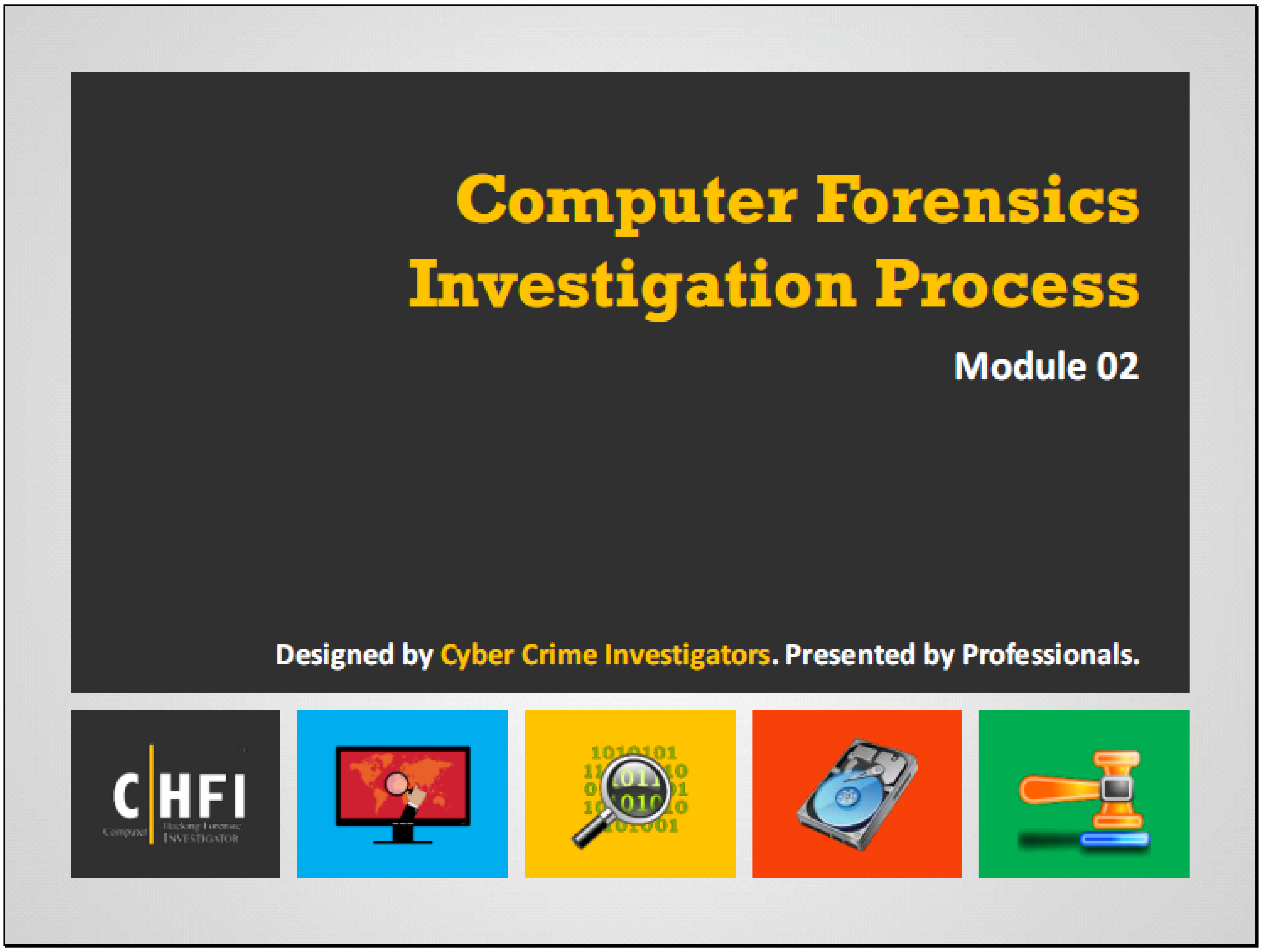
Computer Forensics Investigation Process

Module 02



Computer Forensics Investigation Process

Module 02

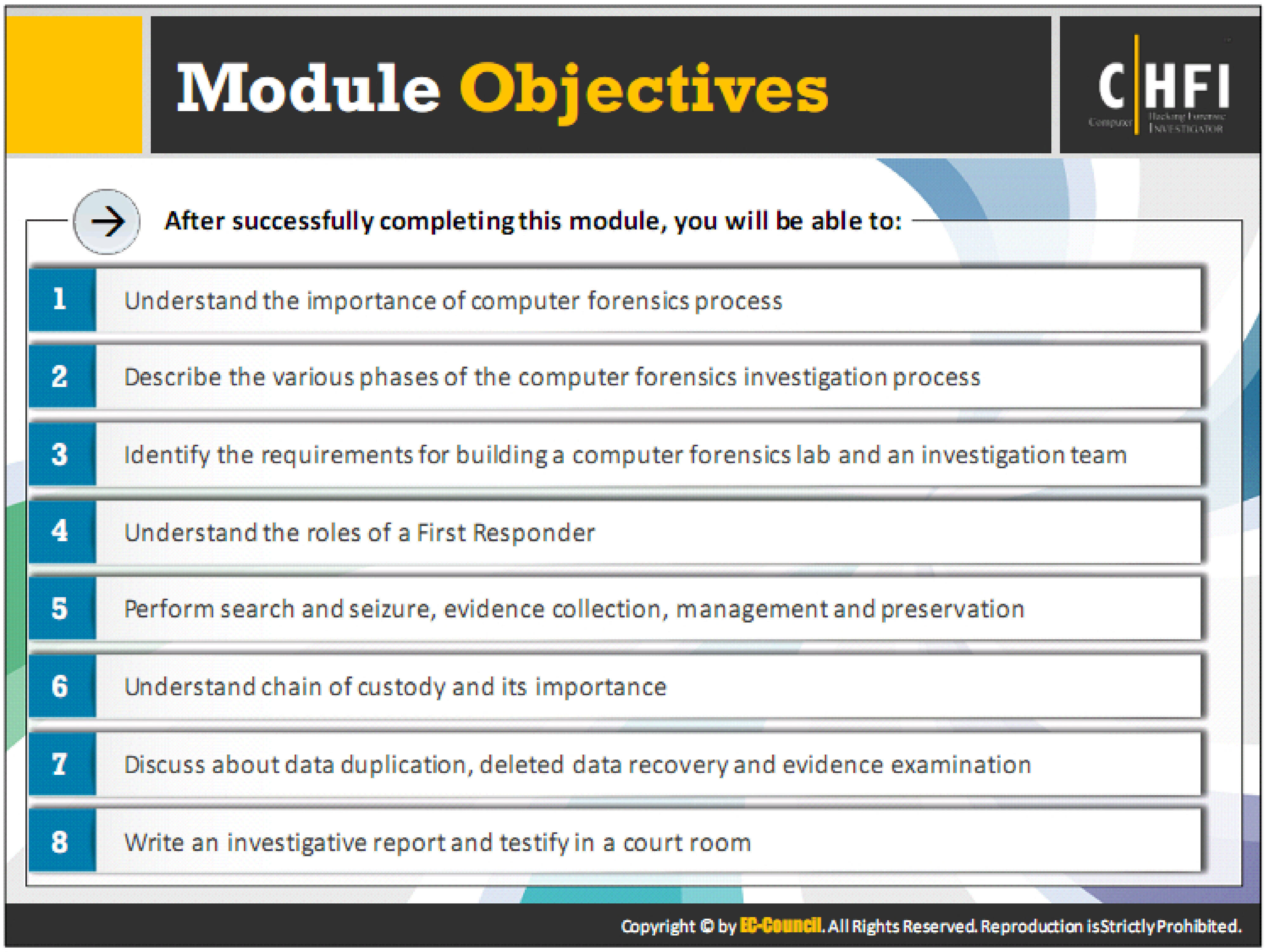
Designed by Cyber Crime Investigators. Presented by Professionals.

CHFI
Computer Hacking Forensic Investigator
1010101

Computer Hacking Forensic Investigator v9

Module 02: Computer Forensics Investigation Process

Exam 312-49

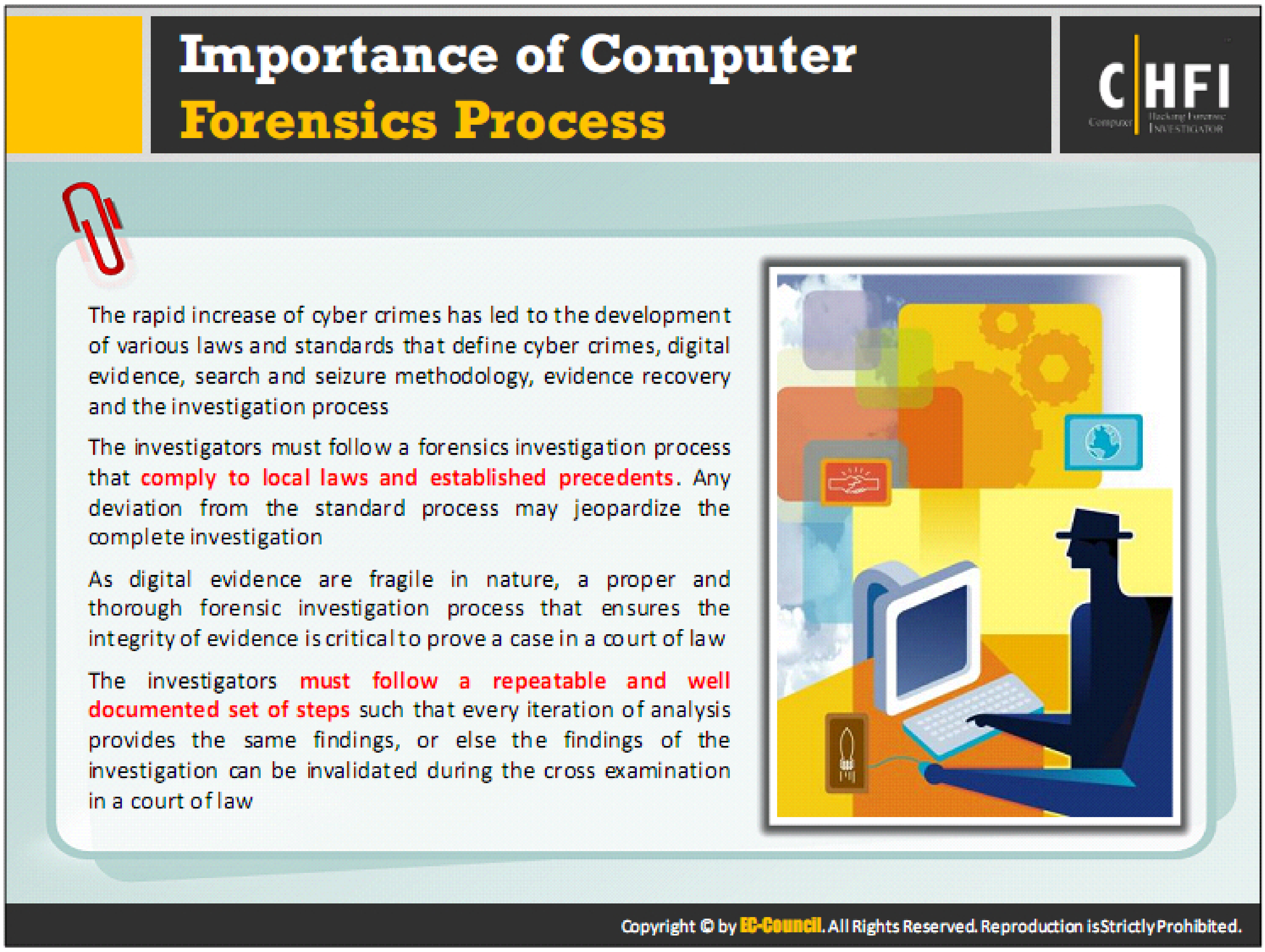


Module Objectives

After successfully completing this module, you will be able to:

1. Understand the importance of computer forensics process
2. Describe the various phases of the computer forensics investigation process
3. Identify the requirements for building a computer forensics lab and an investigation team
4. Understand the roles of a First Responder
5. Perform search and seizure, evidence collection, management and preservation
6. Understand chain of custody and its importance
7. Discuss about data duplication, deleted data recovery and evidence examination
8. Write an investigative report and testify in a court room

The computer forensics investigation process includes a methodological approach for preparing for the investigation, collecting and analyzing digital evidence, and managing the case right from the time of reporting to the conclusion. This module describes the different stages involved in the complete computer investigation process. The module also highlights the role of expert witnesses in solving a computer crime case and the importance of formal investigation reports presented in a court of law during the trial. This module will discuss the topics mentioned in the slide:



Importance of Computer Forensics Process

The rapid increase of cyber crimes has led to the development of various laws and standards that define cyber crimes, digital evidence, search and seizure methodology, evidence recovery and the investigation process

The investigators must follow a forensics investigation process that comply to local laws and established precedents. Any deviation from the standard process may jeopardize the complete investigation

As digital evidence are fragile in nature, a proper and thorough forensic investigation process that ensures the integrity of evidence is critical to prove a case in a court of law

The investigators must follow a repeatable and well documented set of steps such that every iteration of analysis provides the same findings, or else the findings of the investigation can be invalidated during the cross examination in a court of law

The rapid increase in cybercrimes, ranging from theft of intellectual property to cyber terrorism along with litigations involving large organizations, has made computer forensics necessary. The process has also led to the development of various laws and standards that define cybercrimes, digital evidence, search and seizure methodology, evidence recovery, and investigation process.

The staggering financial losses caused by computer crimes have made it necessary for organizations to employ a computer forensic agency or hire a computer forensic expert to protect the organization from computer incidents or solve cases involving the use of computers and related technologies.

The investigators must follow a forensics investigation process that complies with local laws and established standards; any deviation from the standard process may jeopardize the complete investigation.

As digital evidence is fragile in nature, a proper and thorough forensic investigation process that ensures the integrity of evidence is critical to prove a case in a court of law.

The investigators must follow a repeatable and well documented set of steps such that every iteration of the analysis gives the same findings, else the findings of the investigation can be invalidated during the cross examination in a court of law. The investigators should adopt standard computer forensics processes so that the jury can replicate the process whenever required.

Phases Involved in the Computer Forensics Investigation Process

- of actual investigation
- computer forensics lab rkstation, approval

Investigation Phase:

- main phase of the computer forensics investigation process
- reservation, and analysis of evidentiary data to identify the source of crime ulprit behind it

Post-Investigation Phase:

- Deals with the documentation of all the actions undertaken and findings during the course of an investigation
- Ensures that the report is well explicable to the target audience, and provides adequate and acceptable evidence

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, investigation toolkit, the 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 devices involved.

Investigation Phase

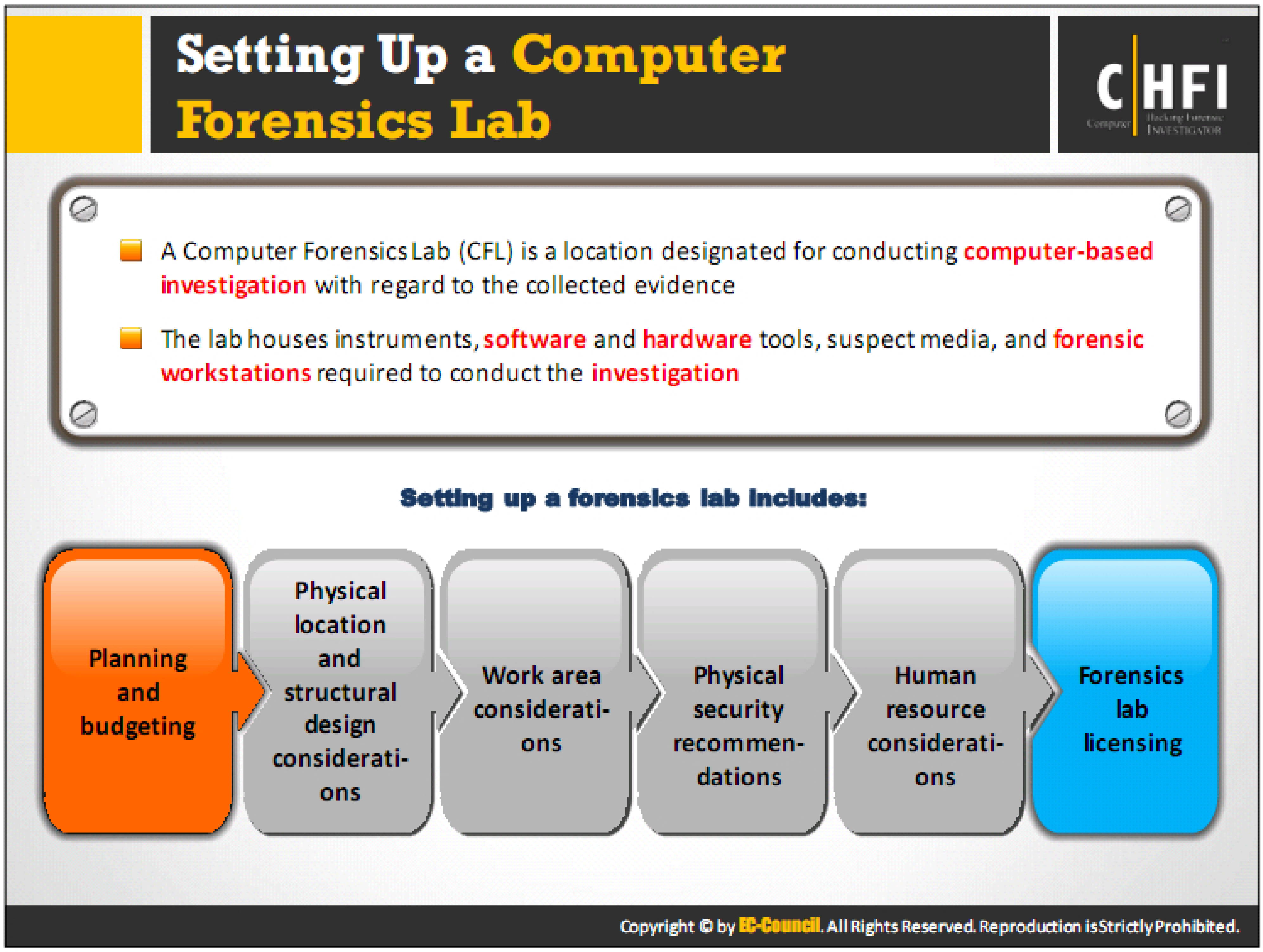
Considered as the main phase of the computer forensics investigation, it involves acquisition, preservation, and analysis of the evidentiary data to identify the source of crime and the culprit. This phase involves implementing the technical knowledge to find the evidence, examine, document, and preserve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

Post-investigation Phase

This phase involves reporting and documentation of all the actions undertaken and the findings during the course of an investigation. Ensure that the target audience can easily understand the report as well as 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 the court of law.

Pre-investigation Phase

Investigators cannot jump into action immediately after receiving a complaint or report of a security incident, but they have to follow a specific protocol that includes gathering of plaintiff information, type of incident, and obtaining permission and warrants for taking further action. All these processes combine to form the pre-investigation phase.



Setting Up a Computer Forensics Lab

- A Computer Forensics Lab (CFL) is a location designated for conducting computer-based investigation with regard to the collected evidence
- The lab houses instruments, software and hardware tools, suspect media, and forensic workstations required to conduct the investigation

Setting up a forensics lab includes:

Planning and budgeting → Physical location and structural design considerations → Work area considerations → Physical security recommendations → Human resource considerations → Forensics lab licensing

A Computer Forensics Lab (CFL) is a designated location for conducting computer-based investigation of the collected evidence in order 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 investigation of all types.

Setting up a forensics lab includes:

Planning and budgeting

Before planning and evaluating the budget for the forensic investigation case, consider the following:

- Break down costs into daily and annual expenditure
- Refer to the investigation expenses in the past
- Be aware of updated technology
- Use of statistics to obtain an idea about the computer crimes that are more likely to occur

Physical location and structural design considerations

- Make sure the lab room is secured
- Heavy construction materials need to be used
- Make sure lab exteriors have no windows

- Ensure that computer systems are facing away from windows
- Consider the room size and ventilation
- Consider the room's temperature and the number of workstations the room can occupy

Work area considerations

The lab area can affect its productivity. A lab has to include a workspace for every examiner. Consider the following for the examiner workspaces:

- Examiner station requires an area of about 50–63 square feet
- The workplace requires a table that is big enough to examine a physical computer
- The forensic workstation requires a large enough space for additional equipment like note pads, printers, etc.

Human resource considerations

All the examiners, technicians, and admins need to have certification and experience in their respective fields.

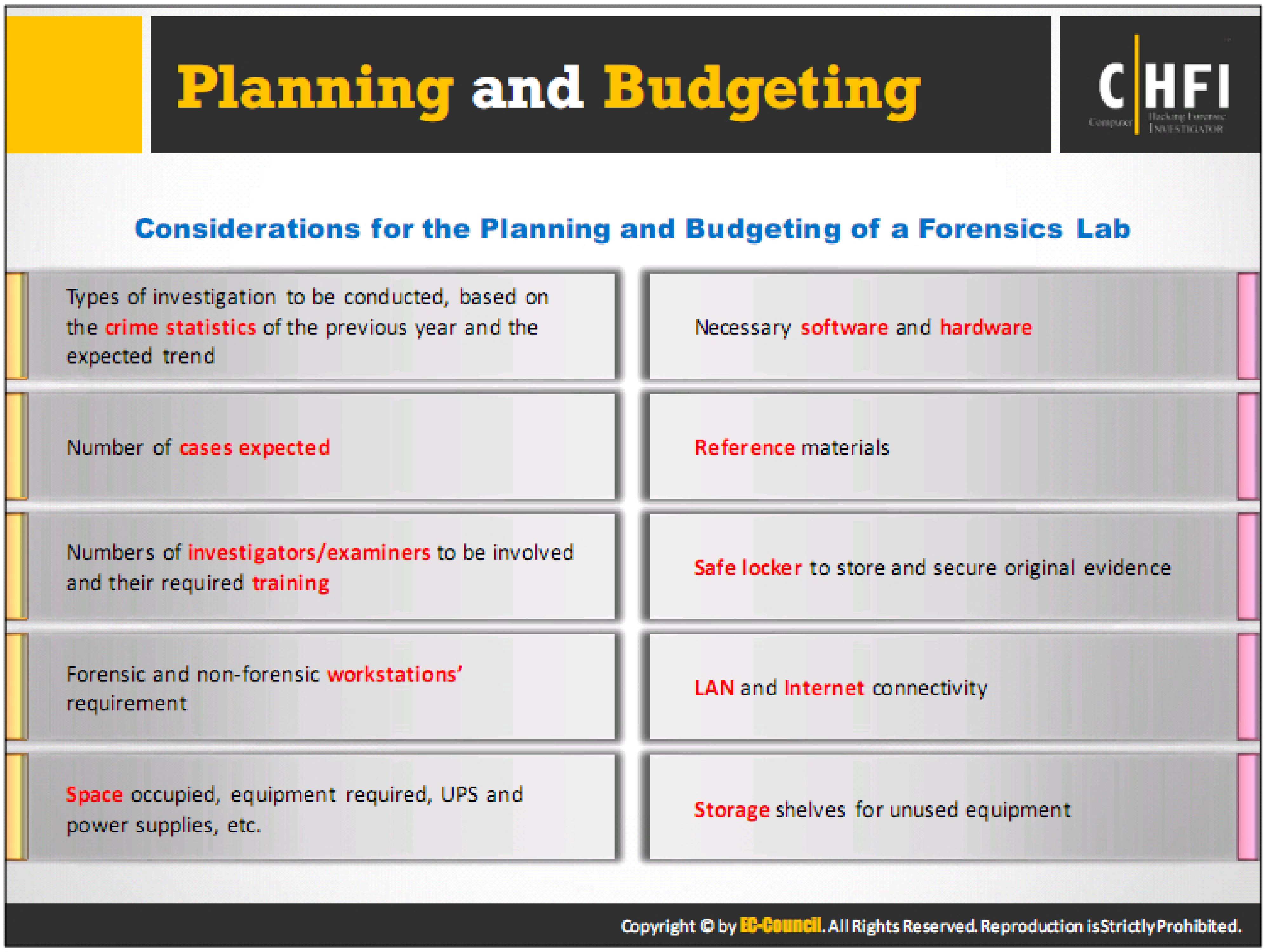
Physical security recommendations

- The room must be small with good flooring and ceiling
- The door must have a strong locking system
- The room must have a secure container like a safe or file cabinet
- Visitor logs must be maintained

Forensics lab licensing

Forensics labs should have licensing from the concerned authorities to be trustworthy. The authorities provide these licenses after reviewing the lab and the facilities it has for performing the investigation. Some such licenses include:

- ASCLD/LAB Accreditation
- ISO/IEC 17025 Accreditation



Planning and Budgeting

CHFI

Considerations for the Planning and Budgeting of a Forensics Lab

- Types of investigation to be conducted, based on the crime statistics of the previous year and the expected trend
- Number of cases expected
- Numbers of investigators/examiners to be involved and their required training
- Forensic and non-forensic workstations' requirement
- Space occupied, equipment required, UPS and power supplies, etc.
- Necessary software and hardware
- Reference materials
- Safe locker to store and secure original evidence
- LAN and Internet connectivity
- Storage shelves for unused equipment

Planning for a Forensics Lab

The planning of a forensics lab includes the following:

1. **Types of investigations being conducted**: Choose the types of crimes the lab needs to investigate based on the crime statistics of the previous year and the expected trend, e.g., criminal, civil, or corporate. If the investigation is for a corporation, then decide if it will be only internal or both internal and external. This will help in allocation of physical resources as well as budget.
2. **Forensic and non-forensic workstations requirement:** The forensics lab should have both forensics and non-forensics workstations for investigative purposes. There should be ample space to disassemble the workstation if the need arises during the investigative process.
3. **Space occupied, equipment required, UPS and power supplies, etc.:** A power failure during an investigative process will prove costly for the investigator. The need for an uninterrupted power supply is a preventive measure, and the lab should have separate backup power generators. Ensure installation of stabilizers and proper maintenance of the electrical connections, as any fluctuations in voltage may also disrupt the power supply or damage equipment.
4. **Reference Material:** During the course of the investigation, investigators may need to access reference materials including books and digital books for assistance. Bookracks in a forensics lab are necessary to store all the required reference books, articles, and magazines. Racks help keep desks uncluttered, giving investigators more space to work.

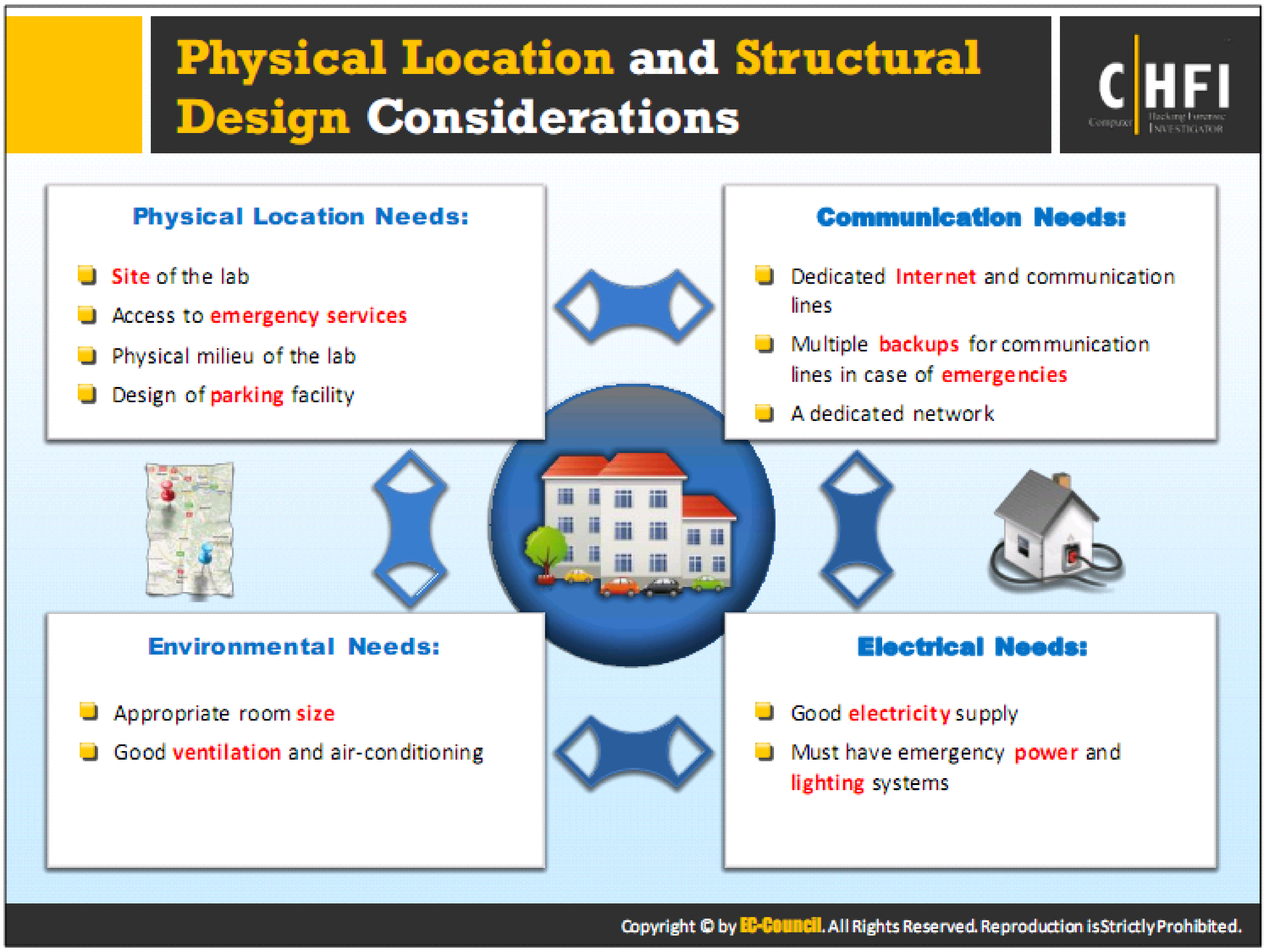
5. **Necessary software:** Ensure use of licensed versions of all the software required for the computer forensics investigation at any time during the investigation. Demo versions of forensics software are not preferable as they offer limited functionality. Having licensed versions also helps investigators during a trial. Use a demo version if and only if it provides full functionality.
6. **Safe locker and storage shelf:** A safe locker large enough to store equipment required for the forensics investigation should be available in the lab. This can help in categorizing the equipment stored on the rack, helping the investigator to locate the necessary equipment during the investigation. Safe lockers are also a means to keep equipment safe and protect them from wear and tear, dust, and other foreign particles that may hamper performance.
7. **LAN and Internet connectivity**: To share information among forensics workstations or to do multiple tasks, a LAN is required. The LAN and internet connectivity are required to perform a forensic investigation of remote networks.
8. **Storage shelves for unused equipment:** Keep the unused equipment on storage shelves away from the main working area for the following reasons:
   - To keep the forensics lab clean, tidy and to avoid unnecessary confusion amidst the large amount of forensic digital equipment in the lab
   - Makes finding a particular lab equipment easy
   - The forensics lab contains sensitive equipment that can have a significant impact if altered, such as magnetic and electrostatic devices
9. **Number of investigators/examiners to be involved**: The number of investigators needed depends on the forensics case. Hiring trained and certified professionals is important for performing proper investigations.

Budget Allocation for a Forensics Lab

Budget allocation for developing a forensics laboratory depends on the total estimated cost needed to meet the accreditation standards of a standardized body that certifies labs. In the area of forensic science, the American Society of Crime Laboratory Directors acts as a certifying body for crime labs. This standard also applies to computer forensics laboratories.

Allocate a yearly budget based on the previous year's statistics as well as estimated future trends for the next year. This includes the number of cases handled, the training required for staff, upgrading hardware and software tools in the lab, additional equipment required for enhancing the security of the lab premises, renovation of the lab, recruitment of additional certified personnel if needed, and many other deciding factors.

Cybercrime statistics can reveal the nature of the damage done and the tools used to commit the crime as well as the affected elements in the networked world. Purchase the necessary specialized software needed to investigate a particular crime. Forensics lab requirements are difficult to estimate, as the requirements change according to type of case and evidence. However, over a period, the forensics lab would become well equipped and self-sufficient, with all the technologies available that are necessary to handle the investigation.



Physical Location and Structural Design Considerations

Physical Location Needs:

- Site of the lab
- Access to emergency services
- Physical milieu of the lab
- Design of parking facility

Communication Needs:

- Dedicated Internet and communication lines
- Multiple backups for communication lines in case of emergencies
- A dedicated network

Environmental Needs:

- Appropriate room size
- Good ventilation and air-conditioning

Electrical Needs:

- Good electricity supply
- Must have emergency power and lighting systems

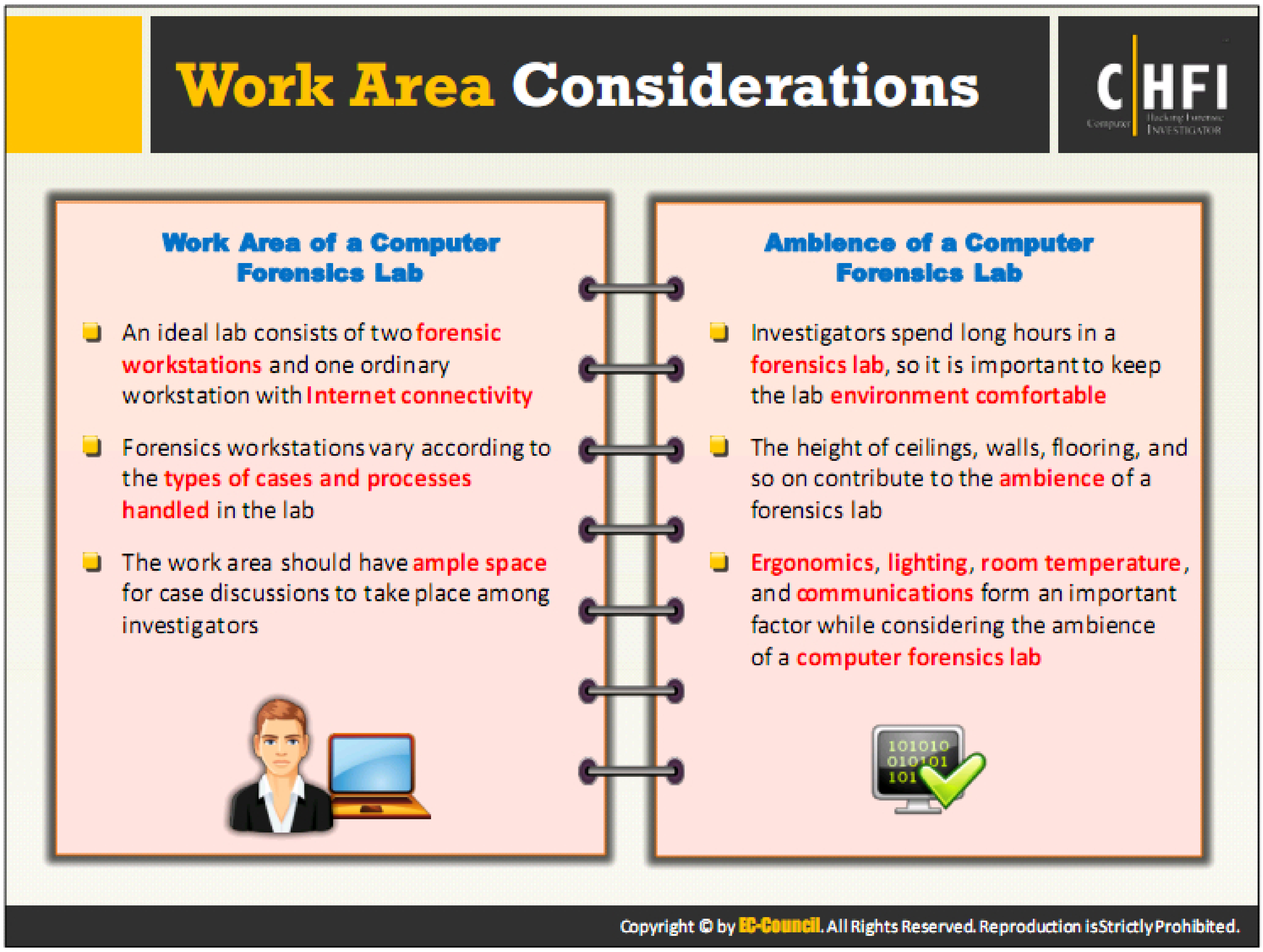
Physical Location Needs of a Forensics Lab

The physical location needs of a forensics lab are:

- **Site of the lab:** The site should have at least two directions of entry to ensure that one can access the lab despite heavy traffic conditions, street maintenance work, or any unexpected site disruptions.
- **Access to emergency services:** There should be easy access to emergency services such as the fire department and other emergency vehicles. It must also have access to shipping and receiving without compromising the physical security of the lab.
- **Lighting at the site:** The site must have proper lighting designed to augment security and discourage vandalism and unauthorized access to the lab. It should be similar to the campus lighting of a university that conducts night classes.
- **Physical milieu of the lab:** The design must avoid:
  - Bushes across 10 feet of the lab surroundings
  - Clusters of bushes around the premises
  - Tall evergreen trees
- **Structural design of parking:** The parking lot of the lab should have different levels. These are a few recommendations for designing the levels of parking:

  - **First level:** It is a low security area; it must be close to the visitor entrance.
  - **Second level:** Partially secured and fenced level used for shipping, waste pick-up, and other activities requiring minimum security.
  - **Third level:** A secured level that provides employees with access to the lab only with the proximity keys or card keys.
  - **Fourth level:** High-security area where only authorized personnel have access and security personnel can monitor it.
- **Environmental Conditions**: The environmental conditions for proper functioning of a lab are:
  - **Dimensions of the lab:** The lab must be large. There must be sufficient space to place all the equipment in the lab, without any congestion.
  - **Exchange rate of air:** There must be a high exchange rate of air in the lab. The exchange rate enhances the fresh air in the room and prevents unwanted odors in the lab.
  - **Cooling systems:** There must be proper cooling systems installed in the lab to overcome the heat that workstations generate. It must be able to handle the RAID server's heat output.
  - **Allocation of workstations**: The dimensions of the lab will determine workstation placement.
  - **Arrangement of workstations**: The design of the lab will determine the arrangement of workstations. There must be different workstations for different sections of the lab.
- **Electrical Needs:** Following are the electrical needs of a computer forensics lab:
  - Amperage: The lab must have good amperage of around 15 and 20 A required to run the laboratory equipment.
  - Emergency power and lighting: The lab should have emergency power and protection for all the equipment from power fluctuations. It should have ample lighting for the following sections of the laboratory:
    - All the evidence sections
    - All the security sections, electronic security systems, and telephones
    - X-ray processing rooms and photography dark rooms
  - Electrical Outlets: There must be easy access to the electrical outlets in the lab.
  - Uninterrupted power supply: For all the workstations and the equipment, a centralized UPS is preferred for a safe shutdown.

- **Communication Needs:** The different communication needs are:
    - Dedicated connection: Install a dedicated ISDN for network and voice communications.
    - Dial-up access: Dial-up Internet access must be available for the workstations in the laboratory.
    - Disconnection: Disconnect the forensic computer from the network when it is not in use.
    - Network: A dedicated network is preferred for the forensic computer, as it requires continuous access to the Internet and other resources on the network.



Work Area Considerations

Work Area of a Computer Forensics Lab

- An ideal lab consists of two forensic workstations and one ordinary workstation with Internet connectivity
- Forensics workstations vary according to the types of cases and processes handled in the lab
- The work area should have ample space for case discussions to take place among investigators

Ambience of a Computer Forensics Lab

- Investigators spend long hours in a forensics lab, so it is important to keep the lab environment comfortable
- The height of ceilings, walls, flooring, and so on contribute to the ambience of a forensics lab
- Ergonomics, lighting, room temperature, and communications form an important factor while considering the ambience of a computer forensics lab

The location of the forensics lab should be in an area with less human traffic. A forensic lab generally has two workstations, but this number increases depending on the number of investigation cases.

Design of the work area is subject to available financial resources. However, as the complexity and number of cases increase, the workstation area will increase. It is advisable to have separate rooms for supervisors and cubicles for investigators.

The work area should have ample space for discussing the cases among investigators as well as enough room for each investigator to align and store all the files and equipment. The productivity of the investigator will decrease in a cluttered workspace, thus hampering the investigative process. The layout of the forensics lab should be scalable with ample room for expansion.

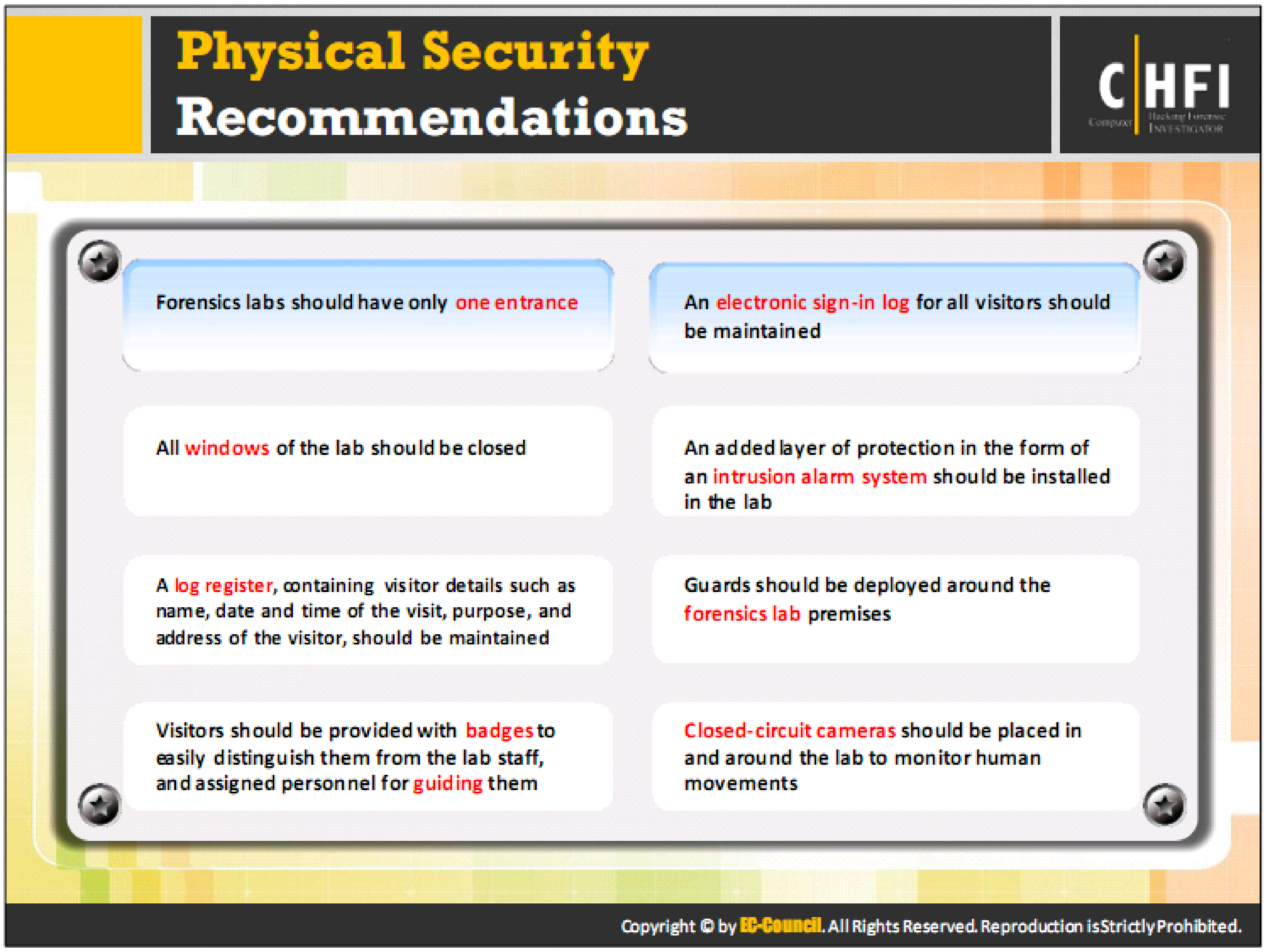
Ambience of a Forensics Lab

Investigators spend long hours in a forensics lab, so it is of utmost importance that the ambience of the lab is comfortable. Ergonomics, lighting, room temperature, and communications form an important factor while considering the ambience of a computer forensics lab.

