as follows:

- **Registers and cache**

  The information in the registers or the processor cache on the computer exists for a matter of nanoseconds. They are always changing and are the most volatile data.

- **Routing table, process table, kernel statistics, and memory**

  A routing table, ARP cache, kernel statistics information is in the ordinary memory of the computer. These are a bit less volatile than the information in the registers, with the life span of ten nanoseconds.

- **Temporary file systems**

  Temporary file systems tend to be present for a longer time on the computer compared to routing tables, ARP cache, and so on. These systems are eventually over written or changed, sometimes in seconds or minutes later.

- **Disk or other storage media**

  Data stored on a disk stays for a while. However, sometimes, things could go wrong and the data could get erased or written over. Therefore, disk data are can be volatile in nature and have a lifespan of only a few minutes.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Remote logging and monitoring data related to the target system**

  The data that travels through a firewall generates logs in a router or a switch. The system might store these logs somewhere else. The issue lies in that these logs can over write themselves, sometimes a day, an hour, or a week later. However, they are generally less volatile compared to a hard drive.

- **Physical configuration and network topology**

  Physical configuration and network topology are less volatile and have longer life spans as compared to some other logs.

- **Archival media**

  A DVD-ROM, a CD-ROM or a tape can have the least volatile data because the digital information does not change automatically, unless damaged by a physical force.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Volatile Data Collection Methodology

Step 1: Incident Response Preparation

- The following items should be ready before an incident occurs:
  - A first responder toolkit (responsive disk)
  - An **incident response team** (IRT) or designated first responder
  - Forensic-related policies that allow forensic data collection

Step 2: Incident Documentation

- Document all the information about the **security incident** needs and **maintain a logbook** to record all actions during the forensic collection

Step 3: Policy Verification

- Points to consider for policy verification:
  - Read and examine all the policies signed by the user of the suspicious computer
  - Determine the forensic capabilities and limitations of the incident responder/investigator by determining the legal rights (including a review of federal statutes) of the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Volatile Data Collection Methodology (Cont'd)

Step 4: Volatile Data Collection Strategy

- No two security incidents will be the same
- Use the first responder **toolkit logbook** and the questions from the graphic to develop the volatile data collection strategy that suits the situation and leaves the smallest possible footprint on the suspicious system

Step 5: Volatile Data Collection Setup

- A volatile data collection setup includes following steps:
  - **Establish a trusted command shell: Do not open or use a command shell** or terminal from the suspicious system
  - **Establish the transmission and storage method:** Identify and record the data transmission from the **live suspicious computer** to the remote data collection system as there will not be enough space on the response disk to collect forensic tool output
  - **Ensure the integrity of forensic tool output:** Compute an **MD5 hash** of the forensic tool output to ensure integrity and admissibility

Step 6: Volatile Data Collection Process

- Record the time, date, and command history of the system
- Establish an audit trail by generating dates and times while executing each forensic tool or command
- Start a command history to document all forensic collection activities; collect all possible volatile information from the system and network
- Do not shut down or restart a system under investigation until all relevant volatile data have been recorded

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Volatile Data Collection Methodology

The collection of volatile data plays a major role in crime scene investigation. To ensure that no data loss occurs during the collection of critical evidence, the investigators or incident responders should follow a proper methodology and provide a documented approach for performing activities in a responsible manner.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

A step-by-step procedure for volatile data collection methodology is discussed below:

- **Step 1: Incident Response Preparation**

  Eliminating or anticipating every type of security incident or threat is not possible. However, to collect all types of volatile data, responders must be ready to effectively react to the security incident. The incident responders who need to gather volatile data must have previous experience in collecting volatile data, proper permissions, and authorization from incident manager or security administrator or a person in authority must be hired before collecting the data.

  The availability of the following items should be ensured before the occurrence of an incident:

  - A first responder toolkit (response disk)
  - An incident response team (IRT) or designated first responder
  - Forensic-related policies allowing forensic data collection

- **Step 2: Incident Documentation**

  Ensure that the logs and profiles are stored in an organized and readable format. For example, use naming conventions for forensic tool output, record time stamps of log activities and include the identity of the forensic investigator or incident responder. Document all the information about the security incident needs and maintain a logbook to record all actions performed during the forensic collection. Use of the first responder toolkit logbook facilitates in choosing the best tools for investigation.

- **Step 3: Policy Verification**

  Ensure that the actions planned do not violate the existing network and computer usage policies and any rights of the registered owner or user as well. Points to consider for policy verification:

  - Read and examine all the policies signed by the user of the suspicious computer
  - Determine the forensic capabilities and limitations of the incident responder by determining the legal rights (including a review of federal statutes) of the user

- **Step 4: Volatile Data Collection Strategy**

  Security incidents can be varied with regard to their type and nature. The first responder toolkit logbook and the questions from the graphic to create the volatile data collection strategy that suits the situation and leaves a negligible amount of footprint on the suspicious system should be used.

  Devise a strategy based on considerations such as the type of volatile data, the source of the data, type of media used, and type of connection. Make sure that there is enough space to copy the complete information.

- **Step 5: Volatile Data Collection Setup**

  Volatile data collection setup includes the following steps:

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Establish a trusted command shell**

  Do not open or use a command shell or terminal from the suspicious system. This minimizes the footprint on the suspicious system and restricts the triggering of any kind of malware installed on the system.

- **Establish the transmission and storage method**

  Identify and record the data transmission from the live suspicious computer to the remote data collection system, as there will not be enough space on the response disk to collect the forensic tool output. For example: Netcat and Cryptcat, which transmit data remotely via a network.

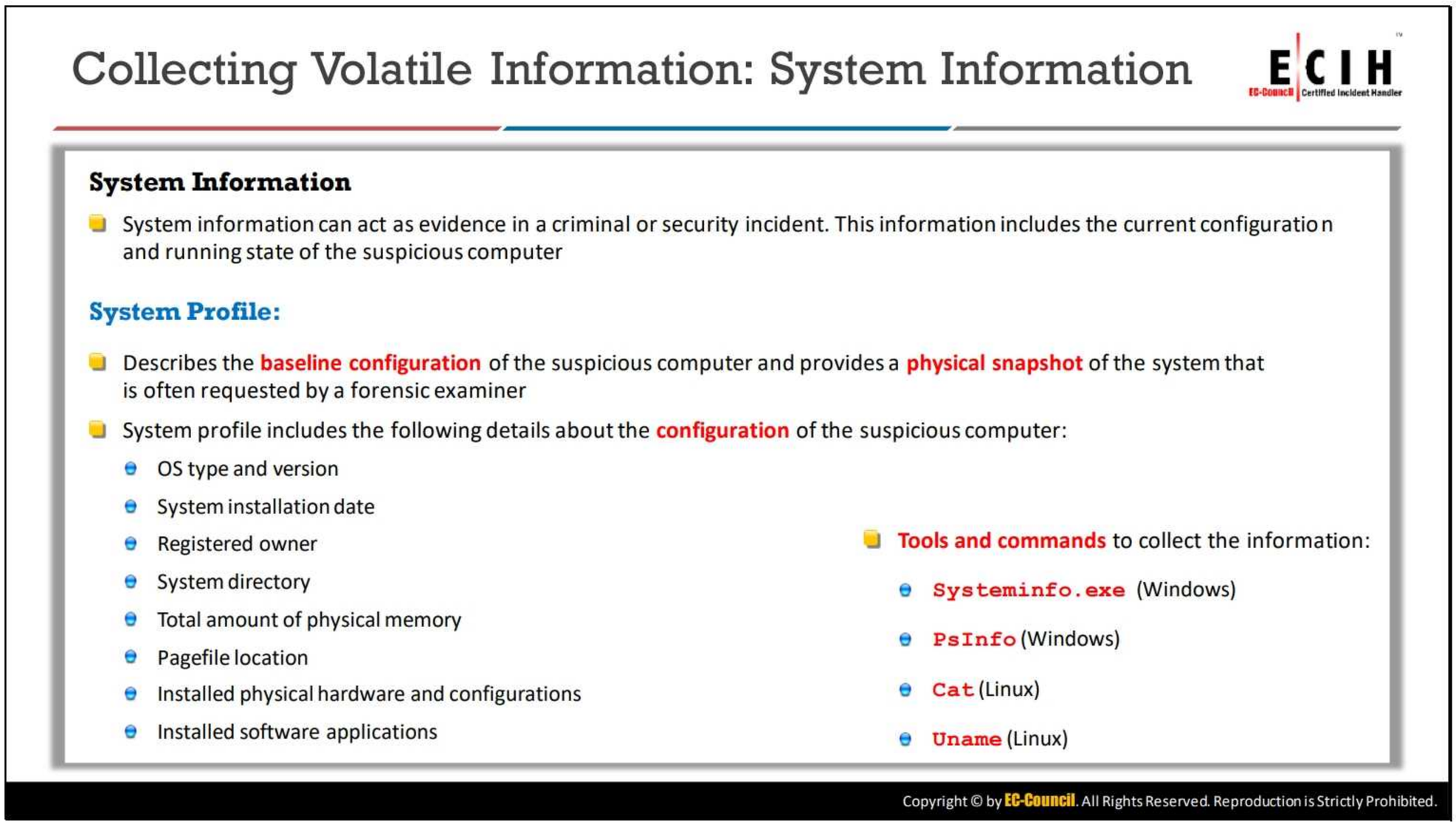
- **Ensure the integrity of forensic tool output**

  Compute an MD5 hash of the forensic tool output to ensure integrity and admissibility.

- **Step 6: Volatile Data Collection Process**
  - Record the time, date, and command history of the system
  - Establish an audit trail to generate the date and time while executing the forensic tool or command
  - Start a command history to document all the forensic collection activities. Collect all possible volatile information from the system and network
  - Do not shut down or restart a system under investigation until all the relevant volatile data have been recorded
  - Maintain a log of all the actions conducted on a running machine
  - Photograph the screen of the running system to document its state
  - Identify the operating system (OS) running on the suspect machine
  - Note the system date, time, and command history, if shown on the screen, and record using the current time
  - Check the system for the use of entire disk or file encryption
  - Avoid the use of the administrative utilities on the compromised system during an investigation, and in particular, be cautious when running diagnostic utilities
  - With the execution of each forensic tool or command, generate the date and time to establish an audit trail
  - Dump the RAM from the system to a forensically sterile removable storage device
  - Collect other volatile OS data and save these to a removable storage device
  - Determine the evidence seizure method (of hardware and any additional artifacts on the hard drive that may be determined to be of evidentiary value)
  - Build a full report documenting all the steps and actions taken

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: System Information

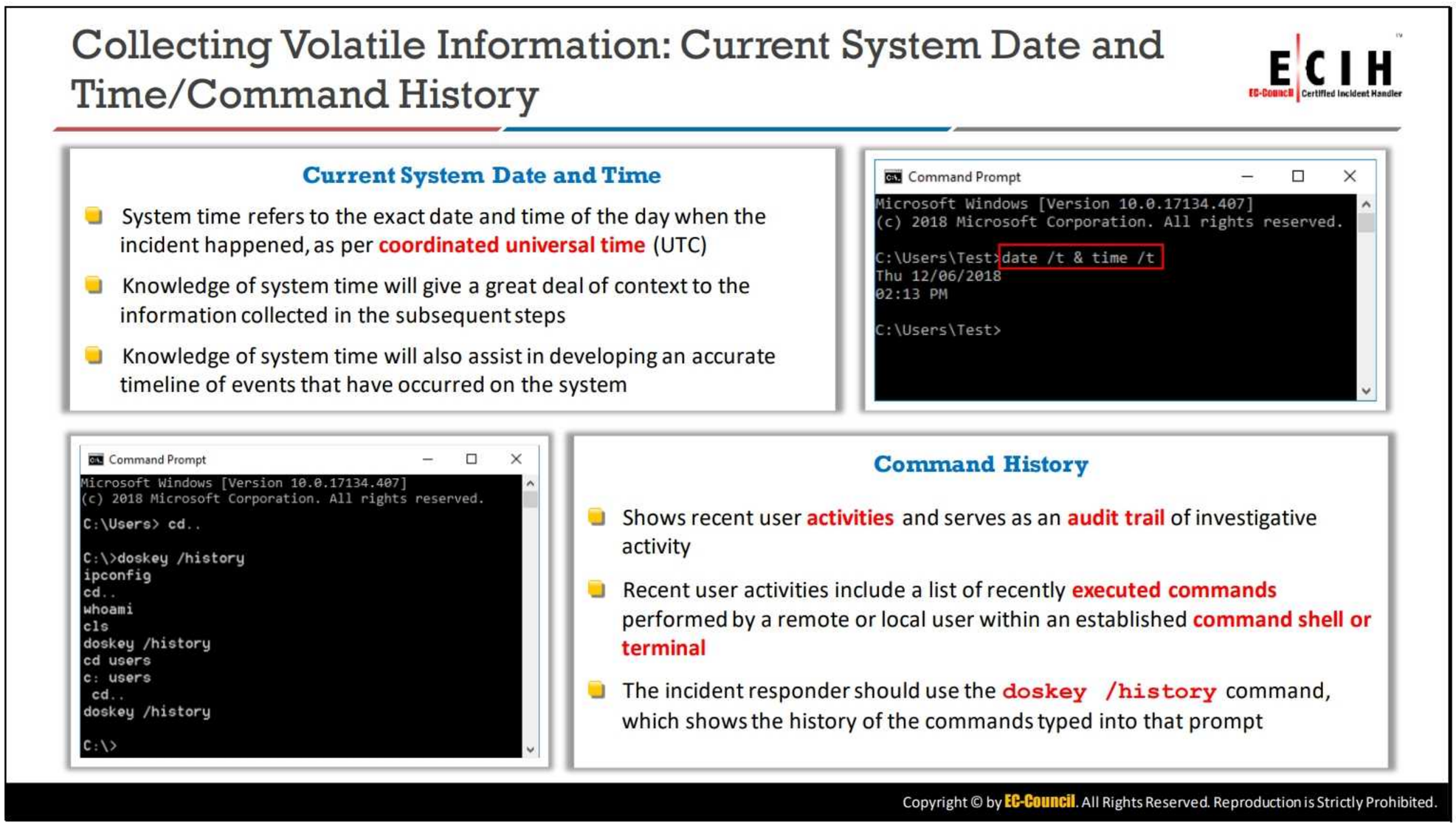
System information can act as an evidence in a criminal or security incident. This information includes the current configuration and running state of the suspicious computer.

System Profile:

- It describes the baseline configuration of the suspicious computer and provides a physical snapshot of the system that is often requested by a forensic examiner
- System profile includes the following details about the configuration of the suspicious computer:
  - OS type and version
  - System installation date
  - Registered owner
  - System directory
  - Total amount of physical memory
  - Pagefile location
  - Installed physical hardware and configurations
  - Installed software applications
- Tools and commands to collect the information:
  - Systeminfo.exe (Windows)
  - PsInfo (Windows)
  - Cat (Linux)
  - Uname (Linux)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Current System Date and Time/Command History

Current System Date and Time

Collection of system time is the first step to investigating an incident. System time refers to the exact date and time of the day when the incident occurred, as per the coordinated universal time (UTC). The system provides the system time so that the applications launched have access to the accurate time and date.

The knowledge of system time will give a great significant amount of context to the information collected in the subsequent steps. It will also assist in developing an accurate timeline of events that have occurred on the system. In addition to the current system time, information about the amount of time that the system has been running, also called the uptime, can also provide a considerable amount of context in the investigation process.

Incident responders also record the real time, also called the wall time, when recording the system time. Comparison of both these durations allows the incident responder to further determine the accuracy of the system clock. The responders can extract system time and date using the date /t & time /t command or the net statistics server command.

An alternative way for obtaining the system time details is by using the GetSystemTime function. This function copies the time details to a SYSTEMTIME structure that contains information of individual logged in members and the exact information of month, day, year, weekday, hour, minute, second, and milliseconds. Hence, this function provides better accuracy to the system time details.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

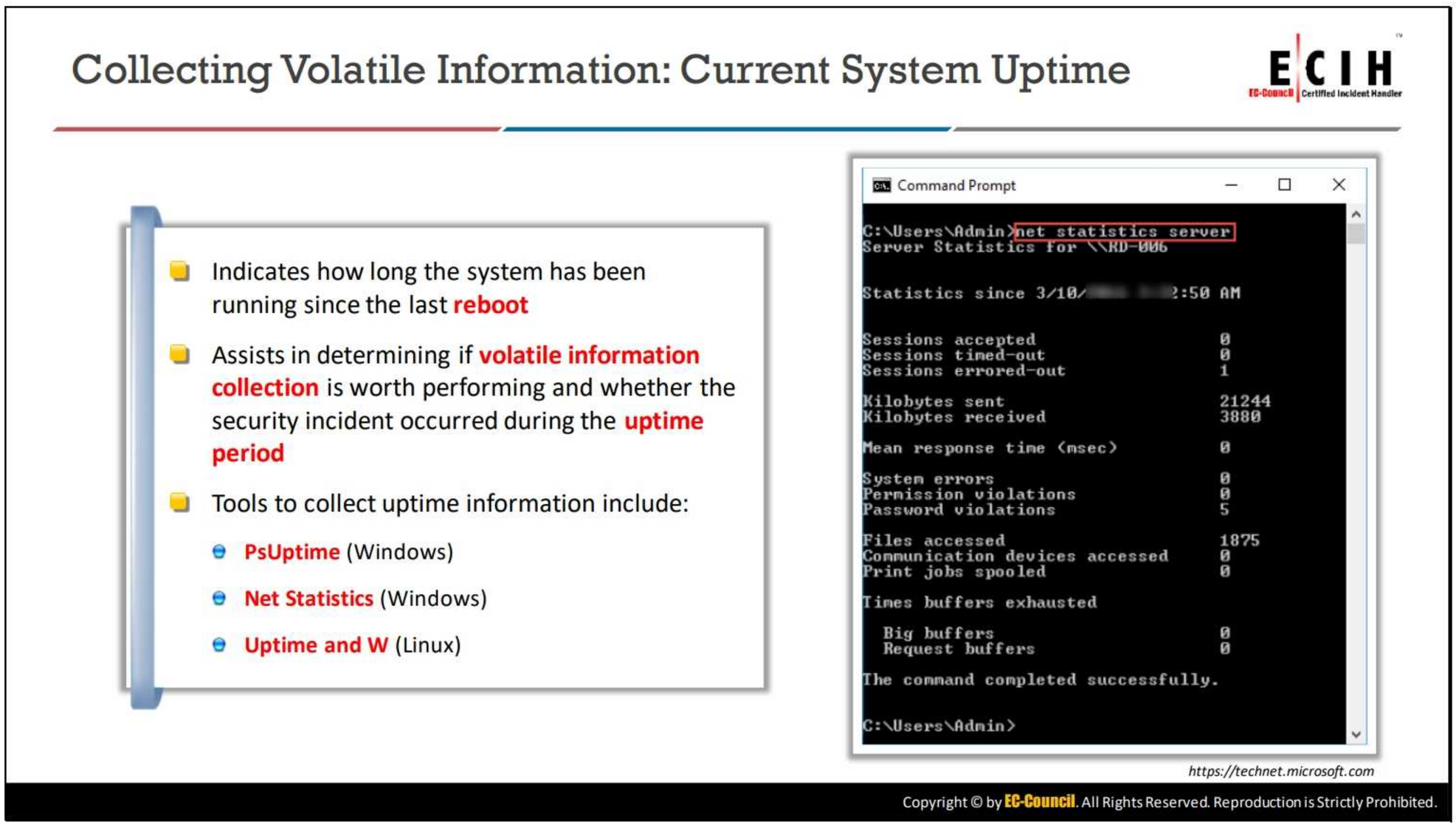
Command History

It shows the recent user activities and serves as an audit trail of the investigative activity. Recent user activities include a list of recently executed commands performed by a remote or local user within an established command shell or terminal. During investigation, if there are too many command prompts, the commands typed by the user, such as ftp or ping, could hide valuable clues.