The Ergonomics Society of the UK defines ergonomics as "the application of scientific information concerning humans to the design of objects, systems and environment for human use." The society also defines ergonomic design as "a way of considering design options to ensure that people's capabilities and limitations are taken into account." Physiology, psychology, and anatomy are the three important elements of ergonomics.

The environment in the lab, such as humidity, airflow, ventilation, and room temperature, also play an important factor. The lab should be able to handle more computers in case there is a plan for expansion. Improper lighting in the lab will lead eyestrain for the investigators, which may hamper their productivity.

Adjust lighting to avoid glare and keep the monitors at an angle of 90 degrees to the windows. Painting on the walls should have a matte finish instead of a glazed finish. The height and make of the ceilings, walls, flooring, etc. contribute to the ambience of a forensics lab. Do not use false ceilings, as they weaken the security of the lab.



Physical Security Recommendations

CHFI
Computer Hacking Forensic Investigator

Forensics labs should have only one entrance

An electronic sign-in log for all visitors should be maintained

All windows of the lab should be closed

An added layer of protection in the form of an intrusion alarm system should be installed in the lab

A log register, containing visitor details such as name, date and time of the visit, purpose, and address of the visitor, should be maintained

Guards should be deployed around the forensics lab premises

Visitors should be provided with badges to easily distinguish them from the lab staff, and assigned personnel for guiding them

Closed-circuit cameras should be placed in and around the lab to monitor human movements

The level of physical security required for a forensics lab depends on the nature of investigations performed in the lab. The assessment of risk for a forensics lab varies from organization to organization. If the organization is a regional forensics lab, then the assessed risk is high as the labs deal with multiple cases and different types of evidence. This may not be true for the forensics lab of a private firm.

Maintain a log register at the entrance of the lab to record the following data: name of visitor with date, time, purpose of the visit, name of contact person, and address of the visitor. Provide visitors with passes to distinguish them from the lab staff. Place an alarm in the lab to provide an additional layer of protection and deploy guards around the premises of the lab. Place closed-circuit cameras in the lab and around its premises to monitor human movement within the lab. Ensure security of the lab by keeping all the windows closed. This helps prevent unauthorized physical access to the lab from a covert channel.

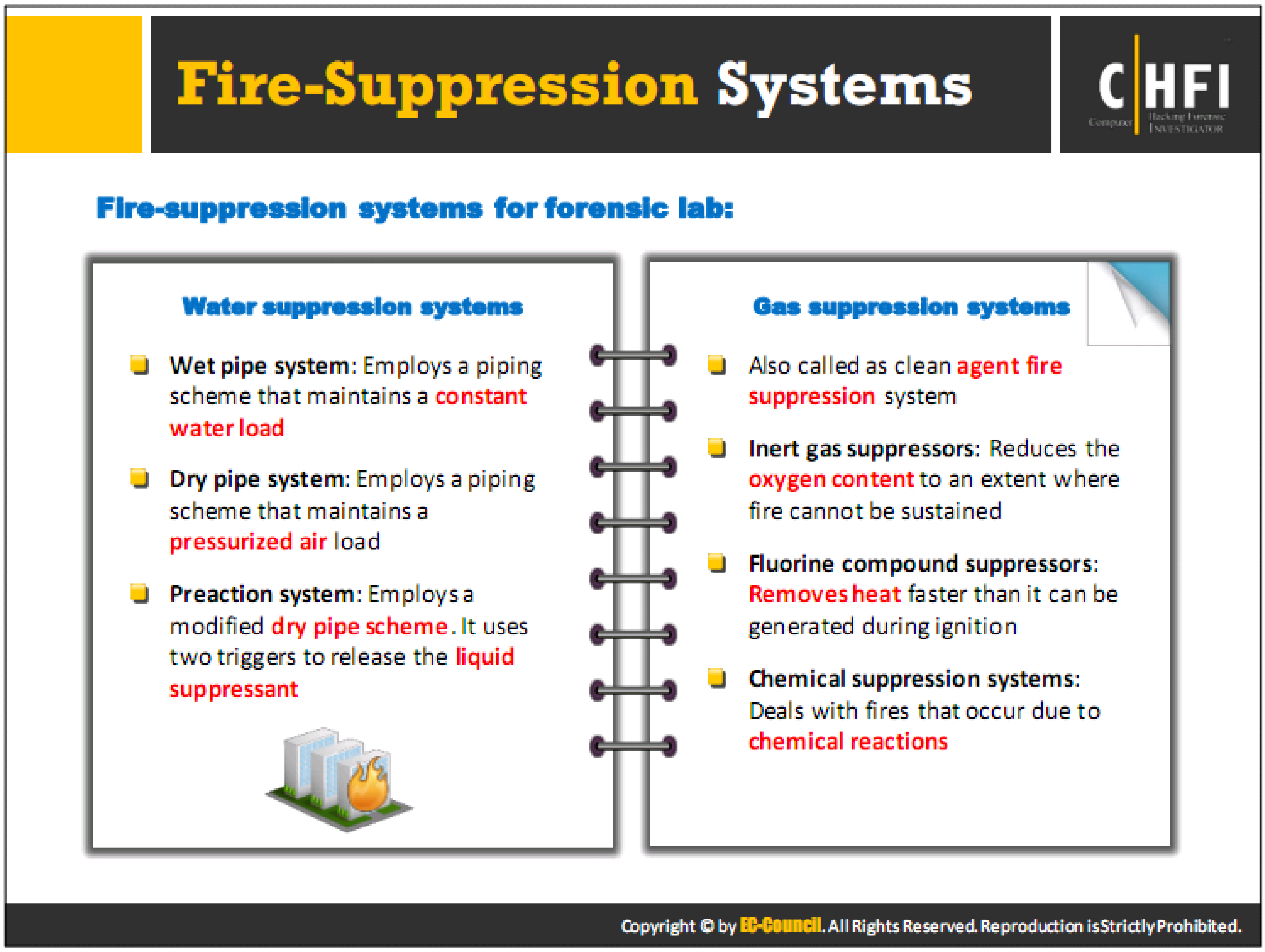
Place fire extinguishers within and outside the lab, and provide training to the lab personnel and guards on how to use the fire extinguisher, so that personnel know how to use the equipment effectively in case of fire.

Shield workstations from transmitting electromagnetic signals, as electronic equipment emit electromagnetic radiation, which can be helpful to discover the data the equipment is transmitting or displaying. The solution is to shield emissions through a process the U.S. Department of Defense has named TEMPEST.

It is stated by The National Industrial Security Program Operating Manual (NISPOM) that, “TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that if intercepted and analyzed will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.”

To prevent eavesdropping, TEMPEST labs use sheets of metal, good conductors such as copper for lining the walls, ceilings, and floor. Insulate the power cables to prevent radiation and add filters to the telephones within the lab.

It is costly to build a TEMPEST lab, as it goes through checks and maintenance at regular intervals. As a replacement for a TEMPEST lab, some vendors have come up with low-radiation workstations. The cost of such kinds of workstations is more than the normal forensics workstation.



Fire-Suppression Systems

Fire-suppression systems for forensic lab:

Water suppression systems

- **Wet pipe system:** Employs a piping scheme that maintains a **constant water load**
- **Dry pipe system:** Employs a piping scheme that maintains a **pressurized air** load
- **Preaction system:** Employs a modified **dry pipe scheme**. It uses two triggers to release the **liquid suppressant**

Gas suppression systems

- Also called as clean **agent fire suppression** system
- **Inert gas suppressors:** Reduces the **oxygen content** to an extent where fire cannot be sustained
- **Fluorine compound suppressors:** **Removes heat** faster than it can be generated during ignition
- **Chemical suppression systems:** Deals with fires that occur due to **chemical reactions**

Fire can be disastrous in the forensic lab. Any electrical device can be a source of fire, though it does not generally happen in the computer. On a few occasions, short circuits can also damage the cable. It might even ignite a flammable item close by.

There may be fire in the computers as well if the servo-voice-coil actuators freeze because of damage in the drive. The frozen actuators interrupt the movement of the head assembly and the internal programming of the disk's circuit forces the movement by applying more power to the servo-voice-coil actuators. The components of the drive can handle a certain amount of power before they fail and overload the ribbon connecting the drive to the computer. The ribbons do not respond to excessive power. High voltage passing through the ribbon causes sparks.

For fire suppression systems:

- Install a dry chemical fire extinguisher system to deal with the fire accidents that occur because of chemical reactions.
- Check the installation of fire sprinklers and make sure they are working.
- The fire extinguishers must be accessible when needed.

A wet sprinkler system has an overhead sprinkler piping generally concealed above the ceiling. This system consists of pipes filled with pressurized water and connected to the sprinkler heads, which infiltrate through the ceiling. Every sprinkler head makes use of the fusible links, which melt in extreme heat allowing the water to flow. This system fulfills the basic requirements and is cost effective. In case of fire, it will trigger the sprinklers only in the affected areas.

The interlocked dry pipe systems use water as the extinguishing agent. This system activates when:

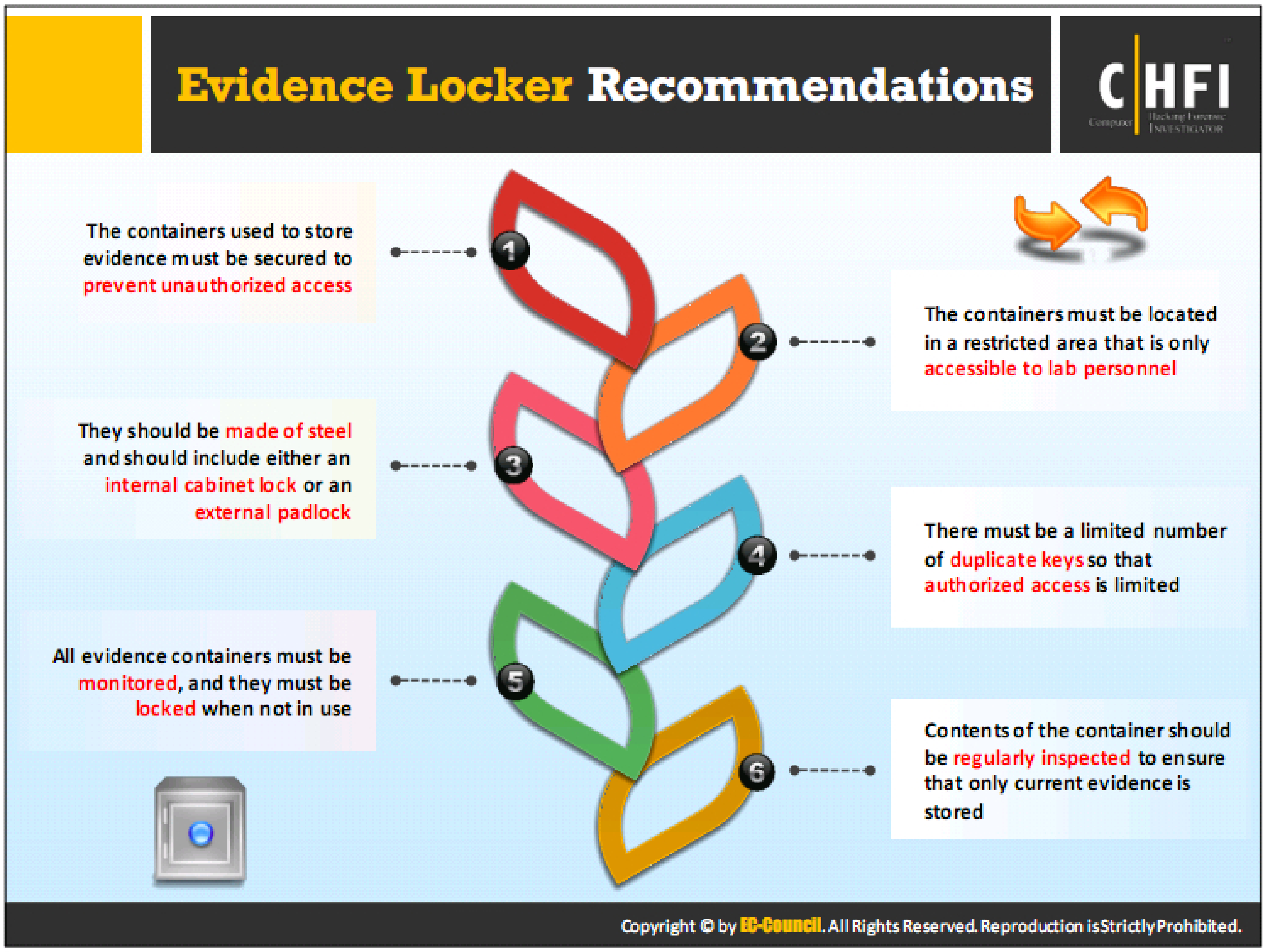
- The temperature rise melts the fusible link on the sprinkler head.
- The electronic detection of fire or smoke opens the sprinkler head valve, allowing water flow into the system.

This system minimizes the risk of inadvertent discharge of water, but has a reasonable first cost premium compared to a wet pipe system.

CO_2 and FM200 are chemical or gaseous system types that use an electronic fire or smoke detection technique to release the extinguishing agent. They are more advantageous and respond rapidly to mitigate a developing fire. These systems require limited cleaning.

Fires in labs produce harmful chemicals, which obstruct the emergency response team. Therefore, install exhaust systems to remove these toxic products.

The dry chemical type fire extinguisher is currently more popular. It extinguishes Class A, B, or C fires. Class A refers to paper, trash, and plastic; Class B refers to flammable liquids and gases; and Class C refers to energized electrical equipment.



Evidence Locker Recommendations

1. The containers used to store evidence must be secured to prevent unauthorized access

2. The containers must be located in a restricted area that is only accessible to lab personnel

3. They should be made of steel and should include either an internal cabinet lock or an external padlock

4. There must be a limited number of duplicate keys so that authorized access is limited

5. All evidence containers must be monitored, and they must be locked when not in use

6. Contents of the container should be regularly inspected to ensure that only current evidence is stored

The evidence lockers are the evidence storage devices and need protection from unauthorized access by using high-quality padlocks and performing routine inspection to check the content of the evidence lockers.

Recommendations for securing evidence lockers:

- Place these containers in restricted areas, which are only accessible to lab officers.
- A minimum number of authorized people should be able to access the evidence.
- Keep records about the people authorized to access the container.
- Close all the evidence lockers when not under direct supervision of an authorized person.

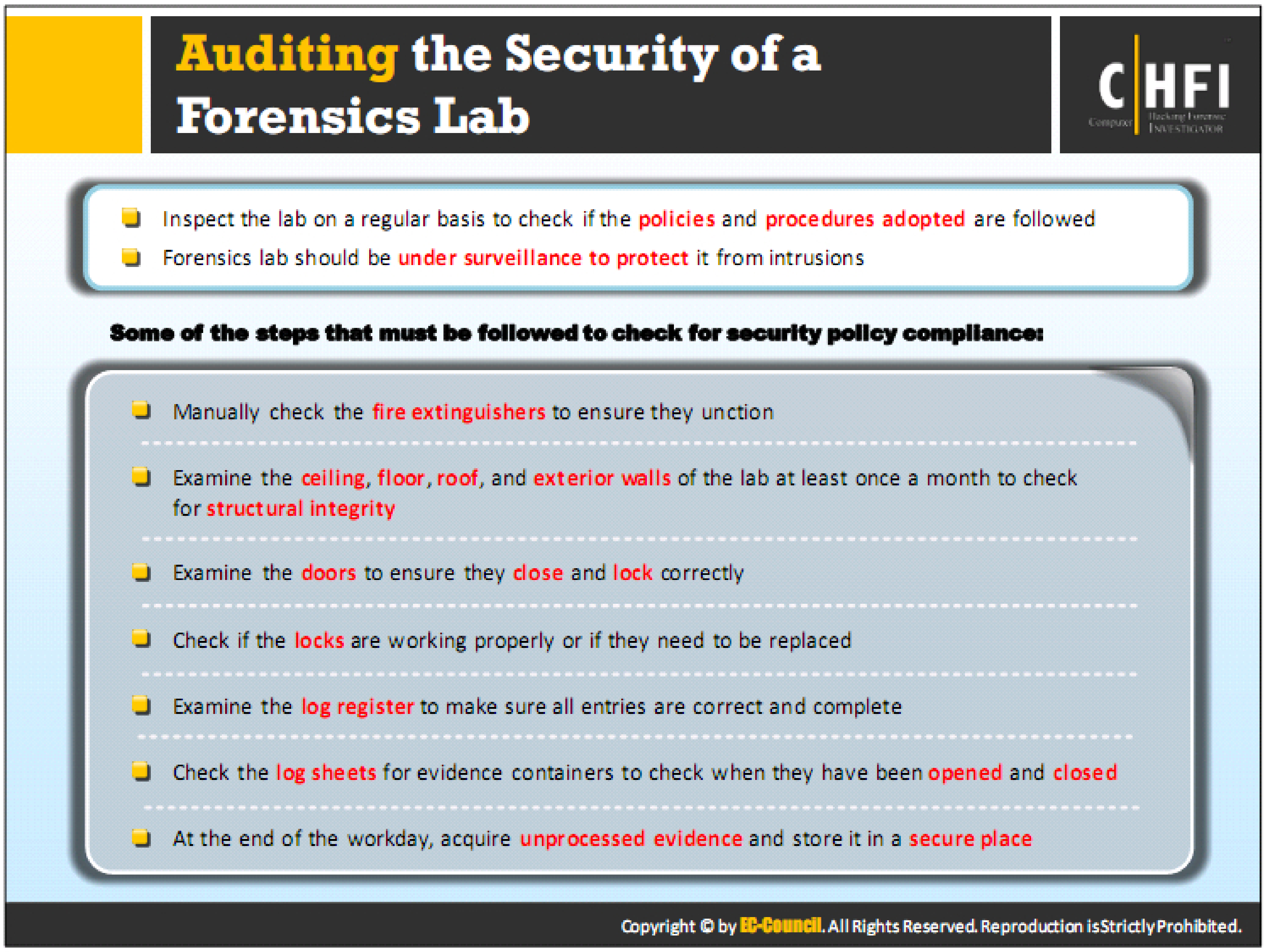
Best practices for using a combination locking system for evidence lockers:

- Provide the same level of security as for the evidence in the container.
- Store the combination in a separate equally secured container.
- Eliminate all the other combinations ever used before setting up a new combination.
- Only authorized personnel should have access to change the lock combinations.
- Change the combination after every six months or whenever any authorized personnel leaves the organization.

Best practices for using a keyed padlock:

- Appoint a person for distributing keys.
- Stamp every duplicate key with sequential numbers.
- Keep a registry that lists the authorized people for each key.
- Perform monthly audits to ensure that no authorized person has lost a key.
- When the responsible person changes, maintain a record of all the keys.
- Put the keys in a locked container, which is accessible only to the lab manager and key custodian of the lab.
- Maintain the same level of security for keys as for evidence lockers.
- Consider changing the locks and keys yearly. If a key is missing, replace all the related locks and the keys.
- Do not maintain a single master key for many locks.

Use evidence lockers made of steel with an external padlock or internal cabinet lock. Acquire a safe that offers high-level protection of evidence from fire damage. If possible, use safes designed to protect electronic media. The evidence storage room can also be helpful in a self-owned computer forensics lab. The evidence room should have the same construction and security as the lab. This room also requires an evidence custodian and a service counter. Maintain a log that lists the time of opening and closing an evidence container. Preserve these logs for at least three years or longer.



Auditing the Security of a Forensics Lab

- Inspect the lab on a regular basis to check if the policies and procedures adopted are followed
- Forensics lab should be under surveillance to protect it from intrusions

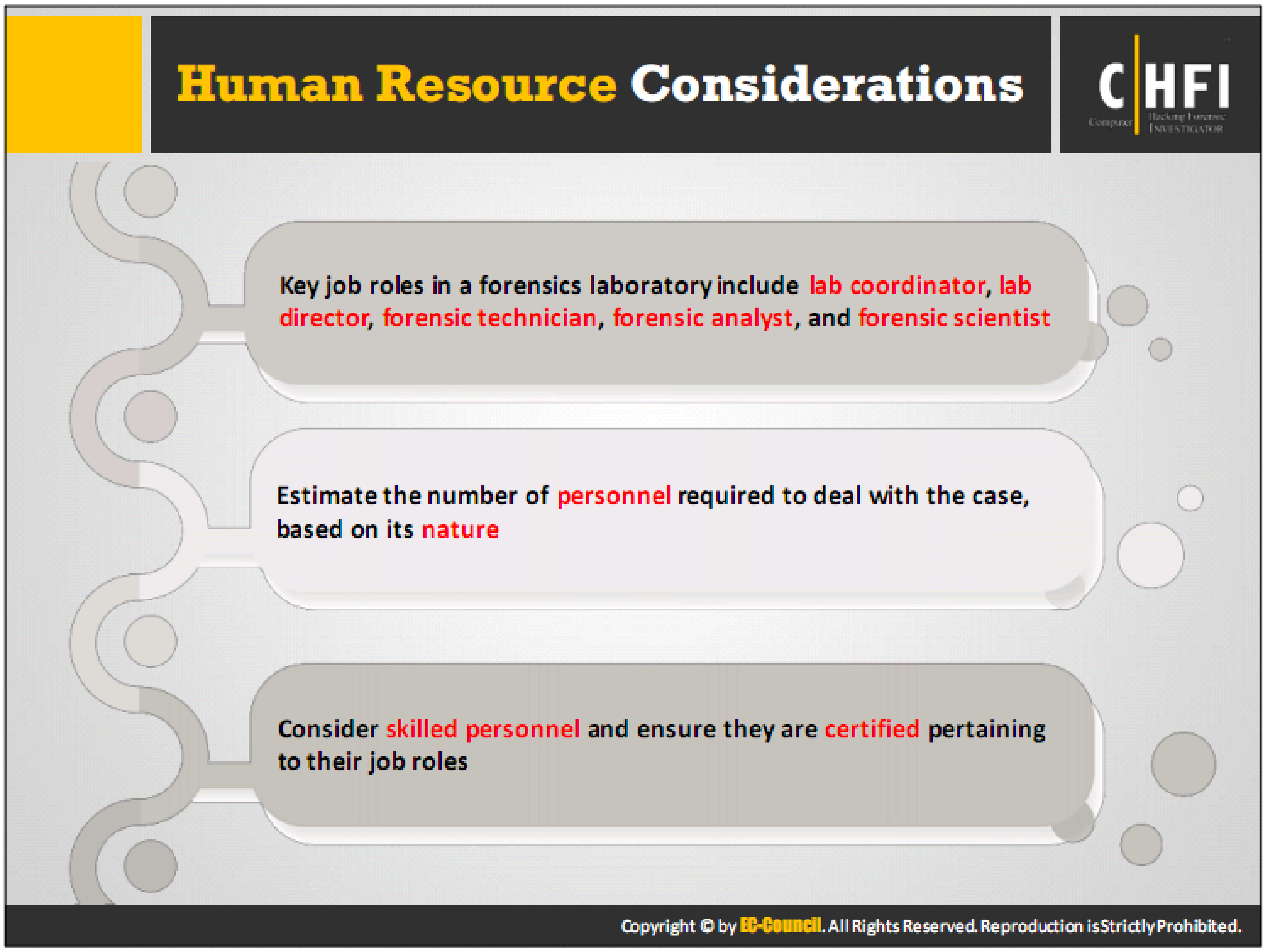
Some of the steps that must be followed to check for security policy compliance:

- Manually check the fire extinguishers to ensure they unction
- Examine the ceiling, floor, roof, and exterior walls of the lab at least once a month to check for structural integrity
- Examine the doors to ensure they close and lock correctly
- Check if the locks are working properly or if they need to be replaced
- Examine the log register to make sure all entries are correct and complete
- Check the log sheets for evidence containers to check when they have been opened and closed
- At the end of the workday, acquire unprocessed evidence and store it in a secure place

Inspect the lab on a regular basis to check for proper implementation of the designed policies and procedures. The forensics lab should be under surveillance to protect it from intrusions.

Some of the steps to check for security policy compliance:

- Check the fire extinguishers manually to ensure their functioning.
- Examine the ceiling, floor, roof, and exterior walls of the lab at least once a month to check for structural integrity.
- Examine the doors to ensure they close and lock correctly.
- Check if the locks are working properly or if they need replacement.
- Examine the log register to make sure all entries are correct and complete.
- Check the evidence container log sheets regularly to keep a record of their opening and closing.
- At the end of the workday, acquire unprocessed evidence and store it in a secure place.



Human Resource Considerations

Key job roles in a forensics laboratory include lab coordinator, lab director, forensic technician, forensic analyst, and forensic scientist

Estimate the number of personnel required to deal with the case, based on its nature

Consider skilled personnel and ensure they are certified pertaining to their job roles

Human resource refers to the trained professionals required to perform a series of functions for an organization or firm in order to complete a bigger objective. Every company has a department of human resource professionals, who are responsible for finding and recruiting the skilled employees for their company.

In the case of a computer forensics laboratory, key job roles include lab cybercrime investigator, coordinator, lab director, forensic technician, forensic analyst, forensic scientist, etc. As part of the human resource consideration, estimate the number of personnel required to deal with the case based on its nature and the skills they should have to complete the tasks. Interview the appropriate candidates and recruit them legally. Ensure they have certification pertaining to their job roles.

Computer Forensics Investigator

Hiring a computer forensics investigator is a vital step in computer forensics. The investigator is a person who handles the complete investigation process, for example, preservation, identification, extraction, and documentation of the evidence.

Skills essential for a computer forensics investigator are:

- Knowledge about general computers such as hardware, software, OS, applications, networking, etc.
- Experience in performing a proper investigation to protect digital evidence.
- Must have certification from authorized organizations.

For searching and seizing some crime evidence, a search warrant is required. A law enforcement officer is the person who persuades a judge that issuing a warrant is necessary. The judge first prepares an affidavit containing the reason for the search and the area of the search. The affidavit also gives a limited right to the police to violate the suspect's privacy.

Law Enforcement Officer

The law enforcement officer should have the following essential skills:

- A lawyer and have knowledge of general computer skills
- Have knowledge of all cybercrime laws
- Must know the way to write an appropriate warrant for searching and seizing a computer

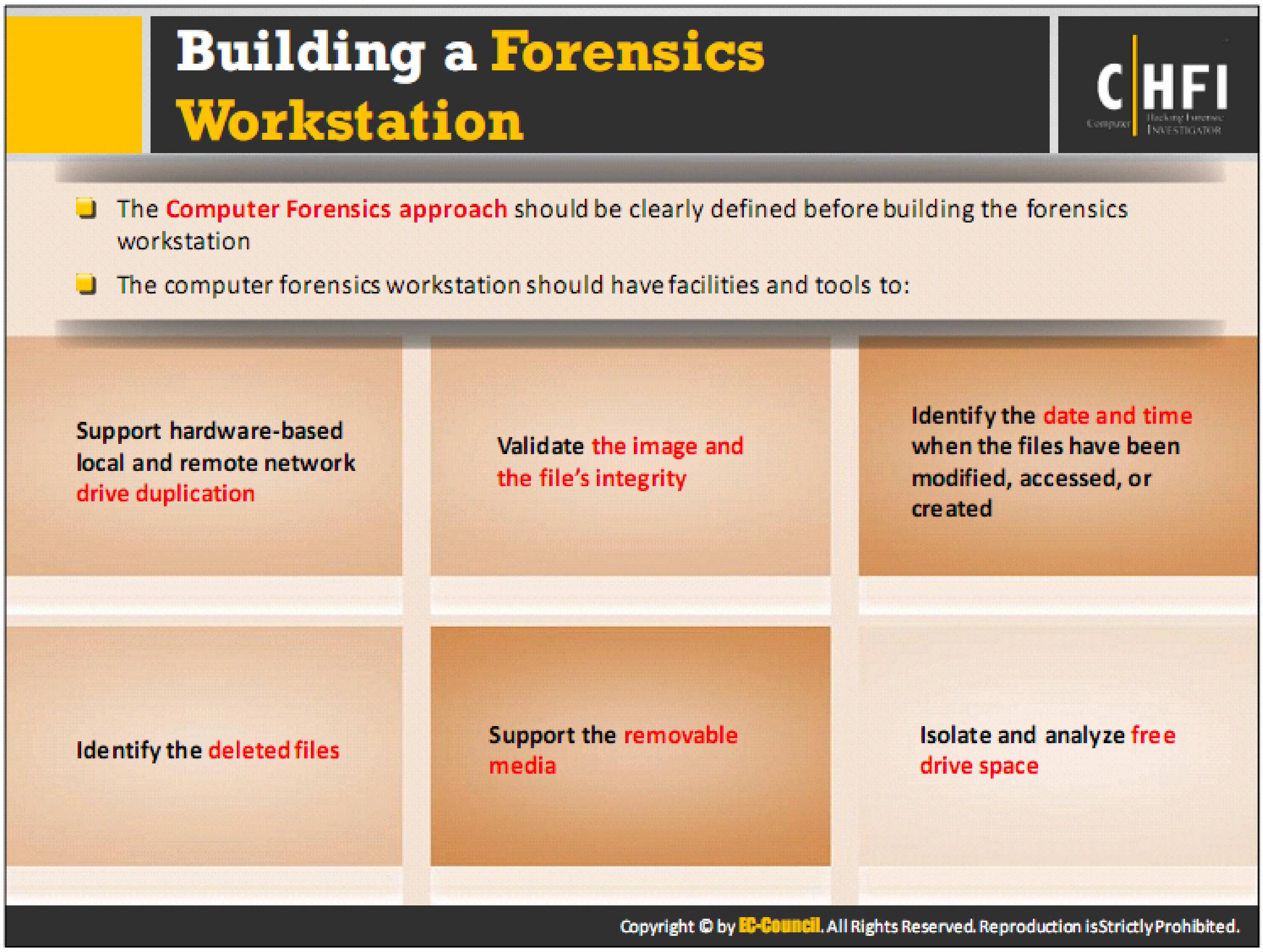
Lab Director

The lab director/manager is responsible for adhering to a specific set of industrial standards. A lab director regularly reviews and manages case-related processes. Apart from regular duties, a lab director needs to promote group consensus in policy making or decision making, understand lab needs, ensure that staff members adhere to ethical standards, and plan for updating the lab.

The prime duty of a lab director is to maintain quality during the entire process of a computer forensic investigation: outlining the case and the path to follow, evidence logging, lab entry privileges, guidelines in filing reports, understanding the lab's status and ensuring its efficiency, and setting production schedules in the investigation process. The director is responsible for lab policies, and the safety and security of the evidence and staff. The lab director is also responsible for day-to-day investigation activities in the lab. Duties even include lab funding and expenditure management.

A lab director must also:

- Have a wide range of forensic knowledge
- Anticipate staffing, equipment, and training needs
- Help ensure compliance with the Quality Assurance (QA) requirements



Building a Forensics Workstation

- The Computer Forensics approach should be clearly defined before building the forensics workstation
- The computer forensics workstation should have facilities and tools to:

Support hardware-based local and remote network drive duplication

Validate the image and the file's integrity

Identify the date and time when the files have been modified, accessed, or created

Identify the deleted files

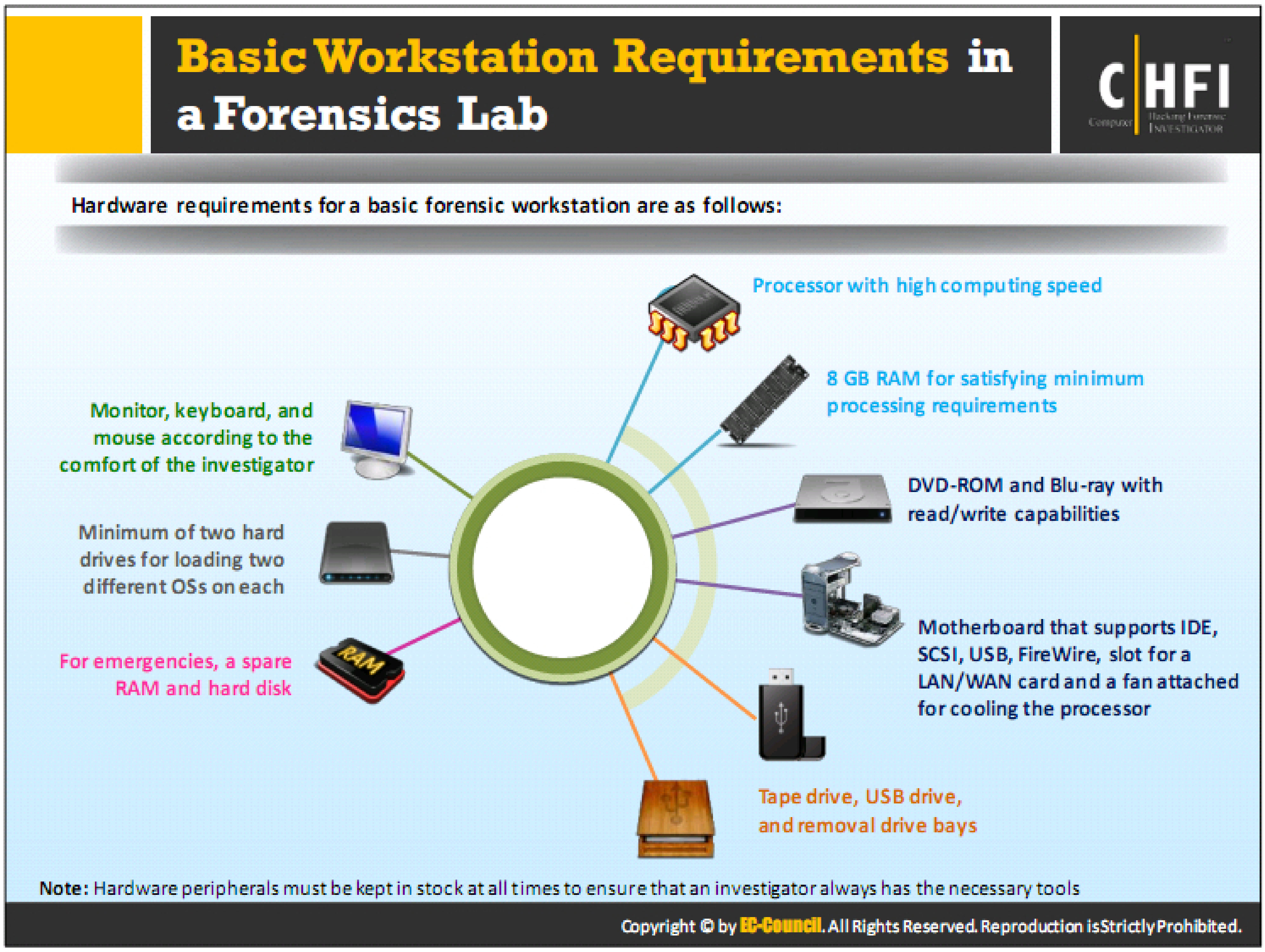
Support the removable media

Isolate and analyze free drive space

Define the computer forensics approach clearly before building the forensics workstation. For developing a forensics laboratory, the total estimated cost incurred to meet the accreditation standards of a standardized body that certifies labs will be the deciding factor for fund allocation. Funding is important in order for a successful implementation of the computer forensics lab. Calculate the yearly budget allocation for a forensics lab, based on the previous year's statistics as well as estimated trends for the next year. This includes the number of cases handled, the training required for staff, upgrading hardware and software tools in the lab, additional equipment required for enhancing the security of the lab premises, renovation of the lab, recruitment of additional certified personnel if needed, and many other deciding factors.

The computer forensics workstation should have facilities and tools to:

- Support hardware-based local and remote network drive duplication
- Validate the image and the file's integrity
- Identify the date and time of creation, access and modification of a file
- Identify deleted files
- Support removable media
- Isolate and analyze free drive space



Basic Workstation Requirements in a Forensics Lab

Hardware requirements for a basic forensic workstation are as follows:

Processor with high computing speed

8 GB RAM for satisfying minimum processing requirements

DVD-ROM and Blu-ray with read/write capabilities

Motherboard that supports IDE, SCSI, USB, FireWire, slot for a LAN/WAN card and a fan attached for cooling the processor

Tape drive, USB drive, and removal drive bays

Monitor, keyboard, and mouse according to the comfort of the investigator

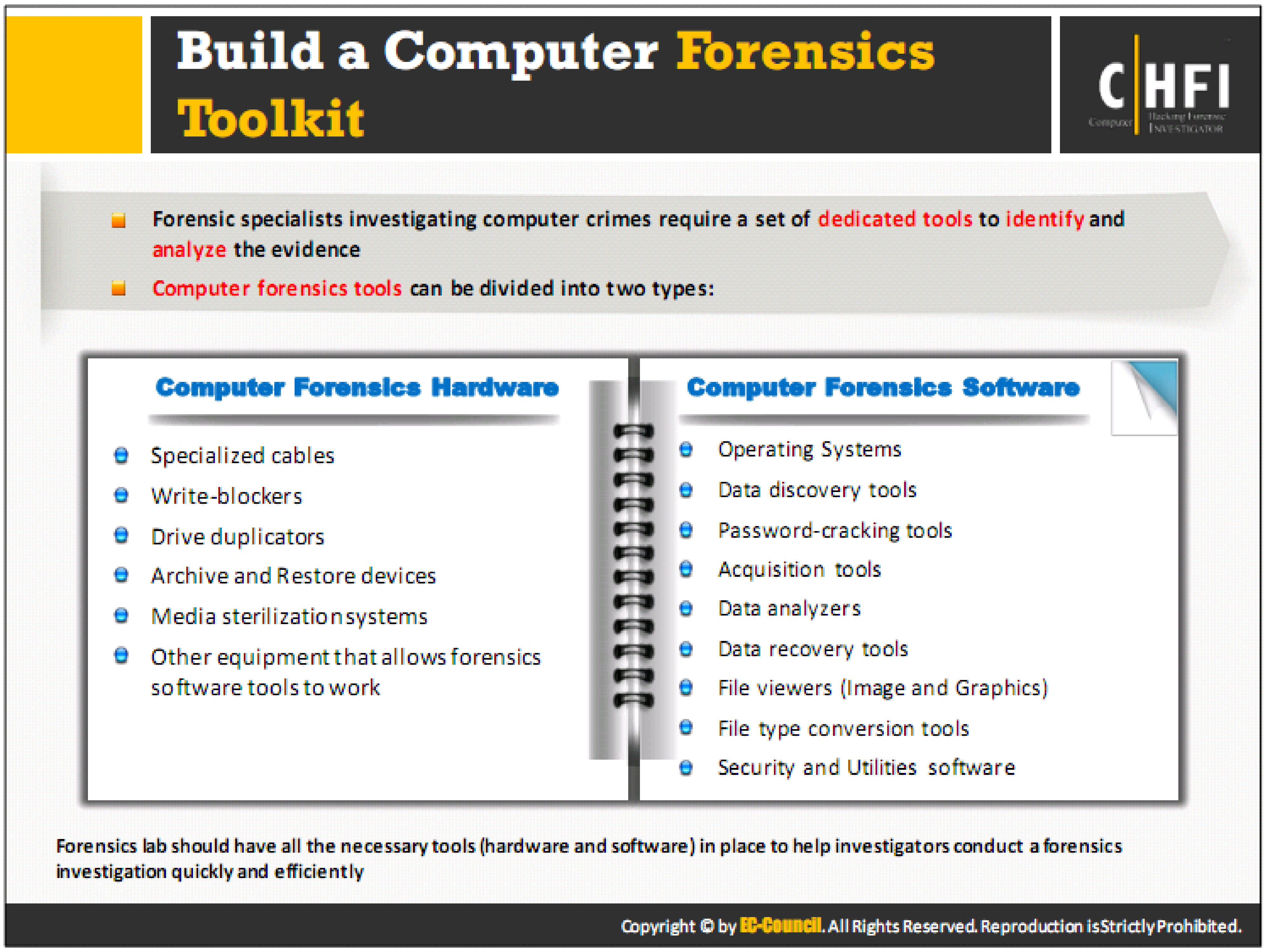
Minimum of two hard drives for loading two different OSs on each

For emergencies, a spare RAM and hard disk

Note: Hardware peripherals must be kept in stock at all times to ensure that an investigator always has the necessary tools

Forensic workstations are high-end computers with fast processing speed, high memory, and disk storage. These workstations can serve critical processes such as duplication of data, recovering data from deleted files, analyzing data over the network, and retrieving data from the slack. These workstations come with forensics tools that help the investigator in an investigation. The investigation includes various high-end and low-end processes; thus, the hardware configuration of forensic workstations used for extreme processing will be different from that of a workstation used for doing routine tasks. The hardware requirements for a basic forensic workstation are as follows:

- Processor with high computing speed
- 8 GB RAM for satisfying minimum processing requirements
- DVD-ROM, Blu-ray with read/write facility
- Motherboard, which supports IDE, SCSI, USB, slot for LAN/WAN card, and a fan attached for cooling the processor
- Tape drive, USB drive, removable drive bays
- Monitor, keyboard, and mouse according to comfort of investigator
- A minimum of two hard drives for loading two different operating systems
  - The two operating systems should preferably be Windows and Linux
- Extra RAM and hard disk in case of any need



Build a Computer Forensics Toolkit

- Forensic specialists investigating computer crimes require a set of dedicated tools to identify and analyze the evidence
- Computer forensics tools can be divided into two types:

Computer Forensics Hardware

- Specialized cables
- Write-blockers
- Drive duplicators
- Archive and Restore devices
- Media sterilization systems
- Other equipment that allows forensics software tools to work

Computer Forensics Software

- Operating Systems
- Data discovery tools
- Password-cracking tools
- Acquisition tools
- Data analyzers
- Data recovery tools
- File viewers (Image and Graphics)
- File type conversion tools
- Security and Utilities software

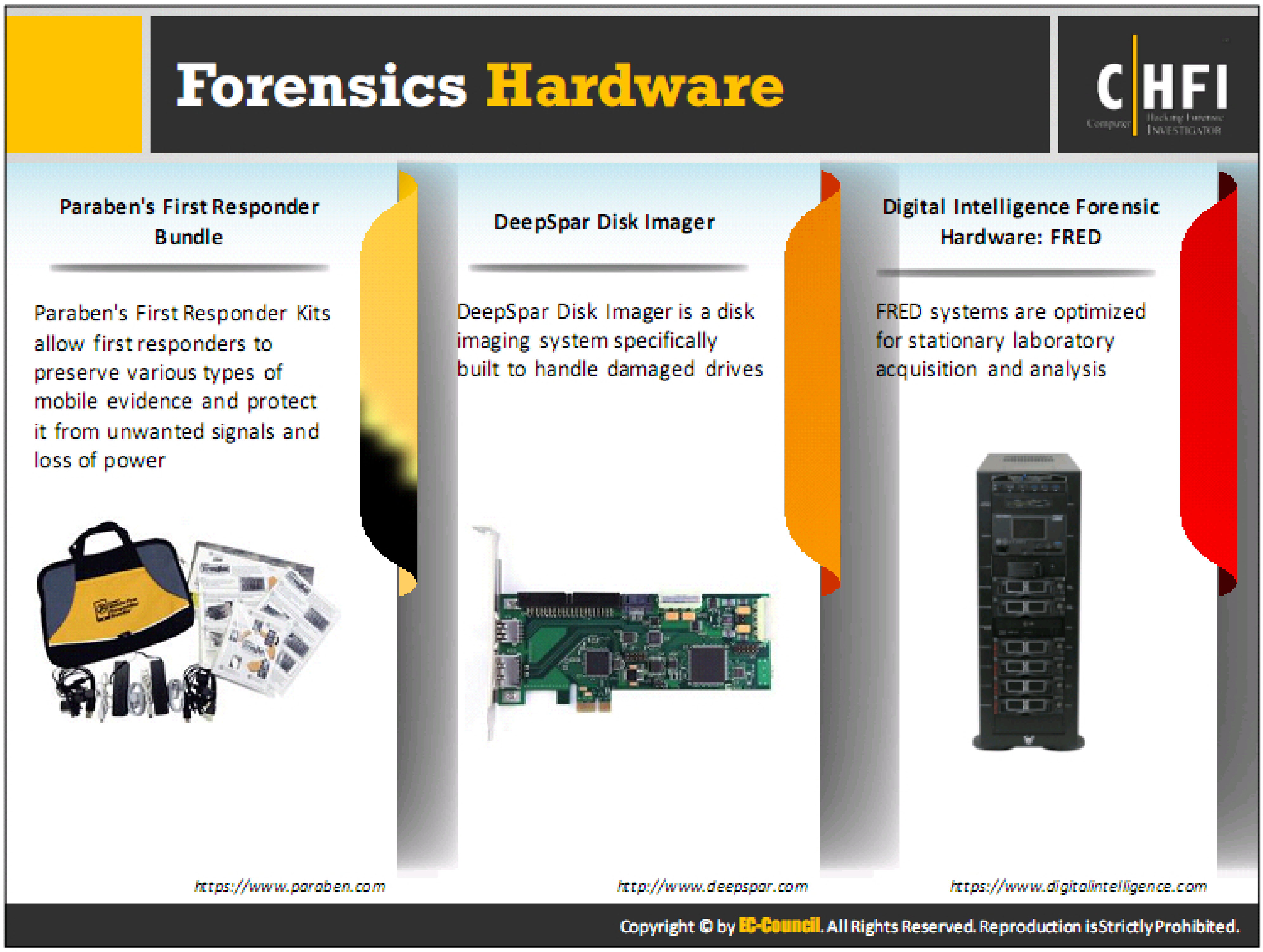
Forensics lab should have all the necessary tools (hardware and software) in place to help investigators conduct a forensics investigation quickly and efficiently

The investigator should have a collection of hardware and software tools for acquiring data during the investigation. If the investigator is familiar with the investigation toolkit, it can offer a quick response during the investigation of the incident. A sophisticated investigation toolkit can reduce the incident impact by stopping the incident from spreading through the systems. This will minimize the organization's damage and aid the investigation process as well.

A computer investigation toolkit contains:

- A laptop computer with relevant software tools
- Operating systems and patches
- Application media
- Write-protected backup devices
- Blank media
- Basic networking equipment and cables

Create the toolkit before commencing an investigation, as the investigating team needs to be familiar with these tools before performing the investigation.



Forensics Hardware

Paraben's First Responder Bundle

Paraben's First Responder Kits allow first responders to preserve various types of mobile evidence and protect it from unwanted signals and loss of power

https://www.paraben.com

DeepSpar Disk Imager

DeepSpar Disk Imager is a disk imaging system specifically built to handle damaged drives

http://www.deepspar.com

Digital Intelligence Forensic Hardware: FRED

FRED systems are optimized for stationary laboratory acquisition and analysis

https://www.digitalintelligence.com

Paraben's First Responder Bundle

Source: https://www.paraben.com

Paraben's First Responder Kits provide first responders the necessary tools to preserve various types of mobile evidence and protect it from unwanted signals and loss of power. Whenever there is a mobile device involved at an incident, there are recommended procedures to follow. Two of the most important steps are to secure the device from unwanted wireless signals that could contaminate or eliminate data and to provide power to the device to prevent losing data. Paraben's Mobile First Responder Bundle provides for both of these steps.

DeepSpar Disk Imager

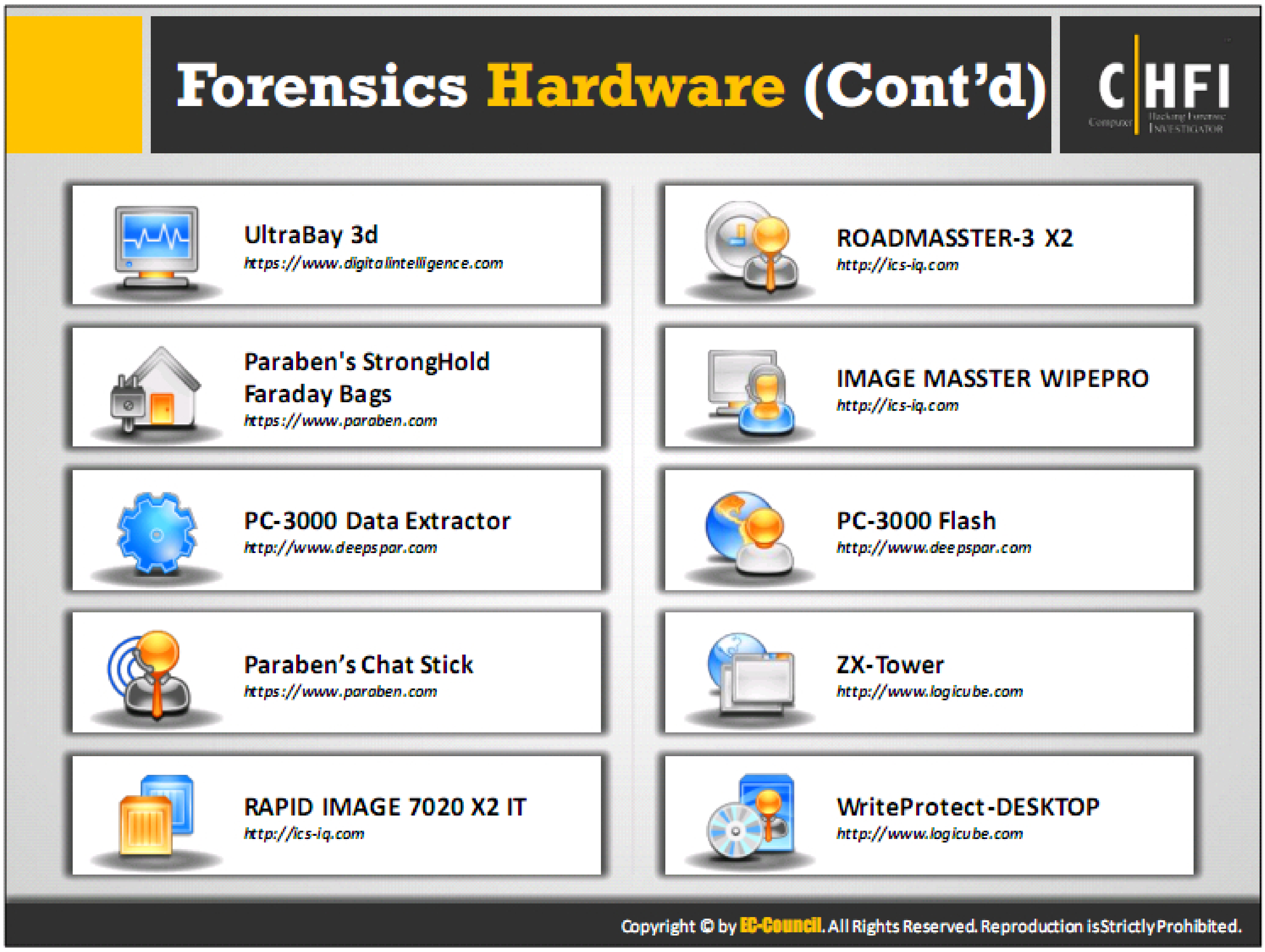
Source: http://www.deepspar.com

- DeepSpar Recovery Environment is a free Windows-based application extending File System Recovery capabilities of the DeepSpar Disk Imager.
- DeepSpar Operations Server is a client communication system that professionalizes your business and the interactions with your clients.
- Forensics Add-on for DeepSpar Disk Imager provides computer forensics capabilities.

Digital Intelligence Forensic Hardware: FRED

Source: https://www.digitalintelligence.com

FRED systems are optimized for stationary laboratory acquisition and analysis. Simply remove the hard drive(s) from the suspect system, plug them into FRED, and acquire the digital evidence. FRED will acquire data directly from IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/USB hard drives and storage devices and save forensic images to Blu-Ray, DVD, CD, or hard drives.



Forensics Hardware (Cont'd)

CHFI
Computer Hacking Forensic Investigator

UltraBay 3d
https://www.digitalintelligence.com

ROADMASSTER-3 X2
http://ics-iq.com

Paraben's StrongHold Faraday Bags
https://www.paraben.com

IMAGE MASSTER WIPEPRO
http://ics-iq.com

PC-3000 Data Extractor
http://www.deepspar.com

PC-3000 Flash
http://www.deepspar.com

Paraben's Chat Stick
https://www.paraben.com

ZX-Tower
http://www.logicube.com

RAPID IMAGE 7020 X2 IT
http://ics-iq.com

WriteProtect-DESKTOP
http://www.logicube.com

UltraBay 3d

Source: https://www.digitalintelligence.com

The UltraBay 3d is a USB 3.0 integrated forensic bridge that includes a touch screen display and a graphical user interface for acquisition process monitoring.

Paraben's StrongHold Faraday Bags

Source: https://www.paraben.com

Paraben's StrongHold bags block out wireless signals from cell towers, wireless networks, and other signal sources to protect evidence.

PC-3000 Data Extractor

Source: http://www.deepspar.com

PC-3000 Data Extractor is a software add-on to PC-3000 that diagnoses and fixes file system issues, so that the client's data can be obtained. It works in tandem with the PC-3000 hardware to recover data from any media (IDE HDD, SCSI HDD, and flash memory readers).

Paraben's Chat Stick

Source: https://www.paraben.com

Paraben's Chat Stick is a thumb drive device that will search the entire computer, scan it for chat logs from Yahoo, MSN 6.1, 6.2, 7.0, & 7.5, ICQ 1999-2003b, Trillian, Skype, Hello, and

Miranda and create a report in an easy to read format so that one can see what kids or employees are saying to people online.

RAPID IMAGE 7020 X2 IT

Source: http://ics-iq.com

The Rapid Image™ Hard Drive Duplicators are designed to copy one "Master" hard drive to up to 19 "Target" hard drives at Fast SATA-III Speeds. It can also be configured to copy multiple Master drives simultaneously. It also supports the duplication of up to 10 Master drives simultaneously.

ROADMASSTER-3 X2

Source: http://ics-iq.com

The RoadMASSter-3 X2 is a forensic portable lab designed as a forensic data acquisition and analysis workstation. The RoadMASSter-3 X2 is rugged and is equipped with all the necessary tools to seize data from drives with common drive interface technologies.

IMAGE MASSTER WIPEPRO

Source: http://ics-iq.com

The Image MASSter™ Wipe PRO is a hard Drive Sanitization Station. It can erase up to 8 Hard Drives simultaneously at speeds exceeding 7 GB/min.

PC-3000 Flash

Source: http://www.deepspar.com

PC-3000 Flash is a hardware and software suite for recovering data from flash-based storage devices like SD cards and USB sticks.

ZX-Tower

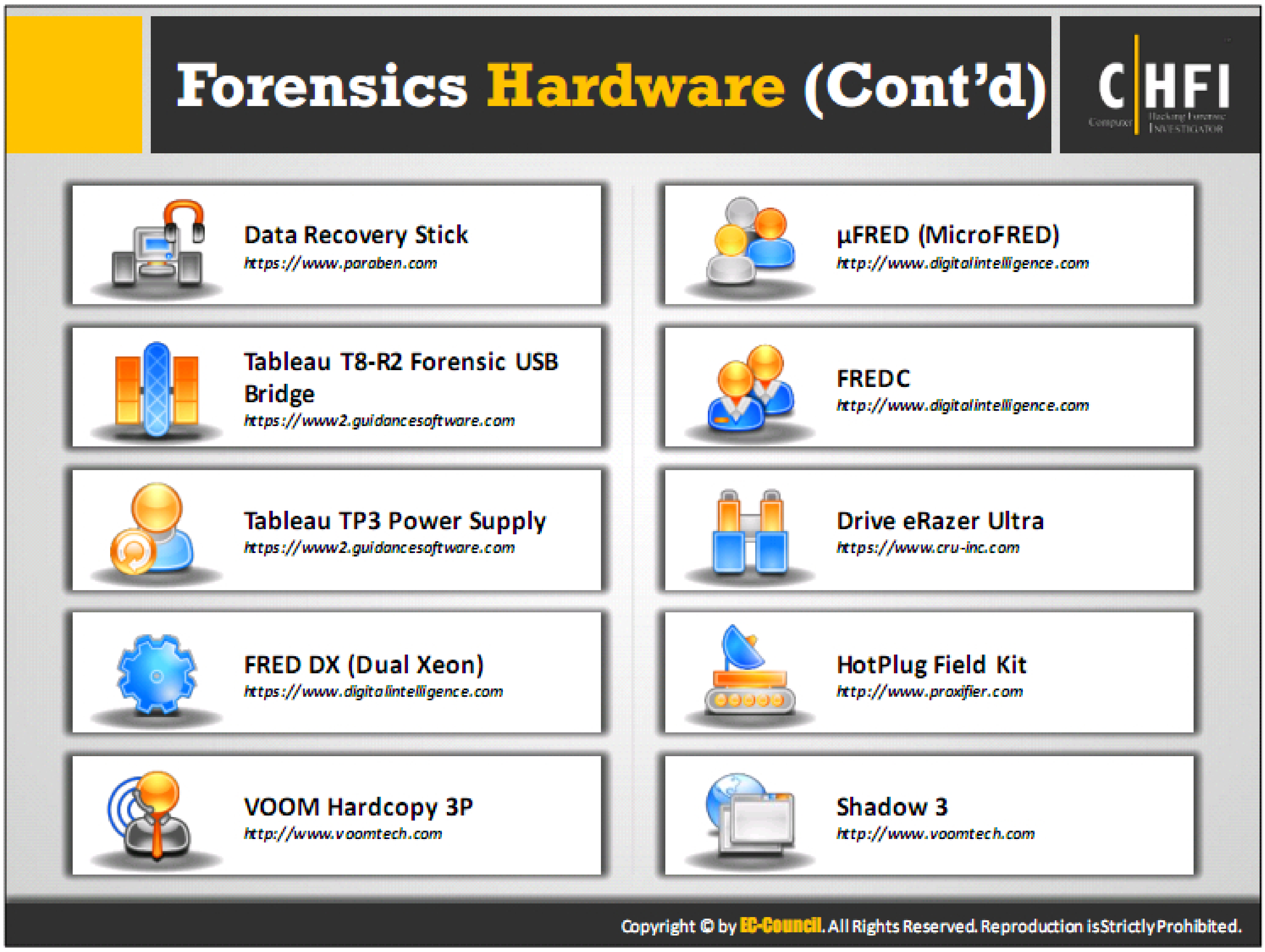
Source: http://www.logicube.com

The ZX-Tower™ solution provides secure sanitization of hard disk drives and delivers wiping at a speed of 24 GB/min. The multi-target ZX-T allows to easily wipe up to 8 target hard drives simultaneously and also allows users to wipe up to 4 USB 3.0 enclosures.

WriteProtect-DESKTOP

Source: http://www.logicube.com

The WriteProtect-DESKTOP provides digital forensic professionals with a secure, read-only write-blocking of suspect hard drives. It is a portable write-blocker that provides support for 5 different interfaces in one device.



Forensics Hardware (Cont'd)

- Data Recovery Stick
  https://www.paraben.com
- Tableau T8-R2 Forensic USB Bridge
  https://www2.guidancesoftware.com
- Tableau TP3 Power Supply
  https://www2.guidancesoftware.com
- FRED DX (Dual Xeon)
  https://www.digitalintelligence.com
- VOOM Hardcopy 3P
  http://www.voomtech.com
- µFRED (MicroFRED)
  http://www.digitalintelligence.com
- FREDC
  http://www.digitalintelligence.com
- Drive eRazer Ultra
  https://www.cru-inc.com
- HotPlug Field Kit
  http://www.proxifier.com
- Shadow 3
  http://www.voomtech.com

Data Recovery Stick

Source: https://www.paraben.com

The Data Recovery Stick can recover deleted files. There's no software to download and install it, just plug the Data Recovery Stick into a USB port, open the software, and start recovery. Even if files have been deleted from the recycle bin, they can be still recovered as long as they have not been overwritten by new data.

Tableau T8-R2 Forensic USB Bridge

Source: https://www2.guidancesoftware.com

Tableau's new T8-R2 Forensic USB Bridge offers secure, hardware-based write blocking of USB mass storage devices.

Tableau TP3 Power Supply

Source: https://www2.guidancesoftware.com

The TP3 is designed to power the Tableau TD1 duplicator and two hard disks.

FRED DX (Dual Xeon)

Source: https://www.digitalintelligence.com

FRED DX (Dual Xeon) is FRED SR's Dual Xeon configuration in a standard FRED chassis. It is used when the power that FRED SR offers in a full-tower footprint is required.

VOOM Hardcopy 3P

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

It is a forensic SATA/IDE Hard Drive Imager, Cloner, and Wiper with NIST approved SHA256 built into the hardware

µFRED (MicroFRED)

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

µFRED (MicroFRED) is a micro Forensic Recovery of Evidence Device. The µFRED system has much of the processing power of a full size FRED system but in a package only a fraction of the size (9" x 8" x 13").

FREDC

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

The FREDC is a fully configured, private cloud, for Forensic Storage. Centralized Storage, centralized administration, centralized security, and centralized backup

Drive eRazer Ultra

Source: *https://www.cru-inc.com*

The CRU® WiebeTech® Drive eRazer™ Ultra is a device that can completely clean hard drives. Simply connect a drive to the Drive eRazer Ultra and it will sanitize the drive and without tying up the computer.

HotPlug Field Kit

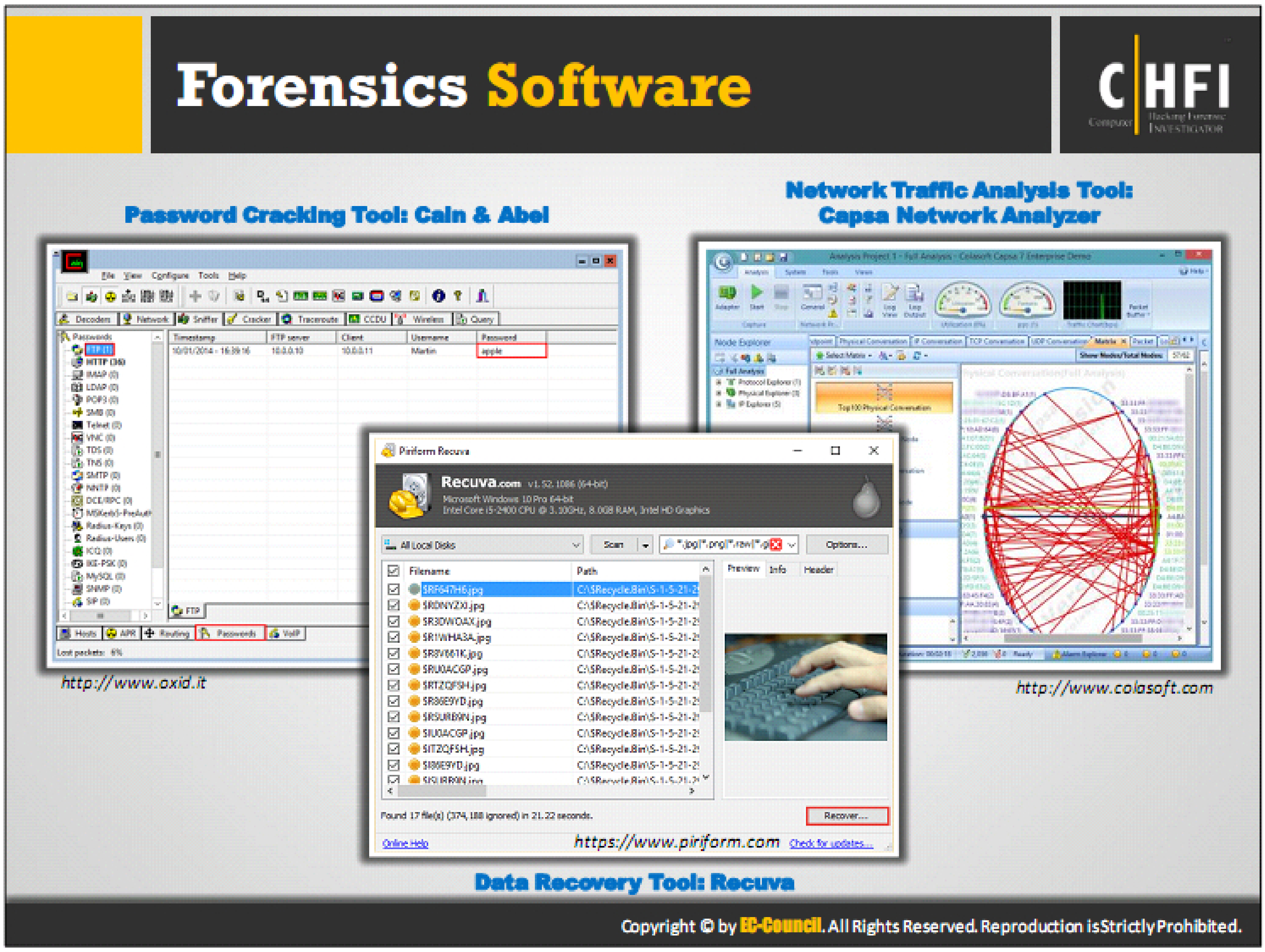
Source: *http://www.proxifier.com*

With the CRU® WiebeTech® HotPlug™ one can transport a computer without shutting it down. The HotPlug allows seizure and removal of computers from the field to anywhere else.

Shadow 3

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

It helps to view suspect computers at the scene of the investigation in real time without prior need to image hard drives and without the need for clumsy virtual viewing software; all without corrupting the evidence.



Forensics Software

Password Cracking Tool: Cain & Abel

http://www.oxid.it

Network Traffic Analysis Tool: Capsa Network Analyzer

http://www.colasoft.com

Data Recovery Tool: Recuva

https://www.piriform.com

Password Cracking Tool: Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols.

Data Recovery Tool: Recuva

Source: https://www.piriform.com

Recuva can recover lost pictures, music, documents, videos, emails or any other file type and it can also recover data from any rewriteable media like memory cards, external hard drives, USB sticks, etc.

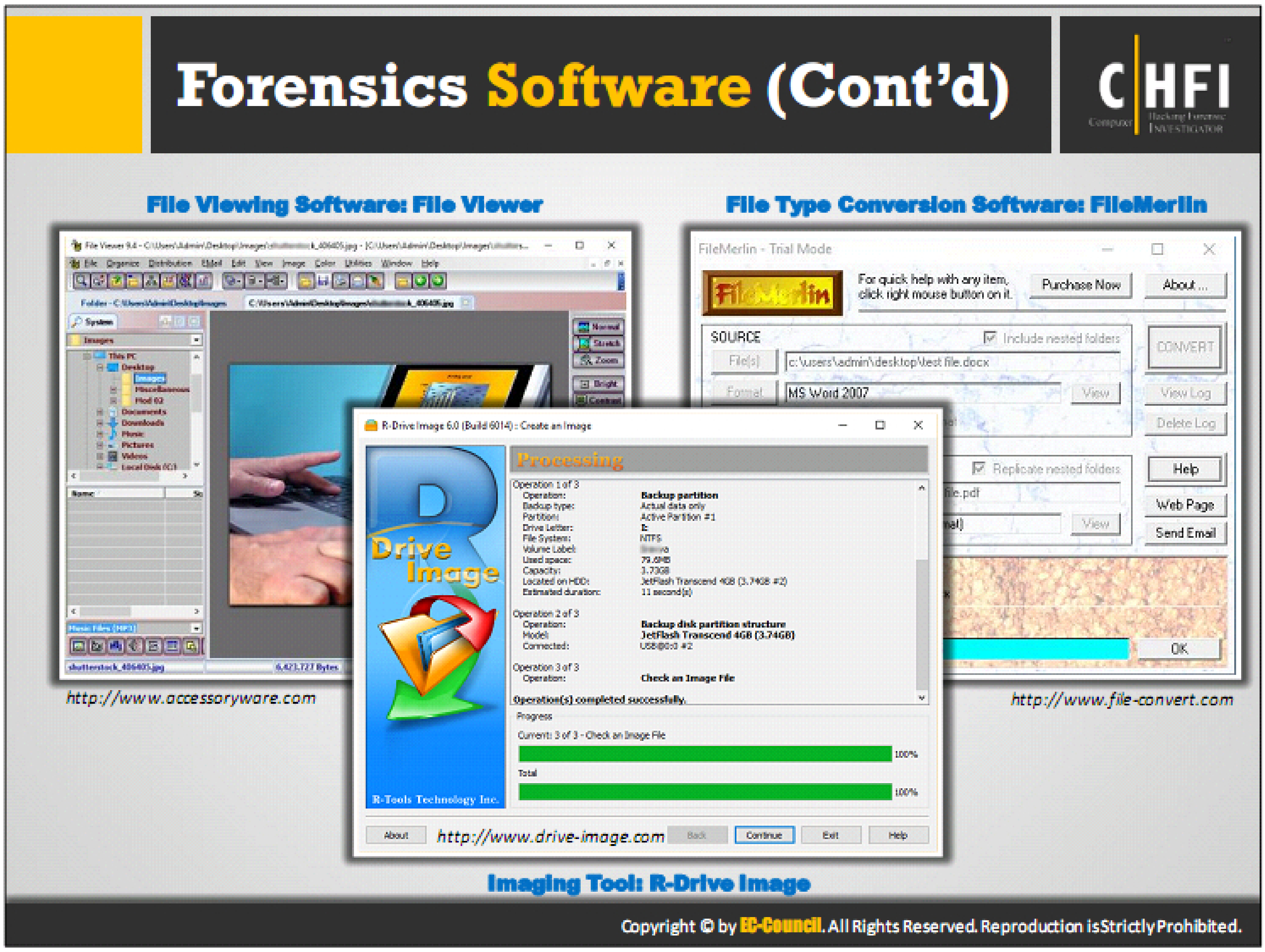
Network Traffic Analysis Tool: Capsa Network Analyzer

Source: http://www.colasoft.com

Capsa Free is a network analyzer that allows monitoring of network traffic, troubleshooting network issues, and analyzing packets. Features include support for over 300 network protocols (including the ability to create and customize protocols), MSN, and Yahoo Messenger filters, email monitor and auto-save, and customizable reports and dashboards.

Features:

- Extended network security analysis
- Versatile traffic & bandwidth statistics
- Advanced network protocol analysis
- Multiple network behavior monitoring
- Automatic expert network diagnosis



Forensics Software (Cont'd)

File Viewing Software: File Viewer

http://www.accessoryware.com

File Type Conversion Software: FileMerlin

http://www.file-convert.com

Imaging Tool: R-Drive Image

```
Processing
Operation 1 of 3
   Operation:          Backup partition
   Backup type:        Actual data only
   Partition:          Active Partition #1
   Drive Letter:       E:
   File System:        NTFS
   Volume Label:       [redacted]
   Used space:         79.6MB
   Capacity:           3.73GB
   Located on HDD:     JetFlash Transcend 4GB (3.74GB #2)
   Estimated duration: 11 second(s)

Operation 2 of 3
   Operation:          Backup disk partition structure
   Model:              JetFlash Transcend 4GB (3.74GB)
   Connected:          USB@0:0 #2

Operation 3 of 3
   Operation:          Check an Image File

Operation(s) completed successfully.

Progress
Current: 3 of 3 - Check an Image File   100%
Total                                   100%
```

http://www.drive-image.com

File Viewing Software: File Viewer

Source: http://www.accessoryware.com

File Viewer is a Disk/File Utility that helps to locate, view, print, organize, and exchange files over the internet using e-mail components. It can search for many common file types, or groups of file types, display, print, organize or send files over the internet, find and display pictures, videos, sounds, music, text files, documents, spread sheets, database, and system files, locally over the LAN or on the internet. Picture file types supported by the file viewer are JPG, JPG2000, GIF, uncompressed TIF, TIFF, BMP, ICO, CUR, PCX, DCX, PCD, FPX, WMF, EMF, FAX, RAW, XPB, XPM, IFF, PBM, CUT, PSD, PNG, TGA, EPS, RAS, WPG, PCT, PCX, CLP, XWD, FLC, ANI, SGI, XBM, etc.

Imaging Tool: R-Drive Image

Source: http://www.drive-image.com

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

Features:

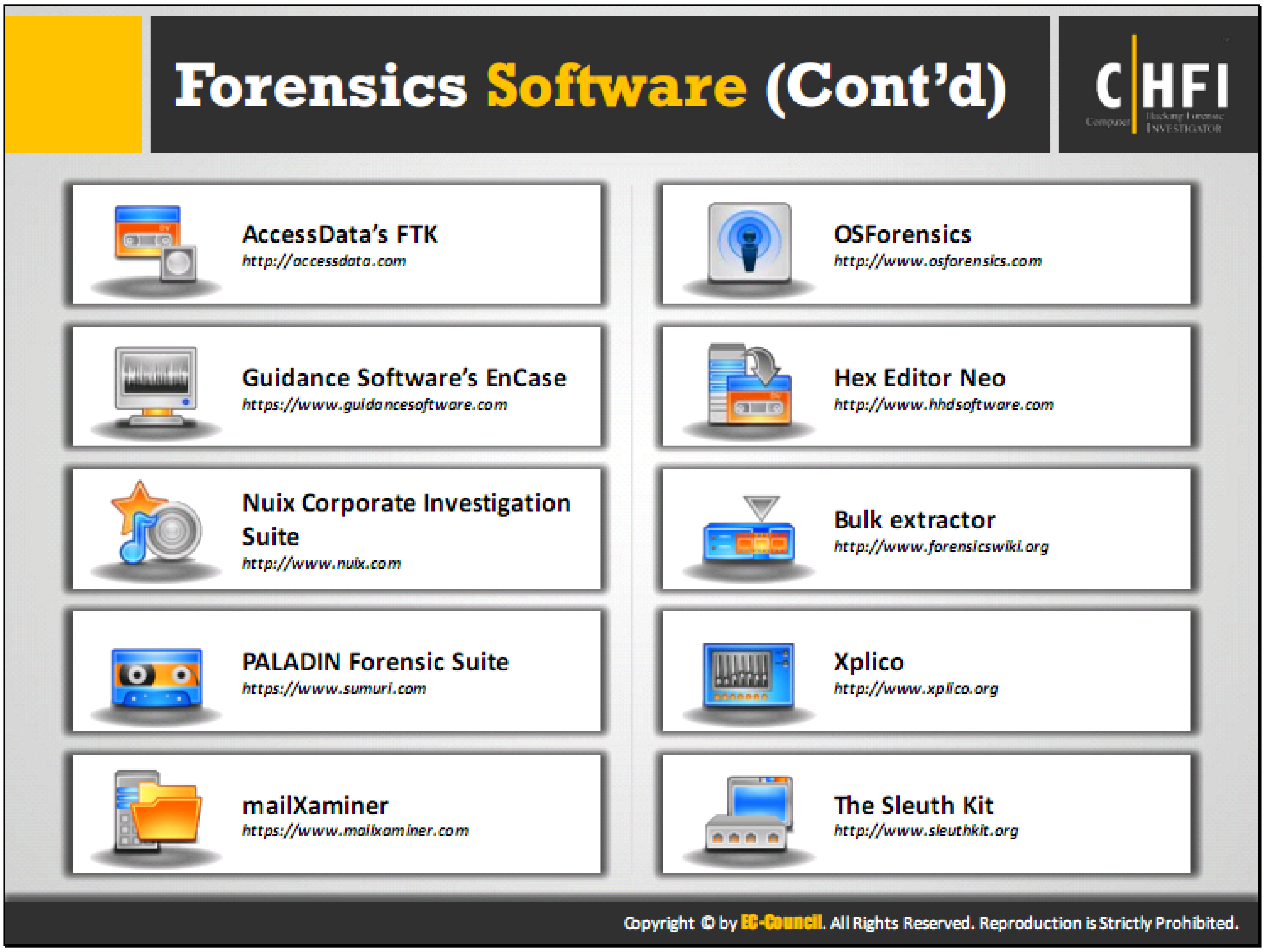
- A simple wizard interface

- Image file compression
- Removable media support
- Image files splitting
- Image Protection

File Type Conversion Software: File Viewer

Source: *http://www.file-convert.com*

FileMerlin converts word processing, spreadsheet, presentation and database files between a wide range of file formats. Widely regarded as the premier document conversion product, it is suitable for straightforward as well as complex documents, and is the most accurate, complete and flexible such solution that we know of.



Forensics Software (Cont'd)

CHFI
Computer Hacking Forensic INVESTIGATOR

AccessData's FTK *http://accessdata.com*	**OSForensics** *http://www.osforensics.com*
Guidance Software's EnCase *https://www.guidancesoftware.com*	**Hex Editor Neo** *http://www.hhdsoftware.com*
Nuix Corporate Investigation Suite *http://www.nuix.com*	**Bulk extractor** *http://www.forensicswiki.org*
PALADIN Forensic Suite *https://www.sumuri.com*	**Xplico** *http://www.xplico.org*
mailXaminer *https://www.mailxaminer.com*	**The Sleuth Kit** *http://www.sleuthkit.org*

AccessData's FTK

Source: *http://accessdata.com*

FTK is a court-cited digital investigations platform. It provides processing and indexing up front, so filtering and searching is fast. FTK can be setup for distributed processing and incorporate web-based case management and collaborative analysis.

Guidance Software's EnCase

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

- Rapidly acquire data from the widest variety of devices
- Unearth potential evidence with disk-level forensic analysis
- Produce comprehensive reports on your findings
- Maintain the integrity of your evidence in a format the courts have come to trust

Nuix Corporate Investigation Suite

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

The Nuix Corporate Investigation Suite is used to collect, process, analyze, review, and report on electronic evidence.

PALADIN Forensic Suite

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

PALADIN is a modified "live" Linux distribution based on Ubuntu used to fulfill various forensics tasks in a forensically sound manner via the PALADIN Toolbox. PALADIN is available in 64-bit and 32-bit versions.

mailXaminer

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

It is used to search and uncover relevant information by conducting, coordinating, and real-time monitoring of a case with an investigative team to get thorough and unambiguous evidence in a court admissible file format.

OSForensics

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

Extract forensic data from computers, and uncover the data hidden inside a PC.

Hex Editor Neo

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

Freeware Hex Editor Neo allows viewing, modifying, analyzing hexadecimal data and binary files, editing, exchanging data with other applications through the clipboard, inserting new data and deleting existing data, as well as performing other editing actions.

Bulk extractor

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

The bulk extractor is a computer forensics tool that scans a disk image, a file or a directory of files and extracts useful information without parsing the file system or file system structures.

Xplico

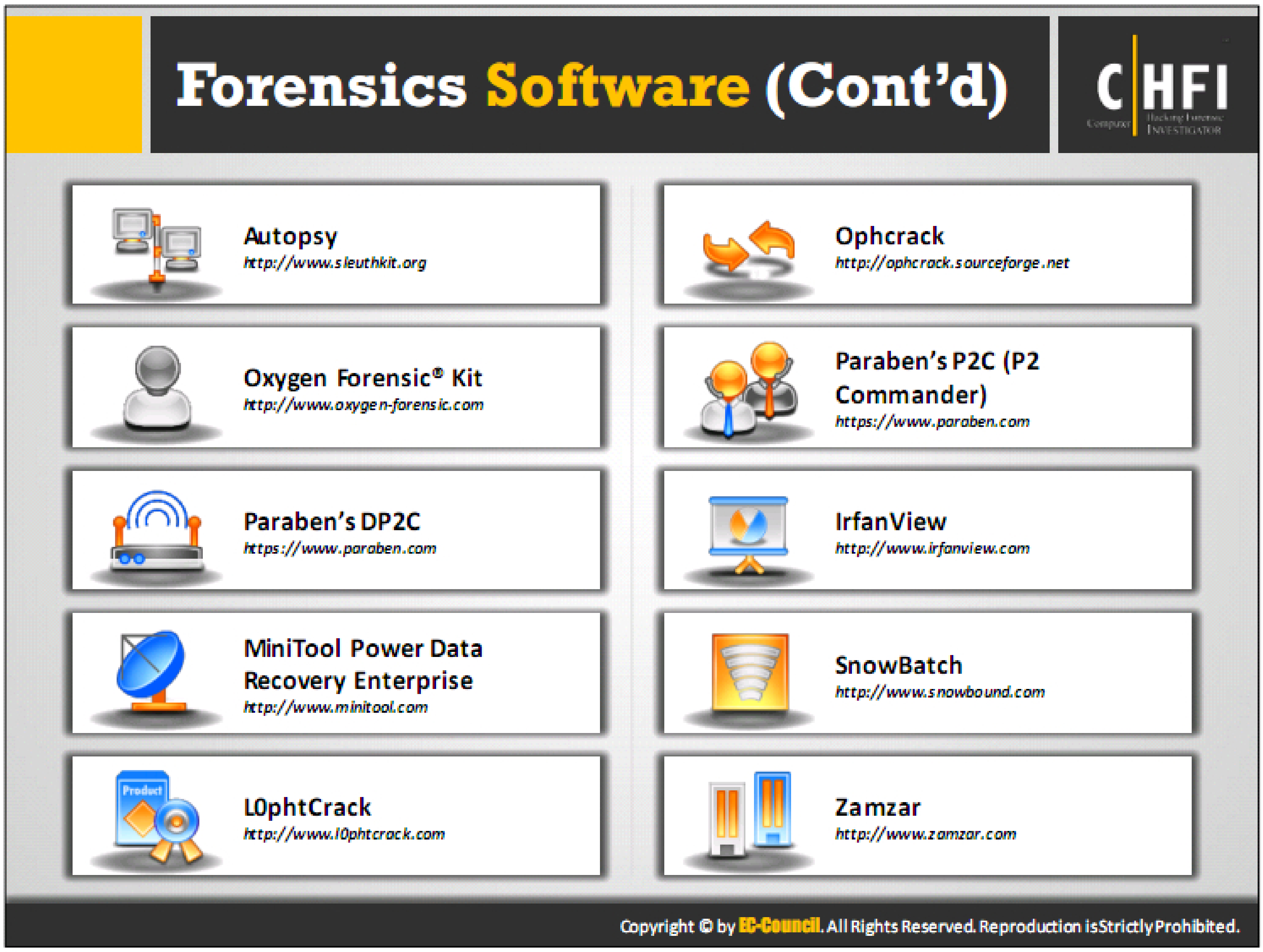
Source: *http://www.xplico.org*

The goal of Xplico is to extract the applications data contained from an internet traffic capture. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico is an open source Network Forensic Analysis Tool (NFAT).

The Sleuth Kit

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

The Sleuth Kit® is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them.



Forensics Software (Cont'd)

CHFI

Autopsy
http://www.sleuthkit.org

Ophcrack
http://ophcrack.sourceforge.net

Oxygen Forensic® Kit
http://www.oxygen-forensic.com

Paraben's P2C (P2 Commander)
https://www.paraben.com

Paraben's DP2C
https://www.paraben.com

IrfanView
http://www.irfanview.com

MiniTool Power Data Recovery Enterprise
http://www.minitool.com

SnowBatch
http://www.snowbound.com

L0phtCrack
http://www.l0phtcrack.com

Zamzar
http://www.zamzar.com

Autopsy

Source: http://www.sleuthkit.org

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate the happenings on a computer. It can even be used to recover photos from a camera's memory card.

Oxygen Forensic® Kit

Source: http://www.oxygen-forensic.com

The Oxygen Forensic® Kit is a ready-to-use and customizable mobile forensic solution for field and in-lab usage. It allows not only extraction of data from the device but also creates reports and analyzes data in the field.

Paraben's DP2C

Source: https://www.paraben.com

DP2C is a data targeted collection tool for triage forensics. DP2C is special software that runs from a USB drive and allows the collection of specific type of data from Windows-based systems to the evidence drive.

MiniTool Power Data Recovery Enterprise

Source: http://www.minitool.com

MiniTool Power Data Recovery Enterprise Edition can recover data including images, texts, videos, music, and emails. It supports different data loss situations like important data lost because of deletion by mistake, formatting, logical damage, etc.

L0phtCrack

Source: http://www.l0phtcrack.com

L0phtCrack is a password auditing and recovery software. It is packed with features such as scheduling, hash extraction from 64 bit Windows versions, multiprocessor algorithms, and network monitoring and decoding.

Ophcrack

Source: http://ophcrack.sourceforge.net

Ophcrack is a free Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms.

Paraben's P2C (P2 Commander)

Source: https://www.paraben.com

P2C is a digital investigation tool used by forensic examiners. It has an integrated database with multi-threading. P2C was built on Paraben's trusted email examination tools for unparalleled network email and personal email archive analysis.

IrfanView

Source: http://www.irfanview.com

IrfanView is a small FREEWARE (for non-commercial use) graphic viewer for Windows 9x, ME, NT, 2000, XP, 2003 , 2008, Vista, Windows 7, Windows 8, Windows 10.

SnowBatch

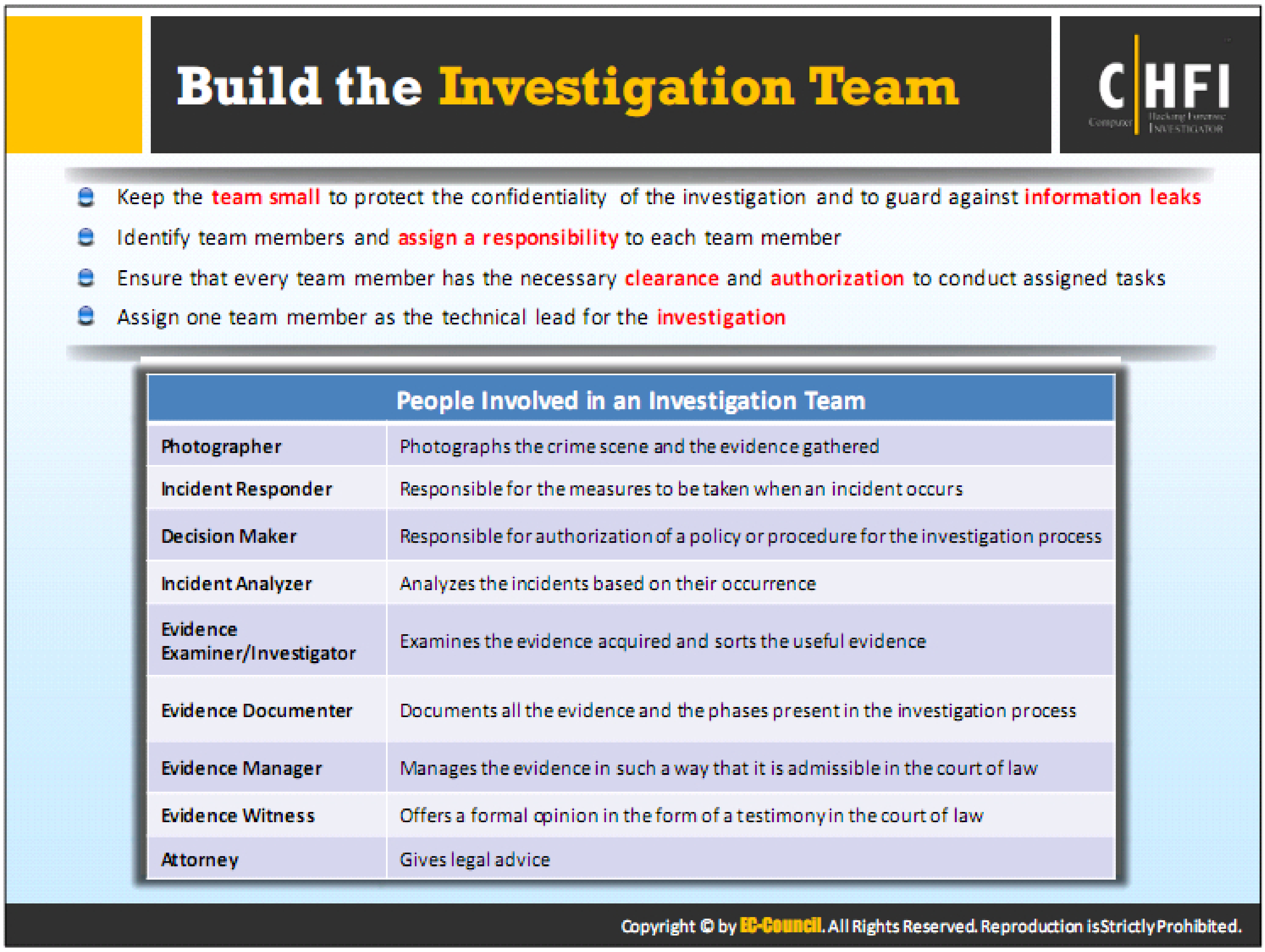
Source: http://www.snowbound.com

SnowBatch® is a Windows-based image conversion and file conversion application that converts large batches of image or document files from one format to another.

Zamzar

Source: http://www.zamzar.com

Zamzar supports over 1200 different conversions such as Video Converter, Audio Converter, Music Converter, eBook Converter, Image Converter, and CAD Converter.