Commands to look for include those used to manage user accounts, install software, and configure peripherals. To view the previously typed commands, the incident responder can run the scroll bar for the command prompt up. If the user had typed the **`cls`** command to clear the screen, the incident responder would not be able to use the scroll bar to see any of the commands that the user had entered. Instead, the incident responder should use the **`doskey /history`** command, which shows the history of the commands typed into that prompt.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Current System Uptime

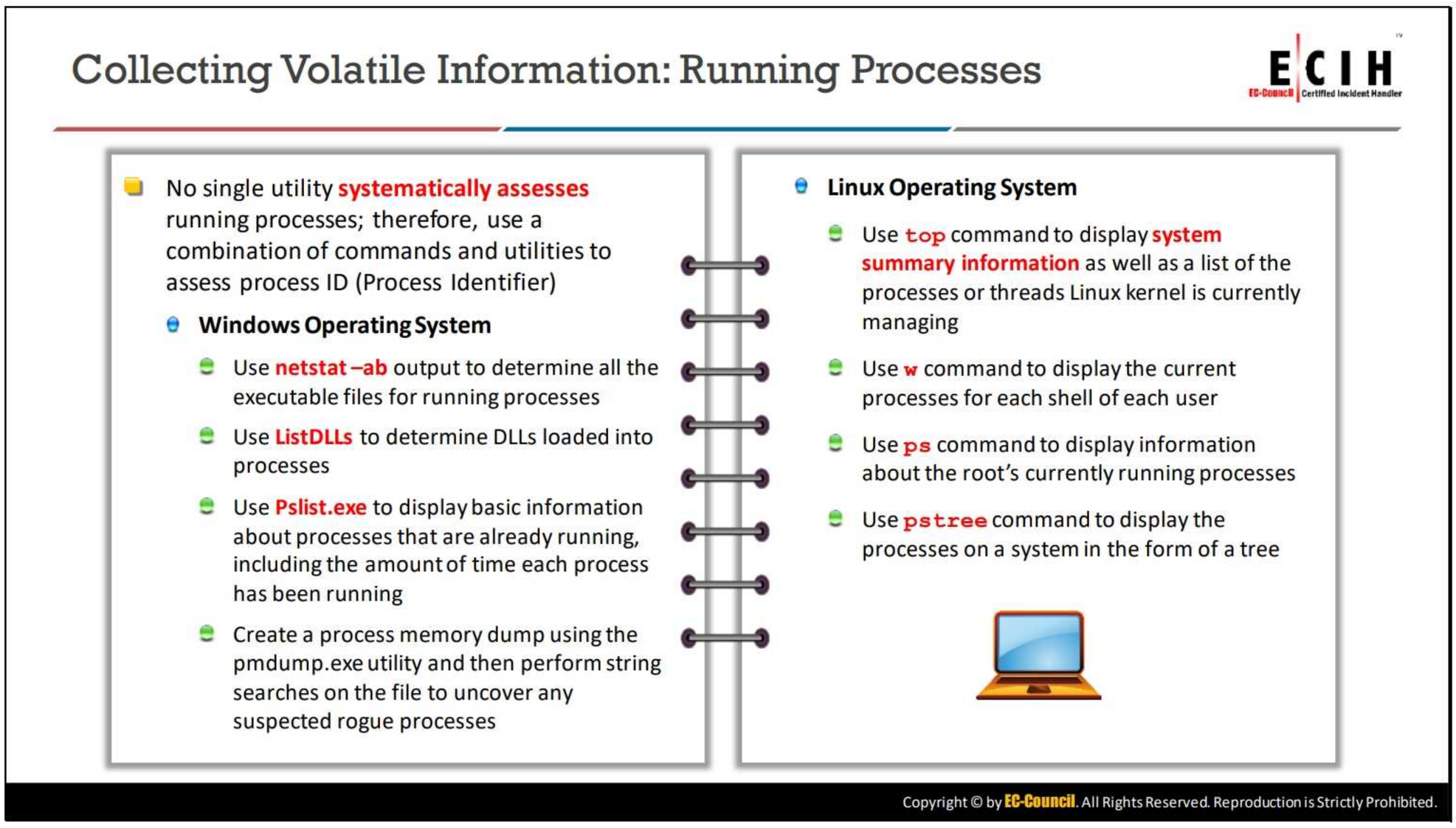
The current system Uptime indicates the duration for which the system has been running since the last reboot. It assists in determining if volatile information collection will be appropriate to perform and whether the security incident has occurred during this period.

The following tools can be utilized to collect uptime information:

- PsUptime (Windows)
- Net Statistics (Windows)
- Uptime and W (Linux)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Running Processes

The responders should gather information about all the processes running on the system. The Task Manager should be used to view information regarding the processes. However, the Task Manager cannot display all the required information at once. To retrieve information of the entire process, the following few parameters listed below should be specified:

- The full path to the executable image (.exe file)
- The command line used to launch the process, if any
- The amount of time that the process has been running
- The security/user context that the process is running in
- The modules the process has loaded
- The memory contents of the process

The responders must learn to adopt certain other sources or tools and commands to collect the complete details regarding the process. No single utility can systematically assess the running processes. Therefore, a combination of the following commands and utilities can be adopted to assess the process ID (Process Identifier):

- **Windows Operating System**
  - Use **netstat –ab** output to determine all the executable files for the running processes.
  - Use **ListDLLs** to determine DLLs loaded into processes. It is a utility that reports the DLLs loaded into processes. You can use it to list all the DLLs loaded into all the processes, into a specific process, or to list the processes that have a particular DLL

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

loaded. ListDLLs can also display the full version information for DLLs, including their digital signature, and can scan processes for unsigned DLLs.

- Use **Pslist.exe** to display basic information about the already running processes on a system, including the amount of time each process has been running (in both kernel and user modes). For example, Pslist-x switch shows processes, memory information, and threads.
- Create a process memory dump using the pmdump.exe utility and then perform string searches on the file to find details about the suspected rogue process.

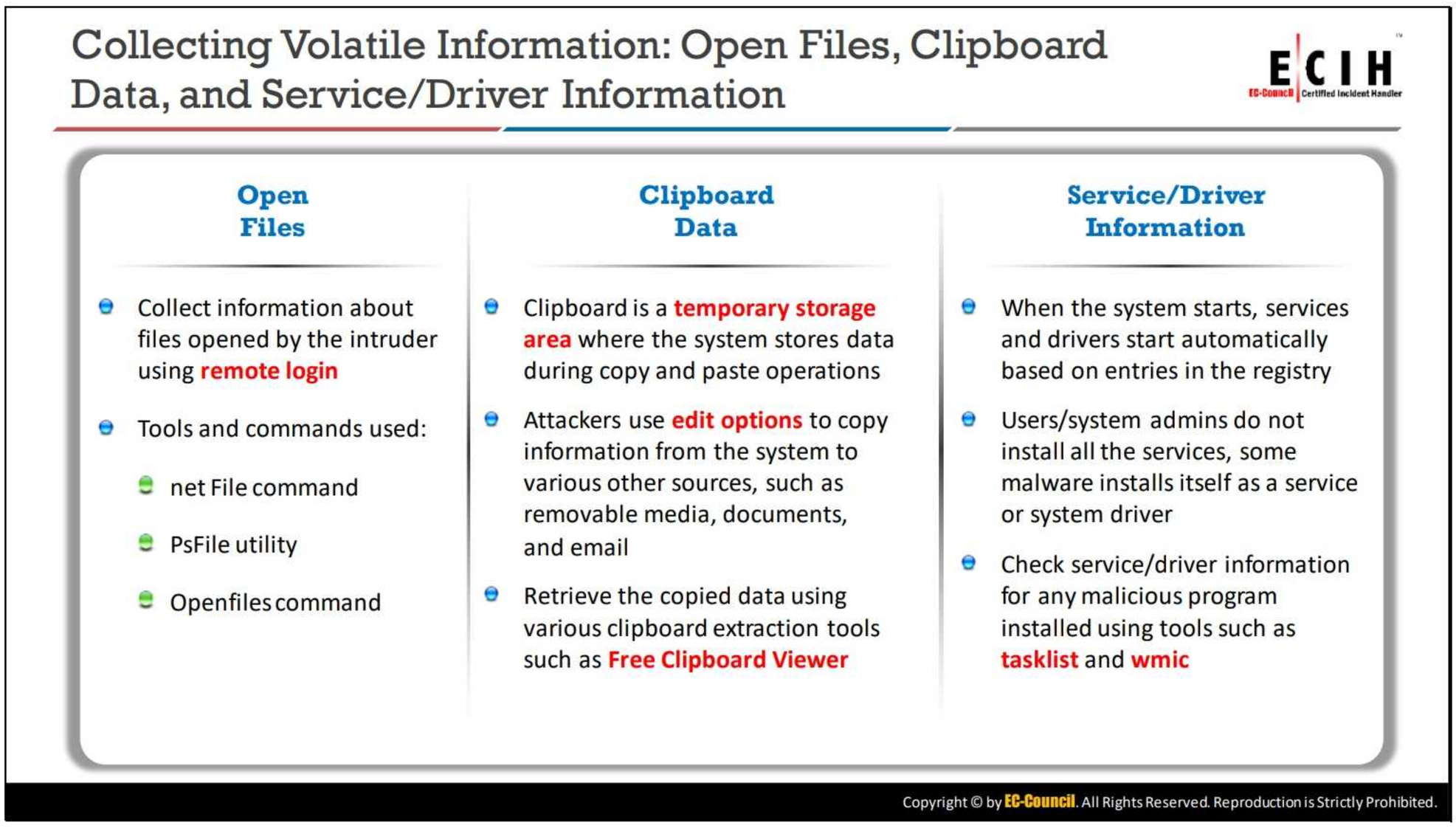
- **Linux Operating System**
  - Use **`top`** command to display system summary information as well as a list of processes or threads the Linux kernel is currently managing
  - Use **`w`** command to display the current processes for each shell of each user
  - Use **`ps`** command to display information about the root's currently running processes
  - Use **`pstree`** command to display the processes on a system in the form of a tree

Collection of information regarding the running processes has the following advantages:

- Assistance to analysts in the detection of legitimate versus malicious or rogue processes
- Identification of unauthorized running software applications
- Identification of premature termination of legitimate processes
- Identification of unusual filenames or extra processes (i.e., those not due to normal, authorized activities)
- Detection of processes that have terminated prematurely
- Identification of processes that are run at unexpected times
- Identification of processes that have unusual user identification associated with them

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Open Files, Clipboard Data, and Service/Driver Information

- **Open Files**

  When the output obtained from psloggedon.exe commands shows the incident responders that there are users logged on to the system remotely, then the incident responders will also want to see what files they have opened, if any. Many a times, when someone accesses a system remotely, they might be looking for something specific while opening the files.

  A user in a corporate environment could have shared available content and allowed other users to view images, download songs, and so on. Anyone can easily gain access to poorly protected systems connected to the internet, with no administrator password (and no firewall), and search for files, and may even copy them. Tools and commands that show files opened remotely on a system include the net file command, psfile.exe, and openfiles.exe.

- **Clipboard Data**

  Clipboard is a temporary storage area, where the system stores data during copy and paste operations. Most Windows applications provide this functionality through the Edit option on the menu bar. Clicking Edit reveals a drop-down menu, which contains choices, like cut, copy, and paste. The user selects text or other data, chooses copy, and then chooses Paste to insert that data somewhere else. The cut functionality removes the data from the document the user is working on, and that data is transferred to the clipboard.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

When a user performs any cut/copy function, and then pastes the content into the document, the information cut/copied is copied to the clipboard and as long as the computer has uninterrupted power supply, or the user does not log out, the system neither adds nor deletes the clipboard contents.

Attackers use edit options to copy information from the system to various other sources, such as removable media, documents, and email. Responders can retrieve the copied data from the clipboard contents, by using various clipboard extraction tools such as Free Clipboard Viewer.

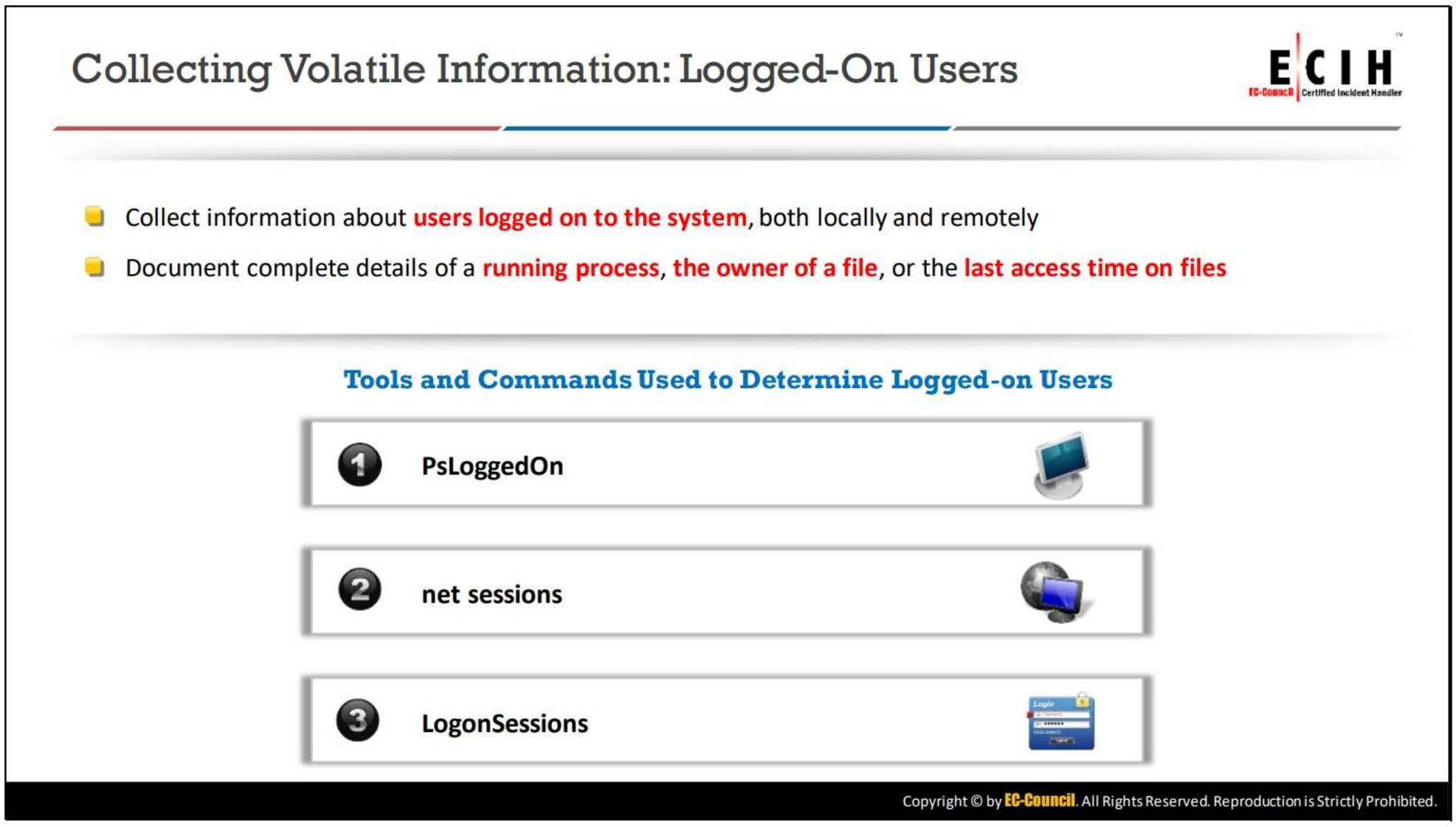
- **Service/Driver Information**

  Based on the entries in the registry, the services and drivers start automatically when the system is started. Most users do not even see these running services as processes, because there are no obvious indications, which differs from the case of regular processes, which are clearly indicated to the user. The user or even the system administrators necessarily do not install all the services. Some malwares install themselves as a service or even as system drivers. Check service/device information for any malicious program installed.

  Responders can gather services information using the **`tasklist`** command line tool. The tool will display image name and related PID services. The responders can also use the Windows Management Instrumentation Command (wmic) to view the list of running services, their process IDs, startmode, state and status.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Logged-On Users

During an investigation, the responders must gather details of all the users logged on to the suspected system. This not only includes the information of people logged on locally (via the console or keyboard) but also those who had remote access to the system (e.g. - via the net use command or via a mapped share). This information allows an incident responder to add context to other information collected from the system, such as the user context of a running process, the owner of a file, or the last access times on files. It is also useful to correlate the collected system time information with the Security event log, particularly if the admin has enabled appropriate auditing.

Some tools and commands that can be used to determine logged-on users are as follows:

- **PsLoggedOn Tool**

  PsLoggedOn is an applet that displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one. If you specify a user name instead of a computer, PsLoggedOn searches the computers in the network neighborhood and tells you if the user is currently logged on.

  Syntax: **`psloggedon [-] [-l] [-x] [\\computername | username]`**

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

-	Shows the options and the measurement units for output values.
-l	Displays only local logons
-x	Does not display logon times.
\\computername	System name for which logon information should be shown
username	Searches the network for those systems to which that user is logged on.