Build the Investigation Team

- Keep the **team small** to protect the confidentiality of the investigation and to guard against **information leaks**
- Identify team members and **assign a responsibility** to each team member
- Ensure that every team member has the necessary **clearance** and **authorization** to conduct assigned tasks
- Assign one team member as the technical lead for the **investigation**

People Involved in an Investigation Team	
Photographer	Photographs the crime scene and the evidence gathered
Incident Responder	Responsible for the measures to be taken when an incident occurs
Decision Maker	Responsible for authorization of a policy or procedure for the investigation process
Incident Analyzer	Analyzes the incidents based on their occurrence
Evidence Examiner/Investigator	Examines the evidence acquired and sorts the useful evidence
Evidence Documenter	Documents all the evidence and the phases present in the investigation process
Evidence Manager	Manages the evidence in such a way that it is admissible in the court of law
Evidence Witness	Offers a formal opinion in the form of a testimony in the court of law
Attorney	Gives legal advice

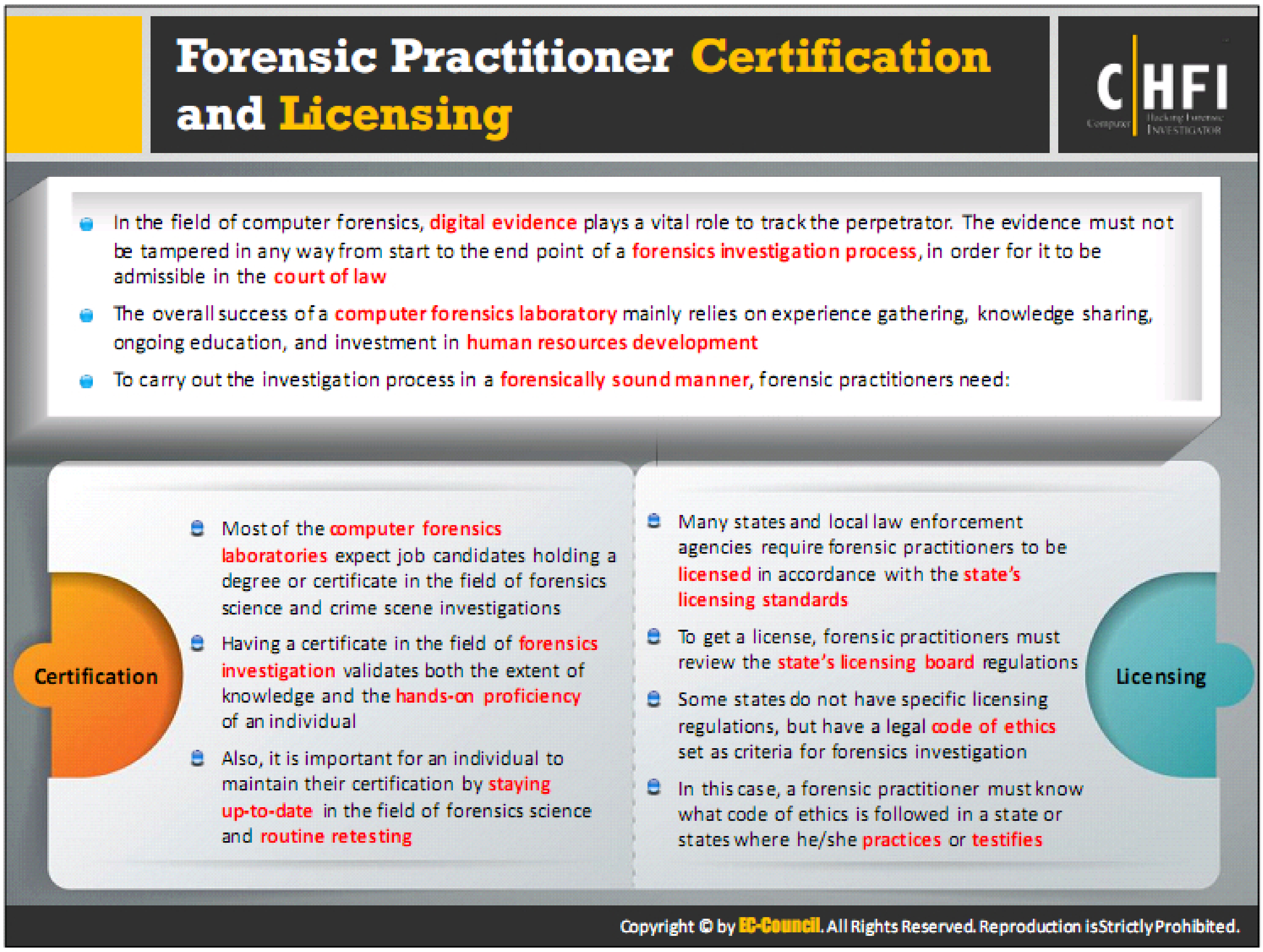
The investigation team plays a major role in solving a case. The team is responsible for evaluating the crime, evidence, and criminals. Every team member should be assigned a few specific tasks (roles and responsibilities) that let the team analyze the incident easily. The guidelines for building the investigation team are as follows:

- Determine the person who has to respond to an incident so that a proper internal computer investigation can be performed
- Organize the team members and give responsibility to each member of team
- Appoint a person as a technical lead for the investigation
- The investigation team has to be as small as possible to achieve confidentiality and avoid information leaks
- Provide each team member with the necessary clearance and authorization to complete assigned tasks
- Enlist help from a trusted external investigation team, if required

Computer forensics is the branch of forensic science that deals with criminal offences performed using technical devices such as computer or any digital media devices. The evidence for such cases is present on digital storage media such as CDs/DVDs, Blu-ray discs, USBs, mobile phones, BlackBerrys, iPods, etc.

To find the appropriate evidence on these digital devices, the following people may be involved:

- **Attorney:** Helps in giving legal advice about how to carry out the investigation, and the legal issues involved in the forensics investigation process.
- **Photographer:** Photographs the crime scene and the evidence gathered. He or she should have an authentic certification. This person is responsible for shooting all the evidence found at the crime scene, which records the key evidence in the forensics process.
- **Incident Responder:** Responsible for the measures taken when an incident occurs. The incident responder is responsible for securing the incident area and collecting the evidence that is present at the crime scene. He or she should disconnect the system from other systems to stop the spread of an incident from one system to another.
- **Decision Maker:** The person responsible for authorization of a policy or procedure during the investigative process. Based on the incident type, makes a decision about the policies and procedures necessary to handle the incident.
- **Incident Analyzer:** Analyzes the incidents based on their occurrence. He or she examines the incident with regard to its type, how it affects the systems, different threats and vulnerabilities associated with it, etc.
- **Evidence Examiner/Investigator**: Examines the evidence acquired and sorts the useful evidence. Examines and sorts the evidence according to its relevancy to the case. Maintains an evidence hierarchy with the most important evidence given a high priority and the evidence with less importance has a lower priority.
- **Evidence Documenter:** Documents all the evidence and the phases present in the investigation process. The evidence documenter gathers information from all the people involved in the forensics process and documents it in an orderly fashion, from incident occurrence to the end of the investigation. The documents should contain complete information about the forensics process.
- **Evidence Manager:** Manages the evidence. The evidence manager has all the information about the evidence, for example, evidence name, evidence type, time, source of evidence, etc. He or she manages and maintains a record of the evidence such that it is admissible in the court of law.
- **Expert Witness:** Offers a formal opinion as a testimony in a court of law. Expert witnesses help to authenticate the facts and witnesses during any complex case. Expert witnesses also assist in cross-examining witnesses and evidence, as various factors may influence a normal witness.



Forensic Practitioner Certification and Licensing

- In the field of computer forensics, digital evidence plays a vital role to track the perpetrator. The evidence must not be tampered in any way from start to the end point of a forensics investigation process, in order for it to be admissible in the court of law
- The overall success of a computer forensics laboratory mainly relies on experience gathering, knowledge sharing, ongoing education, and investment in human resources development
- To carry out the investigation process in a forensically sound manner, forensic practitioners need:

Certification

- Most of the computer forensics laboratories expect job candidates holding a degree or certificate in the field of forensics science and crime scene investigations
- Having a certificate in the field of forensics investigation validates both the extent of knowledge and the hands-on proficiency of an individual
- Also, it is important for an individual to maintain their certification by staying up-to-date in the field of forensics science and routine retesting

Licensing

- Many states and local law enforcement agencies require forensic practitioners to be licensed in accordance with the state's licensing standards
- To get a license, forensic practitioners must review the state's licensing board regulations
- Some states do not have specific licensing regulations, but have a legal code of ethics set as criteria for forensics investigation
- In this case, a forensic practitioner must know what code of ethics is followed in a state or states where he/she practices or testifies

In the field of computer forensics, digital evidence plays a vital role in tracking the perpetrator. Evidence tampered in any way from start to end of the forensic investigation process is not admissible in a court of law. The overall success of a computer forensic laboratory mainly relies on experience gathering, knowledge sharing, ongoing education, and investment in human resources development.

To conduct computer forensic investigations that are legally sound, it is necessary to employ skillful, experienced, licensed, and certified investigators. The experience and skills will help the investigator to solve the case easily, accurately, and in lesser time.

To perform the investigation in a forensically sound manner, forensic practitioners must go through:

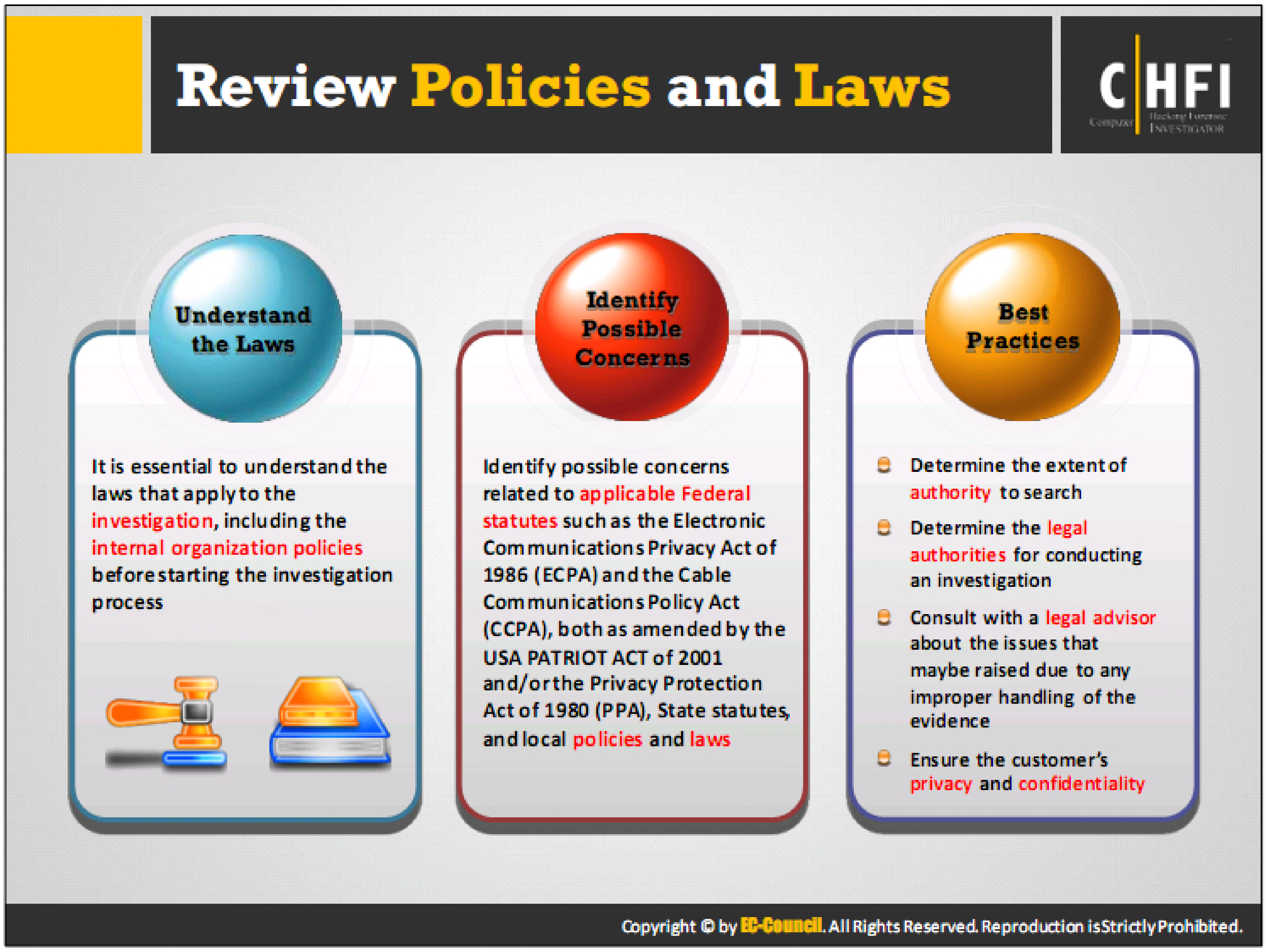
Certification:

Most of the computer forensic laboratories expect job candidates possessing a higher degree and a certification in the field of forensic science and crime scene investigations, as these will make the investigation trustworthy and accurate. Having a certificate in the field of forensic investigation validates both the extent of knowledge and the hands-on proficiency of an individual. The investigators have to annually improve their skills and undergo training to be up-to-date with the new technologies in the field of forensic science and routine retesting.

Licensing:

Many states and local law enforcement require forensic practitioners or computer forensics investigators to have licenses in accordance with the state's licensing standards. To obtain a license, the forensic practitioner must abide by the state's licensing board regulations and pass the regulatory examination or tests. Hiring a licensed investigator will increase the reputation and trustworthiness of a company as well as improve the firm's reliability to provide testimony in court.

Some states do not have specific licensing regulations, but have a set of legal code of ethics as criteria for forensic investigation. In this case, forensic practitioners must know what code of ethics the states follow where they practice or testify.



Review Policies and Laws

Understand the Laws

It is essential to understand the laws that apply to the investigation, including the internal organization policies before starting the investigation process

Identify Possible Concerns

Identify possible concerns related to applicable Federal statutes such as the Electronic Communications Privacy Act of 1986 (ECPA) and the Cable Communications Policy Act (CCPA), both as amended by the USA PATRIOT ACT of 2001 and/or the Privacy Protection Act of 1980 (PPA), State statutes, and local policies and laws

Best Practices

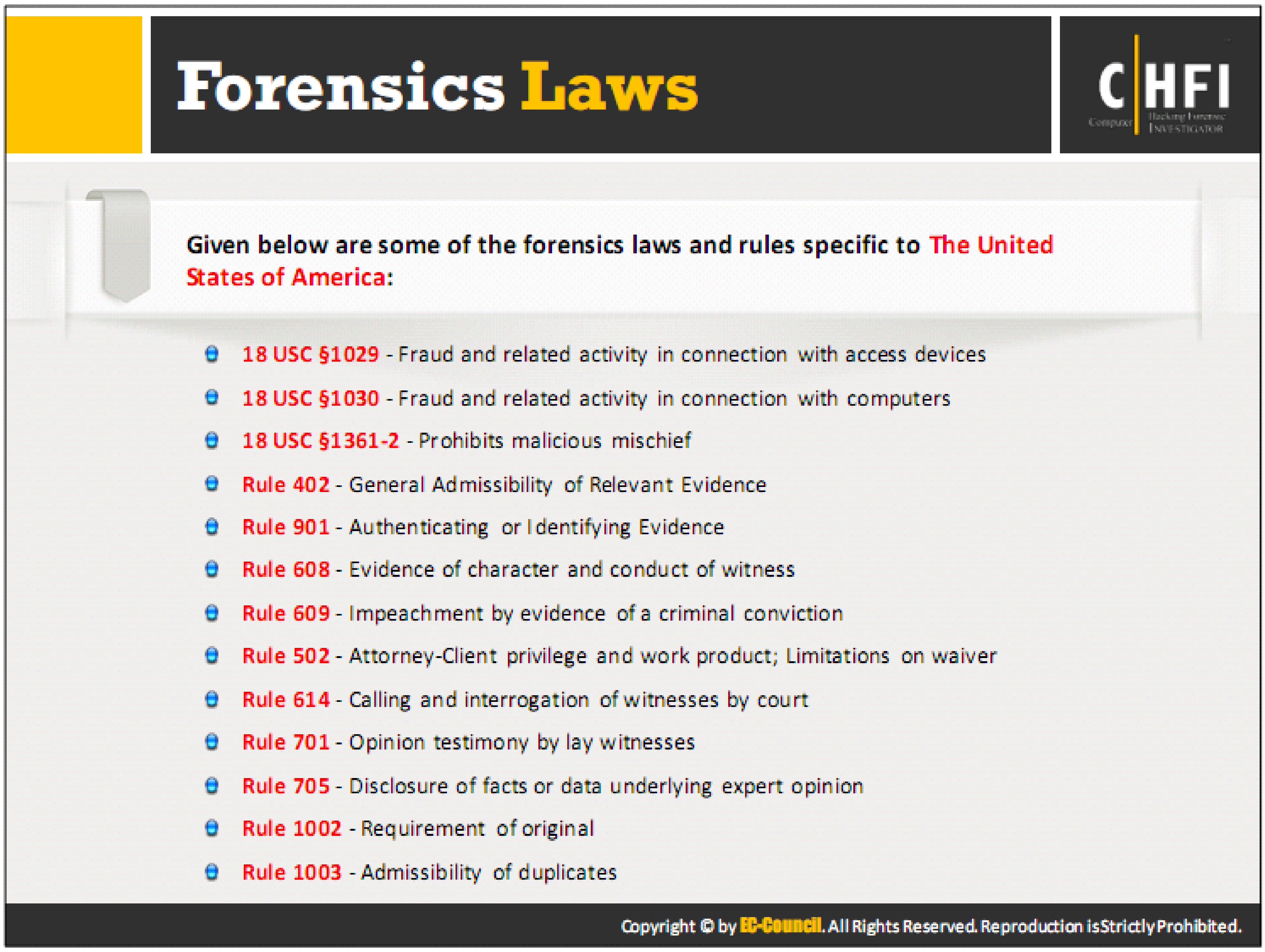
- Determine the extent of authority to search
- Determine the legal authorities for conducting an investigation
- Consult with a legal advisor about the issues that maybe raised due to any improper handling of the evidence
- Ensure the customer's privacy and confidentiality

It is essential to be aware of the laws that will be applicable to the investigation, including the organization's internal policies, before starting the investigation process.

Identify possible concerns related to applicable federal statutes, state statutes, and local policies and laws. Applicable federal statutes include the Electronic Communications Privacy Act of 1986 (ECPA) and the Cable Communications Policy Act (CCPA), both as amended by the USA PATRIOT ACT of 2001, and/or the Privacy Protection Act of 1980 (PPA).

The best practices in reviewing policies and laws include:

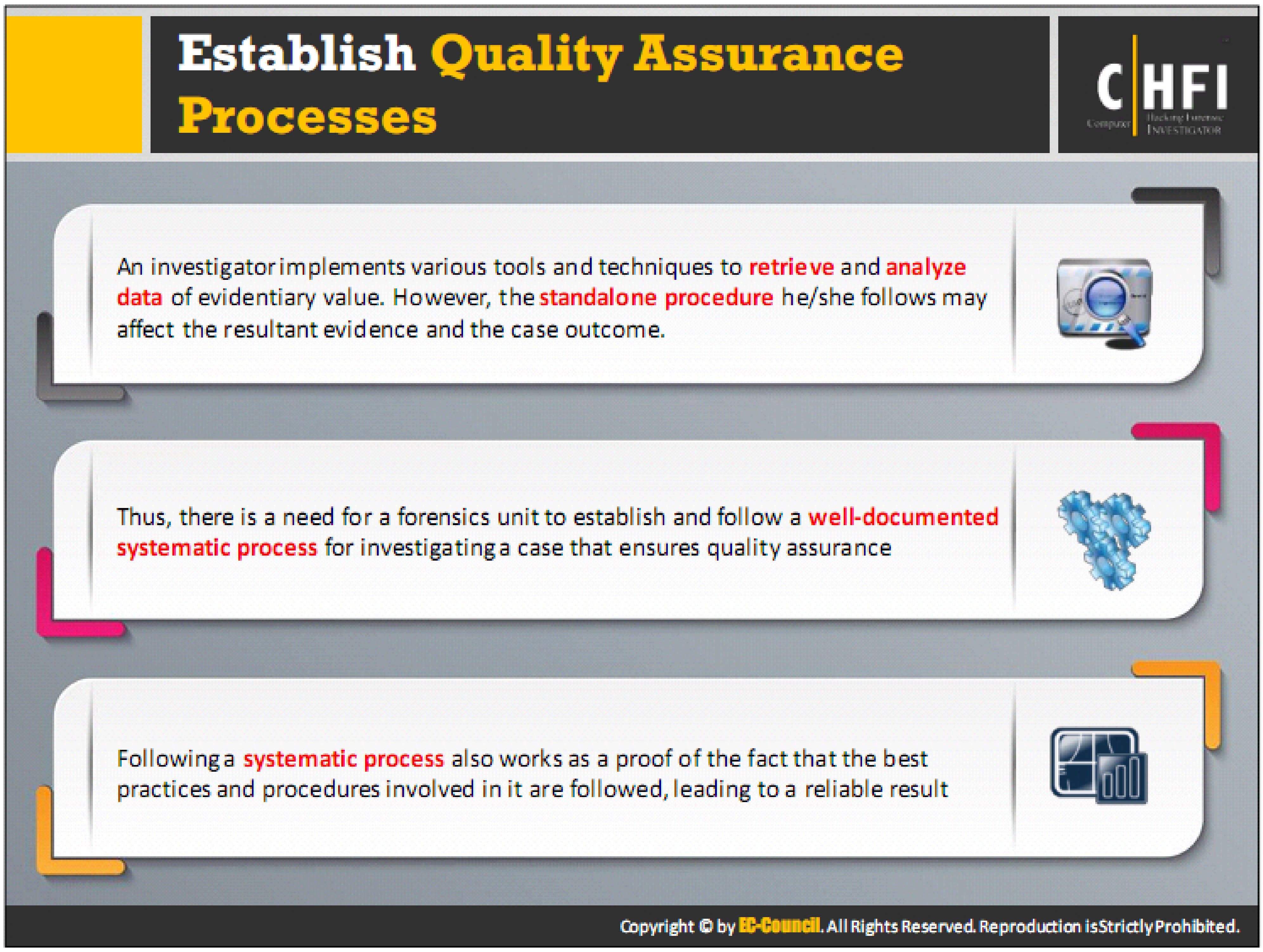
- **Determine the extent of the authority to search:** As the incident can relate to any confidential information, it is necessary to determine the limits/extent of the authority to search for evidence by an investigation team.
- **Determine the legal authorities that perform an investigation:** Establishing policies and procedures that address the privacy rights of the employees, contractors, or any other personnel for determining the legal authorities is necessary.
- **Consult with a legal advisor for the issues arising because of any improper handling of the investigation:** Not all the actions performed during the investigation may be appropriate. Sometimes the handling of evidence is improper. In this situation, it is essential to consult a legal advisor.
- **Ensure the customer's privacy and confidentiality:** Organizations need to check or develop policies that ensure the customer's privacy and confidentiality.



Forensics Laws

Given below are some of the forensics laws and rules specific to The United States of America:

- **18 USC §1029** - Fraud and related activity in connection with access devices
- **18 USC §1030** - Fraud and related activity in connection with computers
- **18 USC §1361-2** - Prohibits malicious mischief
- **Rule 402** - General Admissibility of Relevant Evidence
- **Rule 901** - Authenticating or Identifying Evidence
- **Rule 608** - Evidence of character and conduct of witness
- **Rule 609** - Impeachment by evidence of a criminal conviction
- **Rule 502** - Attorney-Client privilege and work product; Limitations on waiver
- **Rule 614** - Calling and interrogation of witnesses by court
- **Rule 701** - Opinion testimony by lay witnesses
- **Rule 705** - Disclosure of facts or data underlying expert opinion
- **Rule 1002** - Requirement of original
- **Rule 1003** - Admissibility of duplicates



Establish Quality Assurance Processes

CHFI
Computer Hacking Forensic INVESTIGATOR

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

Following a systematic process also works as a proof of the fact that the best practices and procedures involved in it are followed, leading to a reliable result

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

Computer forensics investigation can be effective only when the investigators follow certain standard quality assurance procedures. Frame a standard policy for forensics investigation and strictly implement it before starting the case analysis. With the quality assurance policies in place, the investigators can obtain accurate analysis results and help in solving the case. Therefore, the computer forensics departments must formulate a systematic quality management system to ensure accurate analysis results.

Following a systematic process also acts as a proof that the investigation firm follows best practices and procedures leading to a reliable result. Addressing the following topics and reporting it in a Quality Assurance Manual can demonstrate that Quality Assurance Practices are in place.

Quality Assurance Practices in Digital Forensics

Quality assurance practices play a vital role in ensuring the overall quality of services that a forensics unit offers

Some of the quality assurance practices:

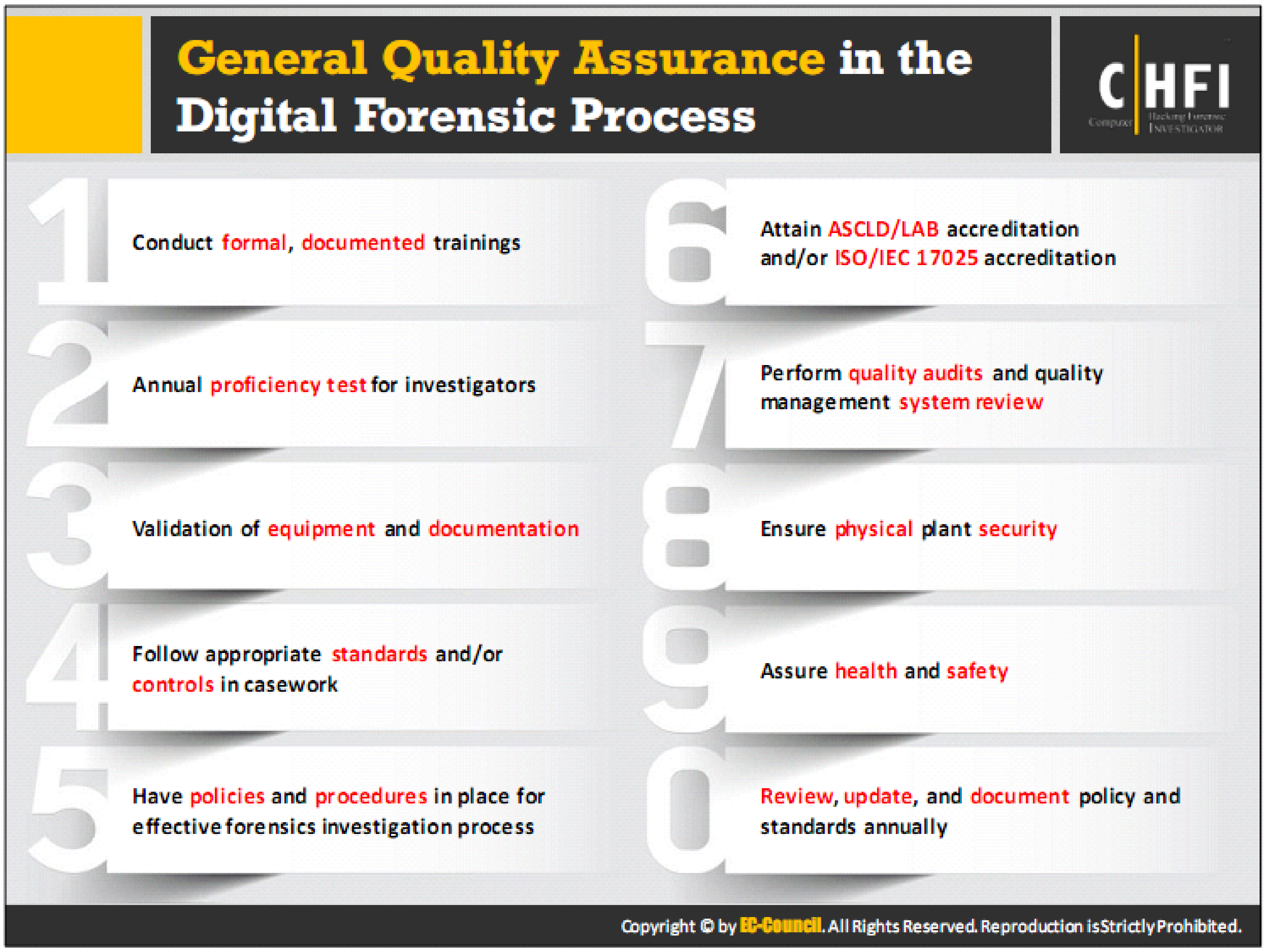
- Tools meant for the forensics examination process must undergo validity testing to check its purpose of design and accuracy of results. Also, the test conducted must be documented in detail to enable reproduction of the results
- The forensics unit must review and update its quality management system at least once in 3 years to ensure that the system meets the quality needs of the unit
- The forensics laboratory unit must have a well-documented Quality Assurance Manual (QAM) and a Quality Manager (QM), who is responsible for all the quality assurance-related issues and developments
- Investigative reports must undergo administrative review for consistency with forensics unit policies and accuracy
- The final computer forensics reports must be technically reviewed by another forensic examiner prior to publishing, to ensure:
  - The report is concise, clear, and understandable
  - The tools and techniques used in the process were sufficiently documented and forensically sound
  - The technical report, accompanying the executive summary report, should contain in-depth details of the complete investigation process so that another investigation of the evidence leads to the same result

Quality assurance practices play a vital role in ensuring the overall quality of services that a forensic unit offers.

Some of the quality assurance practices:

- Tools meant for the forensic examination process must undergo validity testing to check its purpose of design and accuracy of results. In addition, the test conducted must be documented in detail to enable reproduction of the results.
- The forensic unit must review and update its quality management system at least once in 3 years to ensure that the system meets the quality needs of the unit.
- The forensic laboratory unit must have a documented Quality Assurance Manual (QAM) and a Quality Manager (QM), who is responsible for all the quality assurance related issues and developments.
- Investigative reports must undergo administrative review for consistency with forensic unit policies and for report accuracy.
- The final computer forensic reports must be technically reviewed by another forensic examiner prior to publishing, to ensure that:
  - The report is concise, clear, and understandable.
  - The tools and techniques used in the process were sufficiently documented and forensically sound.

- The technical report, accompanying the executive summary report, should contain in-depth details of the complete investigation process so that another investigation of the evidence leads to the same result.



General Quality Assurance in the Digital Forensic Process

1 Conduct formal, documented trainings

2 Annual proficiency test for investigators

3 Validation of equipment and documentation

4 Follow appropriate standards and/or controls in casework

5 Have policies and procedures in place for effective forensics investigation process

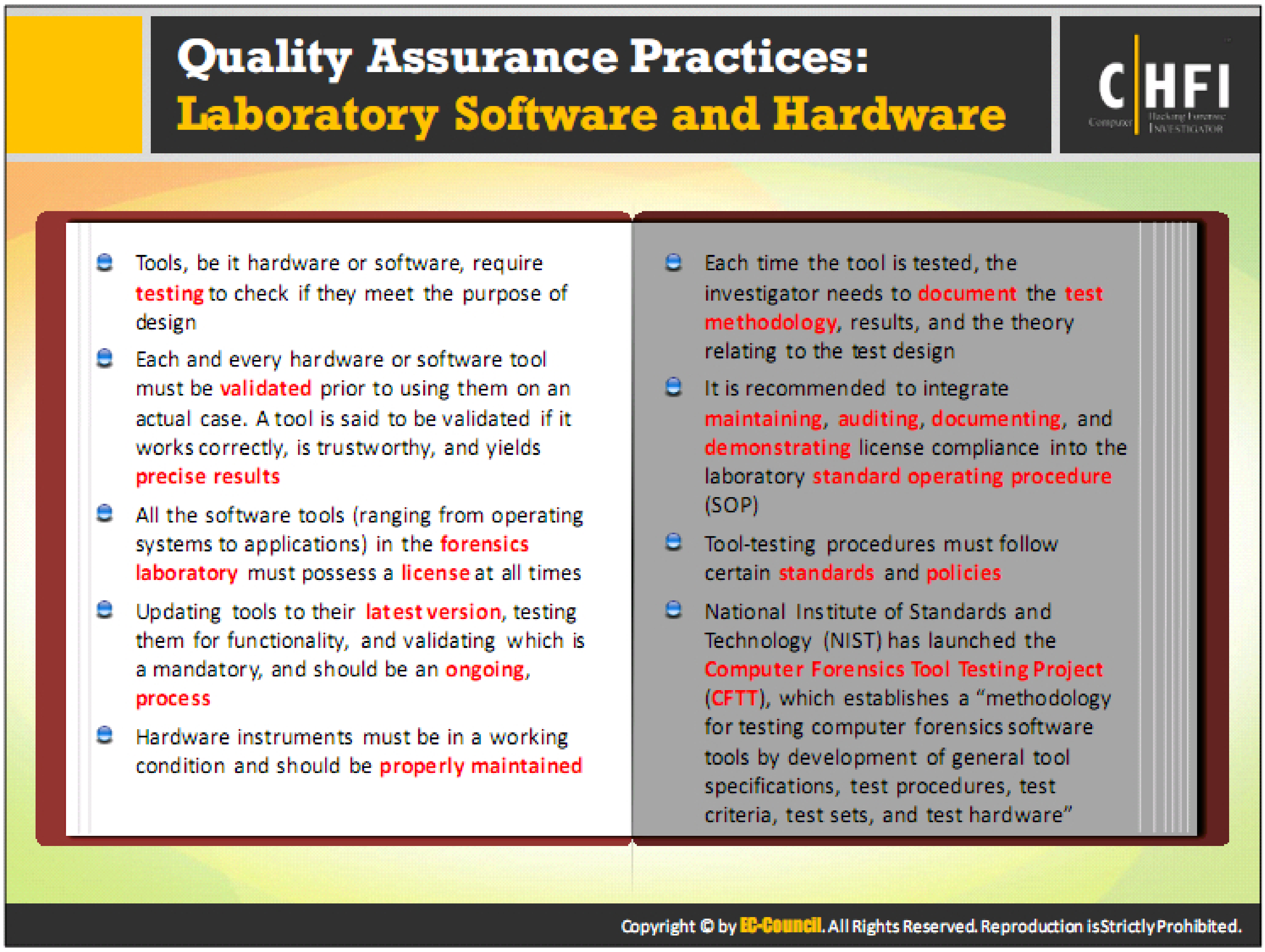
6 Attain ASCLD/LAB accreditation and/or ISO/IEC 17025 accreditation

7 Perform quality audits and quality management system review

8 Ensure physical plant security

9 Assure health and safety

0 Review, update, and document policy and standards annually



Quality Assurance Practices: Laboratory Software and Hardware

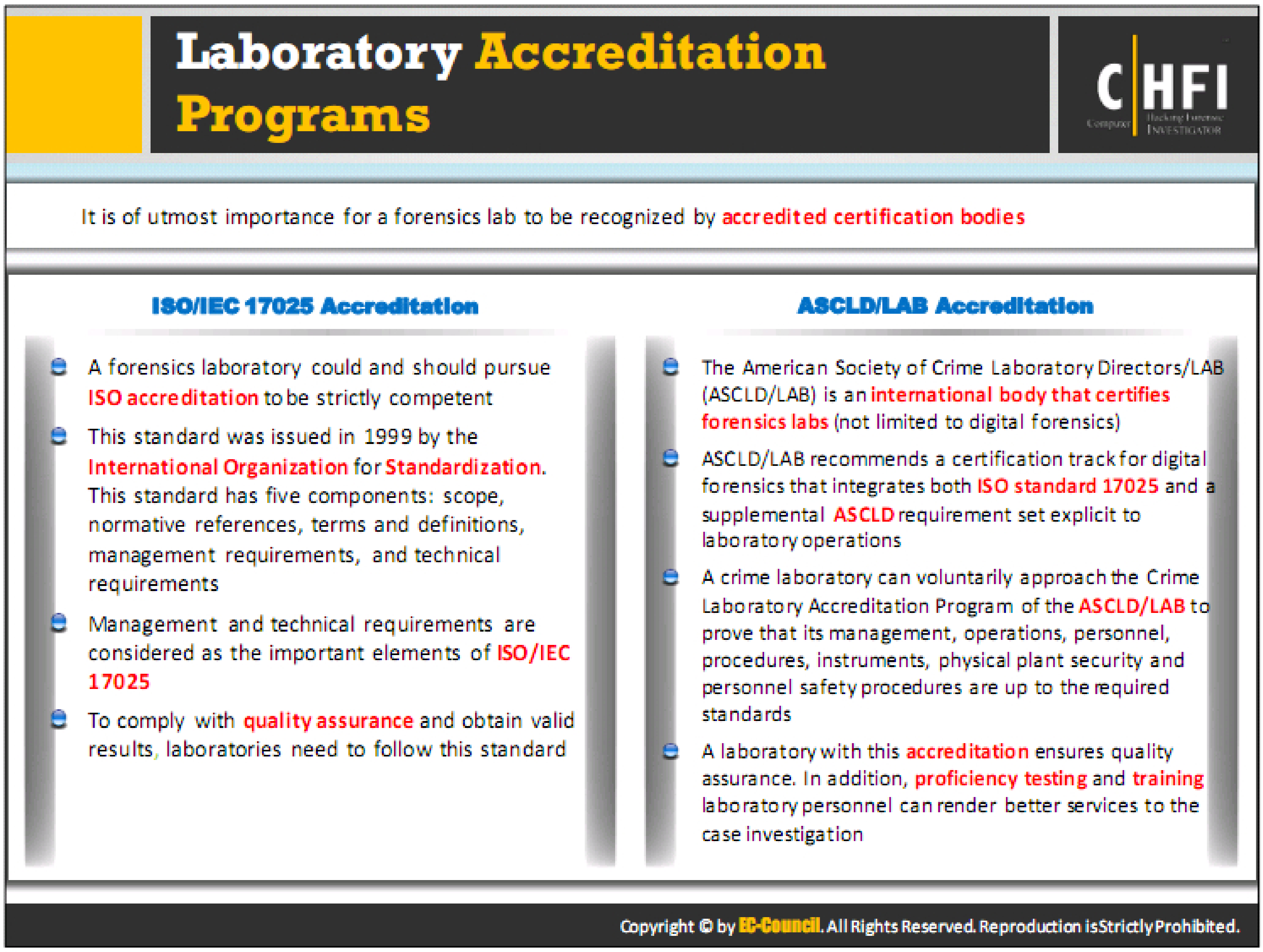
- Tools, be it hardware or software, require testing to check if they meet the purpose of design
- Each and every hardware or software tool must be validated prior to using them on an actual case. A tool is said to be validated if it works correctly, is trustworthy, and yields precise results
- All the software tools (ranging from operating systems to applications) in the forensics laboratory must possess a license at all times
- Updating tools to their latest version, testing them for functionality, and validating which is a mandatory, and should be an ongoing, process
- Hardware instruments must be in a working condition and should be properly maintained
- Each time the tool is tested, the investigator needs to document the test methodology, results, and the theory relating to the test design
- It is recommended to integrate maintaining, auditing, documenting, and demonstrating license compliance into the laboratory standard operating procedure (SOP)
- Tool-testing procedures must follow certain standards and policies
- National Institute of Standards and Technology (NIST) has launched the Computer Forensics Tool Testing Project (CFTT), which establishes a “methodology for testing computer forensics software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware”

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

Quality assurance also includes the practice of checking, repairing and maintaining the resources required to perform the assigned task. In case of forensics investigation, these resources include the software and hardware tools used during the investigation process. The practice that ensures the best outcome from such resources includes:

- Tools, be it a hardware or software require testing to check if they meet the purpose of design
- Validate every hardware or software tool prior to using them on an actual case to ensure if it works correctly, is trustworthy, and yields precise results
- All the software tools (ranging from the operating systems to applications) in the forensic laboratory must have licensed versions and be legal to use
- Updating tools to their latest version, testing them for functionality, and validating is mandatory and should be an ongoing process
- Hardware instruments must be in a working condition and maintained properly
- Investigators need to document the test methodology, results, and theory about the test design while testing the tools
- Integrate maintaining, auditing, documenting, and demonstrating license compliance into the laboratory standard operating procedure (SOP)
- Tool testing procedures must follow certain standards and policies

- NIST has launched the Computer Forensic Tool Testing Project (CFTT), which establishes a "methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware."



Laboratory Accreditation Programs

It is of utmost importance for a forensics lab to be recognized by accredited certification bodies

ISO/IEC 17025 Accreditation

- A forensics laboratory could and should pursue ISO accreditation to be strictly competent
- This standard was issued in 1999 by the International Organization for Standardization. This standard has five components: scope, normative references, terms and definitions, management requirements, and technical requirements
- Management and technical requirements are considered as the important elements of ISO/IEC 17025
- To comply with quality assurance and obtain valid results, laboratories need to follow this standard

ASCLD/LAB Accreditation

- The American Society of Crime Laboratory Directors/LAB (ASCLD/LAB) is an international body that certifies forensics labs (not limited to digital forensics)
- ASCLD/LAB recommends a certification track for digital forensics that integrates both ISO standard 17025 and a supplemental ASCLD requirement set explicit to laboratory operations
- A crime laboratory can voluntarily approach the Crime Laboratory Accreditation Program of the ASCLD/LAB to prove that its management, operations, personnel, procedures, instruments, physical plant security and personnel safety procedures are up to the required standards
- A laboratory with this accreditation ensures quality assurance. In addition, proficiency testing and training laboratory personnel can render better services to the case investigation

ISO/IEC 17025 Accreditation:

ISO (the International Organization for Standardization) and IEC (the International Electro-technical Commission) are part of the specialized system for worldwide standardization. They develop International Standards in association with technical committees established by the respective organization for particular fields of technical activity.

In 1999, the ISO Committee on conformity assessment (CASCO) developed the ISO/IEC 17025, which specifies the general requirements for the competence to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods. This regulation is applicable to all laboratories with any extent of the scope of testing and/or calibration activities.

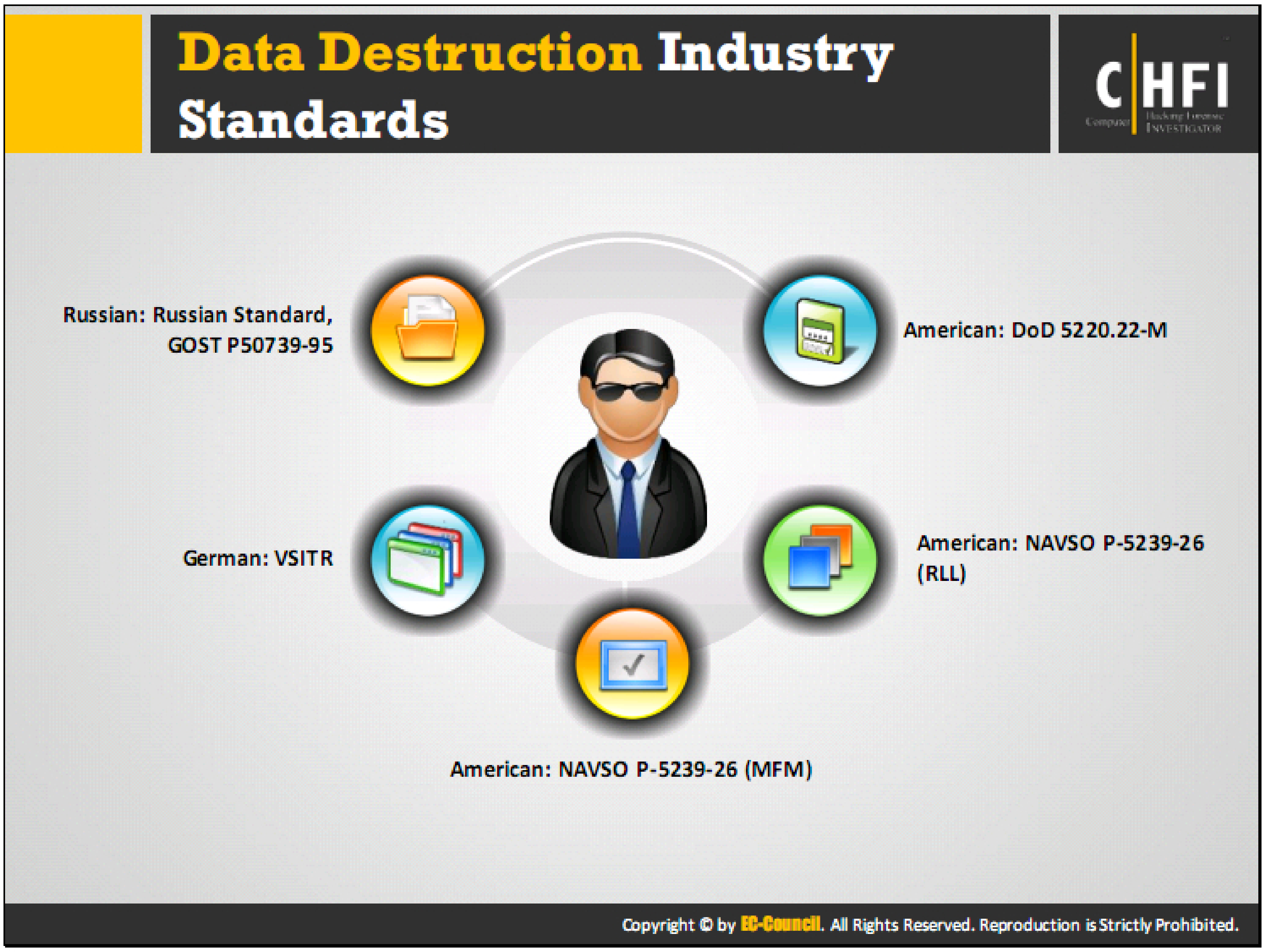
A forensic laboratory could and should pursue ISO accreditation to be strictly competent. This standard has five components: scope, normative references, terms and definitions, management requirements, and technical requirements. Management requirements and technical requirements are the important elements of ISO/IEC 17025. To comply with quality assurance and to obtain valid results, laboratories need to follow this standard.

ASCLD/LAB Accreditation:

The American Society of Crime Laboratory Directors/LAB (ASCLD/LAB) is an international body that certifies forensics labs (not limited to digital forensics). Its main objective is to promote development of laboratory management principles, professional interests, and techniques; to acquire, preserve, and circulate forensic information; to improve and maintain easy communication between crime laboratory directors; and to promote, maintain, and encourage industrial standard practices.

The ASCLD provides guidelines for managing a forensics lab and for acquiring official crime-lab certification. This institution certifies forensics labs that examine other criminal evidence such as fingerprints and DNA samples. This kind of forensics lab is entirely different from a computer forensics lab, which conducts different types of forensic examinations. ASCLD also offers a detailed and wide-ranging certification program known as ASCLD/LAB. This board, called the Laboratory Accreditation Board (LAB), offers objective principles for evaluation of the quality of the work.

ASCLD/LAB recommends a certification track for digital forensics that integrates both ISO standard 17025 and a supplemental ASCLD requirement that is set explicitly to the laboratory operations. A crime laboratory can voluntarily approach the Crime Laboratory Accreditation Program of the ASCLD/LAB to prove that its management, operations, personnel, procedures, instruments, physical plant security, and personnel safety procedures are up to the standards. A laboratory with this accreditation ensures quality assurance. In addition, proficiency testing and training laboratory personnel can provide better services to the case investigation.



Data Destruction Industry Standards

Russian: Russian Standard, GOST P50739-95

American: DoD 5220.22-M

German: VSITR

American: NAVSO P-5239-26 (RLL)

American: NAVSO P-5239-26 (MFM)

Destruction of data using industry standard data destruction methods is essential for sensitive data that one does not want falling into the wrong hands. These standards depend on the levels of sensitivity. Data deletion and disposal on electronic devices is only virtual, but physically it remains, posing a security threat.

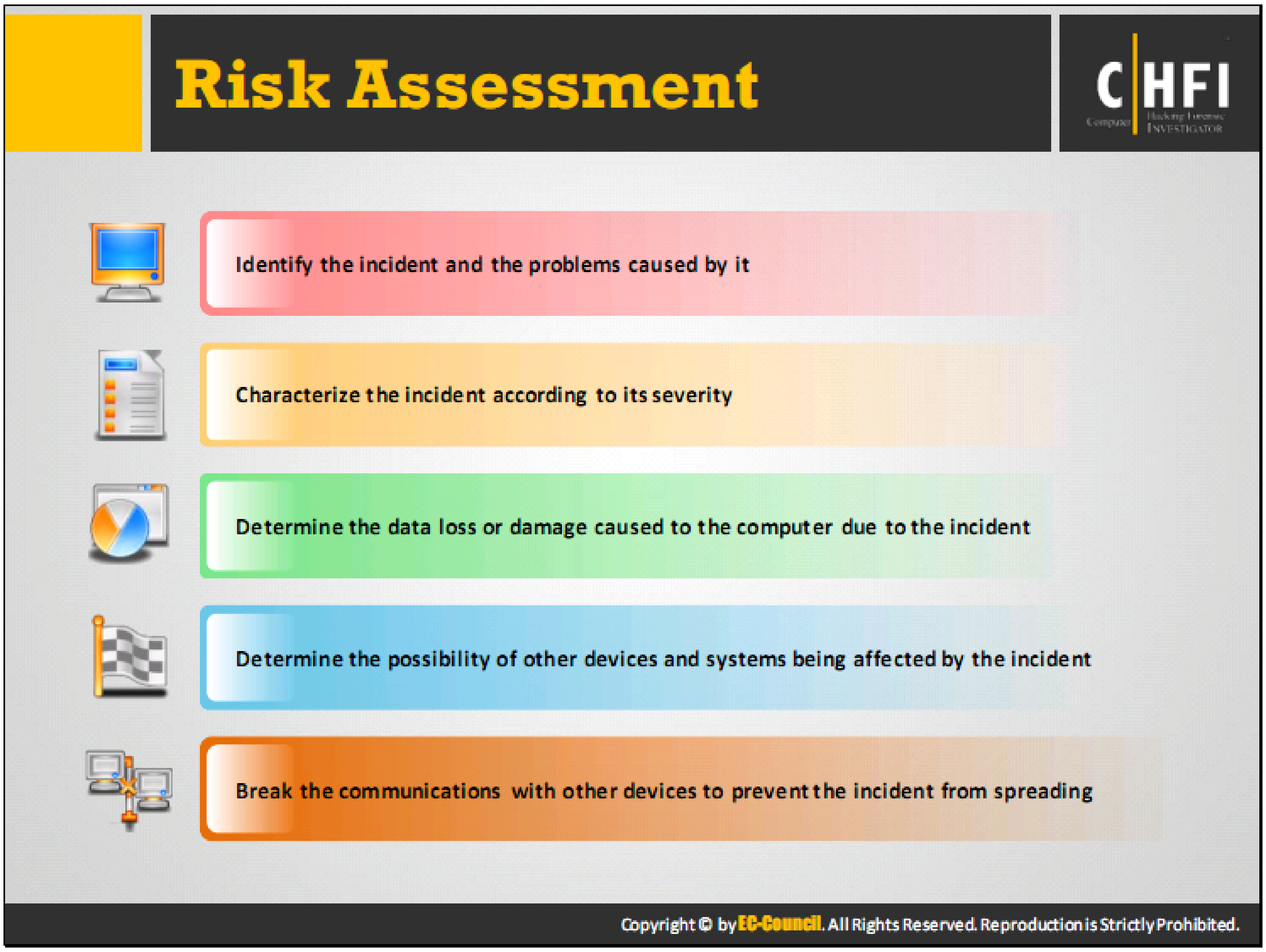
A hard disk stores the data in binary form and when the user tries to delete this data, it is possible to recover the data using recovery tools. Some high-end technology tools also have the provision to recover the overwritten data as well.

Methods like hard drive formatting or deleting partitions cannot delete the file data completely. However, it is important to destroy the data and protect it from retrieval, after the collection of evidence from the computer. Therefore, the only way to erase the data completely and protect it from recovery is to overwrite the data by applying a code of sequential zeroes or ones.

The following are some important standards for data destruction:

- **(American) DoD 5220.22-M:** This standard destroys the data on the drive's required area by overwriting that sector three times with ones and zeros, again verifying whether data is destroyed or not.
- **(American) NAVSO P-5239-26 (RLL):** This is a three-pass overwriting algorithm that verifies in the last pass.

- **(American) NAVSO P-5239-26 (MFM):** This is a three-pass overwriting algorithm that verifies in the last pass.
- **(German) VSITR:** This method overwrites in 6 passes with ones and zeros and then with the letter A.
- **Russian Standard, GOST P50739-95:** It is a wiping method that writes zeros in the first pass and then random bytes in the next pass.

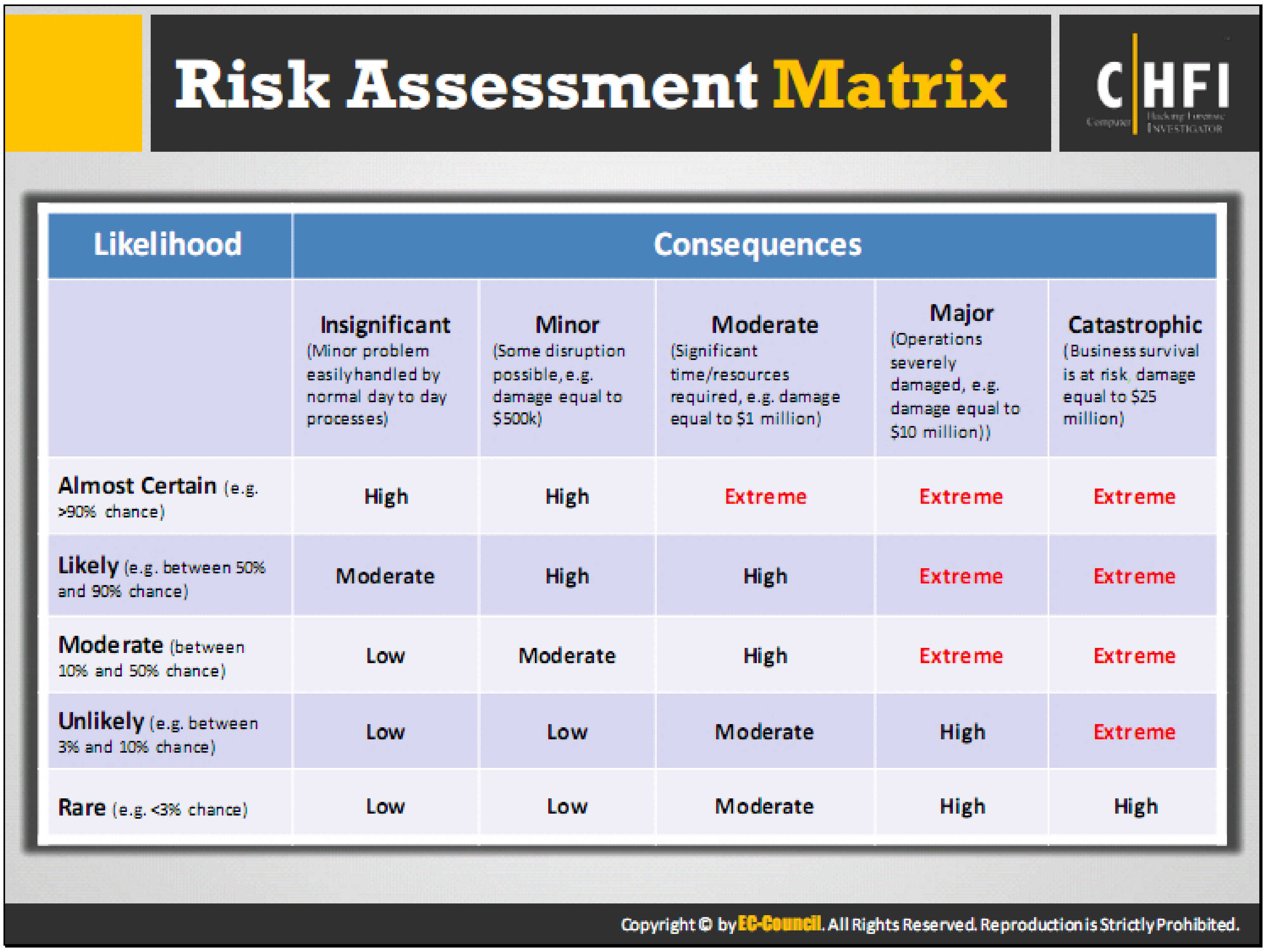


Risk Assessment

- Identify the incident and the problems caused by it
- Characterize the incident according to its severity
- Determine the data loss or damage caused to the computer due to the incident
- Determine the possibility of other devices and systems being affected by the incident
- Break the communications with other devices to prevent the incident from spreading

Risk assessment is useful to understand information security issues in a business context and to assess the impact to the business in case of a security breach.

Risk assessment helps senior management and decision makers in the 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.



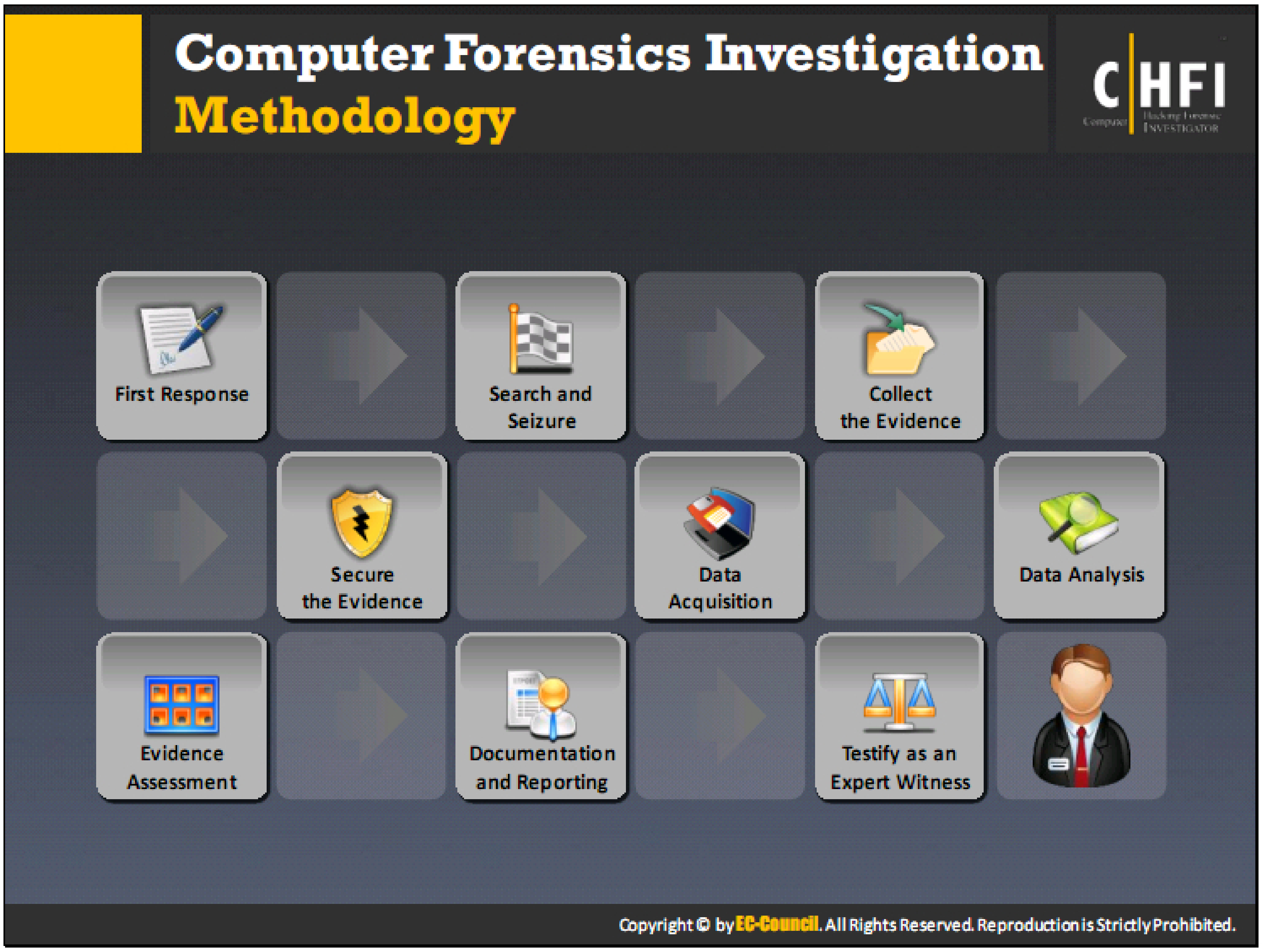
Risk Assessment Matrix

Likelihood	Consequences				
	Insignificant (Minor problem easilyhandled by normal day to day processes)	**Minor** (Some disruption possible, e.g. damage equal to $500k)	**Moderate** (Significant time/resources required, e.g. damage equal to $1 million)	**Major** (Operations severely damaged, e.g. damage equal to $10 million))	**Catastrophic** (Business survival is at risk, damage equal to $25 million)
Almost Certain (e.g. >90% chance)	High	High	Extreme	Extreme	Extreme
Likely (e.g. between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (e.g. between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (e.g. <3% chance)	Low	Low	Moderate	High	High

A risk assessment matrix is a graphical representation of the risks of a particular incident and its impact. It helps to know about the likelihood of occurrence of the incident and severity of its consequences. This matrix is easy to view and understand, as all the information is available in a single table.

Investigation Phase

After obtaining the required permissions and having assessed the case pre-requisites, the investigators are ready to investigate the incident. The investigation phase includes various stages and processes that need careful and systematic execution to obtain better results.



Computer Forensics Investigation Methodology

First Response

Search and Seizure

Collect the Evidence

Secure the Evidence

Data Acquisition

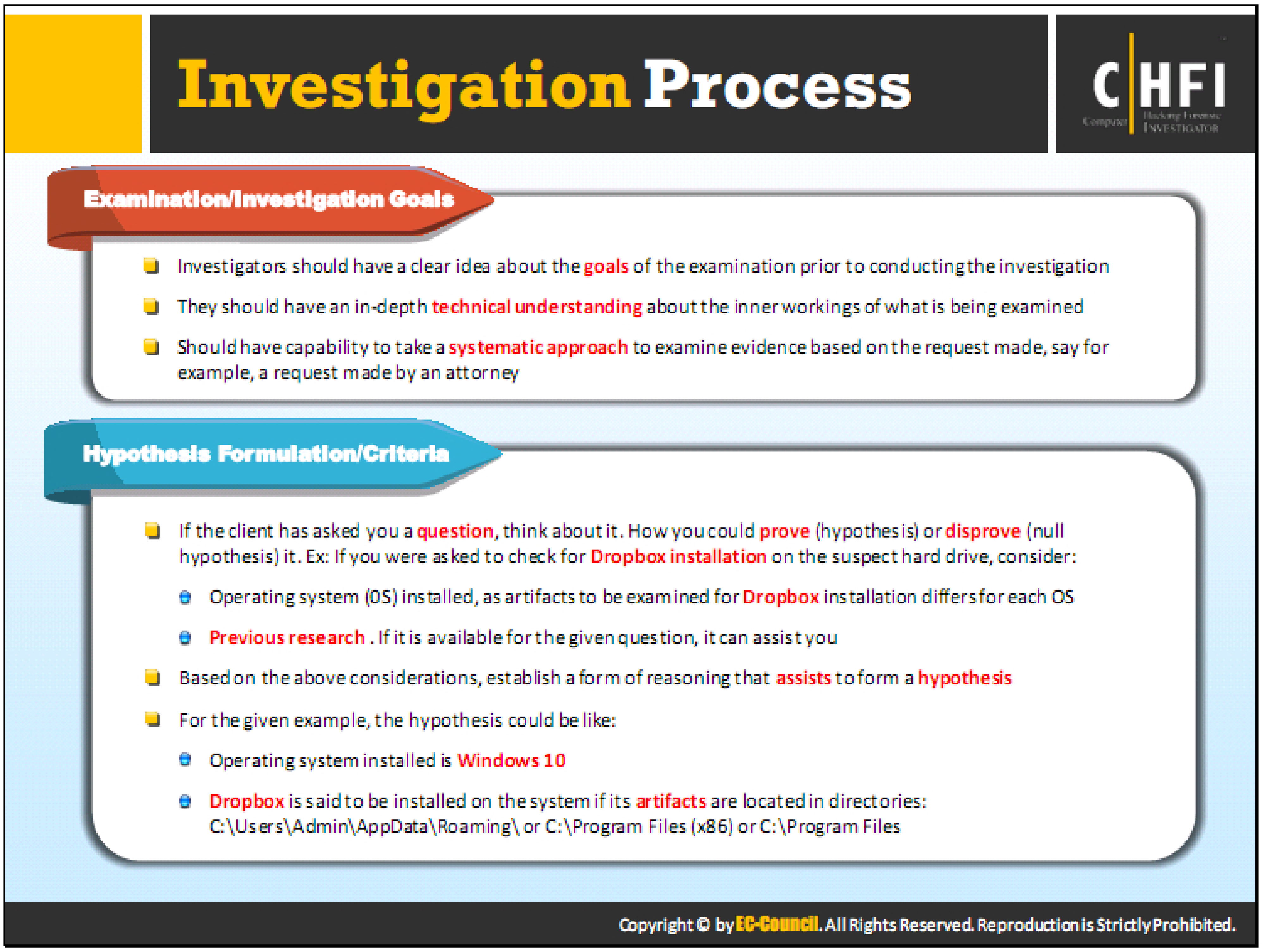
Data Analysis

Evidence Assessment

Documentation and Reporting

Testify as an Expert Witness

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



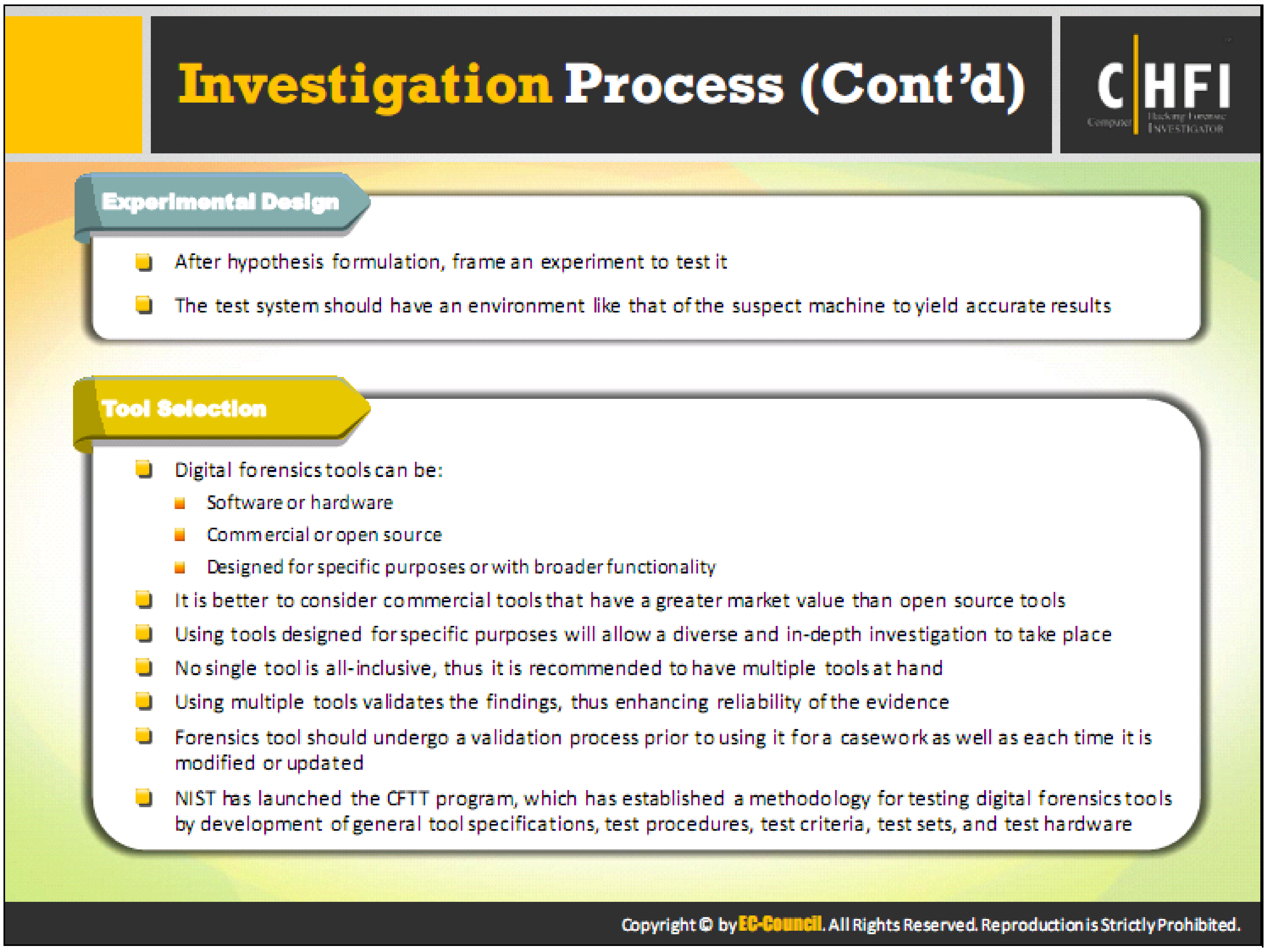
Investigation Process

Examination/Investigation Goals

- Investigators 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
- Should have capability to take a systematic approach to examine evidence based on the request made, say for example, a request made by an attorney

Hypothesis Formulation/Criteria

- If the client has asked you a question, think about it. How you could prove (hypothesis) or disprove (null hypothesis) it. Ex: If you were asked to check for Dropbox installation on the suspect hard drive, consider:
  - Operating system (OS) installed, as artifacts to be examined for Dropbox installation differs for each OS
  - Previous research . If it is available for the given question, it can assist you
- Based on the above considerations, establish a form of reasoning that assists to form a hypothesis
- For the given example, the hypothesis could be like:
  - Operating system installed is Windows 10
  - Dropbox is said to be installed on the system if its artifacts are located in directories: C:\Users\Admin\AppData\Roaming\ or C:\Program Files (x86) or C:\Program Files



Investigation Process (Cont'd)

Experimental Design

- After hypothesis formulation, frame an experiment to test it
- The test system should have an environment like that of the suspect machine to yield accurate results

Tool Selection

- Digital forensics tools can be:
  - Software or hardware
  - Commercial or open source
  - Designed for specific purposes or with broader functionality
- It is better to consider commercial tools that have a greater market value than open source tools
- Using tools designed for specific purposes will allow a diverse and in-depth investigation to take place
- No single tool is all-inclusive, thus it is recommended to have multiple tools at hand
- Using multiple tools validates the findings, thus enhancing reliability of the evidence
- Forensics tool should undergo a validation process prior to using it for a casework as well as each time it is modified or updated
- NIST has launched the CFTT program, which has established a methodology for testing digital forensics tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware

Experimental Design

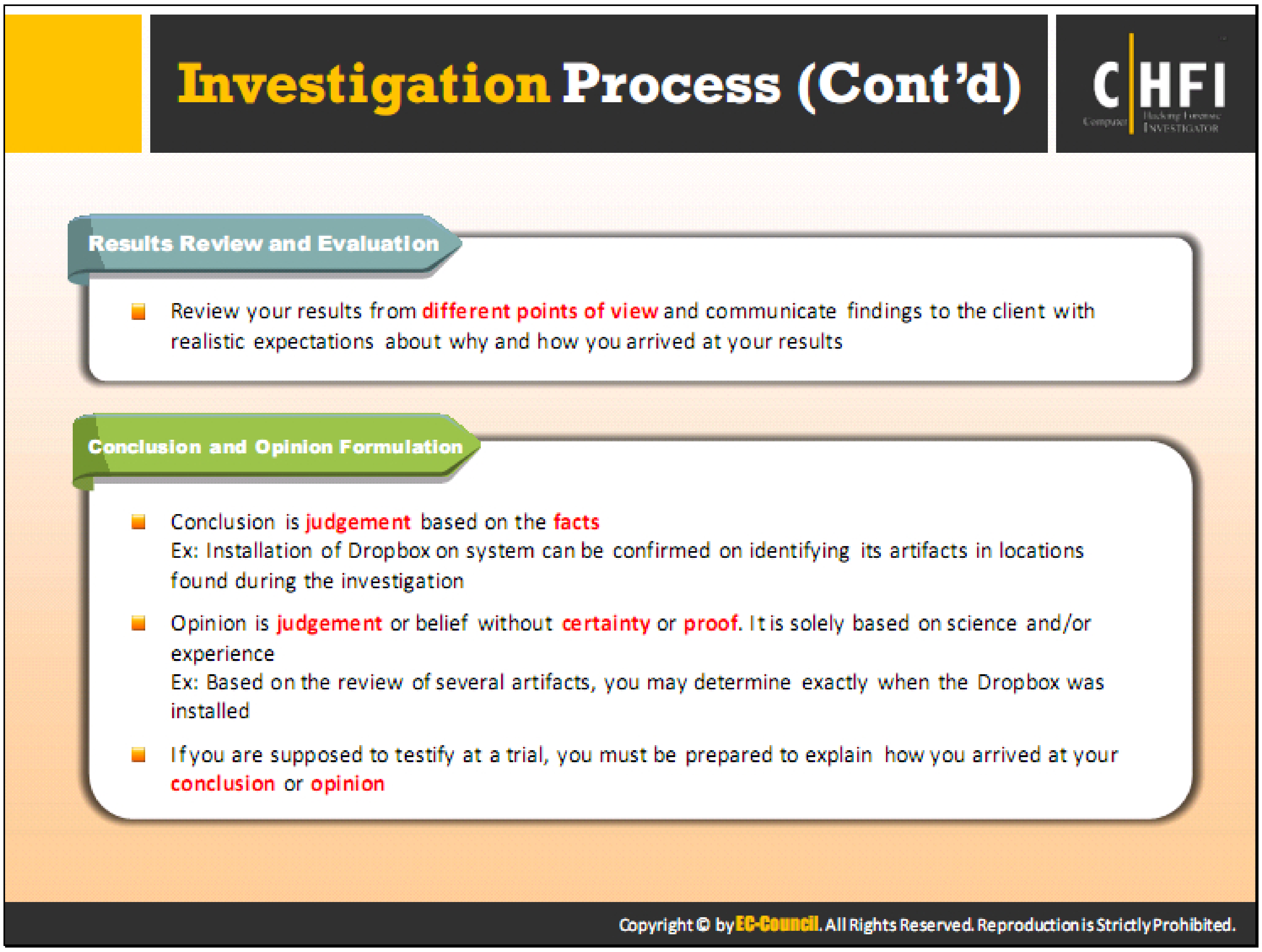
After the formulating the hypothesis, investigators should prepare to experiment and test the plans in order to check that they work. They need to simulate an environment similar to that of the suspect machine to yield accurate results.

This process is a mock drill, and helps the investigator to experiment with various methods, select suitable ones for different cases as well as select the type of tools required for the process.

Tool Selection

Every case is different and needs different methods of approach, while tools also differ depending upon the platform, operating system, and type of the target device. Considerations for selecting a tool include:

- Digital forensic tools can be:
    - Software or hardware
    - Commercial or open source
    - Designed for specific purposes or with a broader functionality
- It is good to consider commercial tools that have a market value compared to open source tools.
- Using tools designed for specific purposes will allow a diverse and in-depth investigation.
- No single tool is all-inclusive; thus, it is recommended to have multiple tools at hand.
- Using multiple tools validates the findings, thus enhancing the reliability of the evidence.
- Forensic tools should undergo a validation process prior to using it for a case as well as each time it is modified or updated.
- The National Institute of Standards and Technology (NIST) has launched the Computer Forensic Tool Testing (CFTT) project, which establishes a methodology for testing digital forensic tools by developing general tool specifications, test procedures, test criteria, test sets, and test hardware.



Investigation Process (Cont'd)

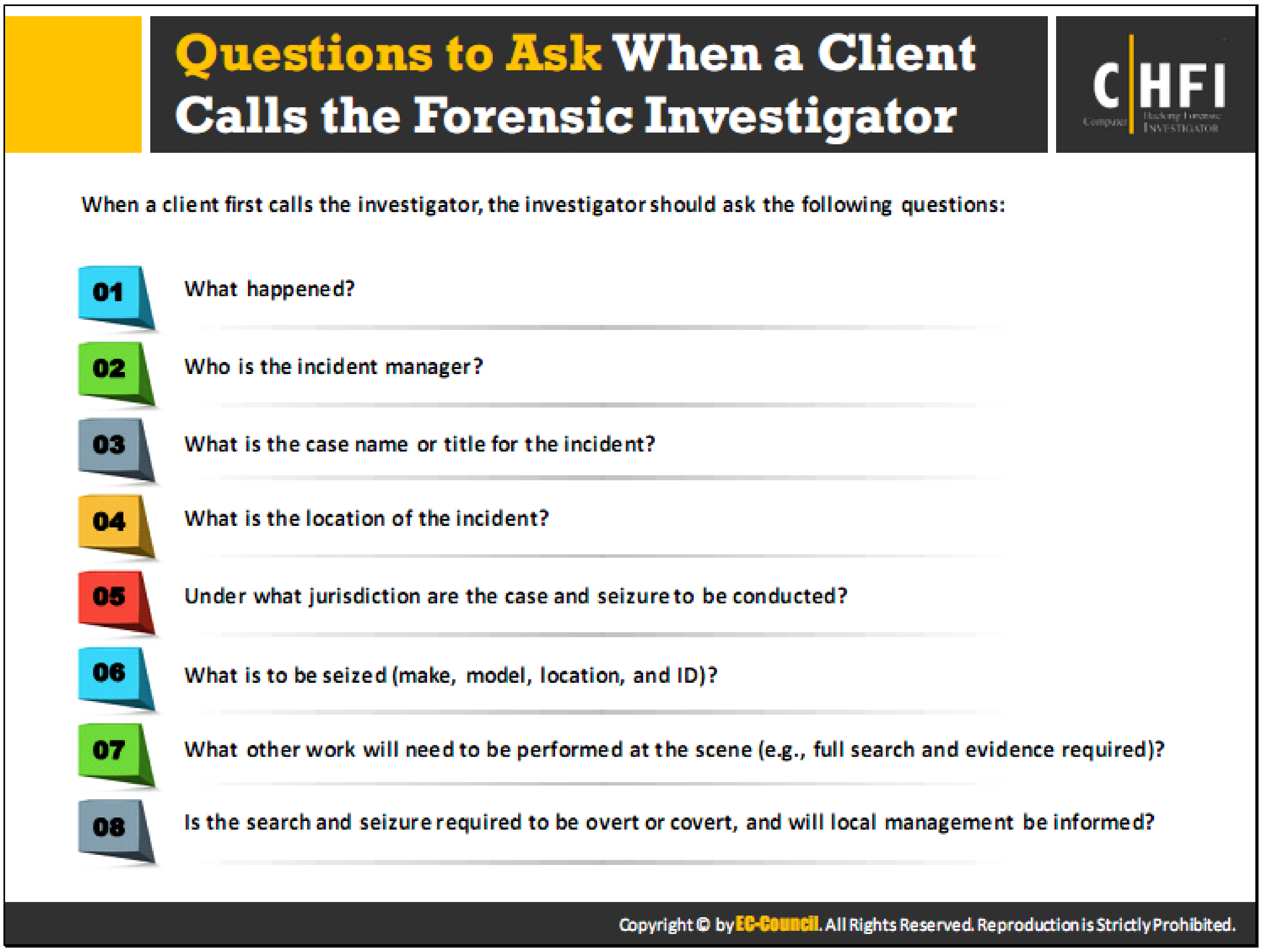
CHFI
Computer Hacking Forensic Investigator

Results Review and Evaluation

- Review your results from different points of view and communicate findings to the client with realistic expectations about why and how you arrived at your results

Conclusion and Opinion Formulation

- Conclusion is judgement based on the facts
  Ex: Installation of Dropbox on system can be confirmed on identifying its artifacts in locations found during the investigation
- Opinion is judgement or belief without certainty or proof. It is solely based on science and/or experience
  Ex: Based on the review of several artifacts, you may determine exactly when the Dropbox was installed
- If you are supposed to testify at a trial, you must be prepared to explain how you arrived at your conclusion or opinion



Questions to Ask When a Client Calls the Forensic Investigator

CHFI
Computer Hacking Forensic Investigator

When a client first calls the investigator, the investigator should ask the following questions:

01 What happened?

02 Who is the incident manager?

03 What is the case name or title for the incident?

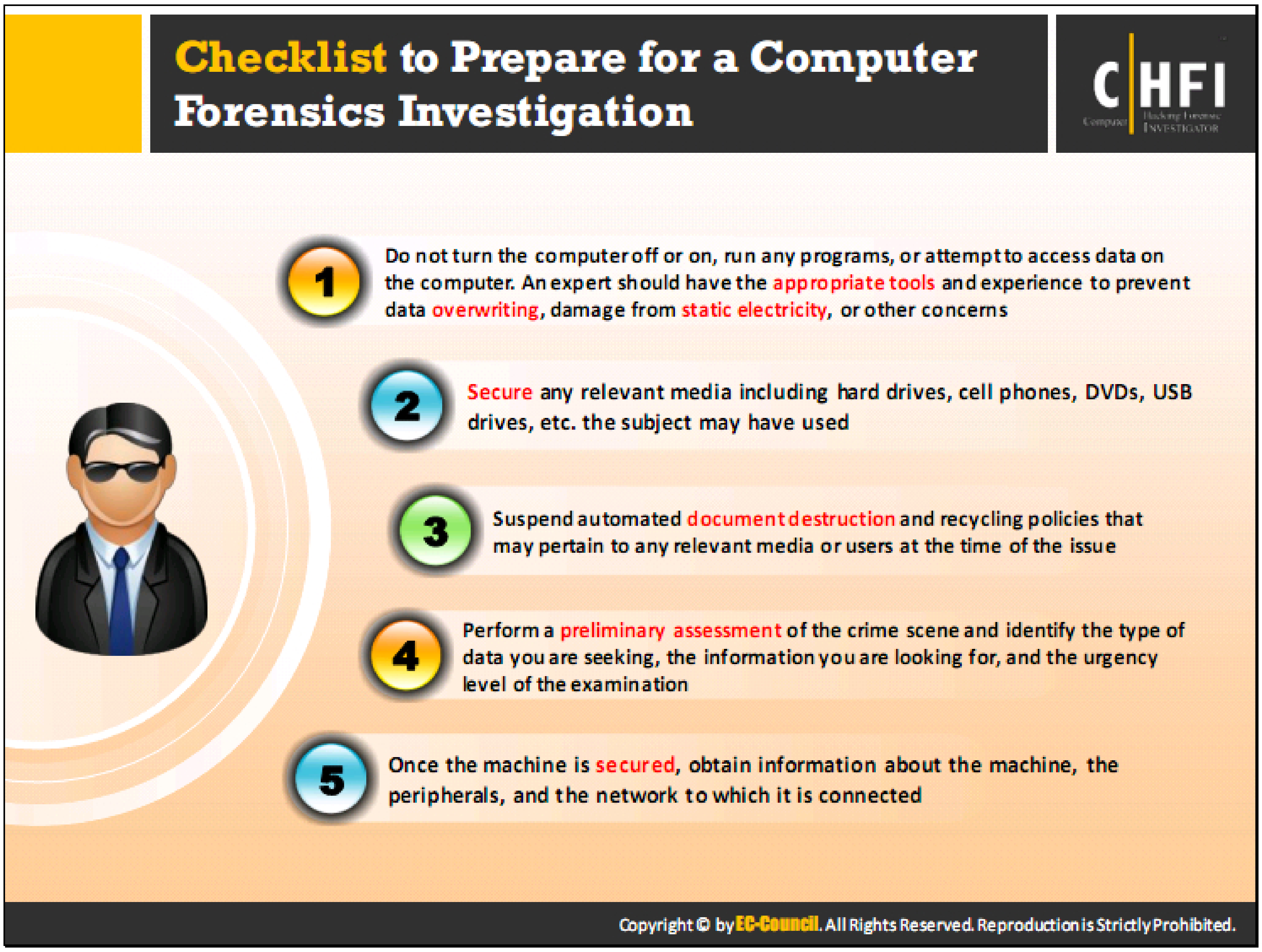
04 What is the location of the incident?

05 Under what jurisdiction are the case and seizure to be conducted?

06 What is to be seized (make, model, location, and ID)?

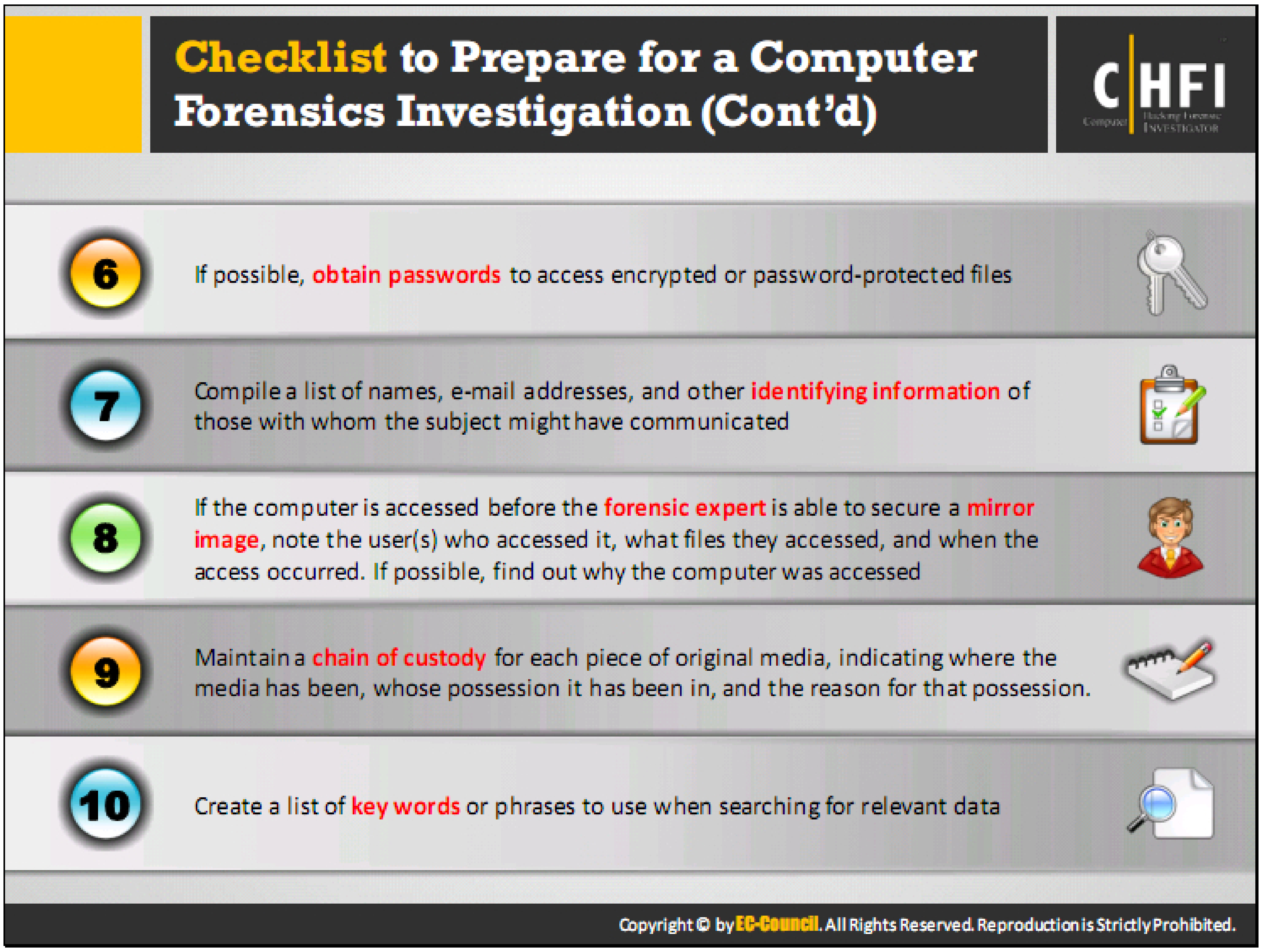
07 What other work will need to be performed at the scene (e.g., full search and evidence required)?