Table 3.1: PsLoggedOn tool options

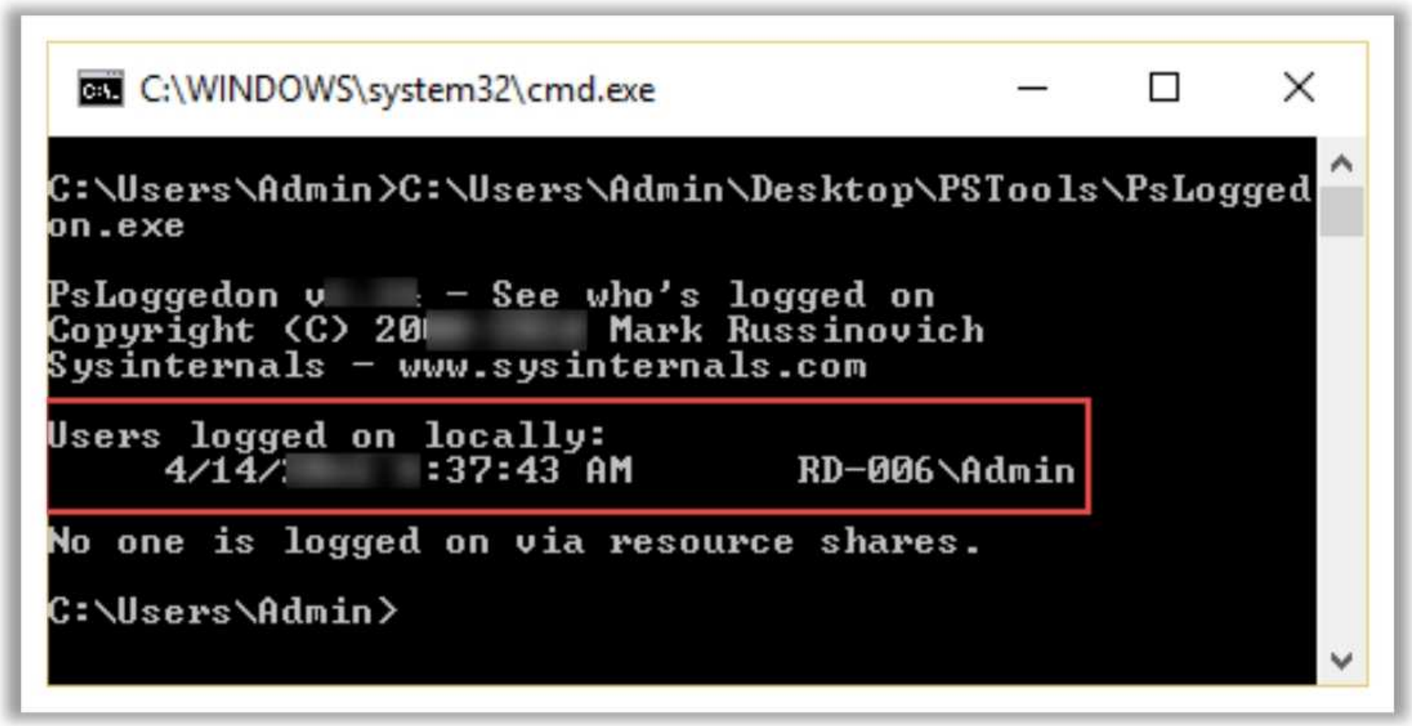


Figure 3.1: Screenshot showing output of PsLoggedOn tool

- **net sessions Command**

  The net sessions command helps to manage server connections. It is used without parameters and it displays information about all logged in sessions of the local computer. By using this command, one can view the computer names and user names on a server. It can also help us to see if users have any open files and how long each user's session has been in the idle mode.

  Syntax: **`net session [\\ComputerName] [/delete]`**

  \\ComputerName: Identifies the computer for which you want to list or disconnect sessions.

  /delete: Ends the computer's session with ComputerName and closes all open files on the computer for the session.

  net help command: Displays help for the specified net command.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

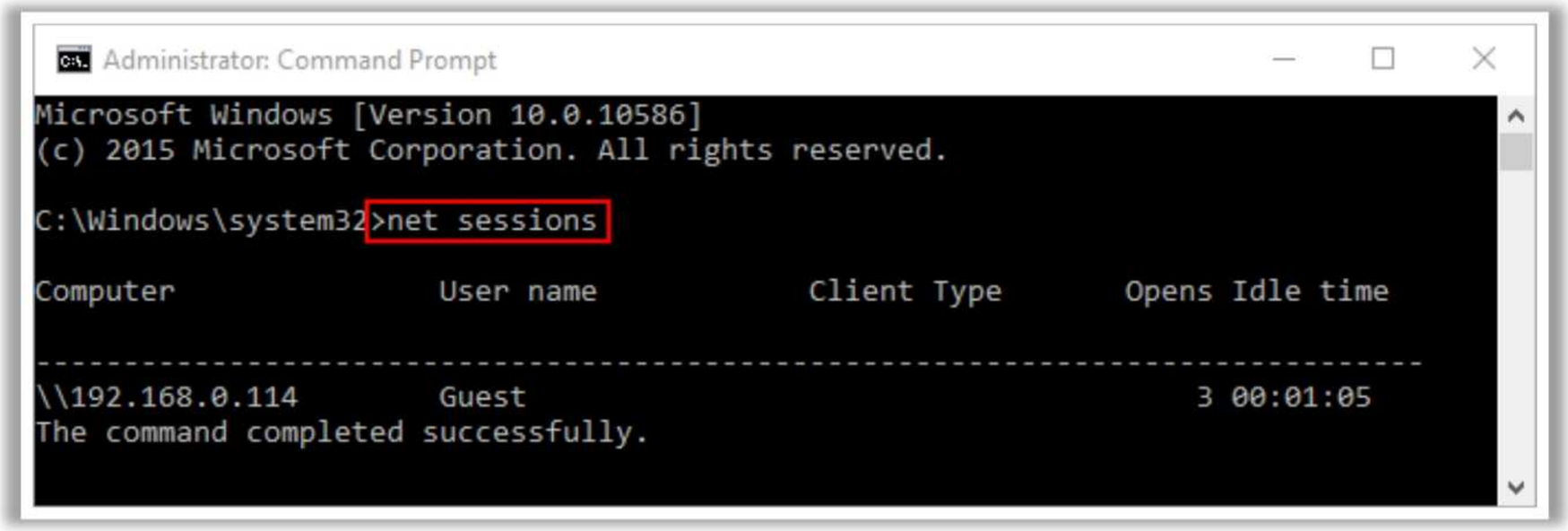


Figure 3.2: Screenshot showing output of net sessions command

- ## LogonSessions Tool

It lists the currently active logged-on sessions and, if you specify the -p option, it can provide you the information regarding the processes running in each session.

Syntax: **`logonsessions [-c[t]] [-p]`**

-c	Prints output as CSV
-ct	Prints output as tab-delimited values
-p	Lists processes running in logged-on sessions

Table 3.2: LogonSessions Tool Options

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

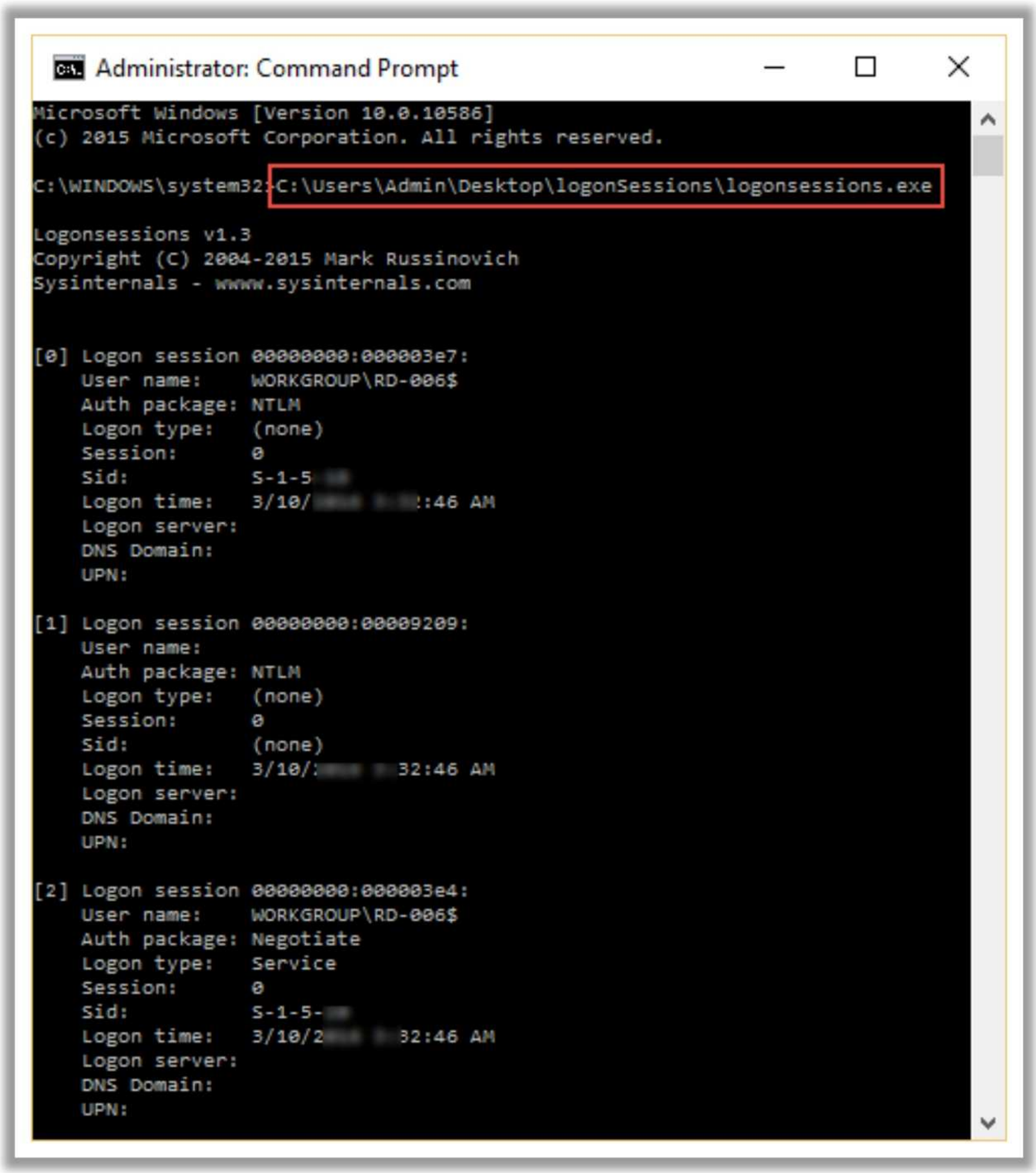


Figure 3.3: Screenshot showing output of LogonSessions tool

- **Who (Linux: Local Users)**

  It displays the user that is currently logged on locally

- **Who Am I, Who –uH (Linux: Local Users)**

  It determines the currently logged on user, whereas Who –uH displays the idle times for logged on users

- **Who –all/–a (Linux: Local and Remote Users)**

  It displays all currently logged on users, local and remote

- **Last (Linux: Local and Remote Users)**

  It displays a history of logged on users, local and remote

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Lastlog (Linux: Local and Remote Users)**

  It displays the last login times for system accounts

- **W (Linux: Local and Remote Users)**

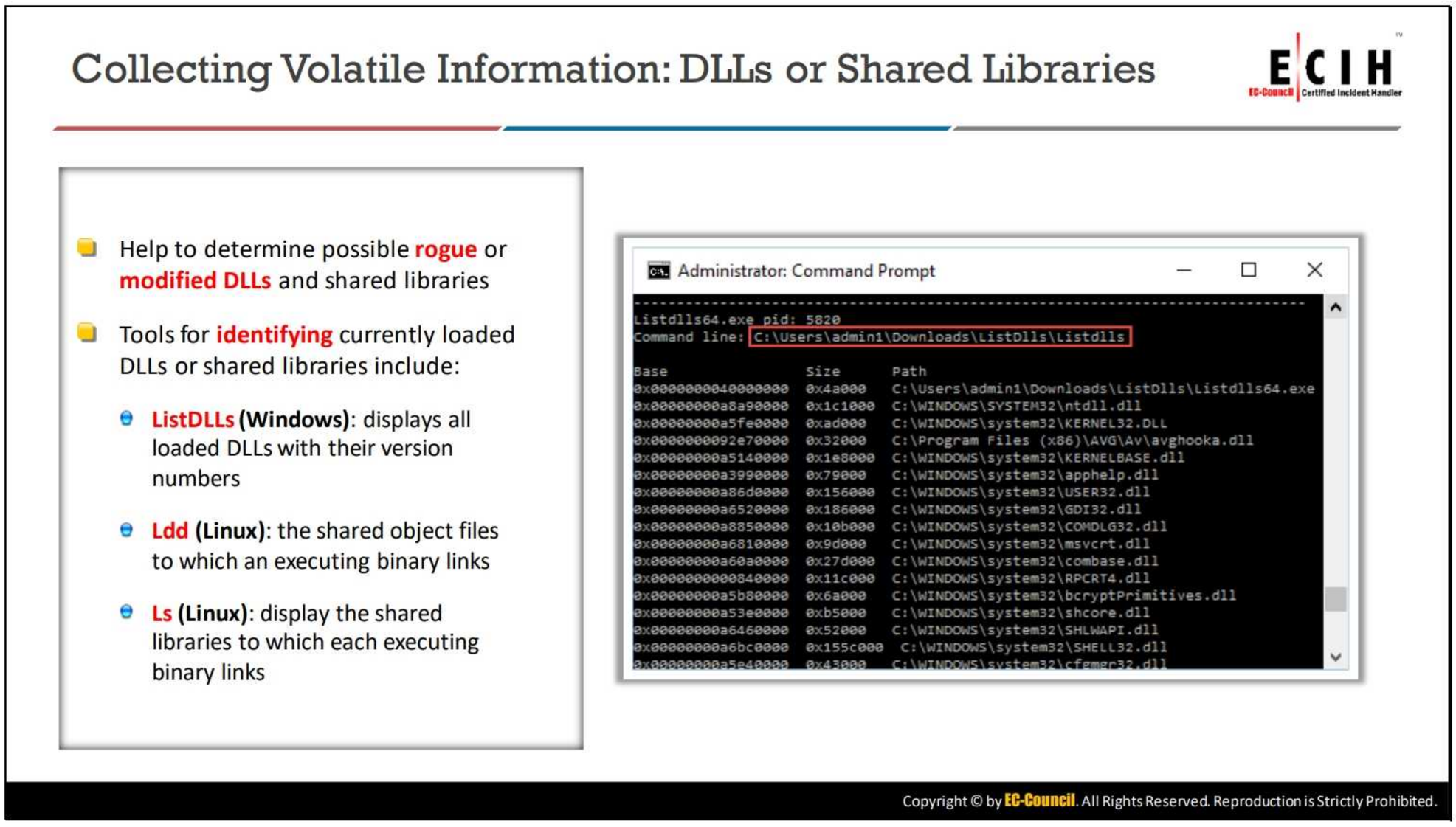
  It displays summaries of system usage, currently logged on users, and logged on user activities

- **Passwd (Linux: Local and Remote Users)**

  It contains user account information, including one-way encrypted passwords

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: DLLs or Shared Libraries

Shared libraries are object files that are used by installed programs and executables to load different modules. These libraries share resources that are common among different applications. Collecting information about shared libraries helps in determining possible rogue or modified DLLs and shared libraries.

Tools that help to identify currently loaded DLLs or shared libraries include: ListDLLs (Windows) displays all loaded DLLs with their version numbers, Ldd (Linux) the shared object files to which an executing binary links, and Ls (Linux) display the shared libraries to which each executing binary links.

- **ListDLLs**

  ListDLLs is a utility that reports the DLLs loaded into processes. You can use it to list all DLLs loaded into all the processes, into a specific process, or to list the processes that have a DLL loaded. ListDLLs can also display the full version information for DLLs, including their digital signature, and can also scan processes for unsigned DLLs.

  Syntax:

  ```
  listdlls [-r] [-v | -u] [processname|pid]
  listdlls [-r] [-v] [-d dllname]
  ```

  Parameters:

  - Processname: Dump DLLs loaded by process (partial name accepted)
  - Pid: Dump DLLs associated with the specified process id
  - Dllname: Shows only processes that have loaded the specified DLL

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

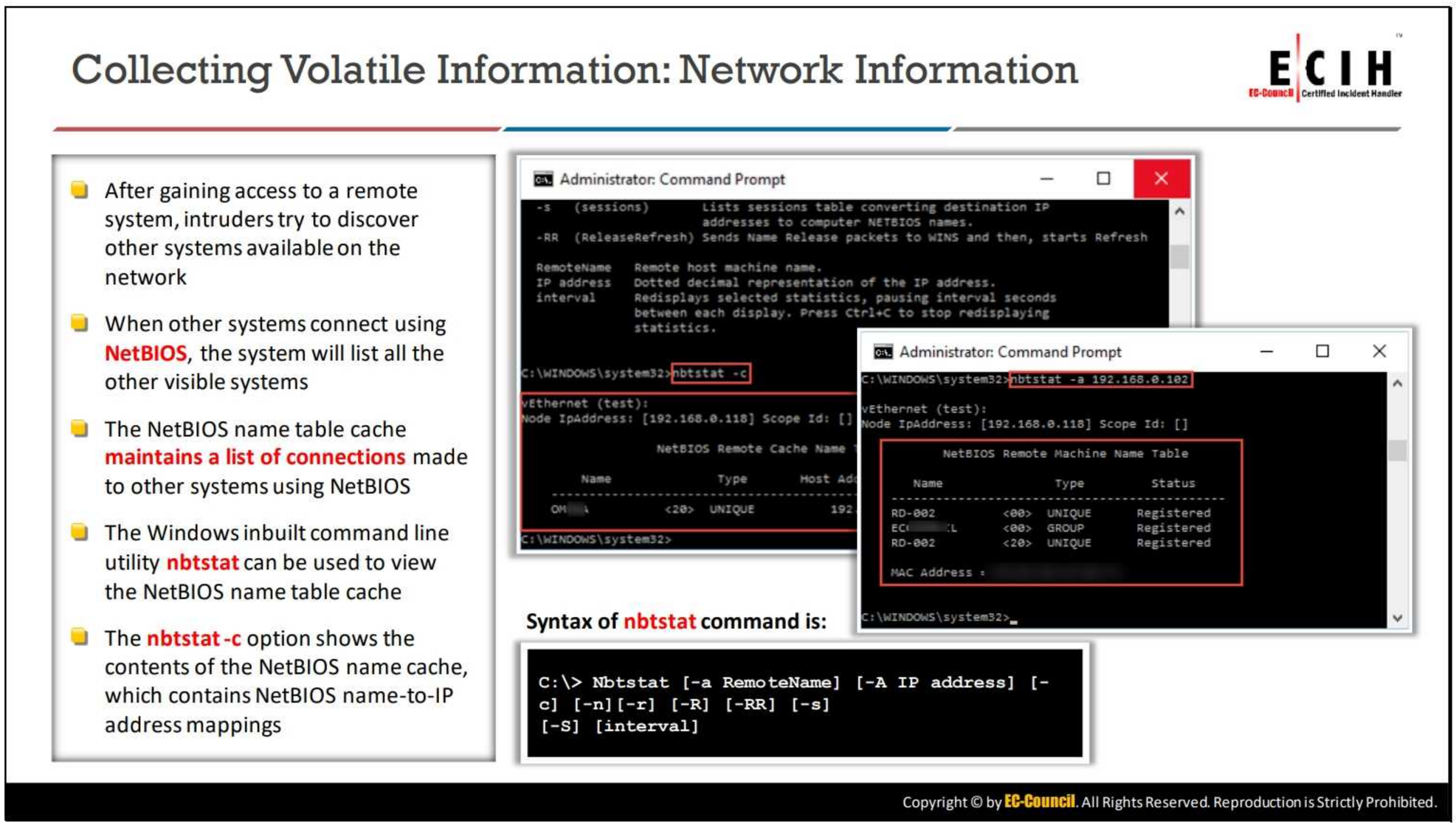
@UN5TABLE

- -r: Flags DLLs that relocated because they are not loaded at their base address
- -u: Lists unsigned DLLs
- -v: Shows DLL version information

The tool displays the full path of the loaded module as well as the version of the loaded DLL. Using this information, the responders can find the actual code. Spyware, Trojans, and even rootkits use a technique called DLL injection to load them into the memory space of a running process.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Network Information

Sometimes when intruders gain remote access to a system, they try to find the other systems connected to the network and visible to the compromised system. To achieve this, the intruders create and execute batch files in the system and launch net view commands via SQL injection (using a browser to send commands to the system through the web and database servers).