08 Is the search and seizure required to be overt or covert, and will local management be informed?



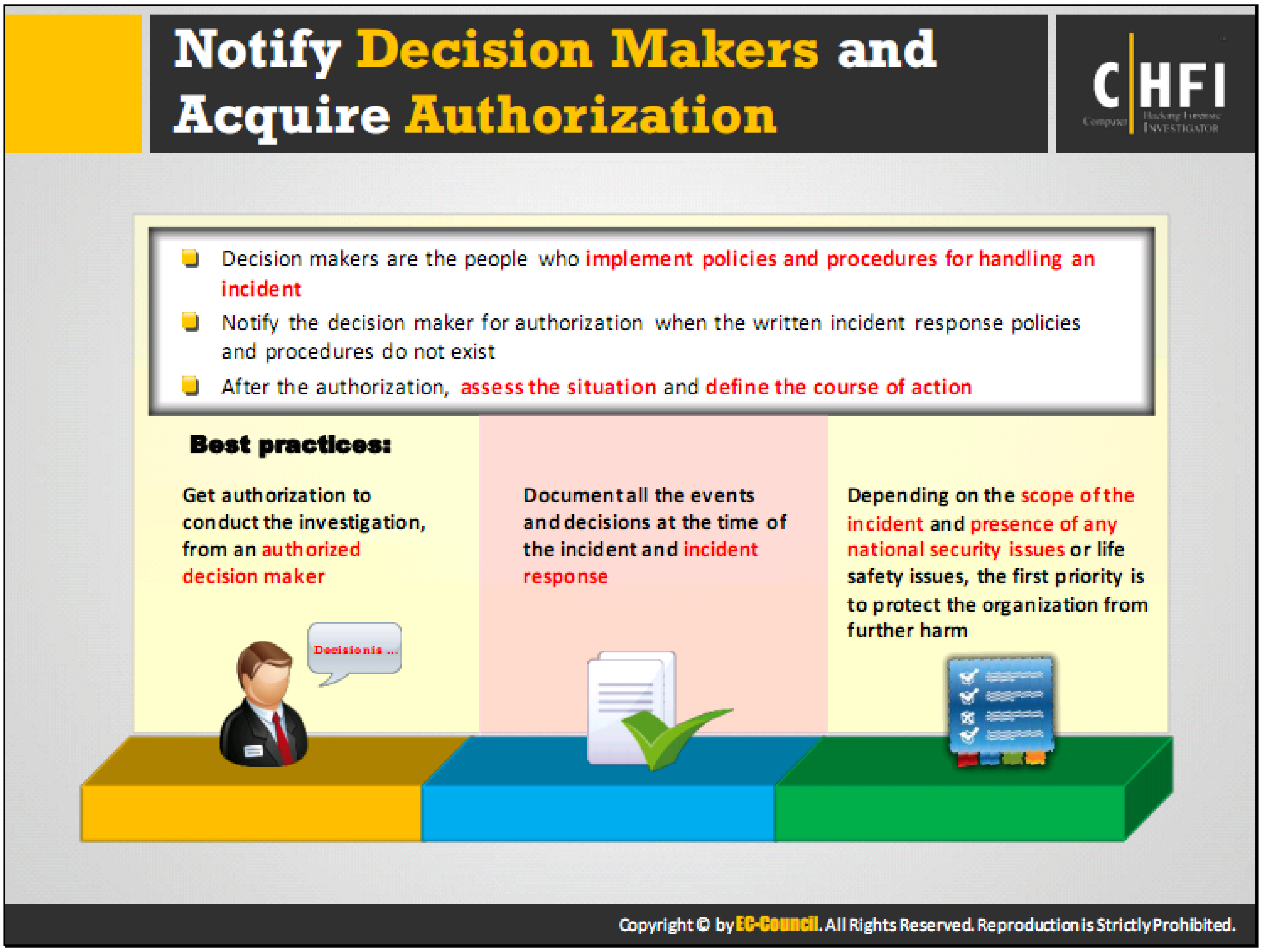
Checklist to Prepare for a Computer Forensics Investigation

1. Do not turn the computer off or on, run any programs, or attempt to access data on the computer. An expert should have the appropriate tools and experience to prevent data overwriting, damage from static electricity, or other concerns
2. Secure any relevant media including hard drives, cell phones, DVDs, USB drives, etc. the subject may have used
3. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at the time of the issue
4. Perform a preliminary assessment of the crime scene and identify the type of data you are seeking, the information you are looking for, and the urgency level of the examination
5. Once the machine is secured, obtain information about the machine, the peripherals, and the network to which it is connected



Checklist to Prepare for a Computer Forensics Investigation (Cont'd)

6. If possible, obtain passwords to access encrypted or password-protected files
7. Compile a list of names, e-mail addresses, and other identifying information of those with whom the subject might have communicated
8. If the computer is accessed before the forensic expert is able to secure a mirror image, note the user(s) who accessed it, what files they accessed, and when the access occurred. If possible, find out why the computer was accessed
9. Maintain a chain of custody for each piece of original media, indicating where the media has been, whose possession it has been in, and the reason for that possession.
10. Create a list of key words or phrases to use when searching for relevant data



Notify Decision Makers and Acquire Authorization

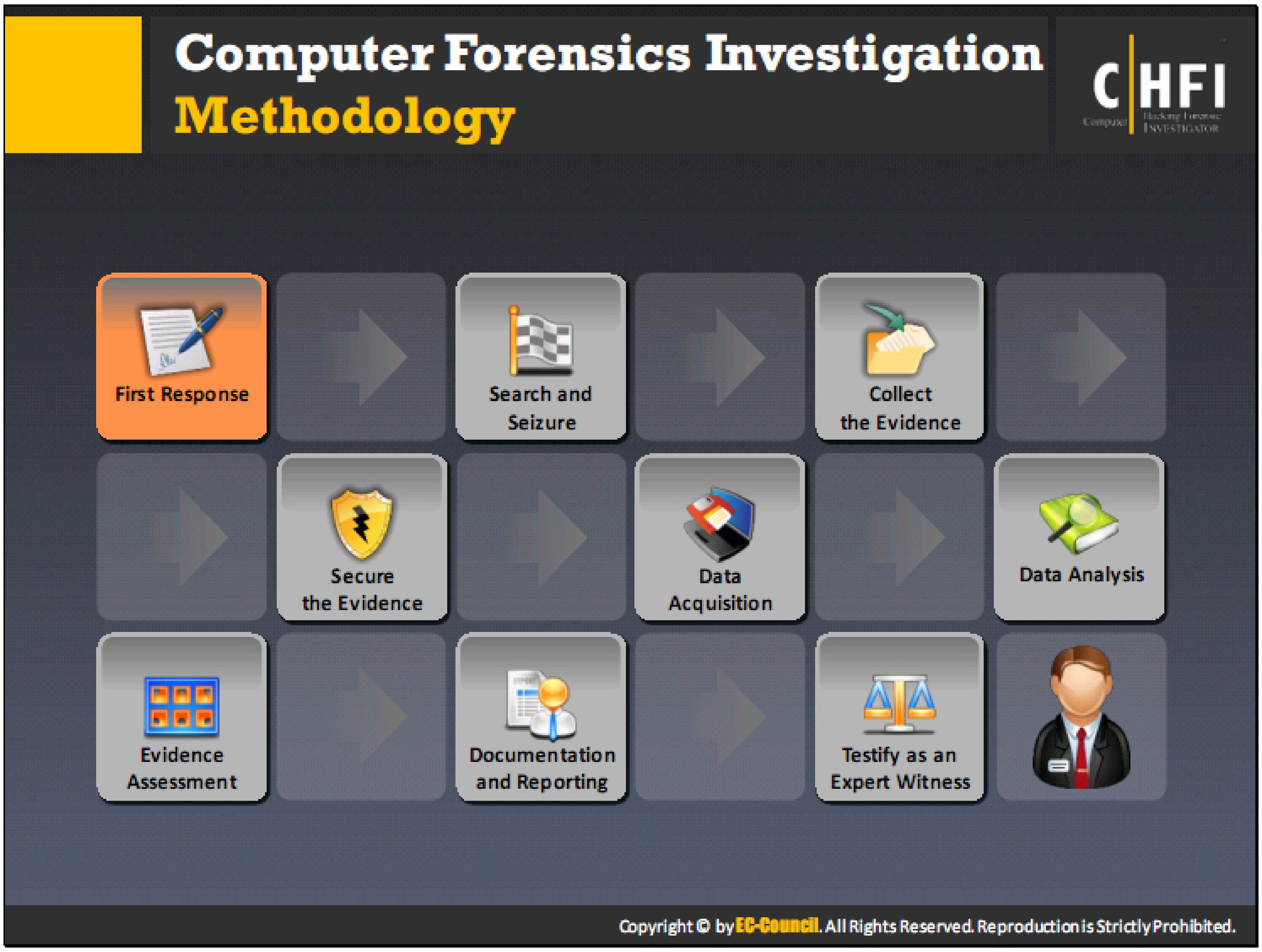
- Decision makers are the people who implement policies and procedures for handling an incident
- Notify the decision maker for authorization when the written incident response policies and procedures do not exist
- After the authorization, assess the situation and define the course of action

Best practices:

Get authorization to conduct the investigation, from an authorized decision maker

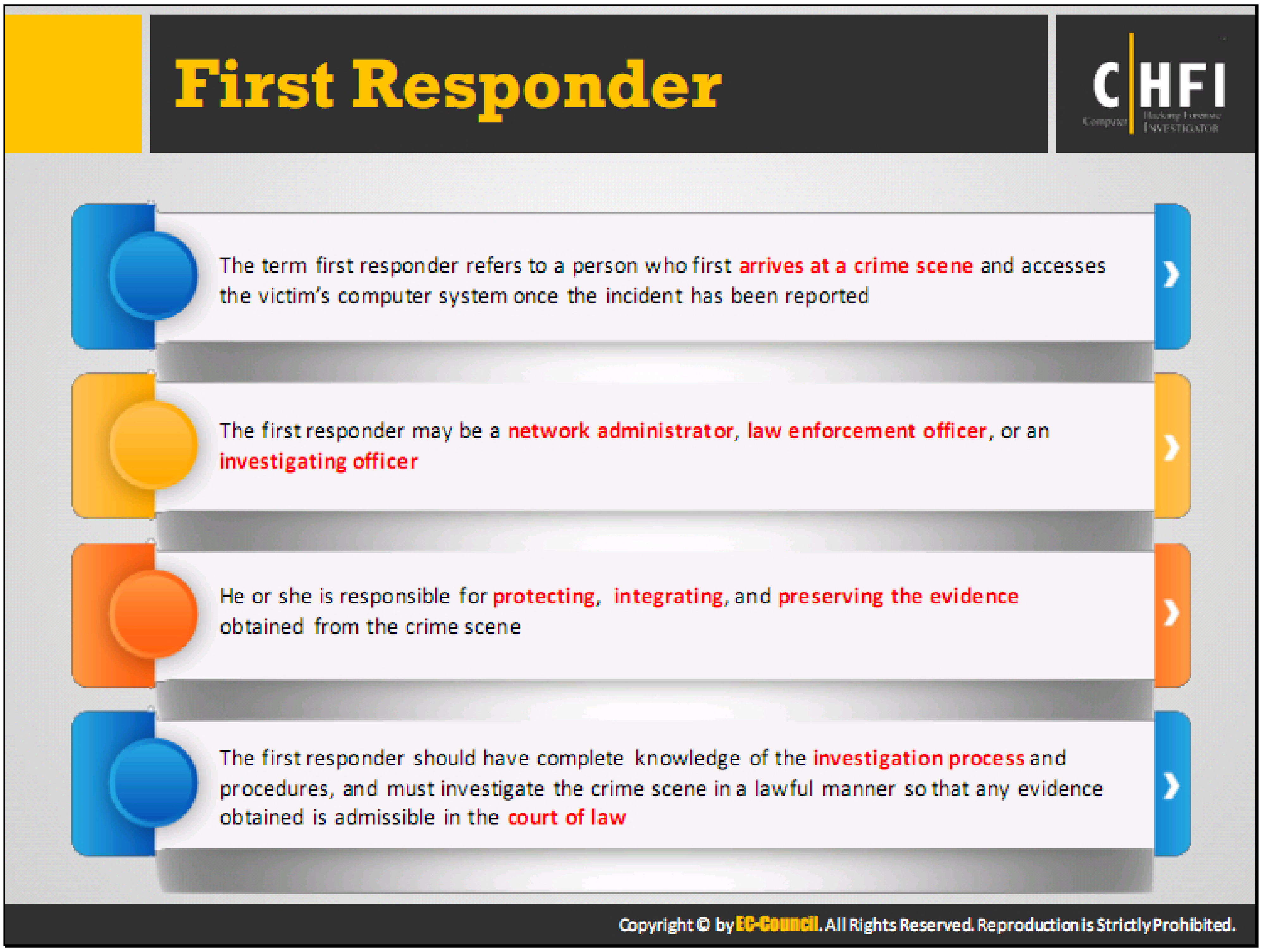
Document all the events and decisions at the time of the incident and incident response

Depending on the scope of the incident and presence of any national security issues or life safety issues, the first priority is to protect the organization from further harm



Computer Forensics Investigation Methodology

First response refers to the first action performed after occurrence of a security incident. Depending on the type of reaction, the first response can help the victim from further damage and can help investigators easily trace the suspect.



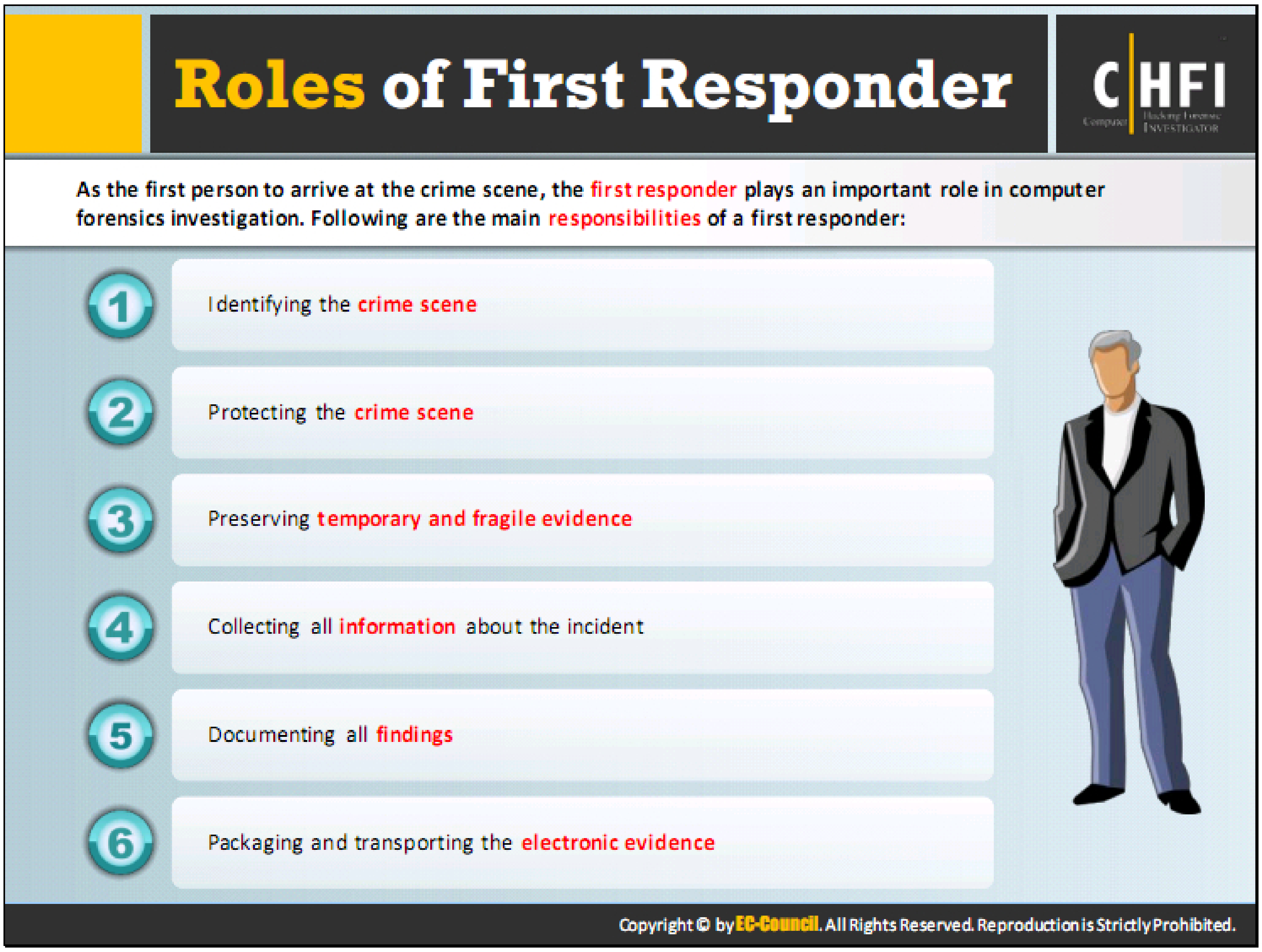
First Responder

- The term first responder refers to a person who first **arrives at a crime scene** and accesses the victim's computer system once the incident has been reported
- The first responder may be a **network administrator**, **law enforcement officer**, or an **investigating officer**
- He or she is responsible for **protecting**, **integrating**, and **preserving the evidence** obtained from the crime scene
- The first responder should have complete knowledge of the **investigation process** and procedures, and must investigate the crime scene in a lawful manner so that any evidence obtained is admissible in the **court of law**

The term first responder refers to the persons who first arrive at the crime scene and access the victim's computer system after the victim has reported the incident. A first responder may be a network 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 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. Then, the laboratory or agency sends the first responder to the crime scene for 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.



Roles of First Responder

As the first person to arrive at the crime scene, the first responder plays an important role in computer forensics investigation. Following are the main responsibilities of a first responder:

1. Identifying the crime scene
2. Protecting the crime scene
3. Preserving temporary and fragile evidence
4. Collecting all information about the incident
5. Documenting all findings
6. Packaging and transporting the electronic evidence

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 initial investigation. The investigation process starts after collecting all the evidence 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 proper evidence.

The main responsibilities of first responders are:

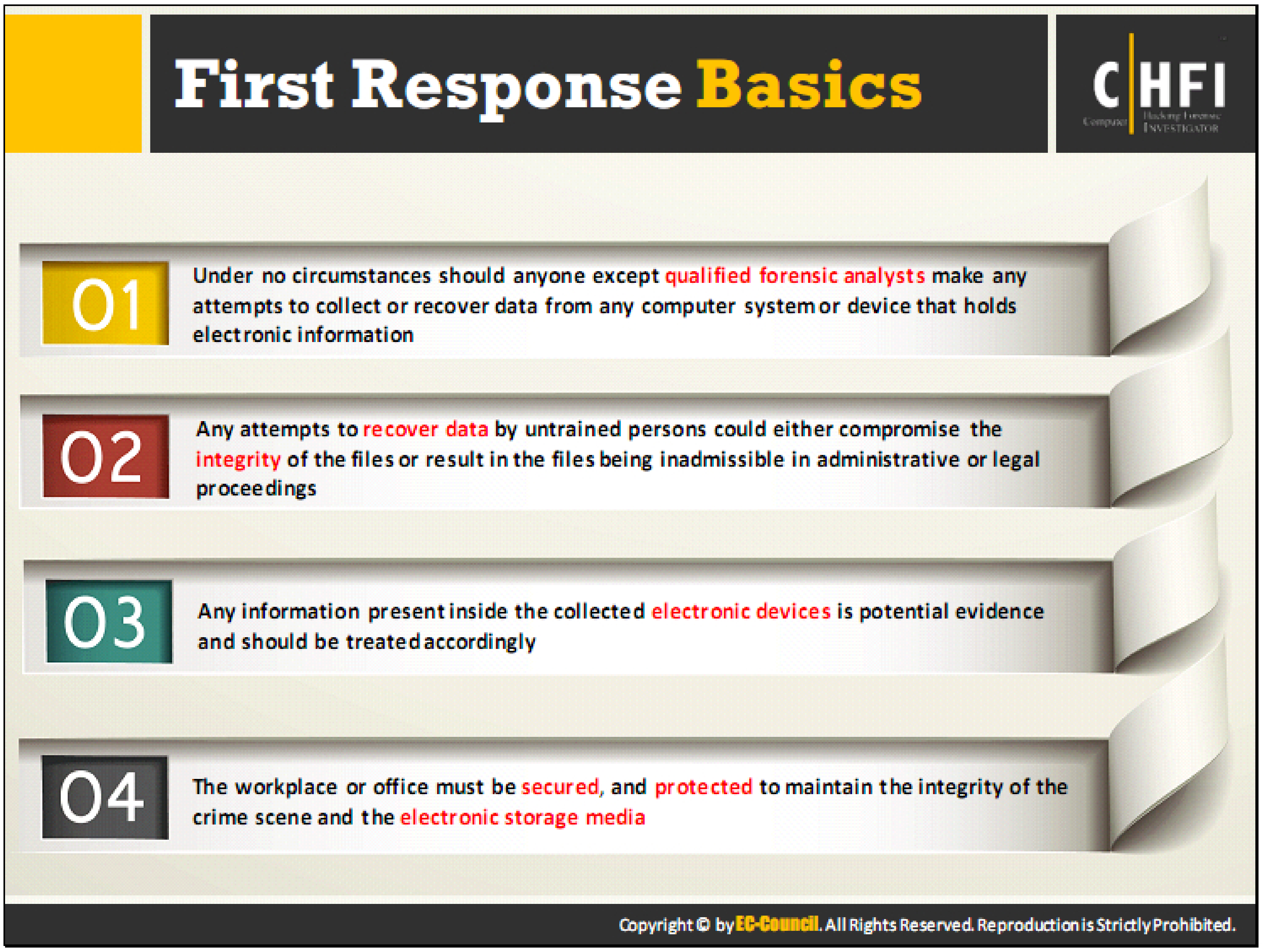
- **Identifying the crime scene:** After arriving at the crime scene, the first responder identifies the scope of the crime scene and establishes a perimeter. Establishing a perimeter includes a particular area, room, several rooms, or a building depending on the networked computers. After that, the first responder starts 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.

- **Collecting complete information about the incident:** For 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 starts documenting 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 collecting the evidence, and a complete description of the item.
- **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. Then, the first responder transports these packed bags to the forensics laboratory.
- **Gather preliminary information at the scene:** At the time of an incident, secure 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 helps in finding the evidence easily, if there is no third-party interference at the incident scene.

Preliminary information helps the 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:

- The type of incident.
- Reason for the occurrence of the incident.
- The potential damage due to the incident.
- Potential evidence from scattered objects outside the attacked system.
- Details of the person who used the system last before the incident.
- People who first knew about the incident's occurrence.



First Response Basics

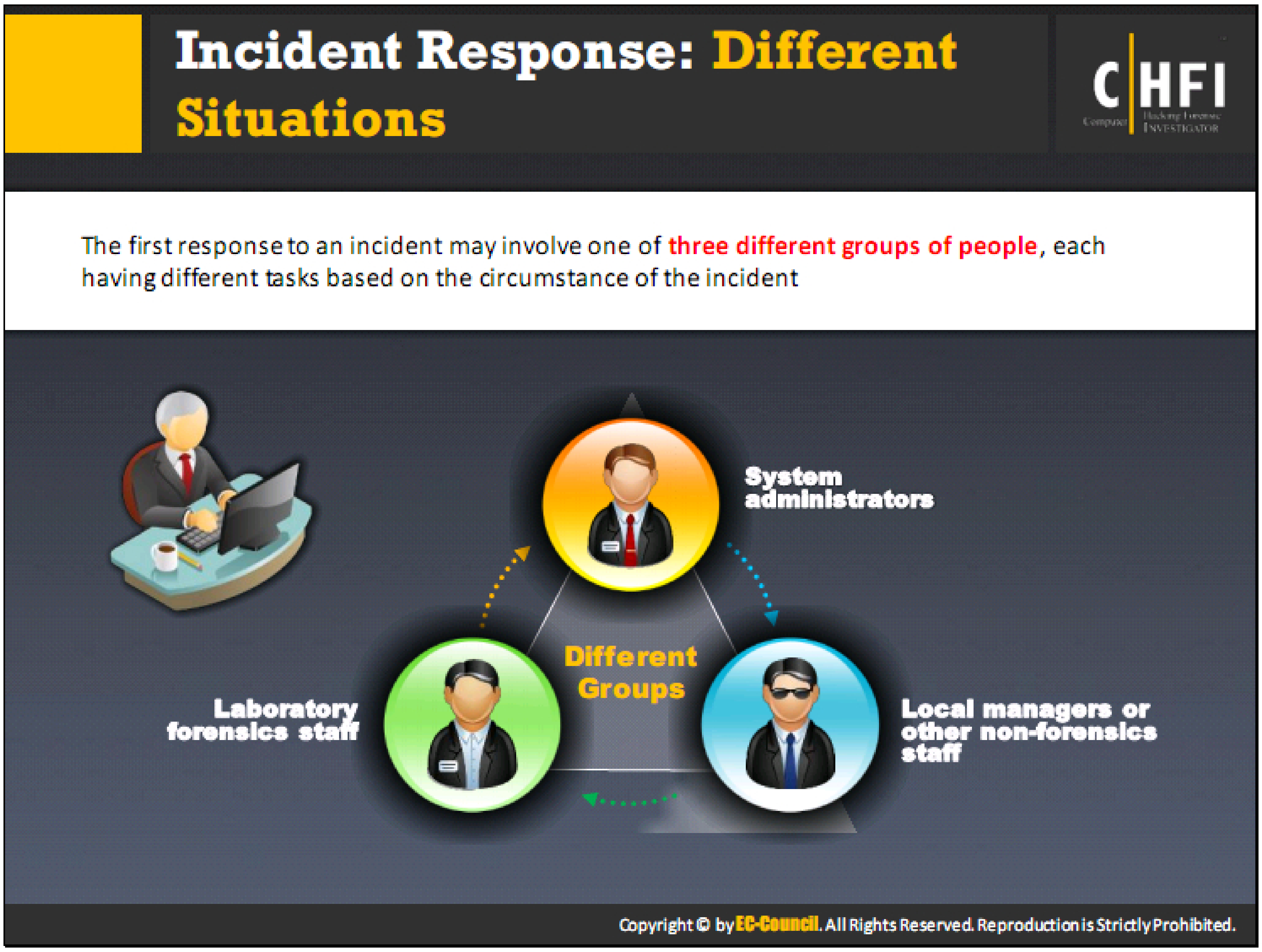
CHFI
Computer Hacking Forensic INVESTIGATOR

01 Under no circumstances should anyone except qualified forensic analysts make any attempts to collect or recover data from any computer system or device that holds electronic information

02 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

03 Any information present inside the collected electronic devices is potential evidence and should be treated accordingly

04 The workplace or office must be secured, and protected to maintain the integrity of the crime scene and the electronic storage media

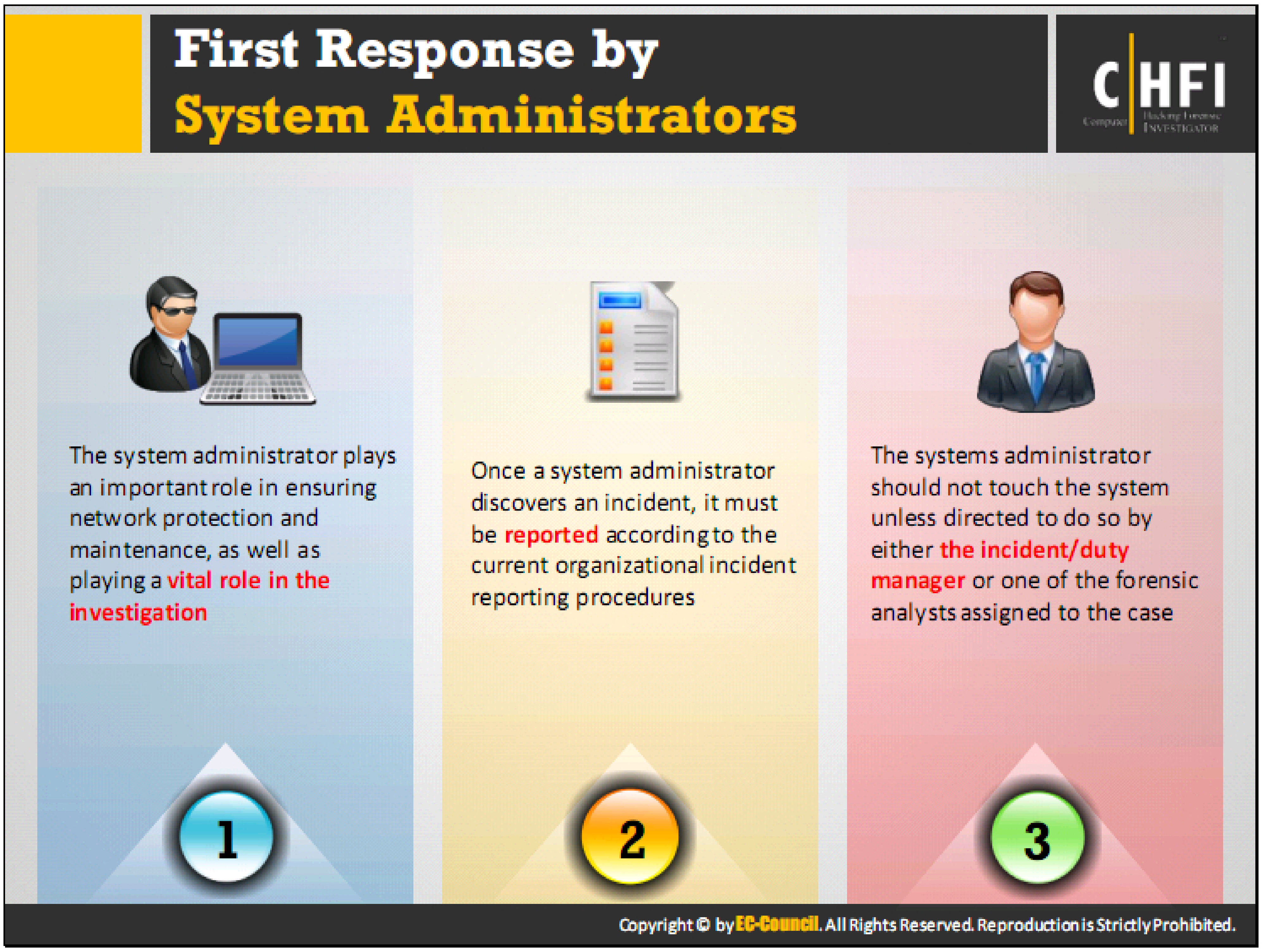


Incident Response: Different Situations

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

System administrators
Different Groups
Laboratory forensics staff
Local managers or other non-forensics staff

The activity the first responder performs at the incident location has a great impact over the investigation processes and can influence the accuracy or the success of the investigation procedure. Therefore, investigation firms need to be careful while deciding the first response team for an incident.



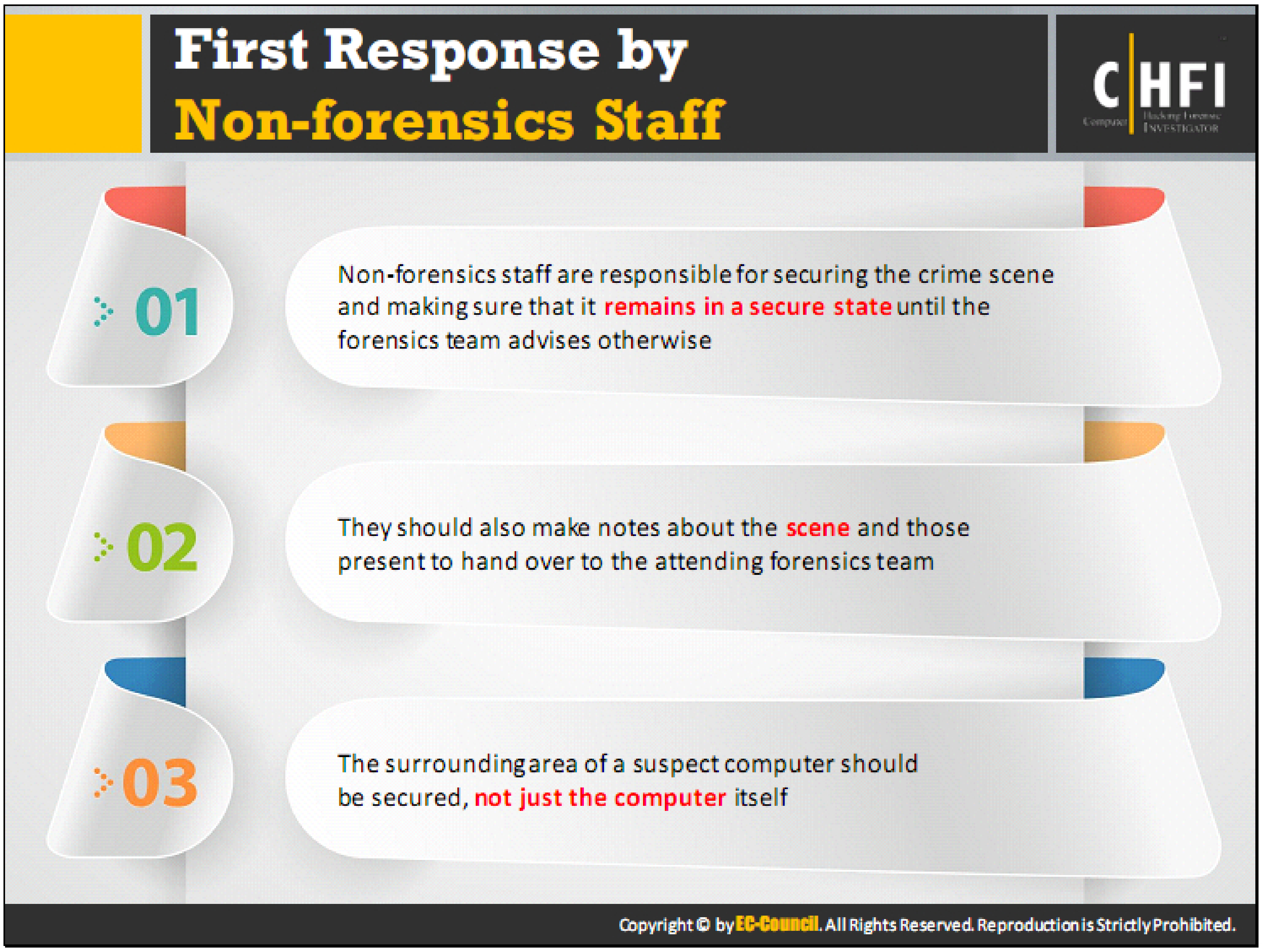
First Response by System Administrators

1. The system administrator plays an important role in ensuring network protection and maintenance, as well as playing a **vital role in the investigation**
2. Once a system administrator discovers an incident, it must be **reported** according to the current organizational incident reporting procedures
3. The systems administrator should not touch the system unless directed to do so by either **the incident/duty manager** or one of the forensic analysts assigned to the case

The system administrator's role is very important in ensuring network security and maintenance as well as investigation of 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 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 give explanation about the measures taken during the initial shutdown or isolation of the subject computer.

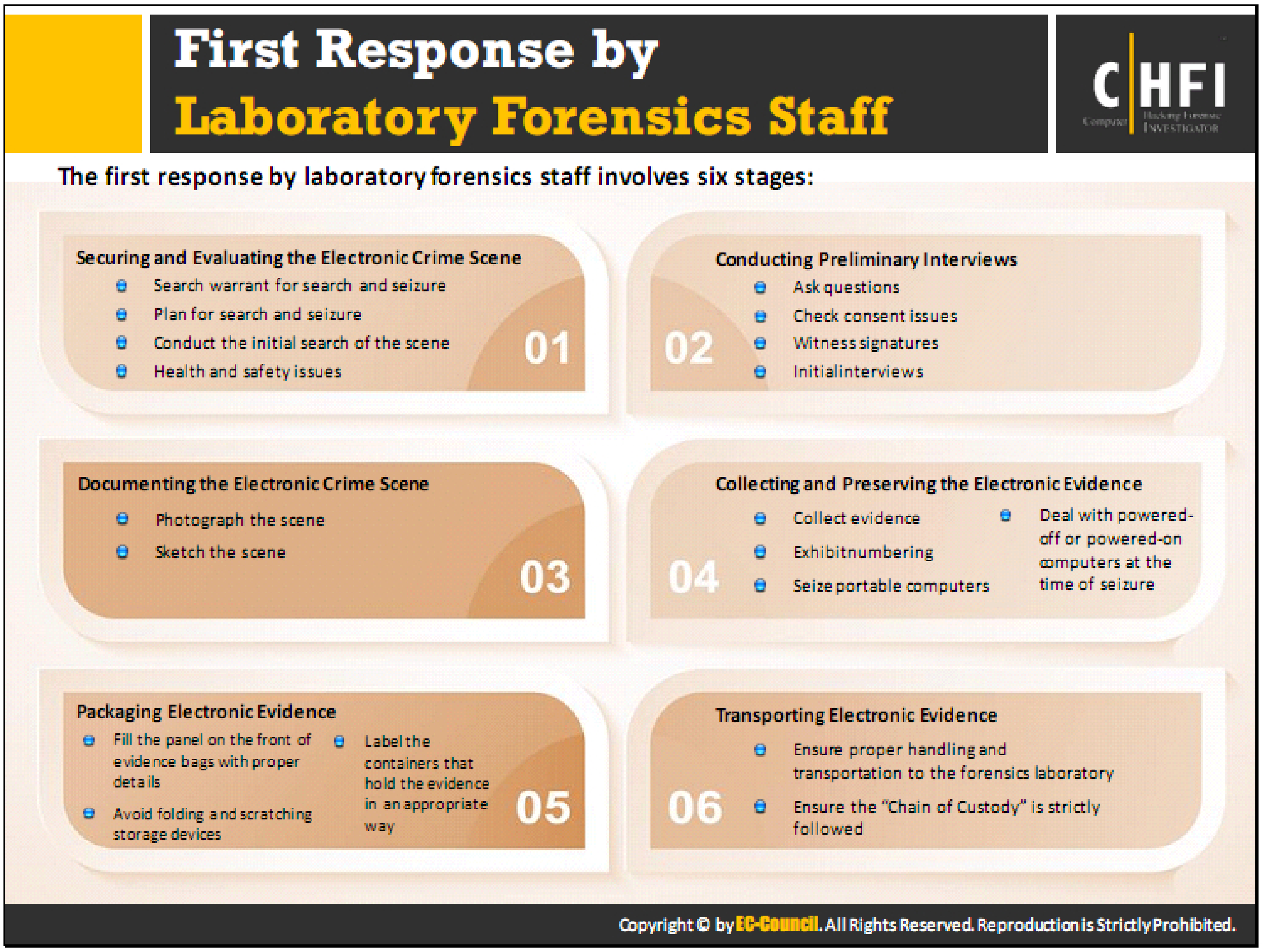


First Response by Non-forensics Staff

01 Non-forensics staff are responsible for securing the crime scene and making sure that it **remains in a secure state** until the forensics team advises otherwise

02 They should also make notes about the **scene** and those present to hand over to the attending forensics team

03 The surrounding area of a suspect computer should be secured, **not just the computer** itself



First Response by Laboratory Forensics Staff

The first response by laboratory forensics staff involves six stages:

01 **Securing and Evaluating the Electronic Crime Scene**
- Search warrant for search and seizure
- Plan for search and seizure
- Conduct the initial search of the scene
- Health and safety issues

02 **Conducting Preliminary Interviews**
- Ask questions
- Check consent issues
- Witness signatures
- Initialinterviews

03 **Documenting the Electronic Crime Scene**
- Photograph the scene
- Sketch the scene

04 **Collecting and Preserving the Electronic Evidence**
- Collect evidence
- Exhibitnumbering
- Seize portable computers
- Deal with powered-off or powered-on computers at the time of seizure

05 **Packaging Electronic Evidence**
- Fill the panel on the front of evidence bags with proper details
- Avoid folding and scratching storage devices
- Label the containers that hold the evidence in an appropriate way

06 **Transporting Electronic Evidence**
- Ensure proper handling and transportation to the forensics laboratory
- Ensure the "Chain of Custody" is strictly followed

First response by laboratory forensic staff involves six stages:

Securing and evaluating the electronic crime scene

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

- Search warrant for search and seizure
- Planning the search and seizure
- Conducting the initial search of the scene
- Health and safety issues

Conducting preliminary interviews

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

- Asking questions
- Checking the consent issues
- Witness signatures
- Initial interviews

Documenting the electronic crime scene

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

- Photographing the scene
- Sketching the scene

Collecting and preserving electronic evidence

Electronic evidence is versatile in nature and easily broken. The staff should be cautious when:

- Collecting evidence
- Dealing with powered OFF/ON computers at the time of seizure
- Seizing portable computers
- Preserving electronic evidence

Packaging electronic evidence

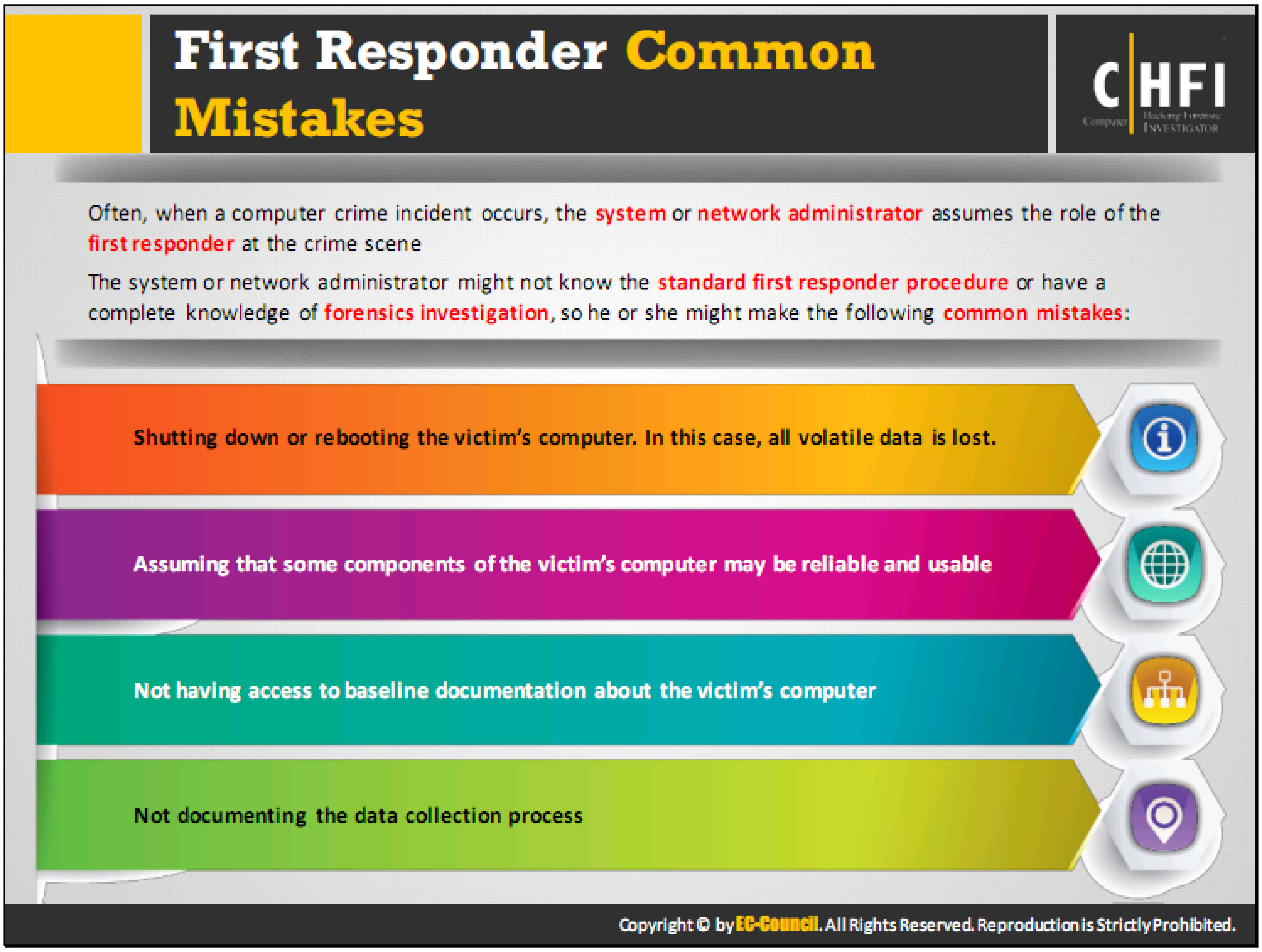
At the time of packaging all collected electronic evidence, the staff must document and enlist the evidence, and all containers should be properly labeled to seize evidence. During packaging:

- 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 way

Transporting electronic evidence

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



First Responder Common Mistakes

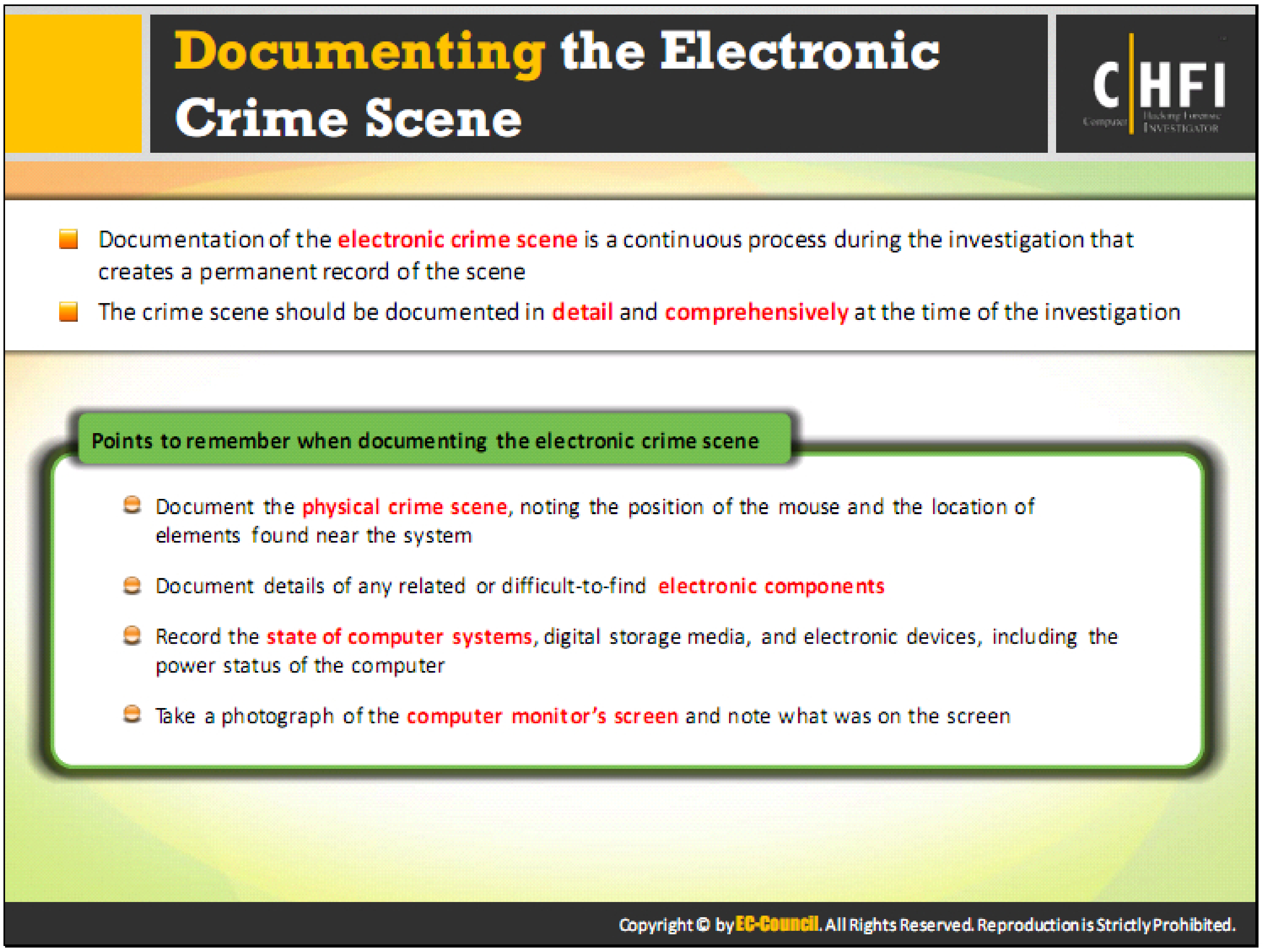
Often, when a computer crime incident occurs, the system or network administrator assumes the role of the first responder at the crime scene

The system or network administrator might not know the standard first responder procedure or have a complete knowledge of forensics investigation, so he or she might make the following common mistakes:

- Shutting down or rebooting the victim's computer. In this case, all volatile data is lost.
- Assuming that some components of the victim's computer may be reliable and usable
- Not having access to baseline documentation about the victim's computer
- Not documenting the data collection process

Most of the time when a computer crime incident occurs in the 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 handle the computer crime security incidents in a proper way because they do not know the first responder procedure or they do not have complete knowledge of forensic investigation. In such cases, they make the following mistakes:

- **Shutting down or rebooting the victim's computer**: In this case, the system loses the complete volatile data, such as MAC time and log files, shuts down processes running when shutting down and rebooting.
- **Assuming that some components of the victim's computer may be reliable and usable:** In this case, using some commands on the victim's computer may activate Trojans, malware, and time bombs to delete vital volatile data.
- Not having access to baseline documentation about the victim's computer.
- Not documenting the data collection process.



Documenting the Electronic Crime Scene

- Documentation of the electronic crime scene is a continuous process during the investigation that creates a permanent record of the scene
- The crime scene should be documented in detail and comprehensively at the time of the investigation

Points to remember when documenting the electronic crime scene

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

Documentation of 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 details should include location of the crime, status of the system, connected network devices, storage media, smart phones, mobile phones, PDAs, Internet and network access.

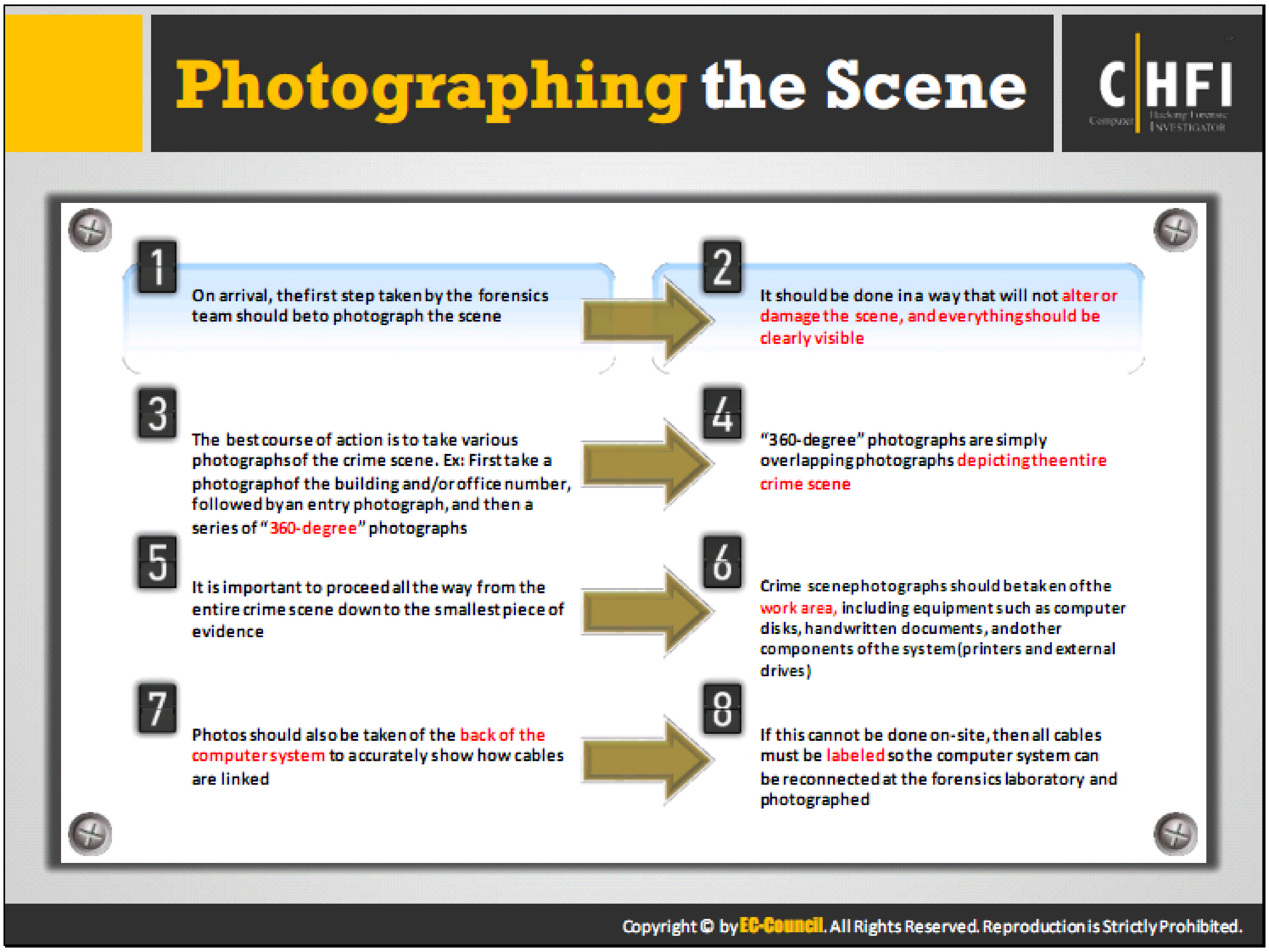
The document will help trace the serial numbers or other identifiers of the procured devices. Documenting also includes taking photographs, video, notes, and sketches of the scene, in order to recreate it later. The investigator needs to document the processes and activities running on the display screens.

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

- Documentation of the electronic crime scene is a continuous process during the investigation that makes a permanent record of the scene.
- It is essential to properly note down the site and state of computers, digital storage media, and other electronic devices.
- 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 you have seen on the screen.

The crime scene documentation should contain comprehensive details at the time of investigation.



Photographing the Scene

CHFI
Computer Hacking Forensic Investigator

1 On arrival, the first step taken by the forensics team should be to photograph the scene

2 It should be done in a way that will not alter or damage the scene, and everything should be clearly visible

3 The best course of action is to take various photographs of the crime scene. Ex: First take a photograph of the building and/or office number, followed by an entry photograph, and then a series of "360-degree" photographs

4 "360-degree" photographs are simply overlapping photographs depicting the entire crime scene

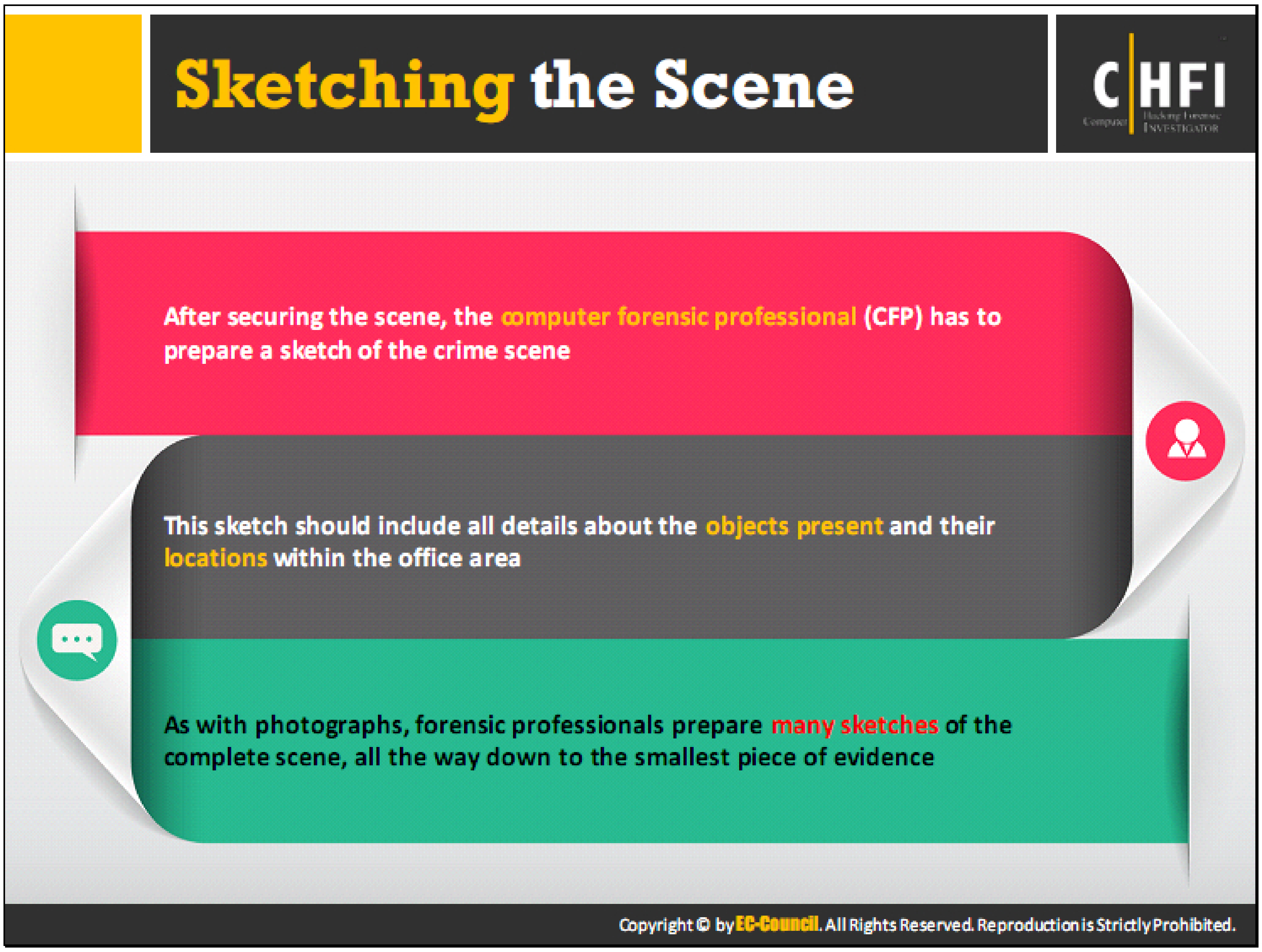
5 It is important to proceed all the way from the entire crime scene down to the smallest piece of evidence

6 Crime scene photographs should be taken of the work area, including equipment such as computer disks, handwritten documents, and other components of the system (printers and external drives)

7 Photos should also be taken of the back of the computer system to accurately show how cables are linked

8 If this cannot be done on-site, then all cables must be labeled so the computer system can be reconnected at the forensics laboratory and photographed

Crime scenes are the main source of physical evidence and photographing it will provide the investigators with a visual reference for future use. The images will also help the investigators recreate the scene when required.



Sketching the Scene

After securing the scene, the computer forensic professional (CFP) has to prepare a sketch of the crime scene

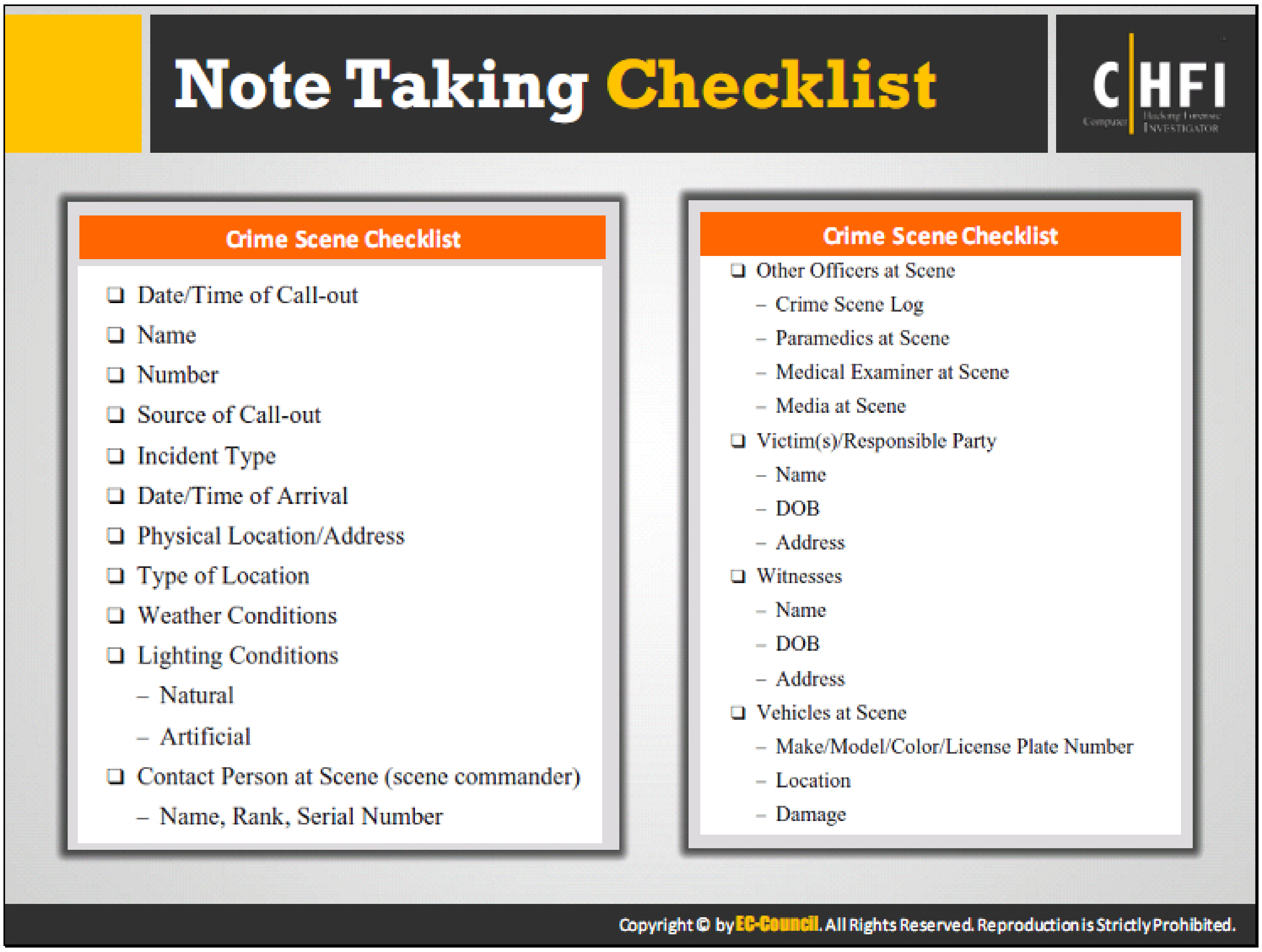
This sketch should include all details about the objects present and their locations within the office area

As with photographs, forensic professionals prepare many sketches of the complete scene, all the way down to the smallest piece of evidence

A sketch conveys the measurement relationship between the crime scene and the evidence found. The sketch explains the data in the documented photos and videos. Sketches can also portray the positions of the camera as well as the photographer.

The points to remember while sketching the scene are:

- After securing the scene, the computer forensic professional (CFP) has to prepare a sketch of the crime scene.
- This sketch should include all details about the objects present and their locations within the office area.
- As with photographs, forensic professionals prepare many sketches of the complete scene, all the way down to the smallest piece of evidence.
- After creating an accurate scene sketch, the CFP should sketch the top of the computer desk, specifying pieces of evidence.



Note Taking Checklist

CHFI
Computer Hacking Forensic Investigator

Crime Scene Checklist

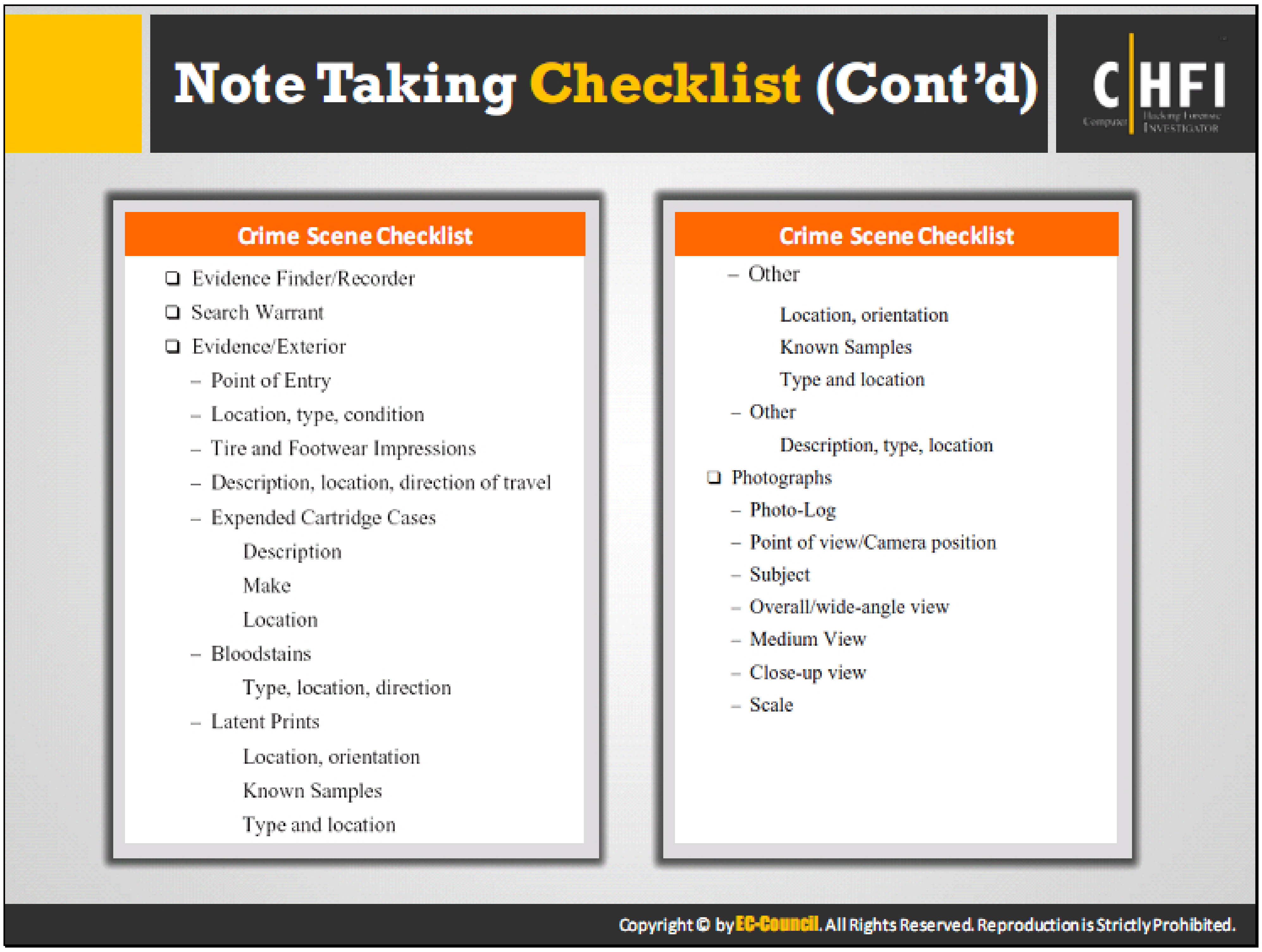
- ❑ Date/Time of Call-out
- ❑ Name
- ❑ Number
- ❑ Source of Call-out
- ❑ Incident Type
- ❑ Date/Time of Arrival
- ❑ Physical Location/Address
- ❑ Type of Location
- ❑ Weather Conditions
- ❑ Lighting Conditions
  - Natural
  - Artificial
- ❑ Contact Person at Scene (scene commander)
  - Name, Rank, Serial Number

Crime Scene Checklist

- ❑ Other Officers at Scene
  - Crime Scene Log
  - Paramedics at Scene
  - Medical Examiner at Scene
  - Media at Scene
- ❑ Victim(s)/Responsible Party
  - Name
  - DOB
  - Address
- ❑ Witnesses
  - Name
  - DOB
  - Address
- ❑ Vehicles at Scene
  - Make/Model/Color/License Plate Number
  - Location
  - Damage

Computer crime scene investigation requires significant effort. The investigation effort varies according to the situation, and without a checklist, it is impossible to remember all the findings of the computer crime investigation. The investigator uses the checklist to note down the findings of the digital evidence search, collection, and preservation processes at the crime scene.

Source: http://www.lawtechcustompublishing.com



Note Taking Checklist (Cont'd)

Crime Scene Checklist

□ Evidence Finder/Recorder

□ Search Warrant

□ Evidence/Exterior

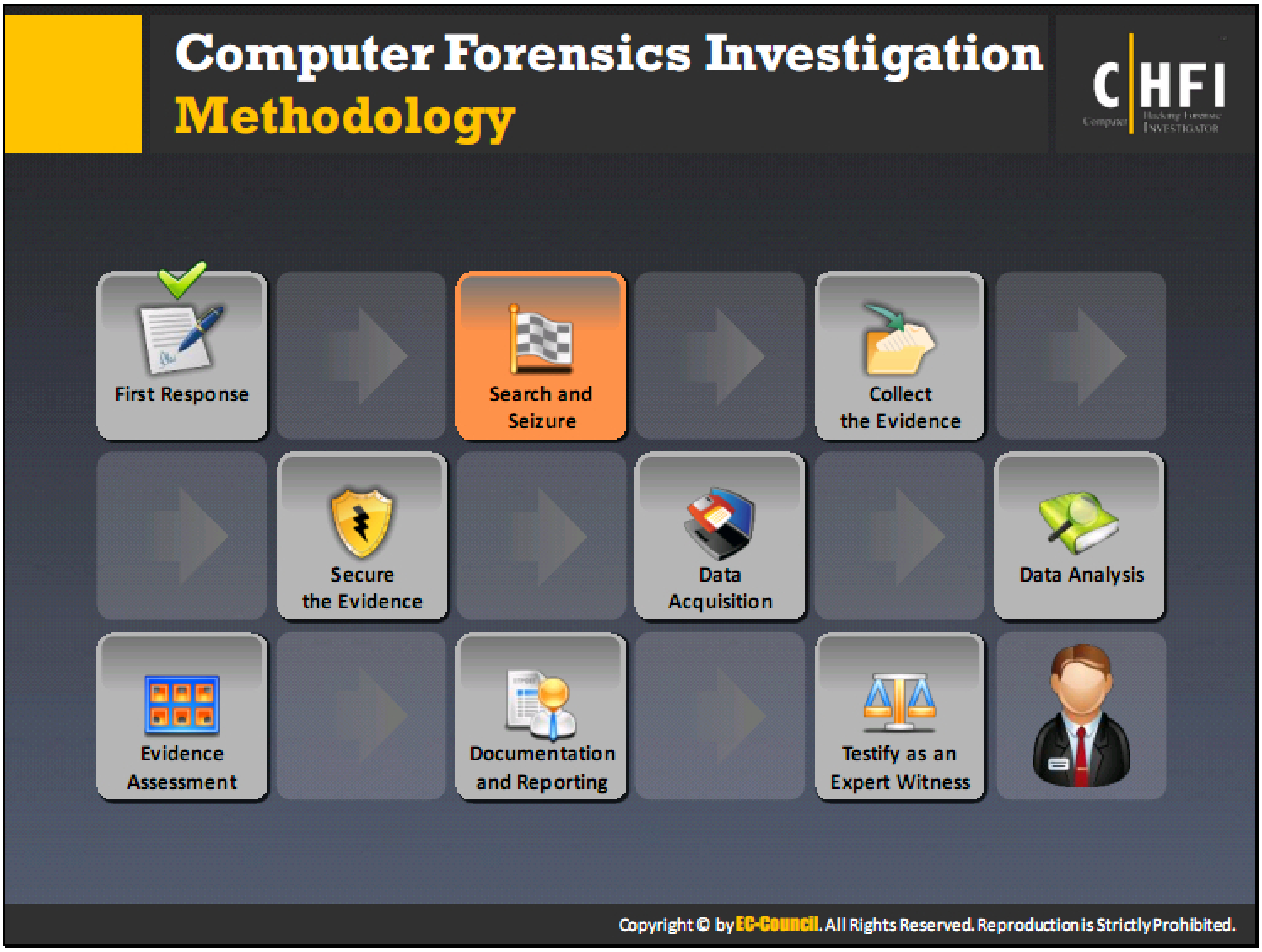
- Point of Entry
- Location, type, condition
- Tire and Footwear Impressions
- Description, location, direction of travel
- Expended Cartridge Cases
  - Description
  - Make
  - Location
- Bloodstains
  - Type, location, direction
- Latent Prints
  - Location, orientation
  - Known Samples
  - Type and location

Crime Scene Checklist

- Other
  - Location, orientation
  - Known Samples
  - Type and location
- Other
  - Description, type, location

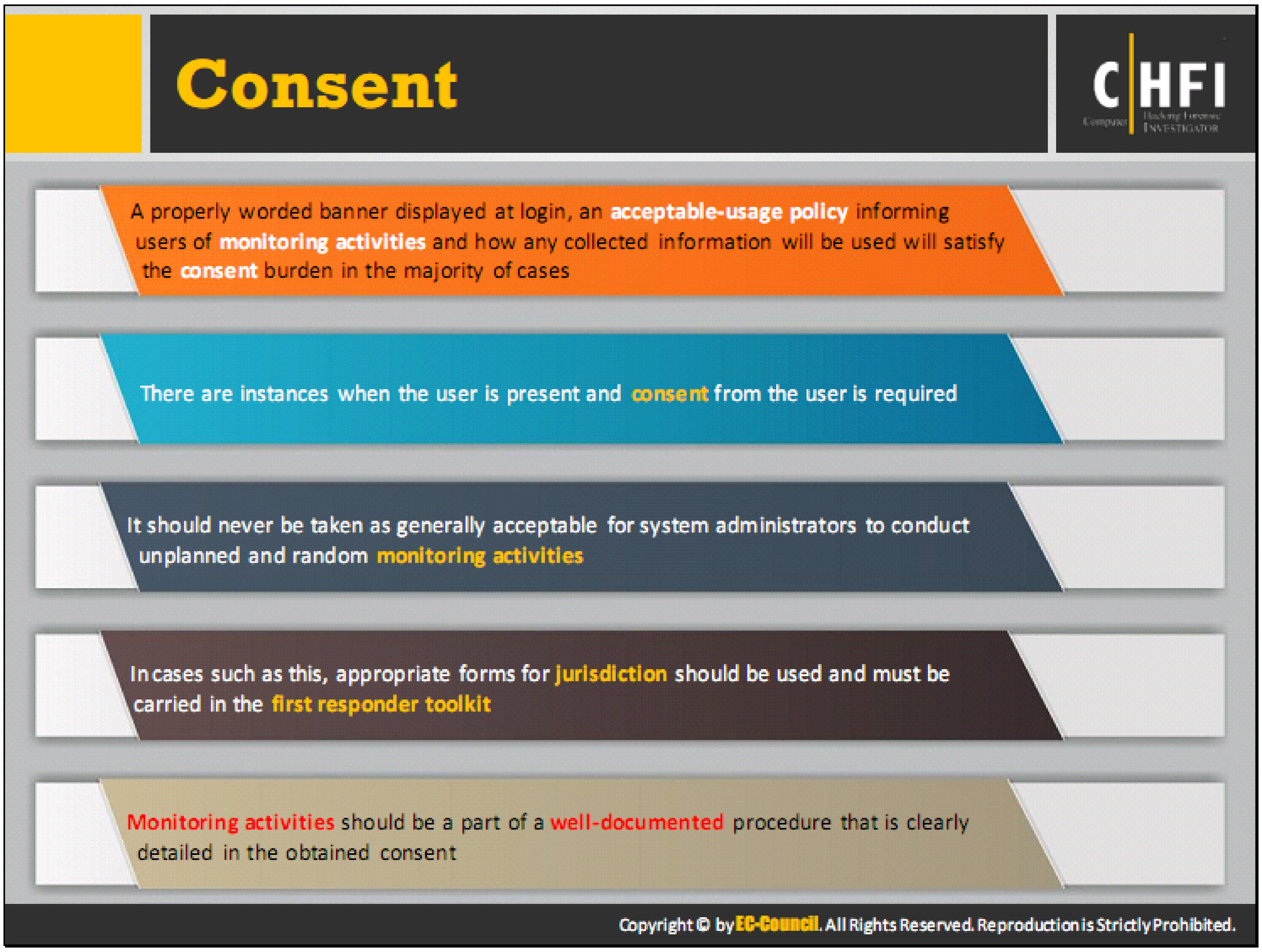
□ Photographs

- Photo-Log
- Point of view/Camera position
- Subject
- Overall/wide-angle view
- Medium View
- Close-up view
- Scale



Computer Forensics Investigation
Methodology
CHFI Computer Hacking Forensic INVESTIGATOR
First Response
Search and Seizure
Collect the Evidence
Secure the Evidence
Data Acquisition
Data Analysis
Evidence Assessment
Documentation and Reporting
Testify as an Expert Witness
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The investigators should have keen knowledge of all the devices that could have played 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 in order to analyze them for evidential data.



Consent

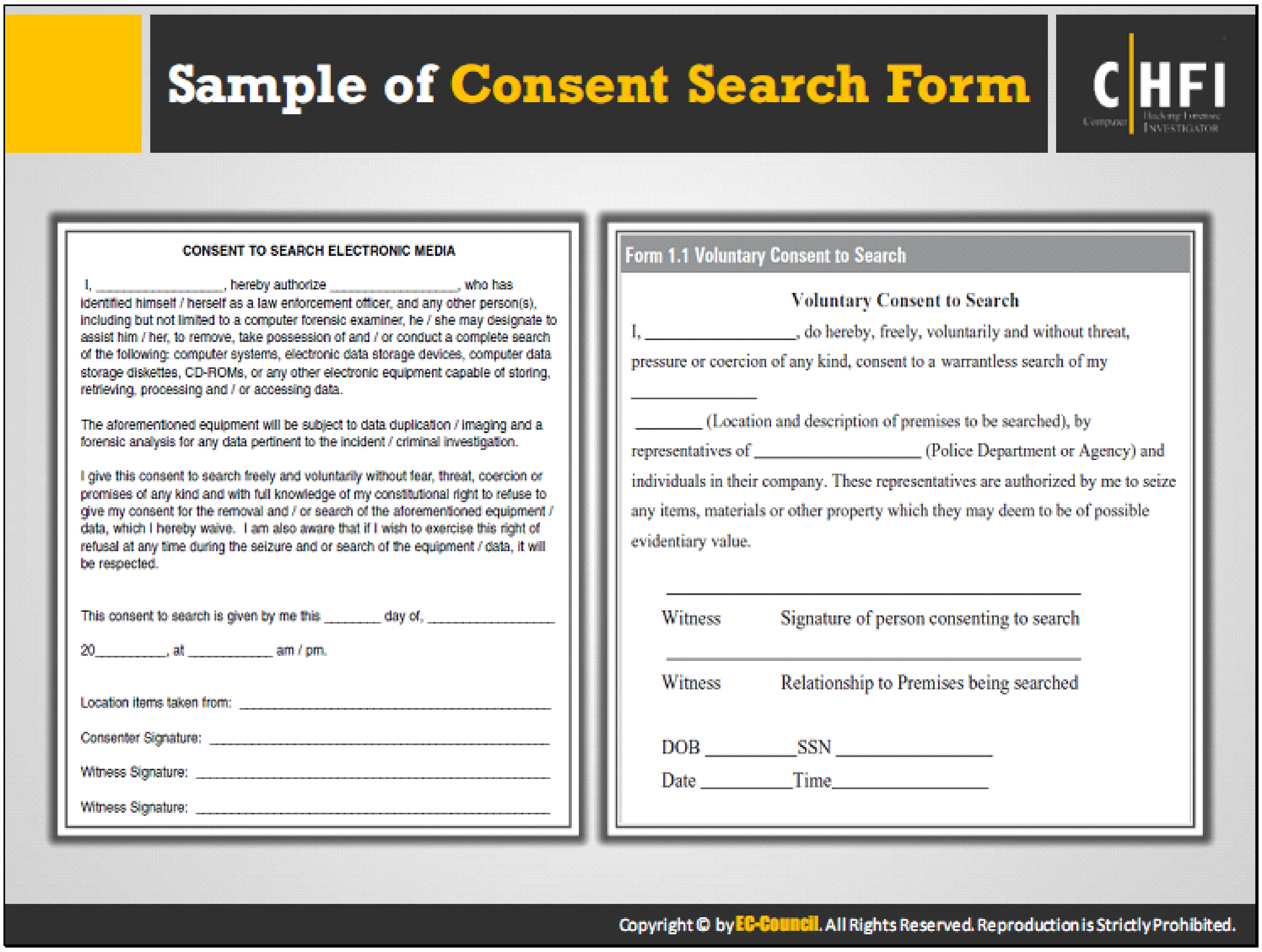
- A properly worded banner displayed at login, an **acceptable-usage policy** informing users of **monitoring activities** and how any collected information will be used will satisfy the **consent** burden in the majority of cases
- There are instances when the user is present and **consent** from the user is required
- It should never be taken as generally acceptable for system administrators to conduct unplanned and random **monitoring activities**
- In cases such as this, appropriate forms for **jurisdiction** should be used and must be carried in the **first responder toolkit**
- **Monitoring activities** should be a part of a **well-documented** procedure that is clearly detailed in the obtained consent

Consent, in computer forensics investigation, refers to the process of obtaining formal permission from the owner of the victim organization or an individual owning the target system to perform a thorough investigation. A written consent from the authority is enough to start the investigation and search process.

At the time of consent, the investigators should use properly written banners with suitable use policies and get them signed from the owner of the evidence scene or devices. If you have a properly worded banner and a suitable use policy informing users of monitoring activities and how to use the information collected from monitoring activities, the consent burden will suffice in a majority of cases.

There are instances when the user is present and has to provide consent as the hardware user. It should never be a general permission for system administrators to conduct unplanned and random monitoring activities.

Use appropriate forms for the jurisdiction and carry these documents in the grab bag to protect from any harm or damage. Monitoring activities related to the consent should be part of a well-documented procedure in the obtained consent.



Sample of Consent Search Form

C|HFI
Computer Hacking Forensic Investigator

CONSENT TO SEARCH ELECTRONIC MEDIA

I, ___________________, hereby authorize ___________________, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to a computer forensic examiner, he / she may designate to assist him / her, to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data.

The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation.

I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and or search of the equipment / data, it will be respected.

This consent to search is given by me this ________ day of, ___________________

20__________, at ____________ am / pm.

Location items taken from: ____

Consenter Signature: ____

Witness Signature: ____

Witness Signature: ____

Form 1.1 Voluntary Consent to Search

Voluntary Consent to Search

I, _________________, do hereby, freely, voluntarily and without threat, pressure or coercion of any kind, consent to a warrantless search of my ______________

_______ (Location and description of premises to be searched), by representatives of ___________________ (Police Department or Agency) and individuals in their company. These representatives are authorized by me to seize any items, materials or other property which they may deem to be of possible evidentiary value.

____

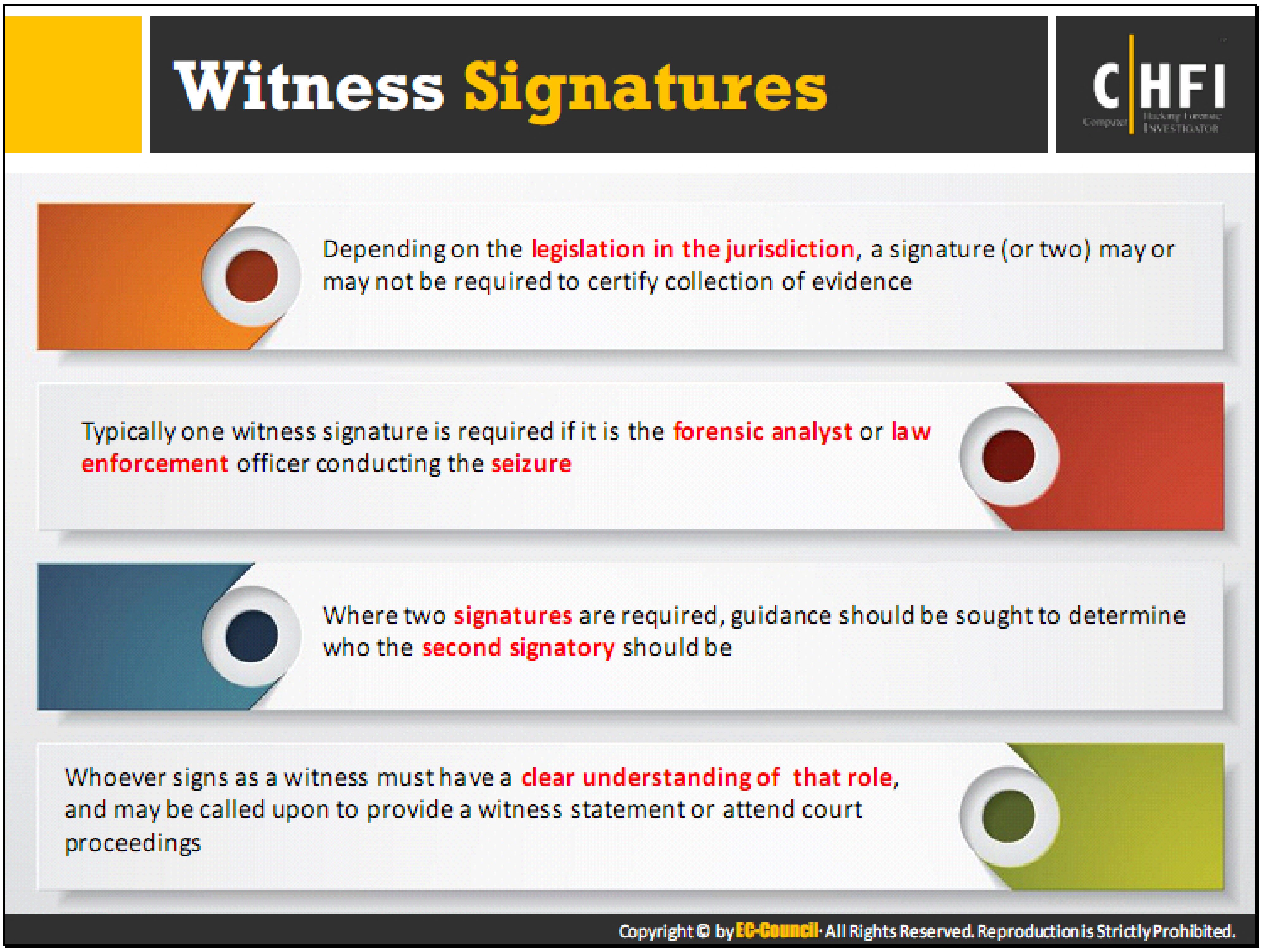
Witness Signature of person consenting to search

____

Witness Relationship to Premises being searched

DOB __________SSN _________________

Date __________Time_________________



Witness Signatures

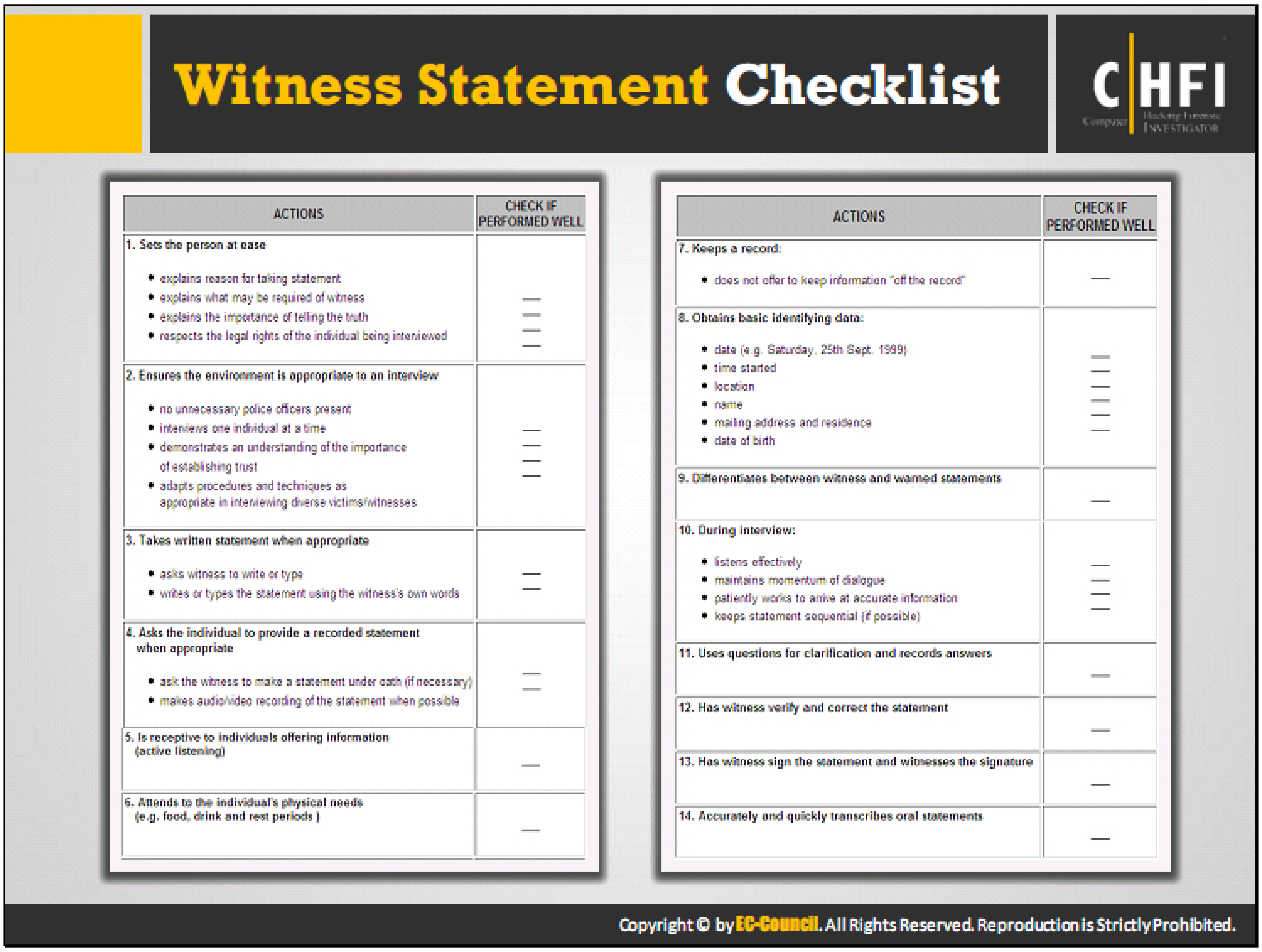
- Depending on the legislation in the jurisdiction, a signature (or two) may or may not be required to certify collection of evidence
- Typically one witness signature is required if it is the forensic analyst or law enforcement officer conducting the seizure
- Where two signatures are required, guidance should be sought to determine who the second signatory should be
- Whoever signs as a witness must have a clear understanding of that role, and may be called upon to provide a witness statement or attend court proceedings

A witness is a person who is present while signing a document or agreement and testifies that the parties mentioned in the agreement have voluntarily signed for it. Depending on the legislation in the jurisdiction, the agreement or contract needs the signatures of one or two witnesses.