When the users establish connections with other systems using NetBIOS Networking, the systems maintain a list of other visible systems. By viewing the contents of the cached name table, the responder may be able to determine other affected systems. The responder should collect different types of network information to find evidence of the suspected incident. The network information useful for the investigation includes the following:

- Data content, such as header information and text
- Session information revealing particular data concerned with the investigation
- IDS/IPS log data
- Other network information such as secure file transfers

Network data captured from various network areas includes information regarding the following:

- IDS/IPS or firewall logs
- Network protocols
- Server or application logs
- Tracing network packets

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Port scan results
- Live data capture

The NetBIOS name table cache maintains a list of connections made to other systems using NetBIOS Networking. It contains the name and IP address of the remote system. You can use the Windows built-in command line utility Nbtstat to view the NetBIOS name table cache.

- **Nbtstat**

  Source: *https://docs.microsoft.com*

  Nbtstat helps in troubleshooting NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to the IP addresses.

  The syntax of the Nbtstat command is as follows:

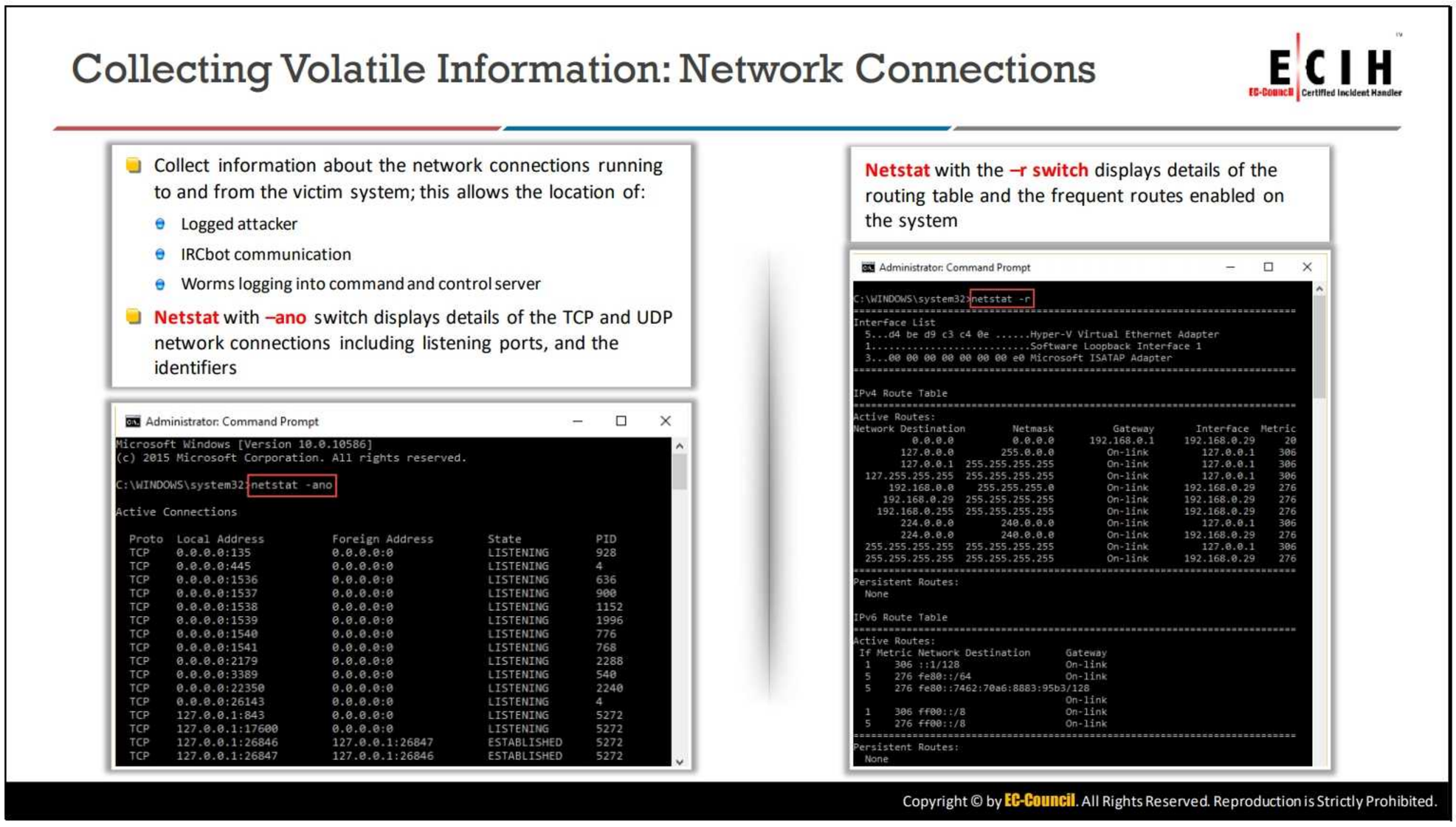
  ```
  Nbtstat [ [-a RemoteName] [-A IP address] [-c] [-n][-r] [-R] [-RR] [-s]
  [-S] [interval] ]
  ```

  Nbtstat with the –c switch shows the NetBIOS name table cache.

  - **`nbtstat -c`**: This option shows the contents of the NetBIOS name cache, which contains the NetBIOS name-to-IP address mappings.
  - **`nbtstat -n`**: This displays the names that have been registered locally on the system by NetBIOS applications such as the server and redirector.
  - **`nbtstat -r`**: This command displays the count of all the NetBIOS names resolved by broadcast and by querying a WINS server.
  - **`nbtstat -S`**: This option is used to list the current NetBIOS sessions and their statuses.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Collecting Volatile Information: Network Connections

The incident responder should collect information regarding network connections to and from the affected system, immediately after the report of an incident. If this is ignored, then the information may expire over time.

The incident responders should thoroughly observe the system and determine if the attacker has logged out or is still accessing the system. It is also crucial to find out if the attacker has installed any worm or IRCbot for communicating the data out of the system, and immediately search for other infected systems, updating itself, or logging into a command and control server. This information can provide vital clues and add context to other information that the incident responder has already collected.

- **Netstat**

  Source: *https://docs.microsoft.com*

  Netstat tool helps in collecting information about network connections operating in a Windows system. This CLI tool provides a simple view of TCP and UDP connections, as well as their state and network traffic statistics. Netstat.exe is a tool built-in with the Windows operating system. The most common way to run Netstat is with the use of the -ano switches. These switches command the program to display the TCP and UDP network connections, listening ports, and the identifiers of the processes (PIDs).

  Using Netstat with the -r switch will display the routing table and show persistent routes enabled in the system, if any. This can provide some vital information to an incident responder or even to an administrator to troubleshoot their system.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Syntax

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

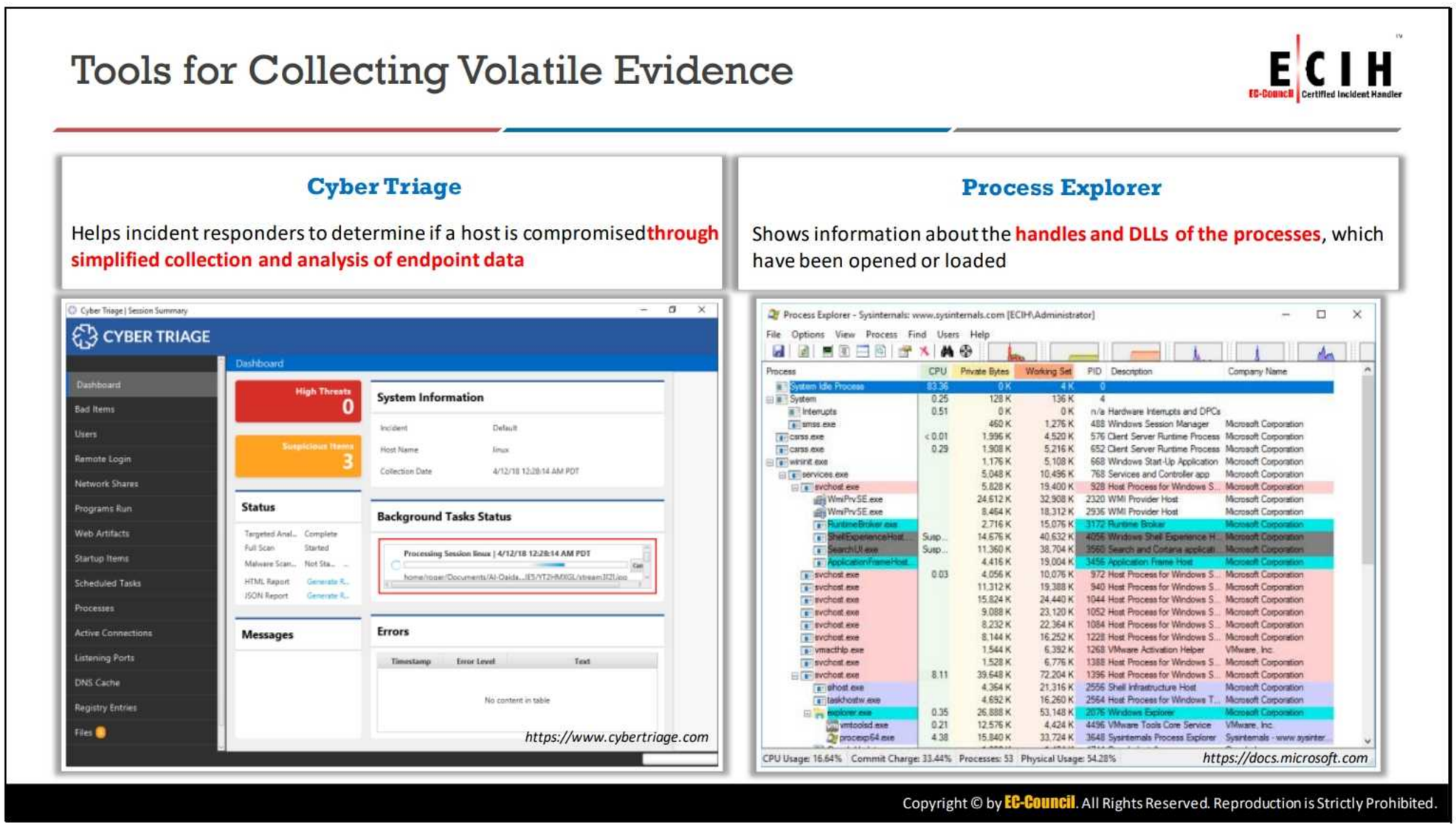
Parameters:

- **-a:** Displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening.
- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined by using -s.
- **-n:** Displays active TCP connections However, the addresses and port numbers are numerically expressed with no specified names.
- **-o:** Displays the active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified. In this case, the Protocol can be TCP, UDP, ICMP, IP, ICMPv6, IPv6 TCPv6, or UDPv6. Using this parameter with –s will display protocol-based statistics. -s: Displays statistics by protocol. By default, this will show the statistics for the TCP, UDP, ICMP, and IP protocols. In case of installed IPv6 protocol, the tool displays statistics for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The use of -p parameter can specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.
- **Interval:** Redisplays the selected information after an interval of a specified number of seconds. Press CTRL+C to stop the redisplay. Omitting this parameter will enable Netstat to print the selected information.

Using Netstat with the –r parameter will display the routing table and also reveal if the system has any persistent routes enabled. This is advantageous for incident responders and also administrators for troubleshooting their system.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Tools for Collecting Volatile Evidence

Some key l for collecting volatile information form running systems are discussed below:

- **Cyber Triage**

  Source: *https://www.cybertriage.com*

  Cyber Triage is an incident response software that helps incident responders and forensic investigators determine if a host is compromised through a simplified collection and analysis of endpoint data. It performs a comprehensive analysis on a system image, a memory image or over a network on a live system. This enables the incident response teams to gather data about a system functioning remotely without having to install an agent on the system.

- **Process Explorer**

  Source: *https://docs.microsoft.com*

  Process Explorer shows the information about the handles and DLLs of the processes, which have been opened or loaded. The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in. If it is in the handle mode, the handles opened by the process selected in the top window are shown; if the Process Explorer is in DLL mode, the DLLs and memory-mapped files that the process has loaded will be shown.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Some additional tools for collecting volatile information are listed below:

- PMDump (*http://www.ntsecurity.nu*)
- ProcDump (*https://docs.microsoft.com*)
- Process Dumper (PD) (*https://www.trapkit.de*)
- PsList (*https://docs.microsoft.com*)
- Tasklist (*https://docs.microsoft.com*)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Understanding the Static Evidence Collection

Collection of static evidence is as important as collecting volatile evidence. First responders can collect critical information from hard drives, slack space, swap files, unallocated drive space, DVD-ROMs, USB thumb drives, and so on.

This section provides an overview of static data acquisition and the process for collecting static data during a forensic investigation.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Static Data Acquisition

- Static data acquisition is defined as acquiring data that remain **unaltered** when the system is **powered off** or **shutdown**
- This type of data is termed "**non-volatile**" and is usually recovered from hard drives; however, it can also exist in slack space, swap files and, unallocated drive space
- Other sources of non-volatile data include **DVD-ROMs**, **USB drives**, **flash cards**, **smart phones**, and **external hard drives**
- **Examples of static data**: emails, word processing documents, web activity, spreadsheets, slack space, swap files, unallocated drive space, and various deleted files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Static Data Acquisition

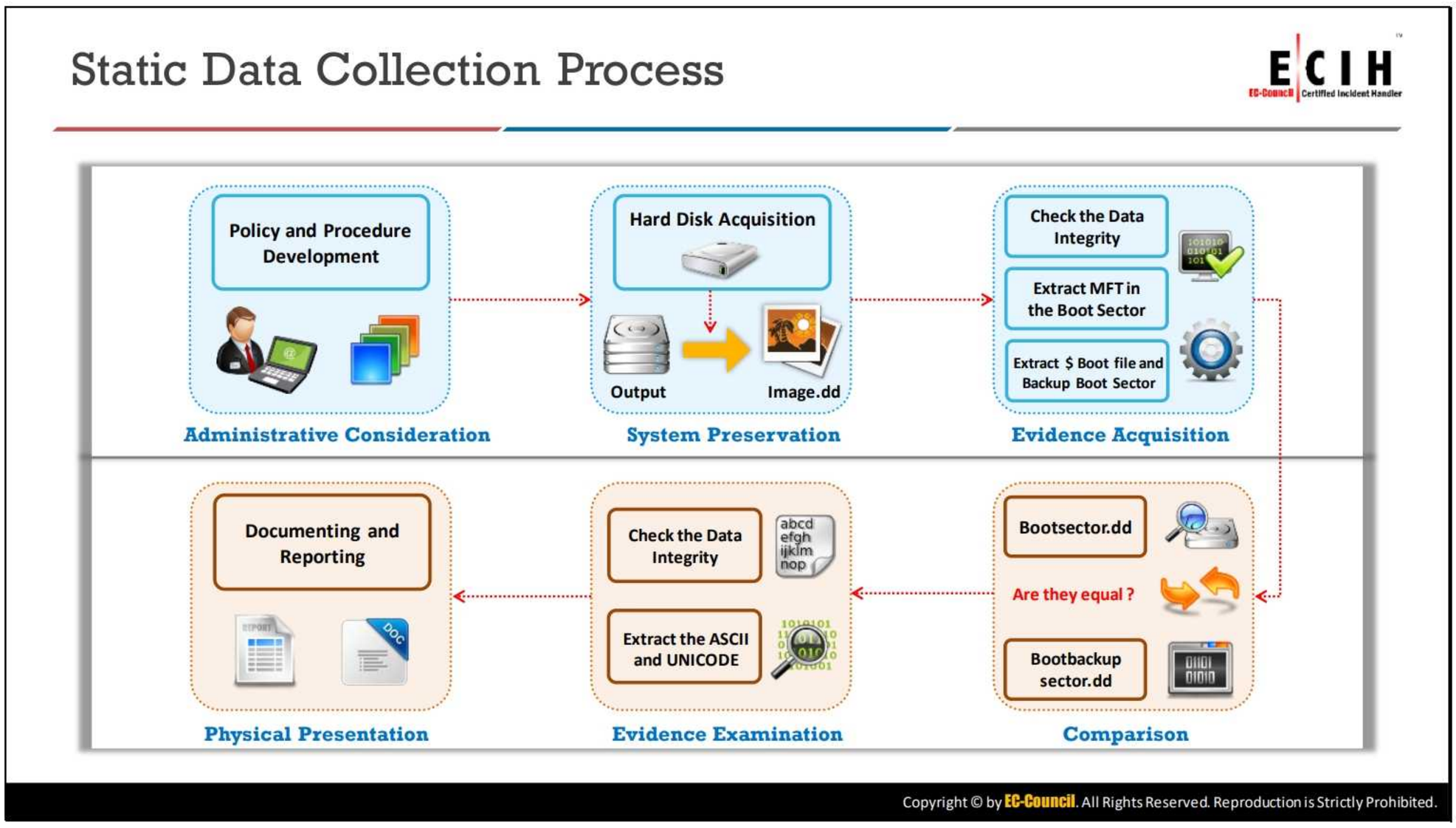
Static data are non-volatile data that do not change state after the system is shut down. Static data acquisition refers to the process of extracting and gathering the unaltered data from storage media. This type of data can be usually recovered from hard drives. Sources of nonvolatile data include hard drives, DVD-ROMs, USB drives, flash cards, smart-phones, and external hard drives. Static data exists in the form of emails, word processing documents, web activity, spreadsheets, slack space, swap files, unallocated drive space, and various deleted files. Incident responders can repeat static acquisitions on well-preserved disk evidence.

Static data recovered from a hard drive include the following:

- Temporary (temp) files
- System registries
- Event/system logs
- Boot sectors
- Web browser cache
- Cookies
- Hidden files

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Static Data Collection Process

The various steps in collecting static data are discussed below:

- **Step 1: Administrative Consideration - Policy and Procedure Development**

  This step discusses the tools suitable for the digital scene analysis as a part of administrative considerations. In this step, the incident responders must determine the mission statement, knowledge, skills, funding, evidence handling, personal requirements, and support from management. They should develop policies and procedures required for collecting static data.

- **Step 2: System Preservation - Hard Disk Acquisition**

  In this step, the incident responders should acquire the hard disks and create forensic duplicates. They can use the DD tool command to perform forensic duplication by obtaining an NTFS image of the original disk. They can then perform a sector-by-sector mirror imaging of the disk and save the output image file as image.dd.

- **Step 3: Evidence Acquisition**

  Evidence acquisition, in turn, involves the following three in-built processing steps:

  - **Data integrity verification**

    The MD5 tool is used to ensure the integrity of the acquired data by reporting a hash function (original media and the resulting image file).

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- **Extraction of the MFT from the boot sector**

  The MFT is extracted from the boot sector. The incident responders use the WinHex hex editor to analyze the MFT, and NTFSINO is used to check the number of sectors allocated to the NTFS file system.

- **Extract $Boot file and the backup boot sector**

  To investigate hidden data, the $Boot file is extracted and the data hidden in the $Boot metadata file system is extracted using the WinHex, TSK, and Autospy tools.

- **Step 4: Comparison**

  In this step, the incident responders perform a comparison of the boot sector and the boot backup sector. They use the WinHex hex-editor and the TSK and Autospy tools to analyze the Bootsector.dd and Backupbootsector.dd files.

- **Step 5: Evidence Examination**

  Evidence examination consists of the following two in-built steps:

  - **Check the data integrity**

    To test for similarities, the incident responders once again perform the data integrity check using the MD5 tool.

  - **Extract the ASCII and UNICODE**

    Incident responders extract the ASCII and the UNICODE characters from the binary files present in the disk image. For matching text or hexadecimal values recorded on the disk, they use strings command tool and keyword search. The keyword search will help to find the files containing the specific words.

- **Step 6: Physical Presentation**

  This is the final step of the static data collection process, where the incident responders document all the findings of the investigation. It involves presenting digital evidence through documentation.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

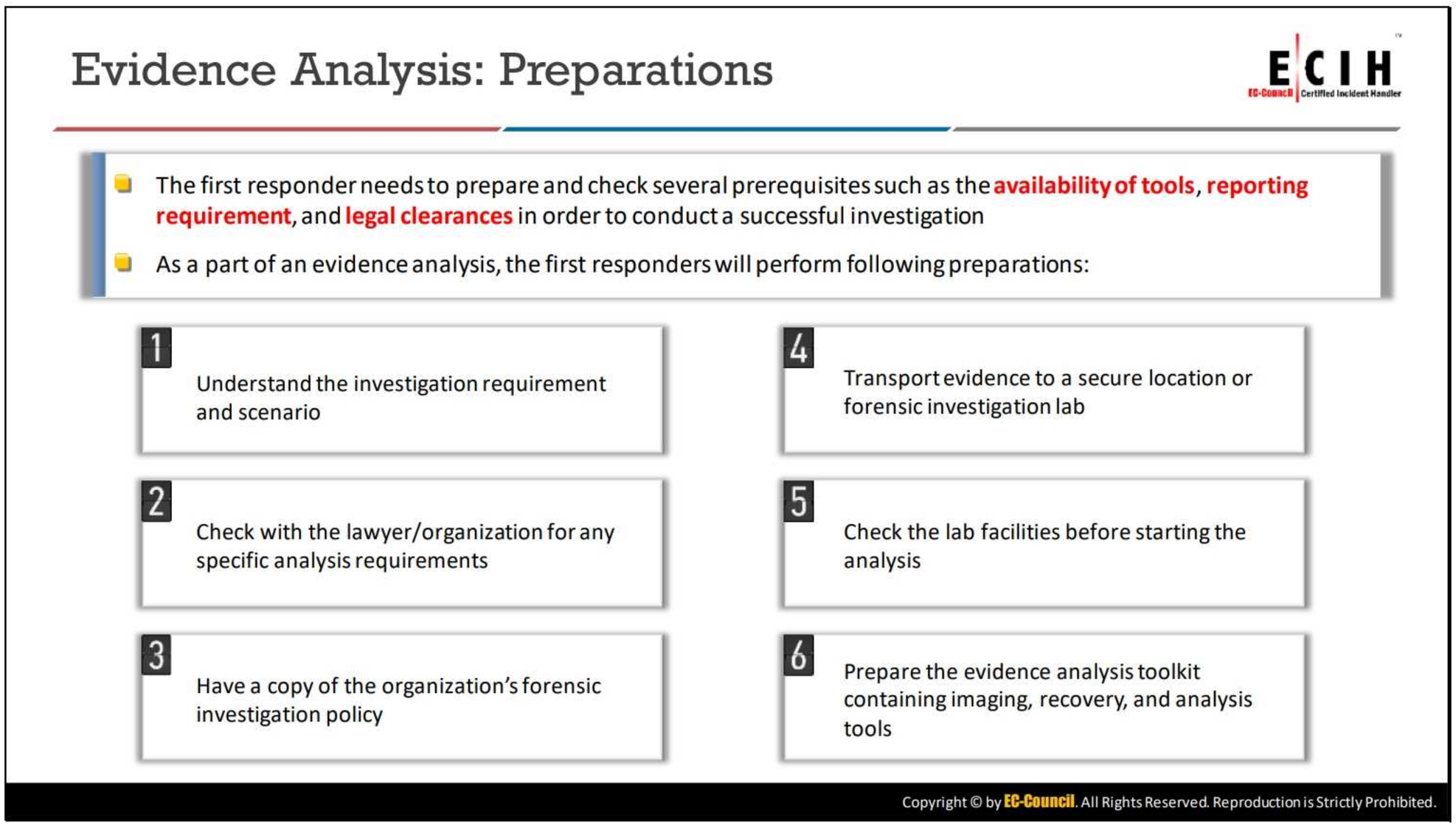
Performing Evidence Analysis

Evidence is not static and not concentrated at a single point on the network. The variety of hardware and software found on the network makes the evidence-gathering process more challenging. An analysis of the collected evidence helps in obtaining a better understanding the crime and identify missing links.

This section discusses evidence analysis in terms its prerequisites, forensic analysis tools, and forensic report.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Evidence Analysis: Preparations

There are several pre-requisites that must be met before conducting an evidence analysis. The first responder has to check for the availability of tools, reporting requirements, and legal clearances to conduct a successful investigation. It is also necessary to plan and consult with concerned persons, before, during, and after the investigation process. Evidence analysis helps in analyzing the evidence to find the attackers and the method of attacks in a legally sound manner.

As a part of an evidence analysis, the first responders will perform the following steps:

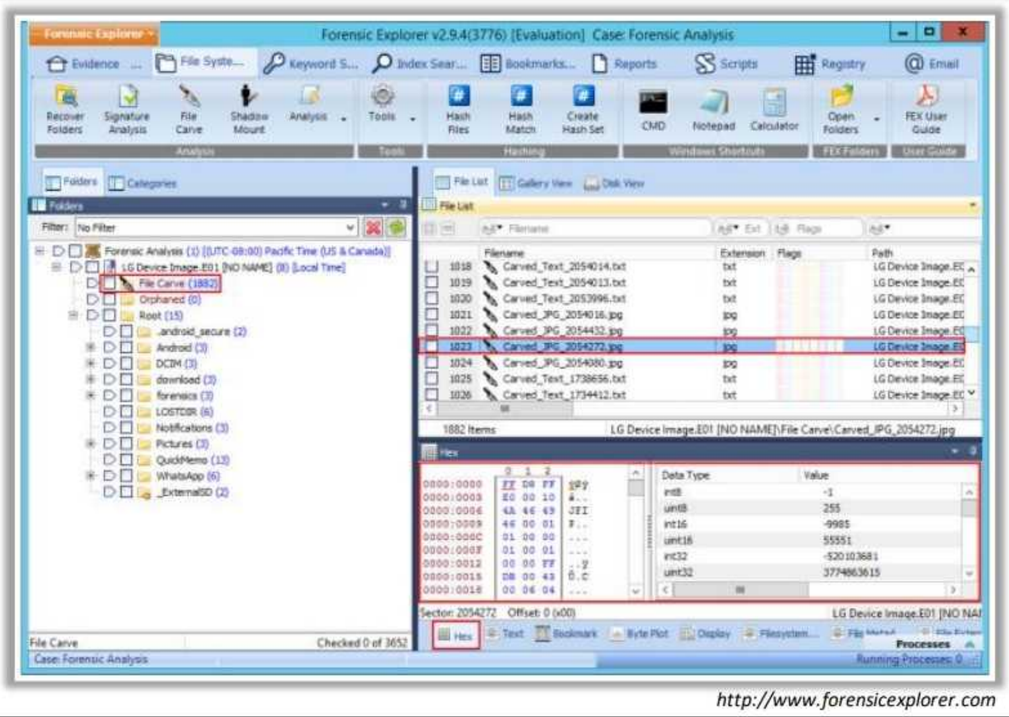
- Understand the investigation requirements and scenarios
- Check with the lawyer/organization for any specific analysis requirements
- Keep a copy of the organization's forensic investigation policy
- Transport evidence to a secure location or forensic investigation lab
- Check the lab facilities before starting the analysis
- Prepare the evidence analysis toolkit containing imaging, recovery, and analysis tools

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

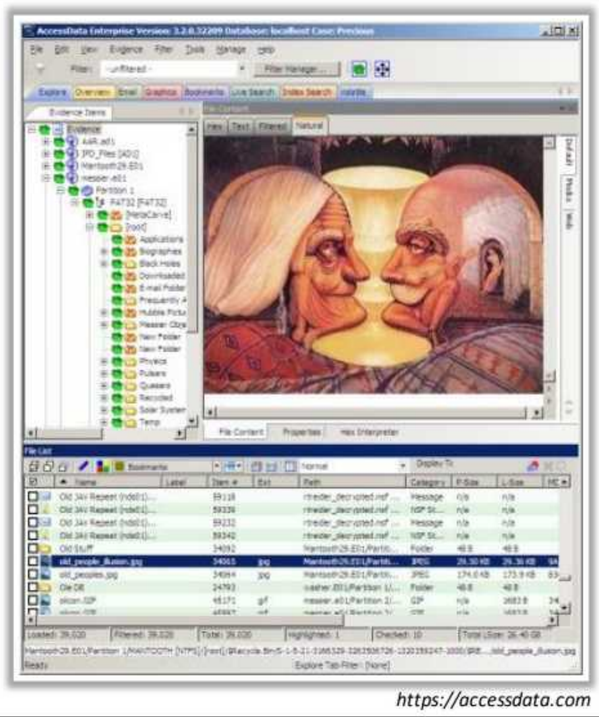
@UN5TABLE

Forensic Analysis Tools

Forensic Explorer	Recovers and analyzes hidden system files, deleted files, slack space, and unallocated clusters
Forensic Toolkit (FTK)	A computer forensic investigation tool that delivers cutting edge analysis, decryption, and password cracking



http://www.forensicexplorer.com



https://accessdata.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

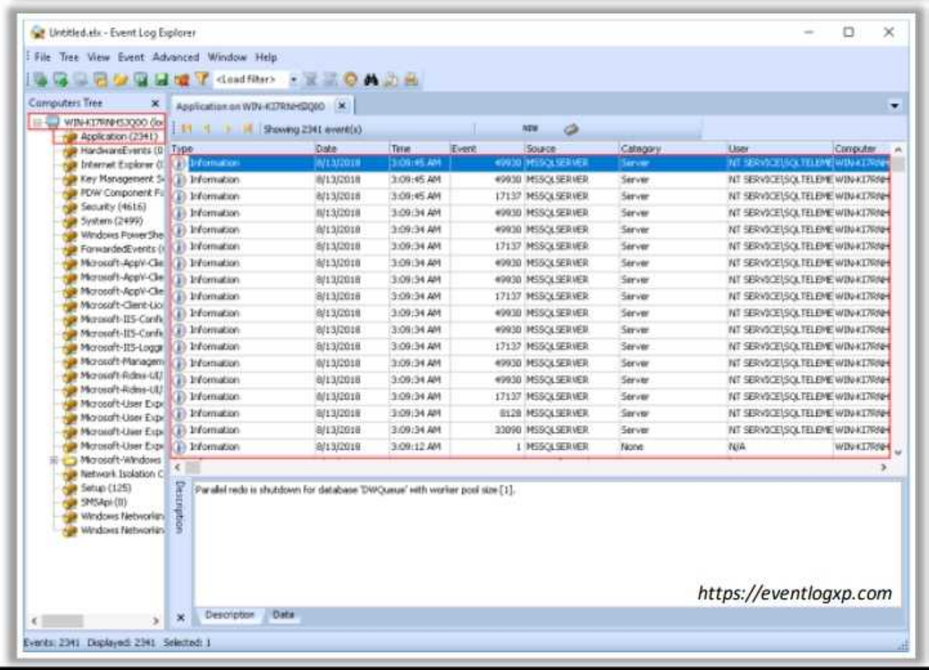
Forensic Analysis Tools (Cont'd)

Event Log Explorer

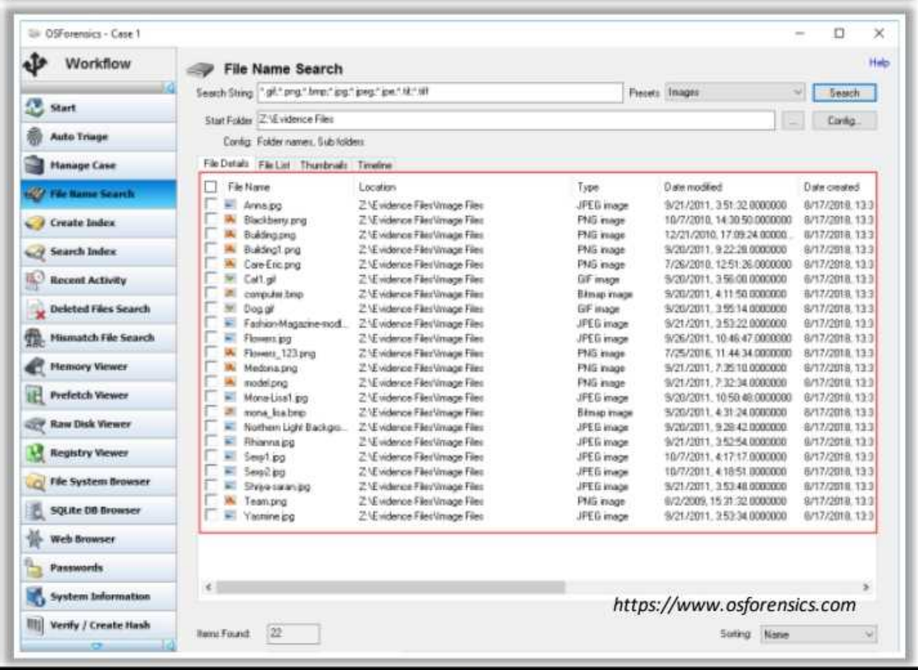
A software solution for **viewing, monitoring, and analyzing events** recorded in security, system, application, and other logs of Microsoft Windows operating systems

OSForensics

Helps **discover relevant forensic data** faster with high performance file searches and indexing and also restores deleted files



https://eventlogxp.com



https://www.osforensics.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

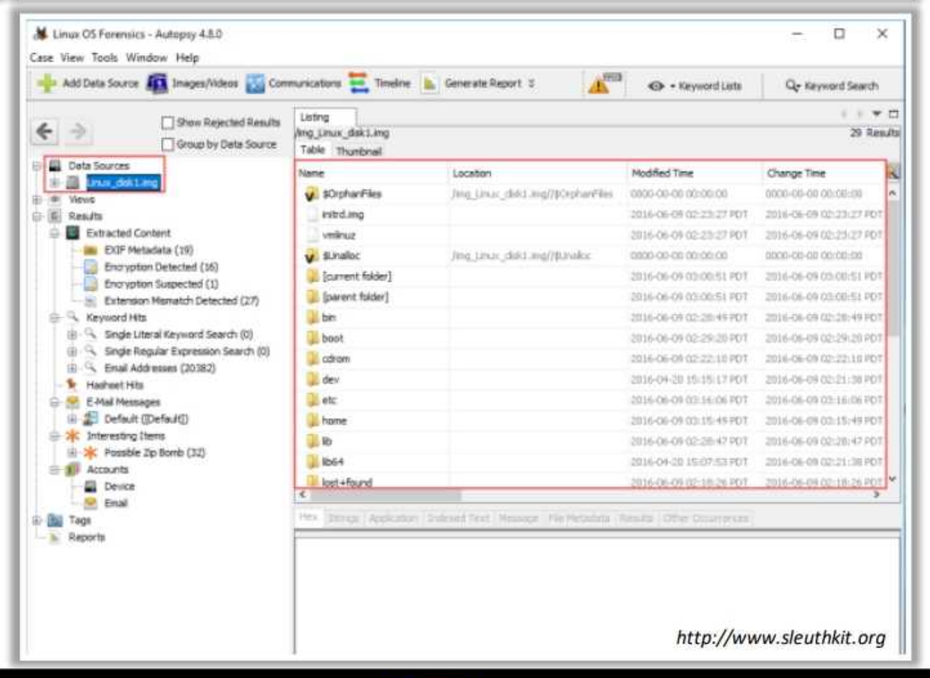
Forensic Analysis Tools (Cont'd)

Helix3

An easy-to-use cyber security solution integrated into your network that gives you **visibility across your entire infrastructure** and reveals malicious activities such as Internet abuse, data sharing, and harassment

Autopsy

Helps incident handlers to **view the file system**, **retrieve deleted data**, and perform timeline analysis during an incident response

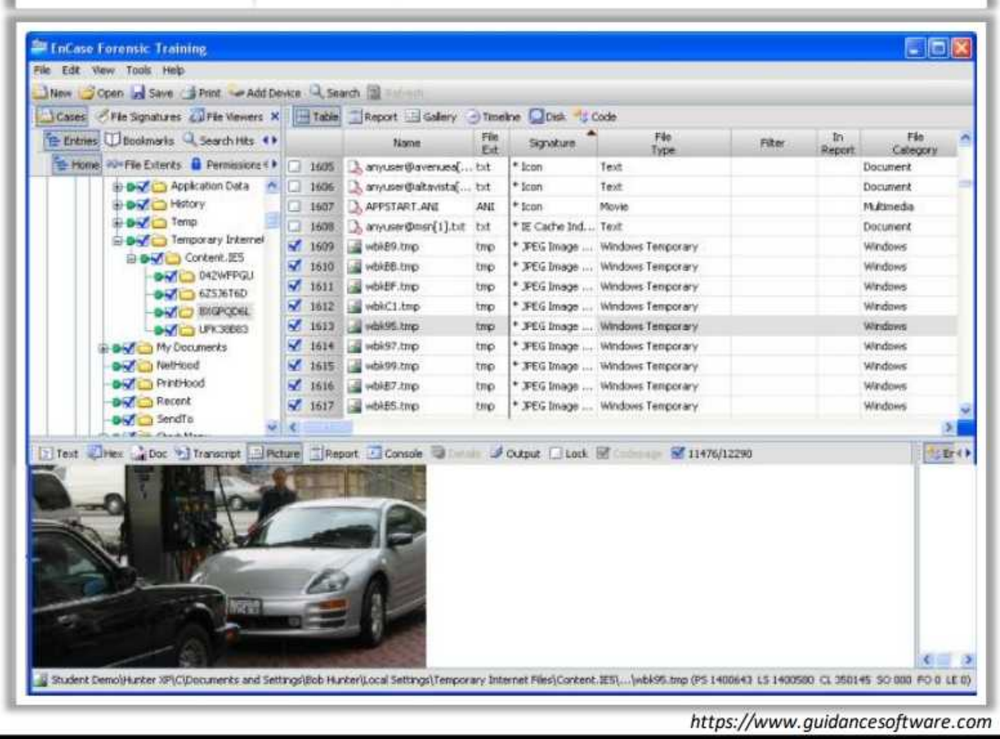


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Analysis Tools (Cont'd)

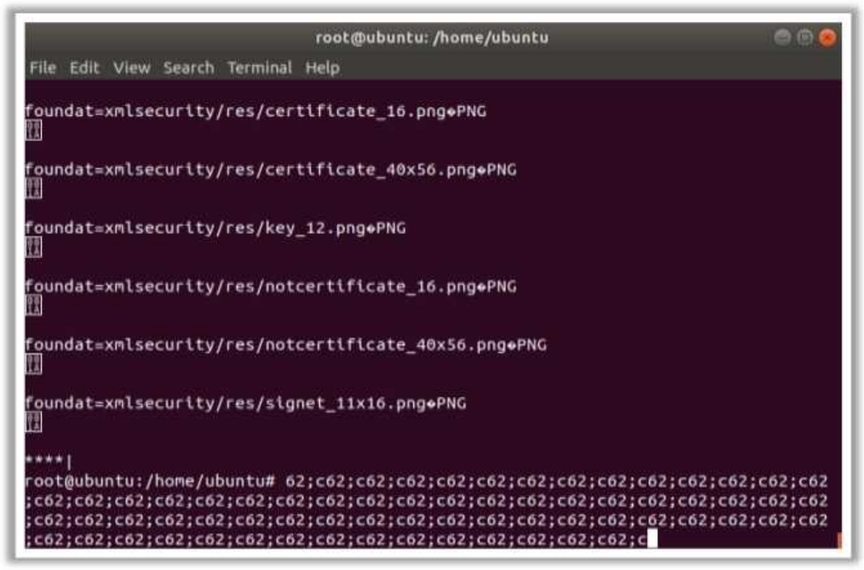
EnCase Forensic

A multi-purpose forensic platform that includes many useful tools to support several areas of the digital forensic process



Foremost

A console program to recover files based on their headers, footers, and internal data structures



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Analysis Tools

Forensics analysis tools help first responders in collecting, managing, transferring, and storing necessary information required during forensics investigation. Using these tools, a first responder can act quickly when investigating a security incident. A sophisticated investigation toolkit can reduce the incident impact by stopping the incident from spreading across the systems. This, in turn, will minimize the damage caused to the organization and effectively aid the investigation process.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Some important forensic analysis tools are discussed as follows:

- **Forensic Explorer**

  Source: *http://www.forensicexplorer.com*

  Forensic Explorer recovers and analyzes hidden and system files, deleted files, file and disk slack and unallocated clusters. Forensic Explorer is a tool for the preservation, analysis, and presentation of electronic evidence. The primary users of this tool are investigation agencies that help in performing analysis of electronic evidence.

  It enables incident responders to execute the following:

  - Manage the analysis of large volumes of information from multiple sources in a case file structure
  - Access and examine all available data, including hidden and system files, deleted files, file and disk slack, and unallocated clusters
  - Automate complex investigation tasks
  - Produce detailed reports
  - Provide non-forensic investigators a platform to review evidence

- **Forensic Toolkit (FTK)**

  Source: *https://accessdata.com*

  Forensic Toolkit (FTK) is computer forensic investigation tool that delivers cutting-edge analysis, decryption, and password cracking. It has an intuitive, customizable and user-friendly interface. It also enables the utilization of a back-end database to handle large datasets.

- **Event Log Explorer**

  Source: *https://eventlogxp.com*

  Event Log Explorer is a software solution for viewing, monitoring, and analyzing events recorded in security, system, application, and other logs of Microsoft Windows operating systems. It helps to quickly browse, find, and report on problems, security warnings, and all other events that are generated within Windows.

  Features:

  - Use a multiple-document or tabbed-document interface, depending on user preferences
  - Favorite computers and their logs are grouped into a tree
  - Back up event logs manually and automatically
  - Event descriptions and binary data are in the log window
  - Advanced filtering is possible by any criteria, including event description text
  - The Quick Filter feature allows you to filter event log in a couple of mouse clicks

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- Log loading options to pre-filter event logs
- Use bookmarks for fast navigation between events
- It is compatible with well-known event knowledgebases (EventID.com and Microsoft knowledgebase)
- Color coding by event ID is possible
- Print and export logs to different formats
- Read damaged EVT files and generate EVT files from event views

- **OSForensics**

  Source: *https://www.osforensics.com*

  It helps discover relevant forensic data faster with high performance file searches and indexing as well as restore deleted files. It identifies suspicious files and activity with hash matching, drive signature comparisons and searches e-mails, memory, and binary data. It also manages digital investigation, organizes information, and creates reports about the collected forensic data.

- **Helix3**

  Source: *http://www.e-fense.com*

  Helix3 is an easy to use cyber security solution integrated into your network to provide visibility across your entire infrastructure and consequently reveal malicious activities such as internet abuse, data sharing, and harassment. It also allows you to isolate and respond to incidents or threats quickly and without the need for user detection through a central administration tool. It allows you to quickly detect, identify, analyze, preserve, and report the evidence to reveal the truth and protect your business.

- **Autopsy**

  Source: *http://www.sleuthkit.org*

  Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other such digital forensics tools. This tool helps incident handlers view the file system, retrieve deleted data, perform timeline analysis, and web artifacts during an incident response.

- **EnCase Forensic**

  Source: *https://www.guidancesoftware.com*

  EnCase is a multi-purpose forensic platform that includes several useful tools to support several areas of the digital forensic process. This tool can collect a considerable amount of data from numerous devices and extract potential evidence. It can also generate evidence reports. EnCase Forensic can help incident responders acquire large amounts of evidence, as fast as possible, from laptops and desktop computers to mobile devices. EnCase Forensic directly acquires the data and integrates the results into the cases.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

This tool enables the searching of several thousands of files that exist on a system with a variety of search choices such as:

- GREP
- Conditional
- Boolean
- Word searches

The integrity of evidence has to be maintained in a format that the courts trust.

- **Foremost**

  Source: *http://foremost.sourceforge.net*

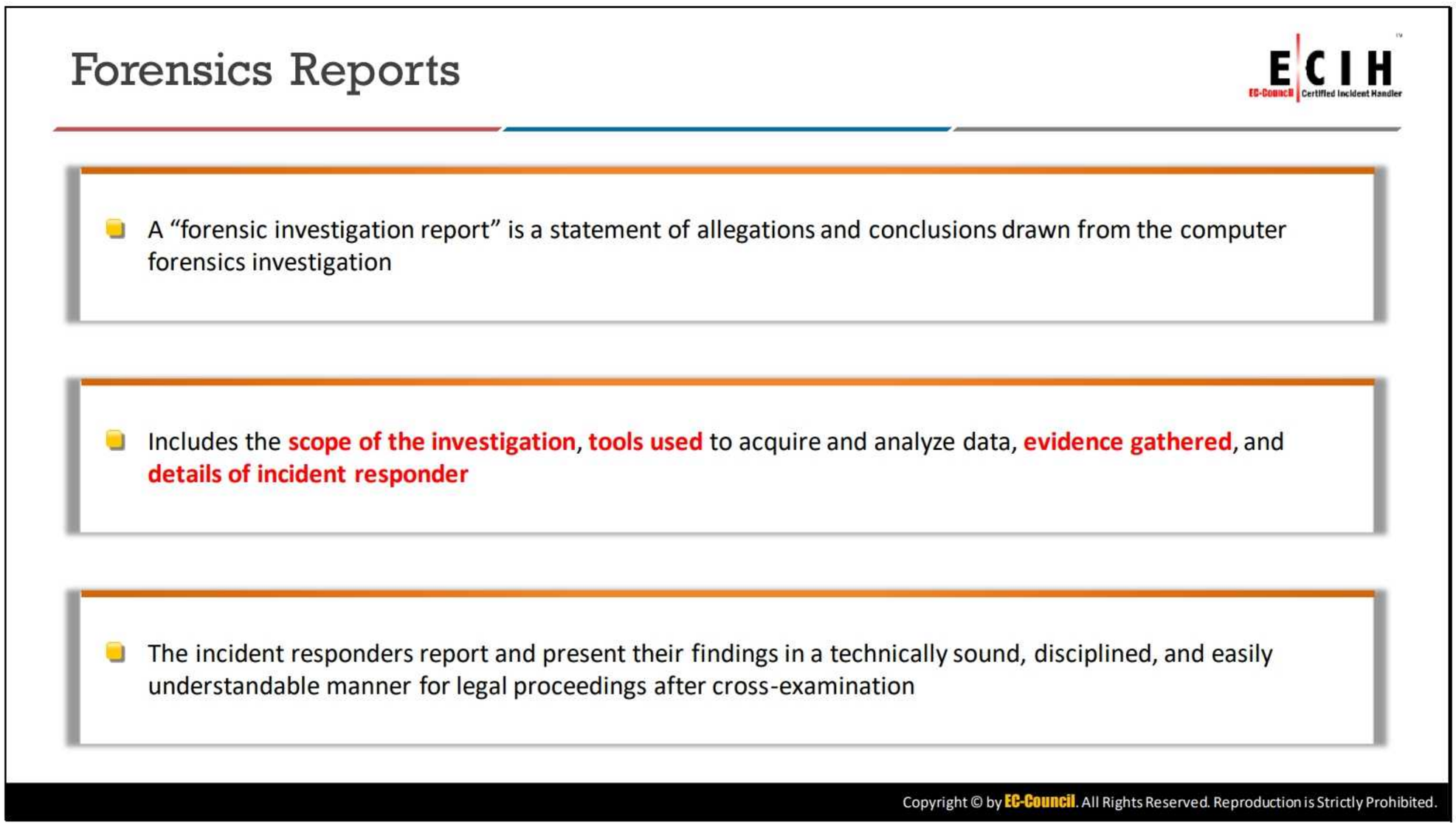
  Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, and Encase or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format, which allows for a more reliable and faster recovery.

Some additional forensics analysis tools are listed as follows:

- Belkasoft Evidence Center (*https://belkasoft.com*)
- RegScanner (*https://www.nirsoft.net*)
- MultiMon (*https://www.resplendence.com*)
- Process Explorer (*https://docs.microsoft.com*)
- Security Task Manager (*https://www.neuber.com*)
- Memory Viewer (*http://www.rjlsoftware.com*)
- Metadata Assistant (*https://new.thepaynegroup.com*)
- HstEx (*https://www.digital-detective.net*)
- XpoLog Log Management (*https://xpolog.com*)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Forensics Reports

A forensic investigation report is a statement of allegations and conclusions drawn from the computer forensics investigation. It includes the scope of investigation, tools used to acquire and analyze data, evidence gathered, details of incident responder, and so on. It contains all the findings of the incident responder in a written form, which makes it concise, precise, accurate, and organized by nature. It represents all the aspects of an investigation in an unbiased, organized, and understandable manner. The incident responders report and present their findings in a technically sound, disciplined, and easily understandable manner for legal proceedings after performing cross-examination. It can present the facts to communicate the expert's opinion.

Points to consider while writing investigative report:

- Investigative report writing involves a well-structured documentation that should be truthful, timely, and understandable to the target audience
- Before creating any investigative report, an incident responder must follow certain objectives
- The reports should provide every minute detail about the incident without compromising on the conciseness and avoid the use of jargons
- The report should be legally admissible
- The report should meet its purpose without any ambiguity and be properly formatted, such that it is easy for the readers to understand
- The report should enclose all the supporting documents such as tables and graphs and multiple references to support it while deriving conclusions
- The results should have sufficient clarity such that it can be easily reproduced by a third party

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

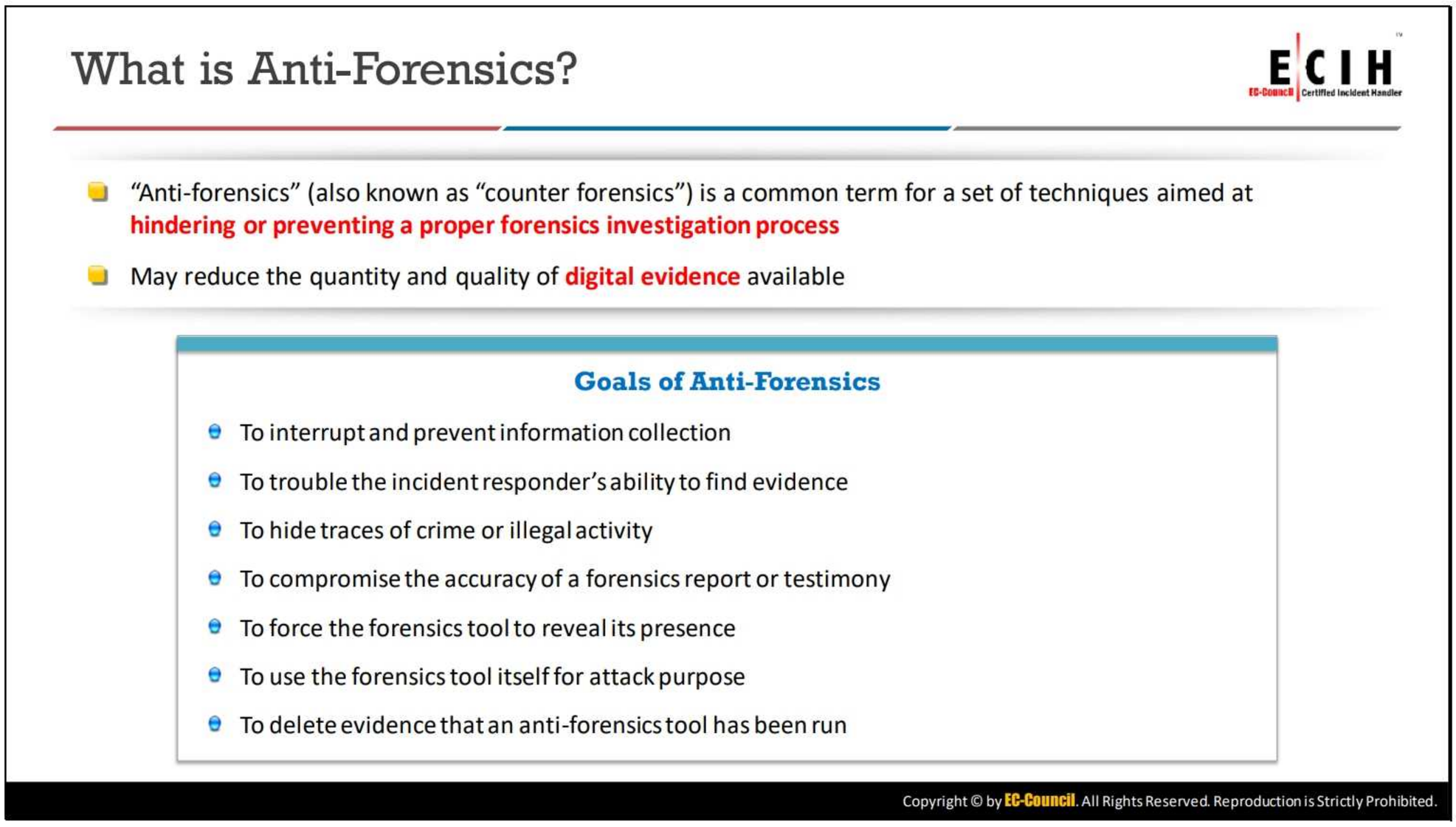
Overview of Anti-forensics

Cybercriminals leave fingerprints that responders/investigators can collect, correlate, and analyze to understand the process of crime and the motive behind it and attempt to identify the person(s) who committed it. To hinder these efforts, criminals develop and promote counter techniques and methodologies, called Anti-Forensics. These methods obstruct the process of acquiring evidence, analysis, or its credibility and sometimes leave the evidence in a manner not admissible in a court of law. Therefore, the incident responders should understand these techniques, their functions, and their impact on the evidence sources.

This section provides an overview on anti-forensics and various techniques used in anti-forensics.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



What is Anti-Forensics?

Anti-forensics, also known as counter forensics, refers to a set of techniques that attackers or perpetrators use to avert or sidetrack the forensic investigation process or try to make it extremely difficult to perform. These techniques negatively impact the quantity and quality of the evidence gathered from a crime scene. Therefore, the incident responder may have to conduct a few more additional steps to fetch the data, which in turn causes a delay in the investigation process.

Goals of Anti-Forensics

- Interrupt and prevent information collection
- Toughen the incident responder's task in finding the evidence
- Hide traces of crime or illegal activity
- Compromise the accuracy of a forensic report or testimony
- Force the forensic tool to reveal its presence
- Use a forensic tool for attack purposes
- Delete evidence that an anti-forensic tool has been used

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques

Anti-forensic techniques are the actions and methods that hinder the forensic investigation process to protect the attackers and perpetrators. These techniques act against the investigation process that include the detection, collection, and analysis of evidence files and sidetrack the incident responders.

Anti-forensic techniques, which include the deletion and overwriting of processes, also help to ensure the confidentiality of the data by reducing the its clarity. Attackers use these techniques to defend themselves against the revelation of their actions. Deceitful employees may use anti-forensic tools for the destruction of data, which may cause huge losses to the organization.

Some important anti-forensic techniques are as follows:

- Golden Ticket
- Data/File Deletion
- Password Protection
- Steganography
- Buffer Overflow against Forensic Tools
- Program Packers
- Virtual Machine and Sandbox Detection
- Artifact Wiping
- Memory Residents
- Alternate Data Stream

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques: Golden Ticket

- In this technique, the attacker with access to an **Active Directory domain** manipulates the Kerberos ticket to impersonate any user in the domain
- Attackers can create a Kerberos-generating ticket that has a lifetime of 10 years or more until the domain administrator resets the key used to generate the ticket
- The ticket helps attackers to assume the identity of any user, including highly **privileged users**, and to perform **malicious tasks**
- Attackers use the credentials of other users to hide their identity and prevent detection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Techniques: Golden Ticket

In this technique, the attackers having access to an Active Directory domain manipulate the Kerberos ticket to impersonate a user in the domain. Golden ticket refers to the forged Kerberos authentication token for the KRBTGT account that allows the attackers to move around inside the network.

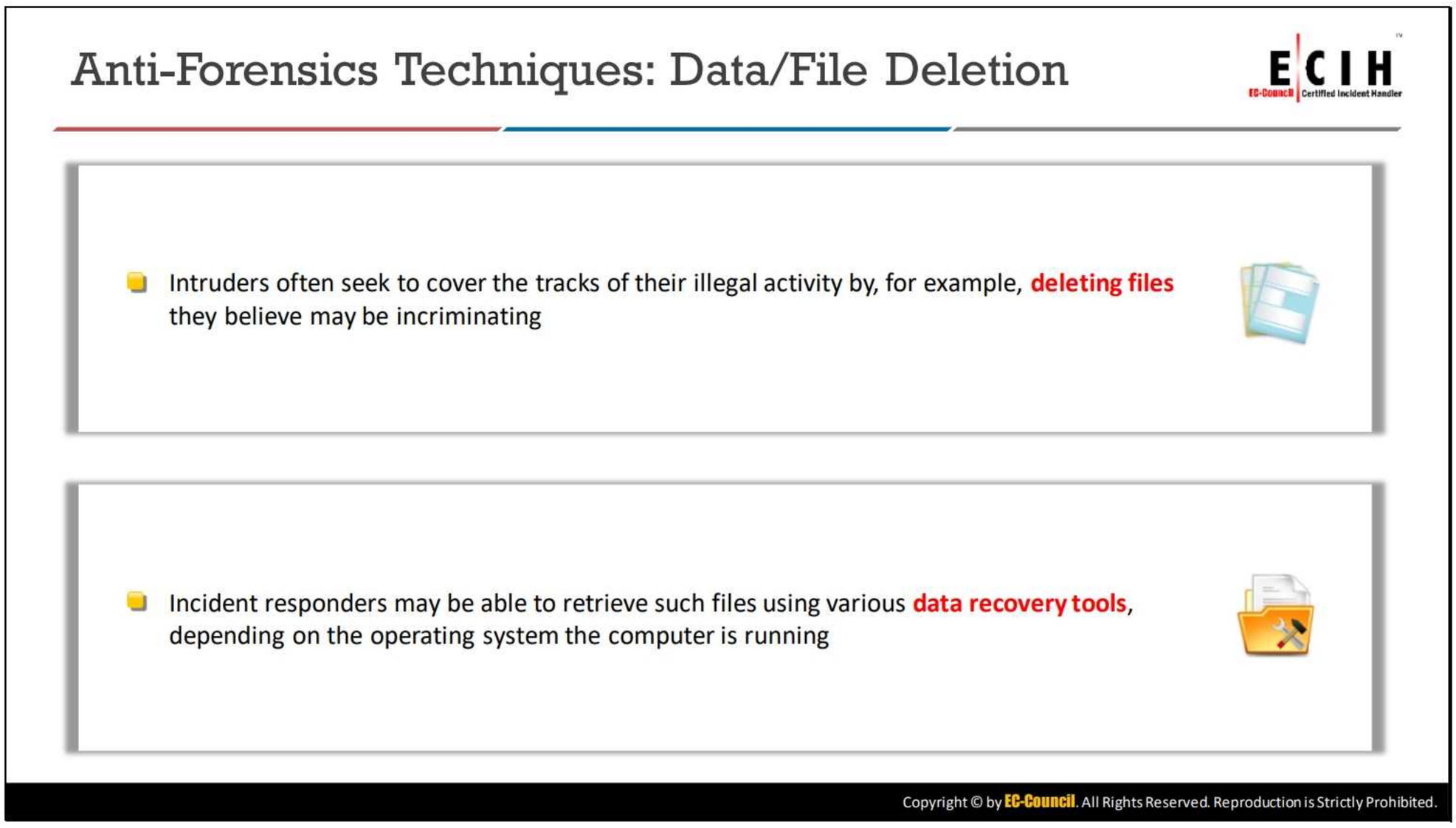
Attackers can create a Kerberos-generating ticket with a life time of 10 years or more, until the domain administrator resets the key used to generate the ticket. This ticket helps attackers to assume the identity of any user present in the group including the highly privileged users, to perform malicious tasks. As attackers use the credentials of other users, they can easily hide their identity, thereby evading detection.

To use a golden ticket, an attacker must do the following:

- Discover a way to penetrate into the network
- Infect the target system with the malware that allows the attacker to have access to the user account or network resources
- Use the domain controller access to get access to an account with privileges
- Create a golden ticket, by logging into domain controller and dump the password hash of KRBTGT account using tools such as Mimikatz
- Access anything on the network by loading the Kerberos taken into any session for any user

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



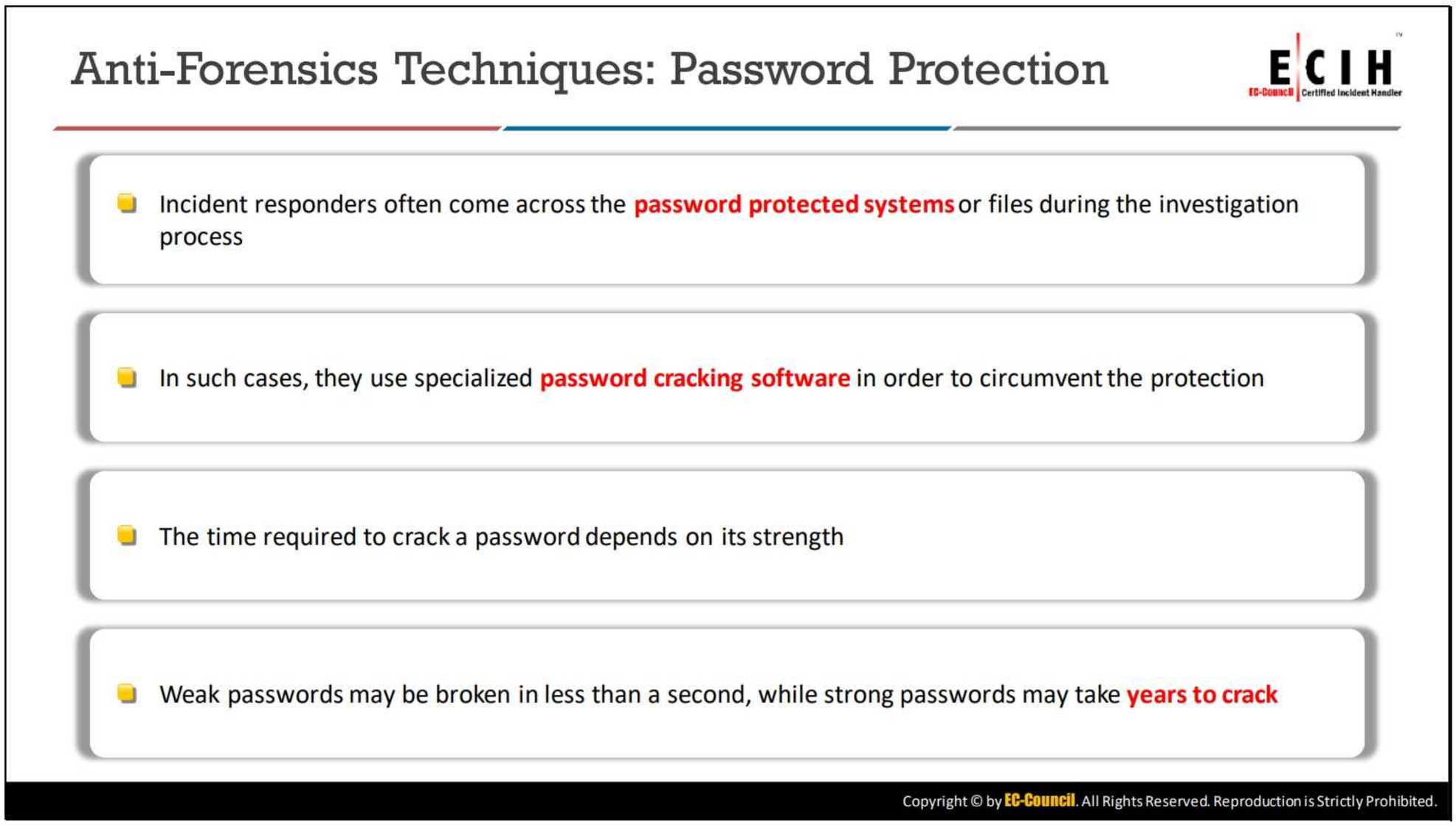
Anti-Forensics Techniques: Data/File Deletion

Intruders are highly concerned about covering the tracks of their illegal activities across a network or system and try to delete the data contained in the hard disk as part of their effort to avert detection. They also try to delete footprints of the files using specialized tools. The process includes the elimination of source files, logs, traces of data from places on the hard drive, and entries on the hard disk drive (HDD), which include attributes, orphan files, and dynamic-link library DLL files. Intruders can also securely delete data or overwrite it to mask the original data.

Intruders use various programs to overwrite data on a storage device, thus making it difficult or impossible to recover. These programs can overwrite data, metadata, or both. However, incident responders may sometimes be able to recover the deleted files using various data recovery tools depending on the operating system (OS) of the computer.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Anti-Forensics Techniques: Password Protection

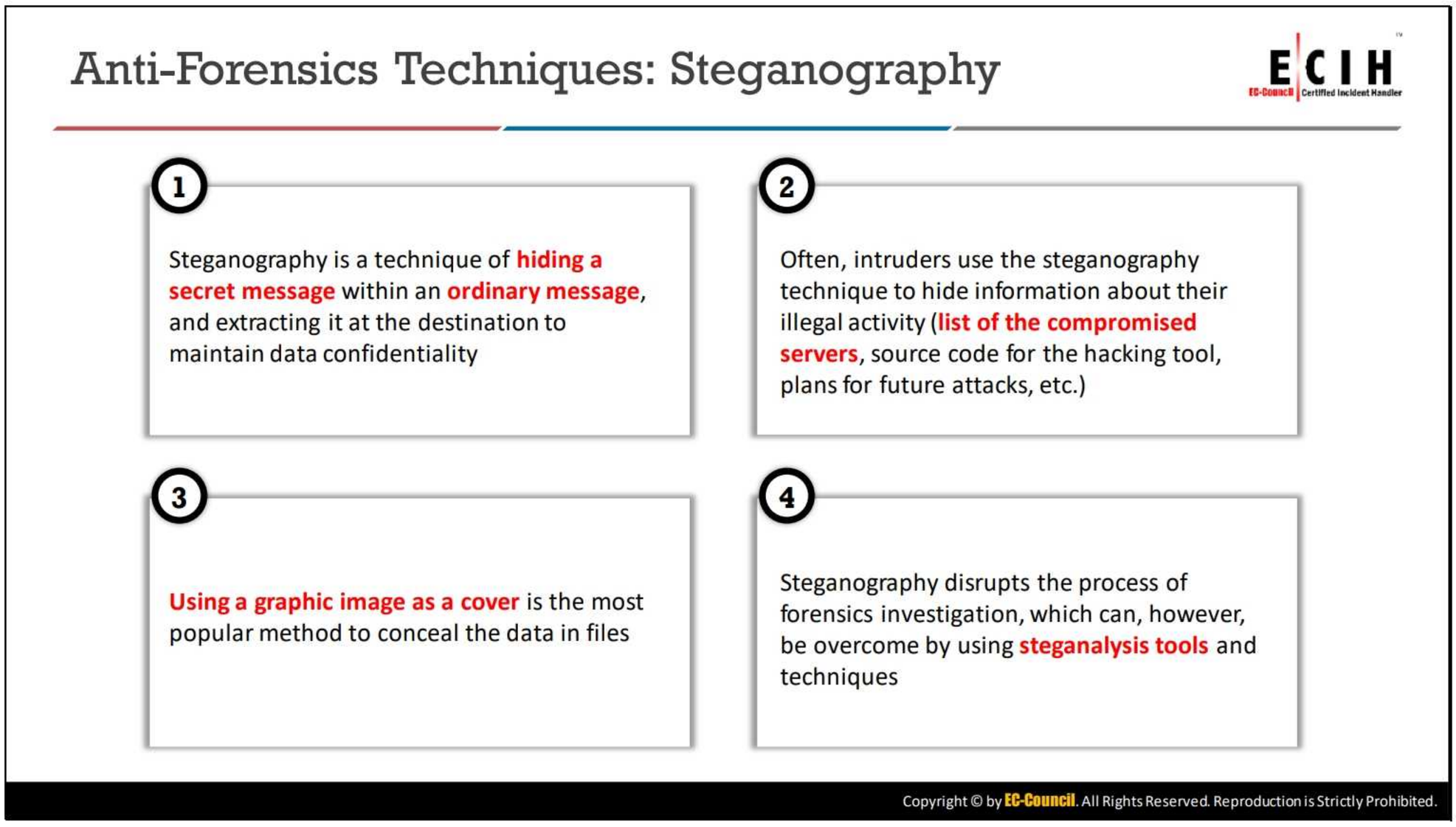
A password refers to a collection of words, letters, numbers, and/or special characters used for security processes such as user authentication or to grant access to a resource. Incident responders can often come across the password protected systems or files during the investigation process. The password ensures that unauthorized users do not access the computer, network resources, or other secured information. In addition, data files and programs may require the use of a password.

Password protection shields information, protects networks, applications, files, documents, and so on from unauthorized users. Many organizations and individuals, who do not want others to access their data, resources, and other products, employ passwords and strong cryptographic algorithms as security measures.

Intruders use these protection techniques to hide evidence data, prevent reverse engineering of applications, hinder information extraction from network devices, and prevent access of system and hard disk. This can make the work of forensic incident responder difficult. In such cases, they use specialized password cracking software to circumvent the protection. Time taken to crack passwords depends on the strength of the passwords. Weak passwords could be broken in less than a second, whereas strong passwords may take years to be cracked.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Anti-Forensics Techniques: Steganography

Steganography, the art of hidden writing, has been in use for centuries. It involves embedding a hidden message in some transport or carrier medium and mathematicians, military personnel, and scientists have been using it. They engage in changing the common language and transferring it through secret and hidden communication.

The history of steganography dates back to the Egyptian civilization. Today, with the emergence of the internet and multimedia, the use of steganography is mostly digital in nature.

In general, incident responders should identify the use of steganography across evidence that does not support encryption. When it is not possible to encrypt a file, the next best option for safe transfer used by the intruders is steganography. The best way to protect sensitive information is to camouflage it, instead of encrypting it. Camouflage is basically a supplement or an alternative for encryption. However, an encrypted file can still hide information using steganography. This way, there would be a double measure of protection, as the encrypted file, once deciphered, would not allow the hidden message to be seen. One must therefore use special steganography software to decipher the hidden message. Many websites allow the downloading of steganography software; they can be freeware or trial software. Usually, steganography involves messages that can be publicly viewed. This can go unnoticed, as the very existence of the message is secret. Stenographic messages or graphic image as a cover is the most popular method to conceal data in files. It disrupts the process of forensics investigation, which can, however, be overcome using steganalysis tools and techniques.

In cryptography, the users cannot read the message as it is in a jumbled form. Therefore, it is correct to state that the incident responders know the existence of the message. This also protects the information present in the cipher. When the incident responder intercepts an

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

encrypted message, it is quite damaging, as it informs the attacker about its two-way communication. Steganography takes the exact opposite approach, as the uninformed user has no idea that there is communication taking place.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques: Program Packers

- Packer is a program used to **compress or encrypt executable programs**
- Intruders use packers to **hide attack tools** to prevent them from being detected by reverse-engineering or scanning
- Some widely used packers include: PECompact, BurnEye, **Exe Stealth Packer**, **Smart Packer Pro**
- Packed programs that require a password to run are considered strong; meanwhile, packed programs that do not require a password are **vulnerable to static analysis**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Techniques: Program Packers

Packer is a program used to compress or encrypt executable programs. Program packers are one of the anti-forensic techniques attackers use to hide their data. The technique is similar to cryptography. The packers compress the files using various methods called algorithms. There are various algorithms and unless the incident responders know the one used to pack and have a tool to unpack it, they will not be able to access the file.

Using this technique, the attacker can hide the evidence files into containers making the files hard to detect. Therefore, during forensic investigations, the incident responder's first approach should be to mount compound files.

Packers can also include active protection against debugging or reverse engineering techniques. The packed programs those need a password to run are equally strong as encryption. Packed programs are also susceptible to static analysis if no password is required.

Intruders use packers to hide attack tools from detection by reverse-engineering or scanning. Packers can carry executable files, malware, and other attack elements. In case of executable files, these programs carry the unpackers built into them as well, which unpack the file when user tries to run it and installs the executable on the host system. Some widely used packers are UPX, PECompact, BurnEye, Exe Stealth Packer, and Smart Packer Pro. The incident responders can dynamically analyze these types of packed executables by running them in a controlled environment and observing their behavior.

Packed programs that require a password to run are strong, whereas, the ones that do not require a password are vulnerable to static analysis.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques: Virtual Machine

- Attackers often use **isolated environments** such as virtual machines and sandboxes to perform attacks
- A virtual machine can be wiped out by deleting all the individual files and folders related to it from the host machine or by uninstalling it from **virtualization software**
- To discover the VMware **virtual hard disk** files, search for files with extensions such as .VMDK, .VMEM, .VMSN, and .VMSD
- A file deleted in a virtual machine is treated in the same way as one deleted in a physical machine, that is, the file is moved to the Recycle Bin or Trash

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Techniques: Virtual Machine

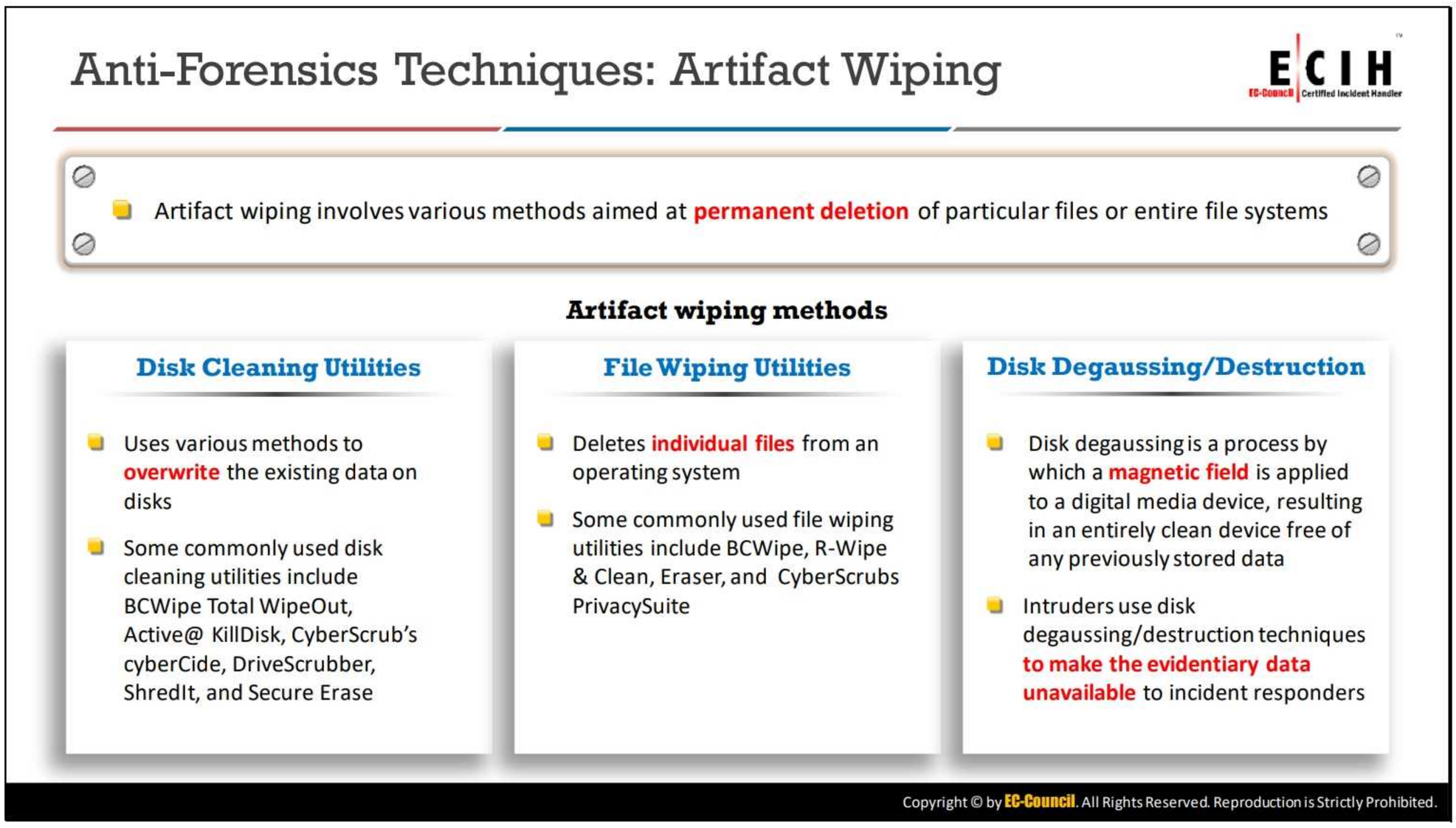
Advancement in virtualization technology made the attackers to use isolated environments such as virtual machines and sandbox to perform attacks. This is chosen as a good platform for crimes because of its hiding nature.

Attackers can completely wipe the traces if Virtual machine by deleting all the individual files and folders, related to VM from the host machine or uninstall it from virtualization software. Deleting the VM using software simply replaces the files in unallocated space.

A file deleted in a VM is treated in the same way as one deleted in a physical machine, the file is moved to the Recycle Bin or Trash. To discover the VMware virtual hard disk files, search for files with extension .VMDK, .VMEM, .VMSN, .VMSD, and so on.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE



Anti-Forensics Techniques: Artifact Wiping

Artifact Wiping refers to the process of deleting or destroying the evidence files permanently using various tools and techniques, such as disk-cleaning utilities file-wiping utilities and disk degaussing/destruction techniques. The attacker permanently eliminates particular files or the file systems.

- **Disk-cleaning utilities**

  The attackers use the tools that can overwrite the data on disks through various methods. However, these tools are not completely effective as they leave footprints. Some commonly used disk-cleaning utilities include CCleaner, BCWipe Total WipeOut, Active@ KillDisk, CyberScrub's cyberCide, DriveScrubber, ShredIt, and Secure Erase.

- **File-wiping utilities**

  These utilities delete the individual files from an OS in a short span and leave a much smaller signature when compared with the disk-cleaning utilities. However, some experts believe that many of these tools are not effective, as they do not accurately or completely wipe out the data and require user involvement. The commonly used file-wiping utilities are BCWipe, R-Wipe & Clean, Eraser, and CyberScrubs PrivacySuite.

- **Disk degaussing and destruction techniques**

  Degaussing process is a technique in which attackers apply a magnetic field to a digital media device to entirely clean the previously stored data. It is an expensive technique and needs specialized equipment. Most attackers commonly depend on physical destruction of the device to destroy the evidence. Methods include disintegration, incineration, pulverizing, shredding, and melting. Intruders use disk degaussing/destruction techniques to make the evidentiary data unavailable to forensics incident responders.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques: Memory Residents

- "Memory residents" refer to programs that always remain in the **internal memory** and **operating system** and for which no permissions exist to swap them out to external storage
- Attackers try to take advantage of these programs or system calls with the following methods:
  - **Syscall Proxying**

    A technique to play with memory, whereby the attacker uploads system call proxy, which receives remote procedure calls from the attacker's machine, executes them on the victim's machine, and sends the results back to himself or herself
  - **Userland Execve Technique**

    This allows a Unix process load and execute an ELF binary image from a memory buffer—without using the Unix execve() kernel call, it loads and runs programs on the victim's machine, thus defeating kernel-based security solutions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Techniques: Memory Residents

Memory residents refer to programs that always remain in the internal memory and operating systems have no permission to swap them out to external storage. Attackers try to take advantage of these programs or system calls by using the following methods:

- **Syscall proxying**

  Rather than uploading the entire exploit program, the attacker can upload a system call proxy to accept the remote procedure calls from the attacker's machine. The victim's machine executes the requested system call and sends the result back to the attacker. By doing so, the attacker need not upload the tools to the compromised machine. However, this increases the amount of network traffic between the compromised machine and the attacker, thereby creating latency. This technique helps in capitalizing the code injection vulnerabilities on a system.

- **Userland Execve Technique**

  The "Userland Execve" technique allows a Unix process to load and execute an ELF binary image from a memory buffer. This enables the programs on the victim computer to load and run without using the Unix execve() kernel call; this allows the attacker to overcome kernel-based security systems that might deny access to execve().

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Anti-Forensics Techniques: Alternate Data Stream

- An "alternate data stream" (ADS) is a feature of Windows' **New Technology classification system** (NTFS) that contains metadata for locating a particular file by author or title
- Creates a valuable place for attackers to hide rootkits, worms, and viruses
- Users cannot detect **ADS data** while browsing the file system or anywhere within Windows unless they have its key
- Attackers manipulate ADS data by inserting **malicious codes** or programs into them and executing them at will
- Undetectable because changes to the ADS file do not alter any noticeable characteristics of the actual file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Forensics Techniques: Alternate Data Stream

Alternate data stream (ADS) is a feature of Windows New Technology file system (NTFS) that contains metadata for locating a file by the author name or title. A file or folder in NTFS consists of several data streams: one is the primary data stream, which comprises the data that expected from the file. The second is the alternate data stream that can hide the presence of another file.

Attackers manipulate the ADS data by inserting malicious codes or programs into the data and executing these codes or programs based on their preferences. The ADS data are therefore valuable for attackers to hide rootkits, worms, virus, and so on. For example, if Windows has a file named "read.txt," the metadata of this file may also contain the information for "EvilVirus.exe."

Users cannot detect the presence of malicious codes in the ADS data while browsing the file system, or anywhere within the Windows unless they have the key. Furthermore, changes to the ADS file do not alter characteristics of the actual file in a noticeable manner. In other words, these changes do not affect the size or functionality of the existing files.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Other Anti-Forensics Techniques

Data Hiding in File System Structures	Intruders use tools and techniques that **hide data in various locations of a computer system** (slack space, memory, hidden directories, hidden partitions, bad blocks, ADSs, etc.) that are often overlooked by modern forensic tools
Trail Obfuscation	The purpose of trail obfuscation is to **confuse**, **disorient**, and **distract the forensics investigation process** Attackers **mislead incident responders** via log tampering, false e-mail header generation, timestamp modification, and various file header modifications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Anti-Forensics Techniques (Cont'd)

Overwriting Data/Metadata	Intruders use various programs to overwrite data on a **storage device**, making it difficult or impossible to recover; these programs can overwrite data, metadata, or both Overwriting programs (disk sanitizers) work in three modes: • Overwrite entire media • Overwrite individual files • Overwrite deleted files on the media
Encryption	Data encryption is one of the commonly used techniques to defeat the **forensics investigation process** Intruders use strong encryption algorithms to encrypt data of investigative value, which renders it virtually unreadable without the designated key

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Other Anti-Forensics Techniques (Cont'd)

ECIH EC-Council Certified Incident Handler

Encrypted Network Protocols

- Intruders deploy **cryptographic encapsulation protocols** such as SSL/TLS and SSH for anti-forensics purposes
- SSL/TLS and SSH protocols encrypt network traffic, protecting only its content; however, protection against traffic analysis requires the use of intermediaries

Rootkits

- The use of Rootkits can be considered another **data hiding technique** that intruders often use to mask their tracks and the presence of malicious applications or processes running on the system
- Rootkits are effective only during a live analysis of the system under investigation

Buffer Overflow against Forensic Tools

- In the buffer overflow exploit, an intruder **injects and executes the code in the address space** of a running program, thereby altering the victim program's behavior
- Usually, buffer overflows are intended to **access the remote system**, after which attack tools are uploaded, which get saved in the target machine's hard disk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Anti-Forensics Techniques (Cont'd)

ECIH EC-Council Certified Incident Handler

Detecting Forensic Tool Activities

- Anti-forensics tools (AFTs) have the capability to change their behavior upon detecting the use of CFT

  (e.g., a worm may not propagate if it discovered that the network is under surveillance)
- Using Self-Monitoring, Analysis and Reporting Technology (SMART)
- SMART built into hard drives report:
  - Power cycle count
  - Power on time
  - Log of high temperatures the drive has reached
  - Other manufacturer-determined attributes
- These counters can be consistently read by user programs and cannot be reset
- AFTs read these SMART counters to identify forensic analysis attempts and modify their behavior accordingly

  (e.g., a high power on time may indicate that the hard drive has been imaged)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Anti-Forensics Techniques

- **Data Hiding in File System Structures**

  Data hiding is one of the anti-forensic techniques employed by attackers to make data inaccessible. NTFS-based hard disks contain bad clusters in a metadata file as $BadClus, and the MFT entry 8 represents these bad clusters. $BadClus is a sparse file, which

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

allows attackers to hide an unlimited amount of data as well as allocate more clusters to $BadClus to hide more data.

Some hard disks have the host protected area (HPA), in which the developers can store the data they want to protect (and hidden) from normal use. In addition to the above - mentioned technique, intruders use other such tools and techniques that hide data in various locations of a computer system, such as slack space, memory, hidden directories, hidden partitions, bad blocks, and ADSs. Modern forensic tools overlook these spaces that helps in preventing forensic investigation.

- **Trail Obfuscation**

  Trail Obfuscation is one of the anti-forensic techniques that attackers use to mislead, divert, complicate, disorient, sidetrack, and/or distract the forensic examination process. The process involves different techniques and tools, such as

  - Log cleaners
  - Spoofing
  - Misinformation
  - Backbone hopping
  - Zombie accounts
  - Trojan commands

  In this process, the attackers delete or modify metadata of some important files to confuse the incident responders. They modify header information and file extensions using various tools. Timestomp, which is part of the Metasploit Framework, is one of the trail obfuscation tool that attackers use to modify, edit, and delete the date and time of a metadata and make it useless for the incident responders. Transmogrify is another tool used to perform trail obfuscation.

  Using the Timestomp application, one can change the modified date and time stamp completely, thereby invalidating the validity of the document and misleading the investigation process.

- **Overwriting Data/Metadata:**

  Intruders use various programs to overwrite data on a storage device, thus making it difficult or impossible to recover. These programs can overwrite data, metadata, or both to avert forensics investigation process. Overwriting programs work in the following three modes:

  - Overwrite entire media
  - Overwrite individual files
  - Overwrite deleted files on the media
  - Overwriting data can be accomplished by using disk sanitizers

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Overwriting Metadata:

Metadata refers to the information that stores details of data. It plays a crucial role in the computer forensics investigation process by offering details such as the time of creation, names of the systems used for creation and modification, author name, time and date of modification, names of the users who modified the file, and other such details.

incident responders can create a timeline of the attackers' actions by organizing the file's timestamps and other details in a sequential order. Attackers use various tools to wipe the metadata of the files that draw the attention of incident responders and render the construction of timeline difficult. Attackers uses tools such as Timestomp, which is part of the Metasploit Framework, to change MACE (Modified-Accessed-Created-Entry) attributes of the file. Another way to overwrite metadata is to access the computer in such a way that metadata is not created.

Attackers mount a partition as read-only or access it through the raw device to prevent updating of the file access times. They can also manipulate settings of the Windows registry key in "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate" to 1 to disable updating of the last-accessed timestamp.

- **Encryption**

  Encryption is the process of translating data into secret code such that only the authorized personnel can access it. It is an effective way to secure data. To read the encrypted file, users require a secret key or a password that can decrypt the file. Therefore, encryption is most widely used by the attackers owing to the fact that it is one of the best anti-forensic techniques.

  Data encryption is one of the commonly used techniques to defeat forensic investigation process and involves encryption of codes, files, folders, and sometimes complete hard disks. Intruders use strong encryption algorithms to encrypt data of investigative value, which renders it virtually unreadable without the designated key. Some algorithms avert the investigation processes by performing additional functions including use of a key file, full-volume encryption, and plausible deniability.

- **Encrypted Network Protocols**

  Attackers use the encrypted network protocols to protect the identification of the network traffic and its content from forensic examination. Few cryptographic encapsulation protocols such as SSL and SSH can only protect the content of the traffic. However, to protect against the traffic analysis, attackers should also anonymize themselves whenever possible.

  Attackers use virtual routers such as, the Onion routing approach, which provides multiple layers of protection. Onion routing is the technique used for secret communication over a computer network. This network encapsulates messages in layers of encryption, similar to the layers of an onion and employs a worldwide volunteer

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

network of routers that serve to anonymize the source and destination of communications. Therefore, tracing this type of communication and attributing it to a source is exceedingly difficult for incident responders.

- **Rootkits**

  Rootkits are one of the anti-forensic techniques that attackers use to hide data, malicious files, and processes. This software is intended to hide processes that could expose an attack from the OS itself. Rootkits allow viruses and malware to "hide in plain sight" by concealing files in ways that the antivirus software might overlook them, thereby disguising files as legitimate system files, by unlinking processes, and even avoid being detected by the OS. Rootkits are not considered to be harmful, but they store and hide malware, bots, and worms. Therefore, they are challenges to forensic incident responders.

  Different types of rootkits include:

  - Hypervisor Level Rootkit
  - Hardware/Firmware Rootkit
  - Kernel Level Rootkit
  - Boot Loader Level Rootkit
  - Application Level Rootkit
  - Library Level Rootkits

- **Buffer Overflow against Forensic Tools**

  In the buffer overflow exploit attack, the attackers use buffer overflows as an entry to the remote system to inject and run the code in the address space of a running program, thereby successfully altering the victim program's behavior. Usually, attackers use buffer overflows to access the remote system, following which they upload the attack tools, which get saved in the hard disk of the target machine.

- **Detecting Forensic Tool Activities**

  Attackers are fully aware of the computer forensic tools that incident responders use to find and analyze evidence from a victim's computer or network. Therefore, they try to incorporate forensic tools and process identification programs into the system or malware they are using. These programs act intelligently and change behavior on detecting the CFT. For example, a worm may stop propagation and even destroy the evidence when it is under surveillance.

  Almost all the current hard drives have built-in self-Monitoring, Analysis and Reporting Technology (SMART) that reports the following:

  - The total number of power cycles (Power_Cycle_Count)
  - The total time that a hard drive has been in use (Power_On_Hours or Power_On_Minutes)

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

- A log of high temperatures that the drive has reached
- Other manufacturer-determined attributes
- Various malicious programs can read these attributes, which users cannot reset

The attackers use these details and modify their behavior with the anti-forensic tools to avert the process of investigation.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE

Module Summary

- In this module, we discussed:
  - Computer forensics and its role in incident handling, the computer forensics investigation process, the importance of forensic readiness, and various forensic readiness procedures
  - The importance of first response and the roles of the first responder
  - Digital evidence, along with its types, characteristics, and role
  - The principles of digital evidence collection
  - Various methods for collecting, preserving, and securing evidence
  - Data acquisition, along with different types of data acquisition, such as volatile and static evidence collection
  - Performing evidence analysis using various forensic analysis tools
  - Various anti-forensic techniques
- In the next module, we will discuss handling and responding to malware incidents.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

In this module, we discussed computer forensics and its role in incident handling. It explained in detail the various phases of computer forensics investigation process. We also discussed the importance of forensic readiness and various forensic readiness procedures. It explained first response and the roles of the first responder. Besides digital evidence along with its types, characteristics, and role, which provided an overview of the principles of digital evidence collection. It explained the various methods involved in collecting, preserving, and securing the evidence. This module also discussed data acquisition, along with the different types of data acquisition such as volatile and static evidence collection. It provided an overview of performing evidence analysis using various forensic analysis tools. This module ended with a detailed discussion of the various anti-forensic techniques.

In the next module, we will discuss the handling and responding to malware incidents.

EC-Council Certified Incident Handler Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

@UN5TABLE