Typically, one witness signature suffices if the forensic analyst or law enforcement officer is performing the seizure. When the case requires two witness signatures, seek guidance to determine the second signatory.

The witness signature verifies that the information in the consent form and other written documents are correct and have also been explained to and understood by the other party, and they had given the consent voluntarily.

Whoever signs as witness should have a clear understanding of their role and may have to provide a witness statement or attend court.

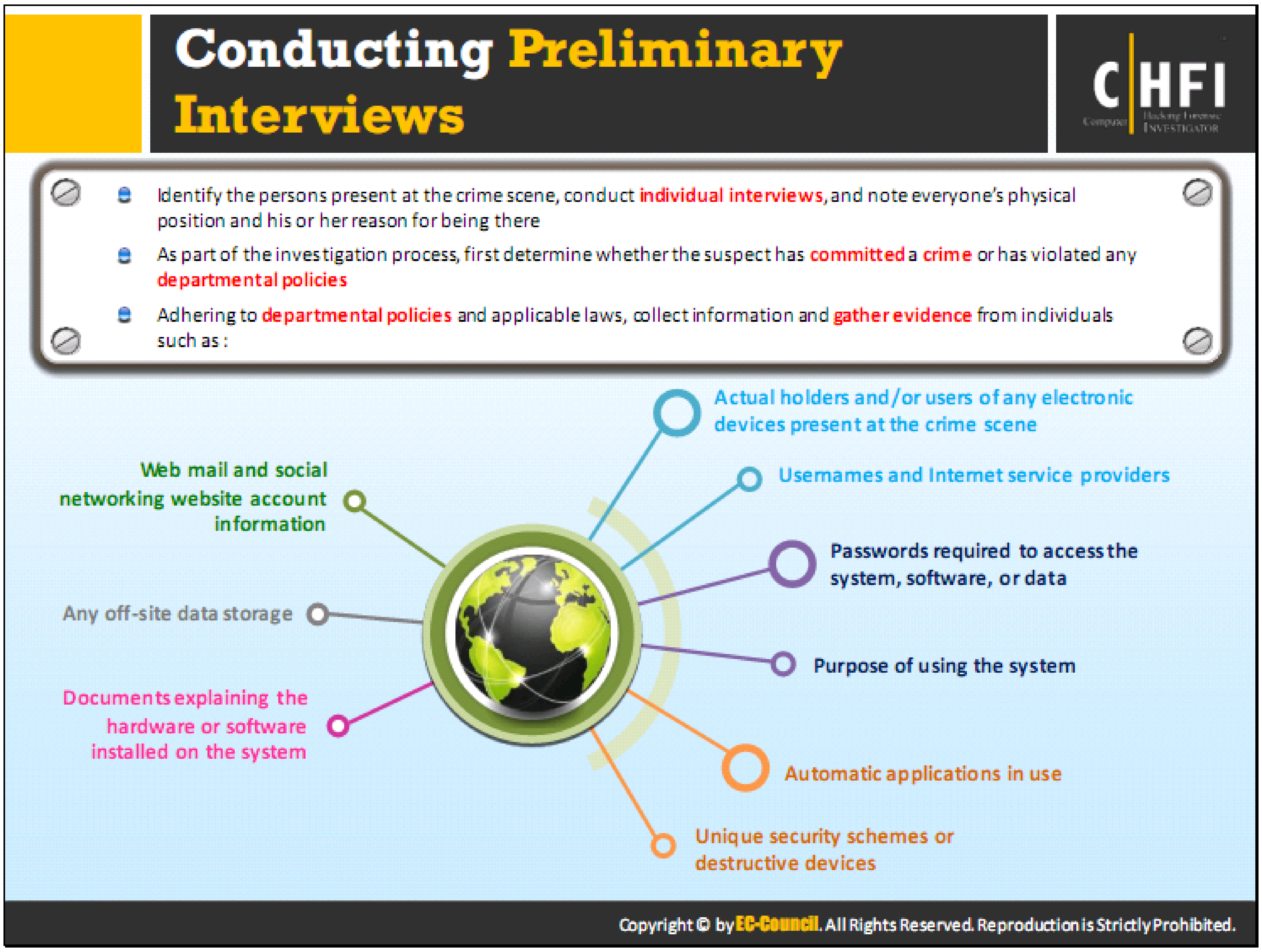


Witness Statement Checklist

CHFI
Computer Hacking Forensic INVESTIGATOR

ACTIONS	CHECK IF PERFORMED WELL
1. Sets the person at ease • explains reason for taking statement • explains what may be required of witness • explains the importance of telling the truth • respects the legal rights of the individual being interviewed	— — — —
2. Ensures the environment is appropriate to an interview • no unnecessary police officers present • interviews one individual at a time • demonstrates an understanding of the importance of establishing trust • adapts procedures and techniques as appropriate in interviewing diverse victims/witnesses	— — — —
3. Takes written statement when appropriate • asks witness to write or type • writes or types the statement using the witness's own words	— —
4. Asks the individual to provide a recorded statement when appropriate • ask the witness to make a statement under oath (if necessary) • makes audio/video recording of the statement when possible	— —
5. Is receptive to individuals offering information (active listening)	—
6. Attends to the individual's physical needs (e.g. food, drink and rest periods)	—

ACTIONS	CHECK IF PERFORMED WELL
7. Keeps a record: • does not offer to keep information "off the record"	—
8. Obtains basic identifying data: • date (e.g. Saturday, 25th Sept. 1999) • time started • location • name • mailing address and residence • date of birth	— — — — — —
9. Differentiates between witness and warned statements	—
10. During interview: • listens effectively • maintains momentum of dialogue • patiently works to arrive at accurate information • keeps statement sequential (if possible)	— — — —
11. Uses questions for clarification and records answers	—
12. Has witness verify and correct the statement	—
13. Has witness sign the statement and witnesses the signature	—
14. Accurately and quickly transcribes oral statements	—



Conducting Preliminary Interviews

- 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, first determine whether the suspect has committed a crime or has violated any departmental policies
- Adhering to departmental policies and applicable laws, collect information and gather evidence from individuals such as :

Actual holders and/or users of any electronic devices present at the crime scene

Usernames and Internet service providers

Passwords required to access the system, software, or data

Purpose of using the system

Automatic applications in use

Unique security schemes or destructive devices

Documents explaining the hardware or software installed on the system

Any off-site data storage

Web mail and social networking website account information

When preparing a case, Computer Forensic Professionals (CFPs) follow a standard system analysis to solve a problem. They start their investigation by collecting evidence and conducting preliminary interviews. As a part of their preliminary investigation, they enquire about all those who were present on the site at the time of the offense. After identifying the persons present at the time of the crime, they conduct individual interviews and recognize all personnel (witnesses and others) available at the crime scene and note down their position at the time of entry and their reason for being there.

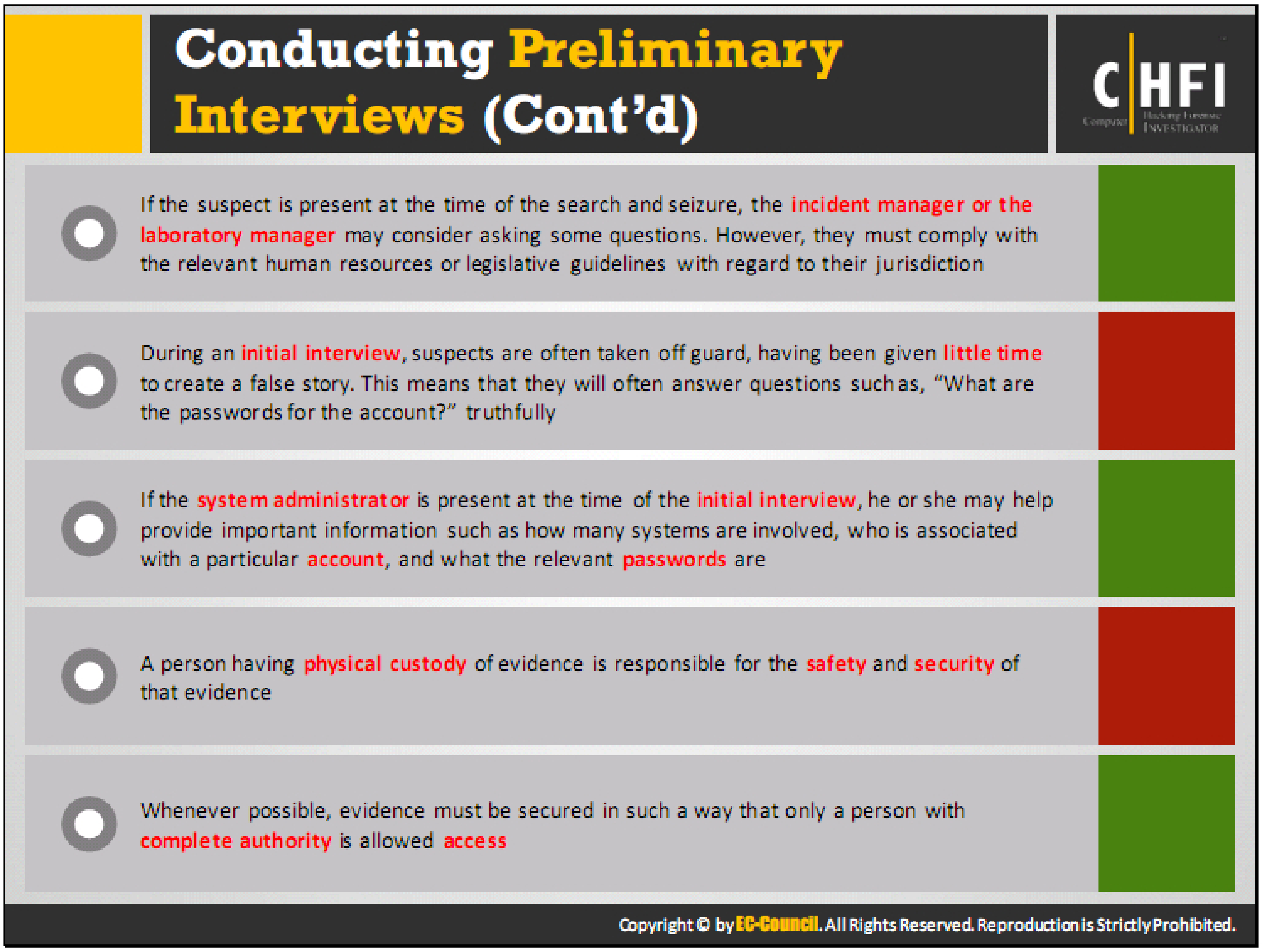
As part of their investigation process, CFPs first determine whether the suspect has committed a crime or has violated any departmental policies. Usually, departments establish certain policies regarding the usage of computers.

Consistent with departmental policies and applicable laws, the CFP gathers evidence and collects information from individuals, such as:

- Actual holders or users of any electronic devices present at the crime scene.
- Usernames and Internet service provider.
- Passwords required to access the system, software, or data.
- Purpose of using the system.
- Automatic applications in use.
- Any offsite data storage.

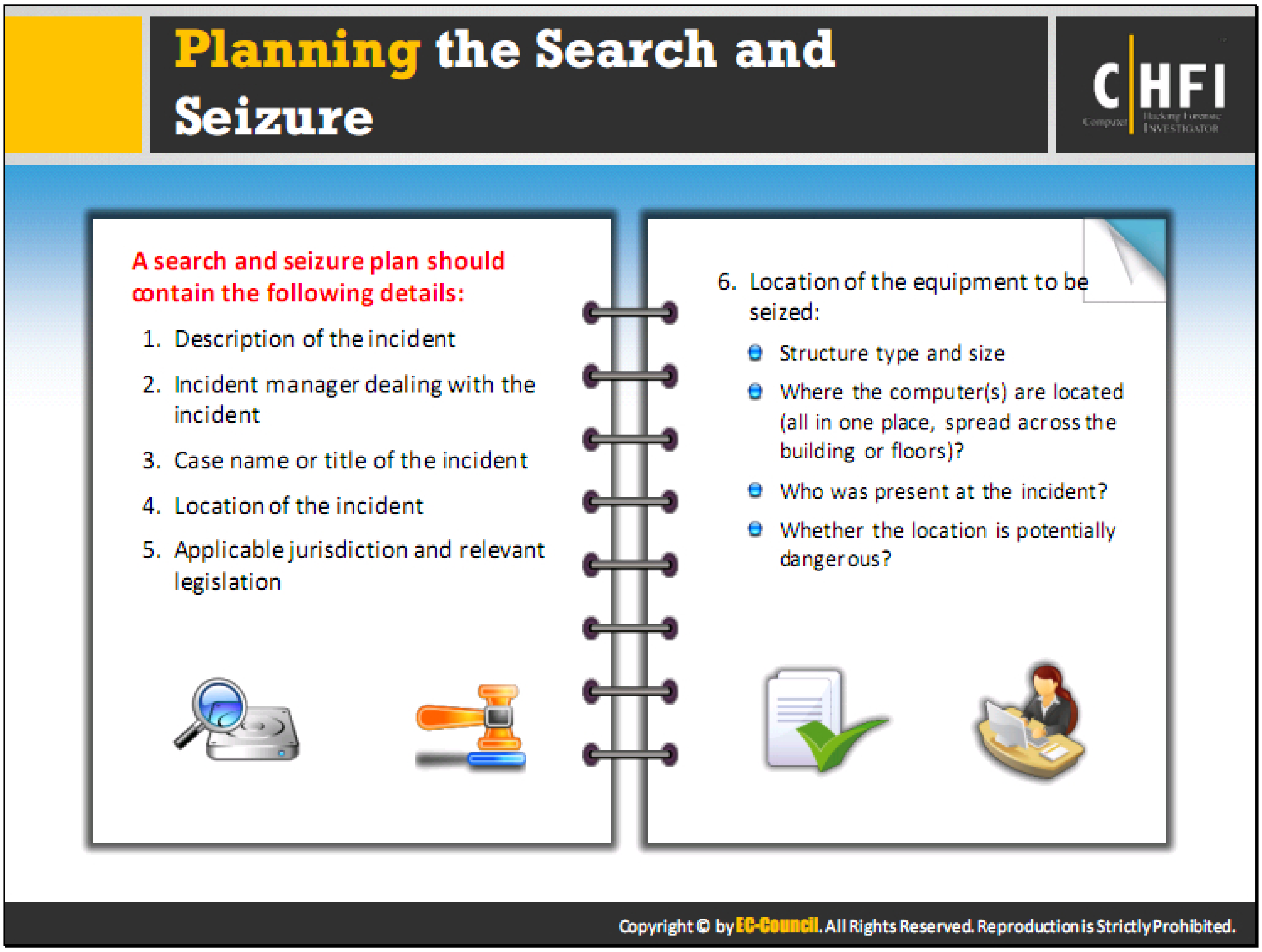
- Unique security schemes or destructive devices.
- Documents detailing installation of a hardware or software on the system.
- Any offsite data storage.
- Web mail and social networking website account information.

If the evidence gathered by the CFP suggests that the suspect has committed a crime, he or she will produce that evidence in court. If the evidence suggests that the suspect has breached company policy, the CFP will hand over the evidence at the corporate enquiry.



Conducting Preliminary Interviews (Cont'd)

- If the suspect is present at the time of the search and seizure, the incident manager or the laboratory manager may consider asking some questions. However, they must comply with the relevant human resources or legislative guidelines with regard to their 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 questions such as, "What are the passwords for the account?" truthfully
- If the system administrator is present at the time of the initial interview, he or she may help provide important information such as how many systems are involved, who is associated with a particular account, and what the relevant passwords are
- A person having physical custody of evidence is responsible for the safety and security of that evidence
- Whenever possible, evidence must be secured in such a way that only a person with complete authority is allowed access

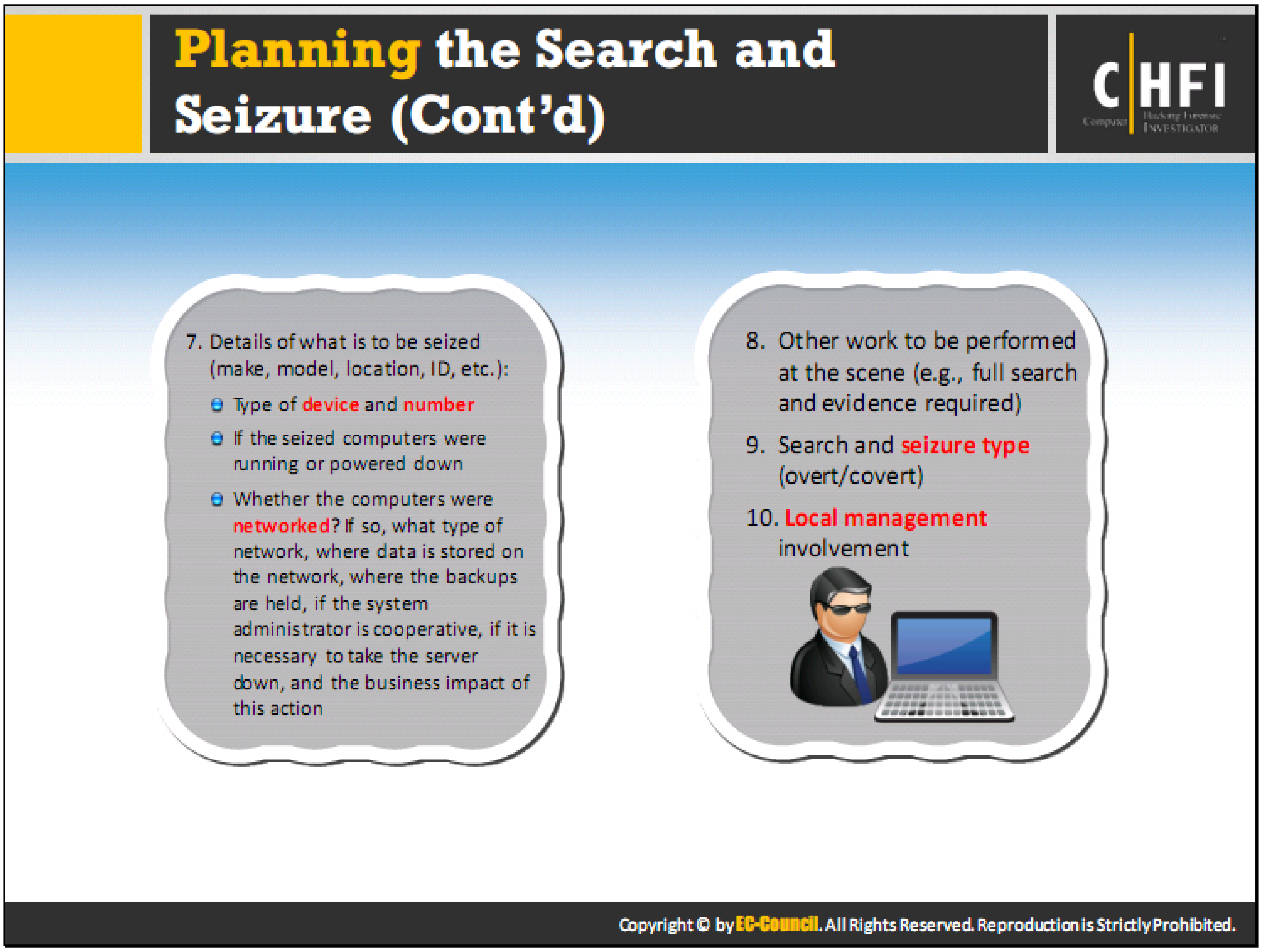


Planning the Search and Seizure

A search and seizure plan should contain the following details:

1. Description of the incident
2. Incident manager dealing with the incident
3. Case name or title of the incident
4. Location of the incident
5. Applicable jurisdiction and relevant legislation
6. Location of the equipment to be seized:
   - Structure type and size
   - Where the computer(s) are located (all in one place, spread across the building or floors)?
   - Who was present at the incident?
   - Whether the location is potentially dangerous?

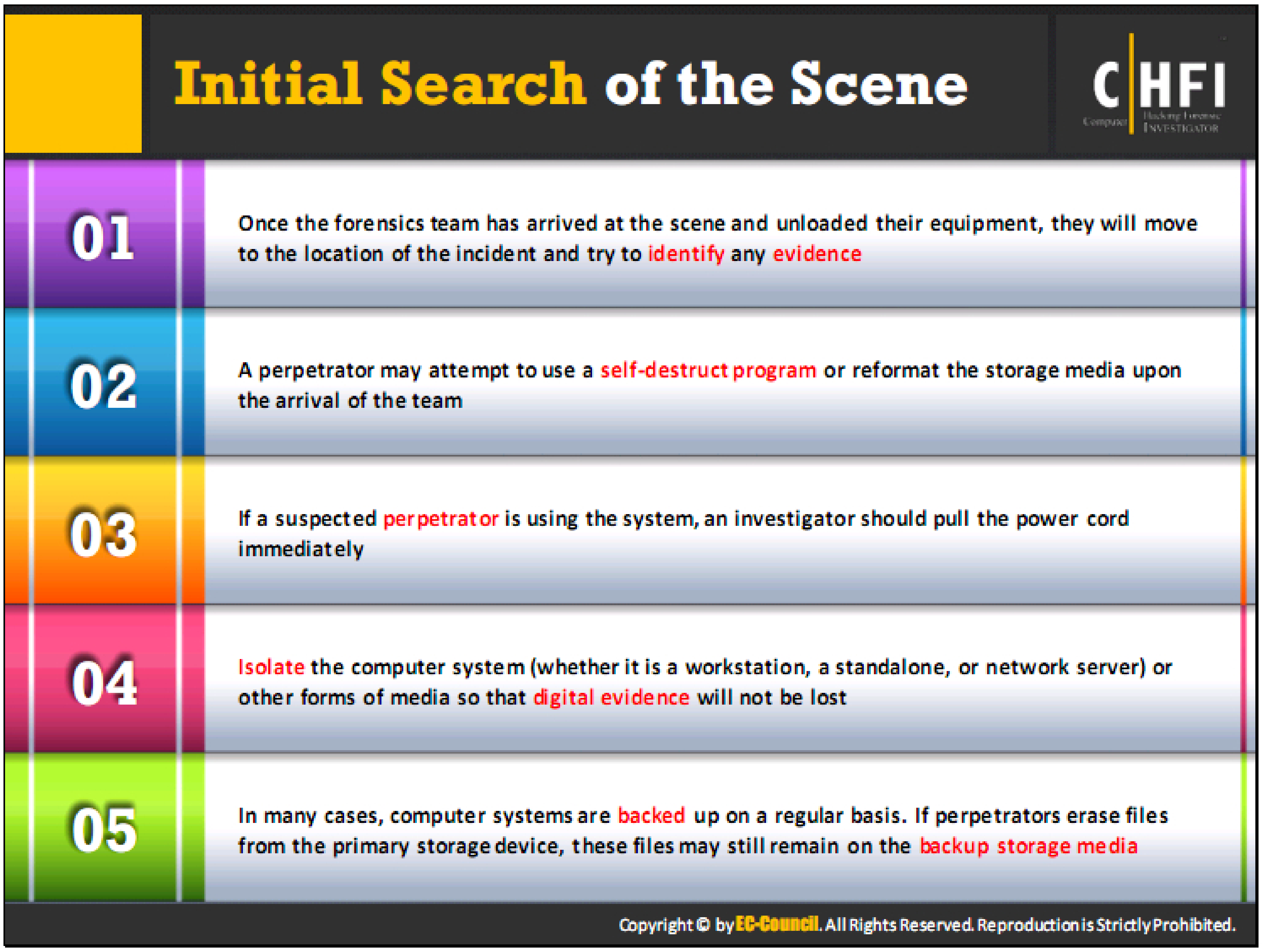
The investigators need to design a strategic process to conduct the search and seizure process after analyzing the crime scene. This will help them distribute tasks between the team members to complete the seizure and allow the team to use time and tools in a well-defined manner.



Planning the Search and Seizure (Cont'd)

7. Details of what is to be seized (make, model, location, ID, etc.):
   - Type of device and number
   - If the seized computers were running or powered down
   - Whether the computers were networked? If so, what type of network, where data is stored on the network, where the backups are held, if the system administrator is cooperative, if it is necessary to take the server down, and the business impact of this action

8. Other work to be performed at the scene (e.g., full search and evidence required)
9. Search and seizure type (overt/covert)
10. Local management involvement



Initial Search of the Scene

01 Once the forensics team has arrived at the scene and unloaded their equipment, they will move to the location of the incident and try to identify any evidence

02 A perpetrator may attempt to use a self-destruct program or reformat the storage media upon the arrival of the team

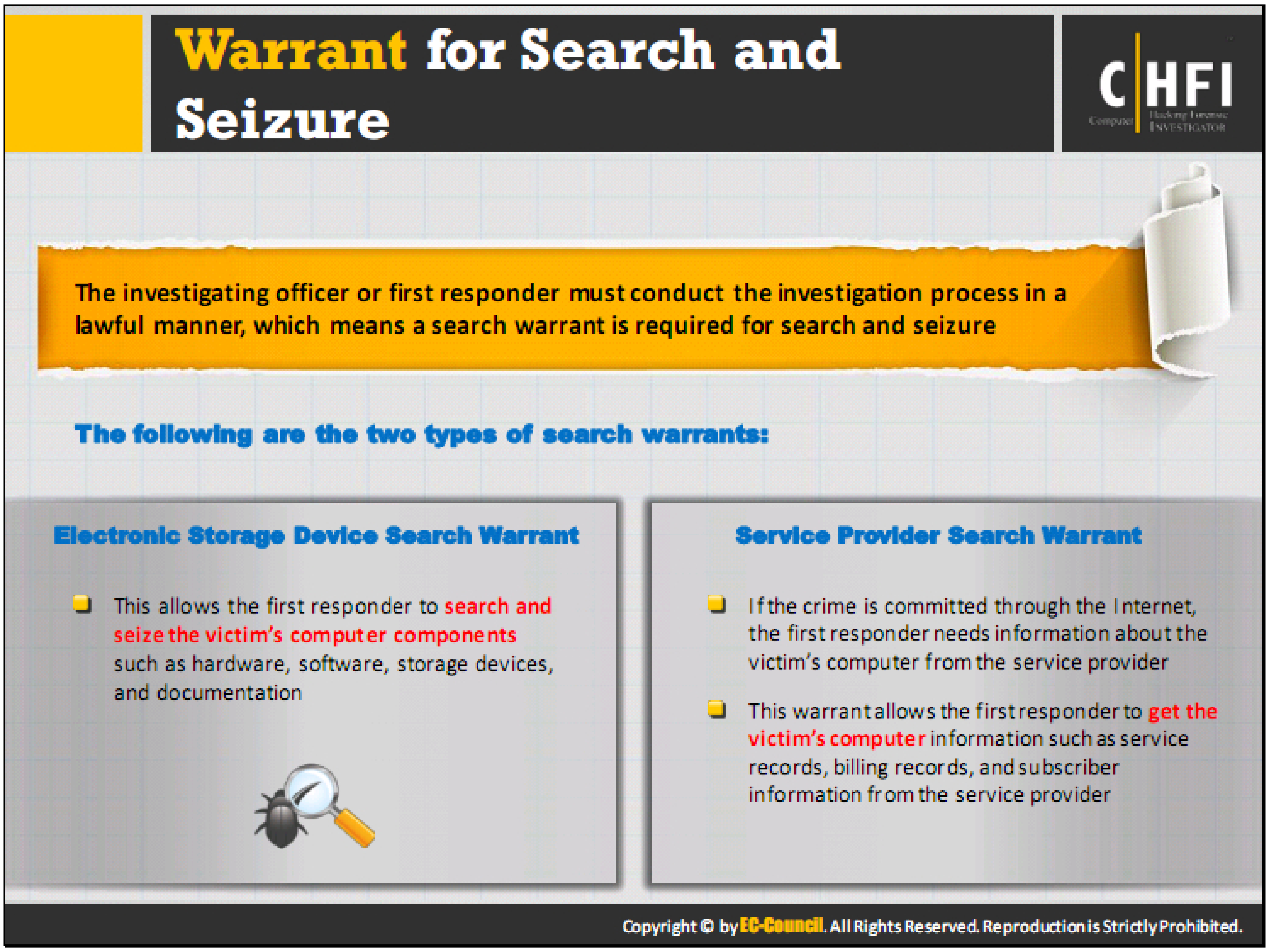
03 If a suspected perpetrator is using the system, an investigator should pull the power cord immediately

04 Isolate the computer system (whether it is a workstation, a standalone, or network server) or other forms of media so that digital evidence will not be lost

05 In many cases, computer systems are backed up on a regular basis. If perpetrators erase files from the primary storage device, these files may still remain on the backup storage media

Once the forensic team has arrived at the scene and unloaded their equipment, they will move to the scene of the incident and try to identify any evidence. A perpetrator may use a self-destruct program or reformat the storage media upon the arrival of the team. To account for such possibilities, pull the power cord connected to the central processing system immediately.

- Identify, collect, label, preserve, and protect all digital evidence at the scene.
- Isolate the computer system (workstation, standalone, or network server) or other forms of media so that digital evidence will not be lost.
- In many cases, computer systems create backups on a regular basis. Though an attacker might delete files from the primary storage media, these files could still exist on the backup storage media.
- Include a search and seizure evidence log containing brief descriptions of all computers, devices, or media located during the search for evidence.
- Make a note of the locations on the crime scene sketch as well.
- Photograph and sketch the crime scene, along with a detailed account of all computer evidence.
- Document everything at the crime scene and the location where the evidence is found.
- Pack and transport the digital evidence safely.



Warrant for Search and Seizure

The investigating officer or first responder must conduct the investigation process in a lawful manner, which means a search warrant is required for search and seizure

The following are the two types of search warrants:

Electronic Storage Device Search Warrant

- This allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation

Service Provider Search Warrant

- If the crime is committed through the Internet, the first responder needs information about the victim's computer from the service provider
- This warrant allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider

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

The investigating officer or first responder must perform the investigation process in a lawful manner; otherwise, a court of law will reject the collected evidence. The first responder needs a search warrant for search and seizure of the electronic devices. A search warrant is a written permission from a concerned authority that mentions the electronic devices that the investigating officer or the first responder can search and seize. The court of law can also issue a search warrant. A magistrate may issue the search warrant if the first responder has convinced the magistrate of evidence of a crime.

Search warrants for electronic devices focus on the following:

Electronic storage device search warrant

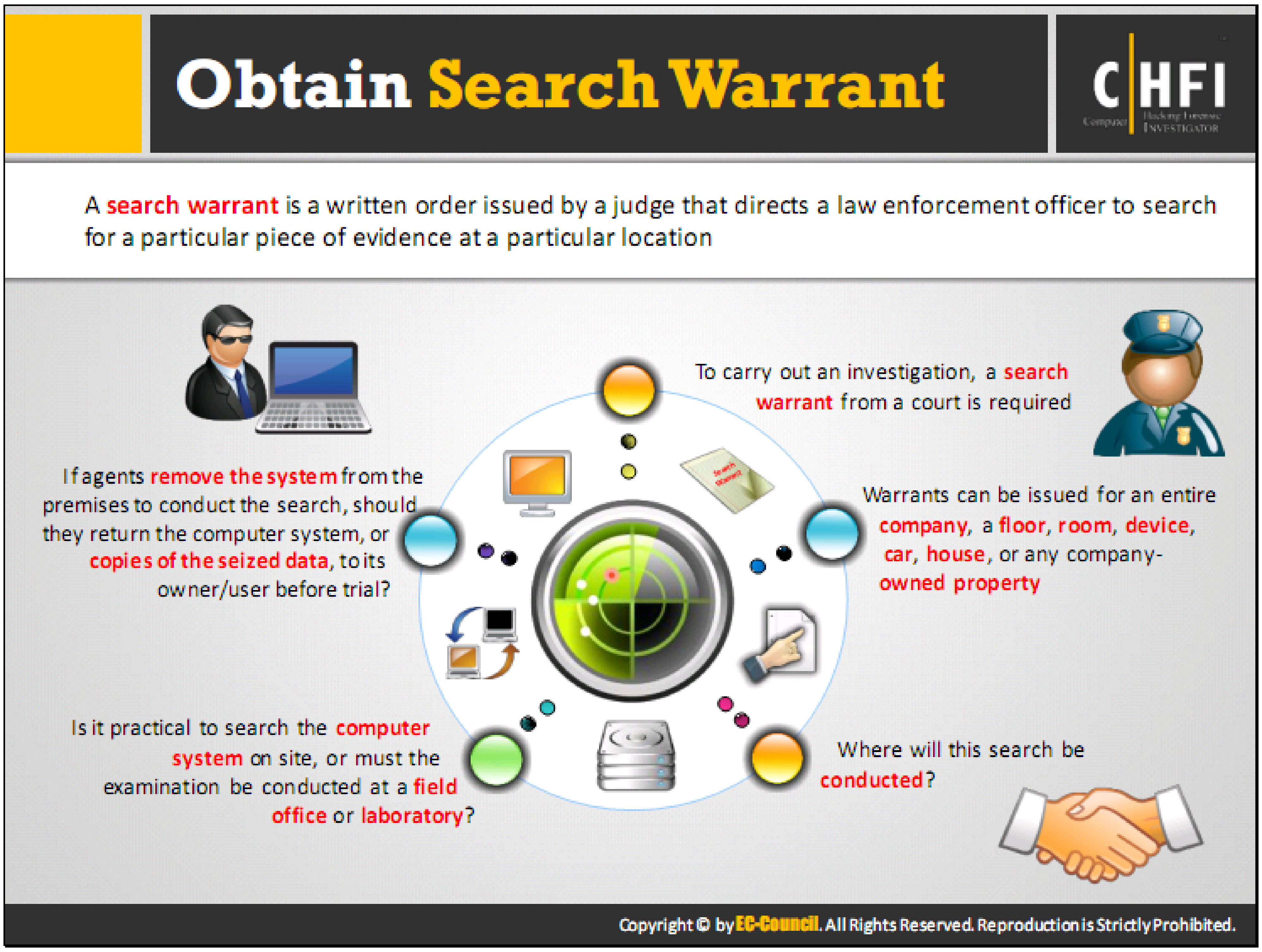
An electronic storage device search warrant allows the first responder to search and seize the victim's computer components such as:

- Hardware
- Software
- Storage devices
- Documentation

Service provider search warrant

If the crime involves the Internet, the first responder needs information about the victim's computer from the service provider end. A service provider search warrant allows first responders or investigators to consult the service provider and obtain the available victim's computer information. First responders can obtain the following information from the service provider:

- Service records
- Billing records
- Subscriber information



Obtain Search Warrant

A search warrant is a written order issued by a judge that directs a law enforcement officer to search for a particular piece of evidence at a particular location

To carry out an investigation, a search warrant from a court is required

Warrants can be issued for an entire company, a floor, room, device, car, house, or any company-owned property

Where will this search be conducted?

Is it practical to search the computer system on site, or must the examination be conducted at a field office or laboratory?

If agents remove the system from the premises to conduct the search, should they return the computer system, or copies of the seized data, to its owner/user before trial?

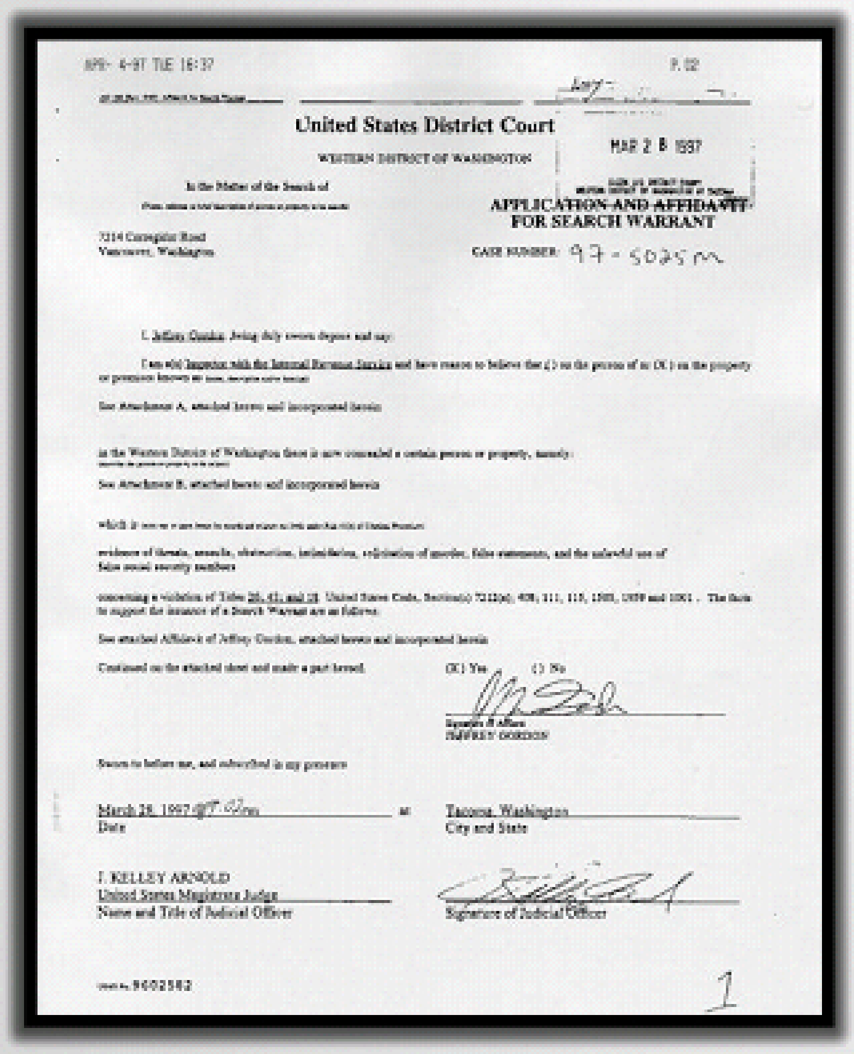
An investigator can perform the investigation once investigation planning is over. It is advisable to perform some legal formalities, such as obtaining a search warrant to perform the investigation from the court. Successful computer search warrants should include the particulars of the objects that investigators want to seize, and the search strategy used in the investigation. These steps help the examiner in focusing and executing the search in a better way.

Depending upon the situation of the case, the warrant can include:

- Entire company or part of the company's property
- Floor
- Room
- Car or any Device
- House

The proposed warrant is a one-page form along with attachments incorporated by reference, which indicates the person or things the investigators need to seize and the place they will search. If the investigators mention the cause of search, elements that come under search, and the information about the place of search properly, then the judge will sign the warrant. Under the federal rules of criminal procedure, the warrant is valid for ten days from the day of signing.

Example of Search Warrant



APR- 4-97 TUE 16:37 P.02

AO 106 (Rev. 7/87) Affidavit for Search Warrant

MAR 2 8 1997
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA

United States District Court

WESTERN DISTRICT OF WASHINGTON

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

7214 Corregidor Road
Vancouver, Washington

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 97-5025M

I, Jeffrey Gordon being duly sworn depose and say:

I am a(n) Inspector with the Internal Revenue Service and have reason to believe that ( ) on the person of or (X) on the property or premises known as (name, description and/or location)

See Attachment A, attached hereto and incorporated herein

in the Western District of Washington there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment B, attached hereto and incorporated herein

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of threats, assaults, obstruction, intimidation, solicitation of murder, false statements, and the unlawful use of false social security numbers

concerning a violation of Titles 26, 42, and 18 United States Code, Section(s) 7212(a), 408, 111, 115, 1503, 1959 and 1001. The facts to support the issuance of a Search Warrant are as follows:

See attached Affidavit of Jeffrey Gordon, attached hereto and incorporated herein

Continued on the attached sheet and made a part hereof. (X) Yes ( ) No

Signature of Affiant
JEFFREY GORDON

Sworn to before me, and subscribed in my presence

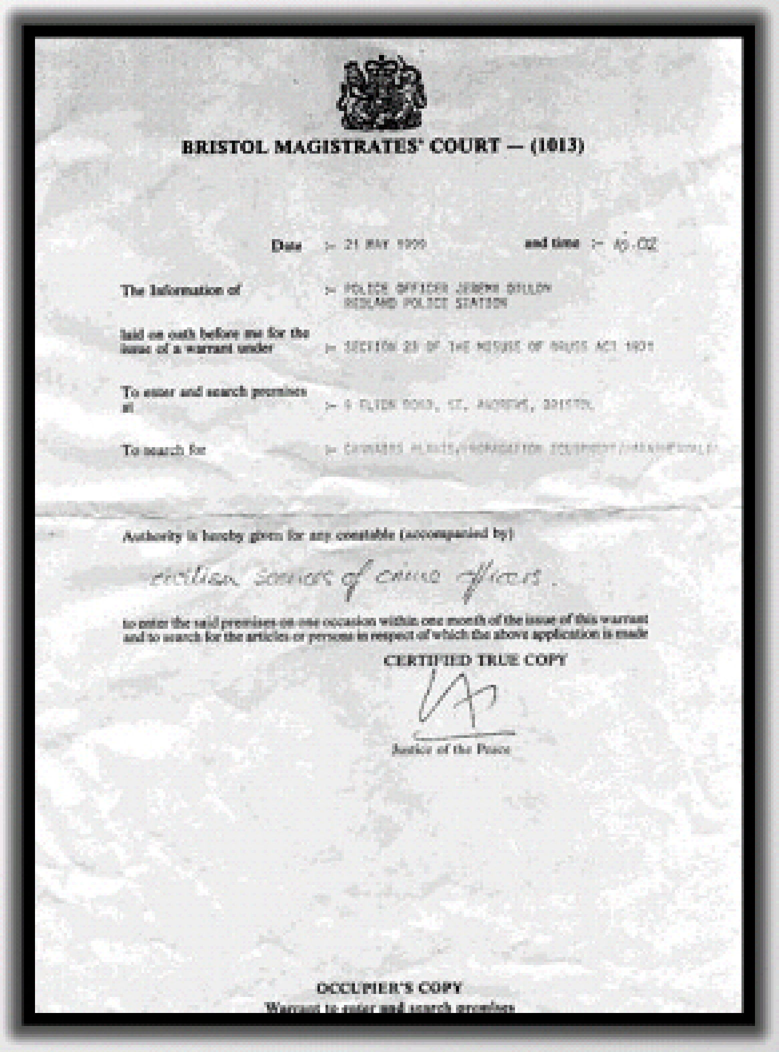
March 28, 1997 @ 7:02pm at Tacoma, Washington
Date City and State

J. KELLEY ARNOLD
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

9602582

1



BRISTOL MAGISTRATES' COURT — (1013)

Date :- 21 MAY 1999 and time :- 15.02

The Information of :- POLICE OFFICER JEREMY DILLON
REDLAND POLICE STATION

laid on oath before me for the issue of a warrant under :- SECTION 23 OF THE MISUSE OF DRUGS ACT 1971

To enter and search premises at :- 6 ELTON ROAD, ST. ANDREWS, BRISTOL

To search for :- CANNABIS PLANTS/PROPAGATION EQUIPMENT/PARAPHERNALIA

Authority is hereby given for any constable (accompanied by)

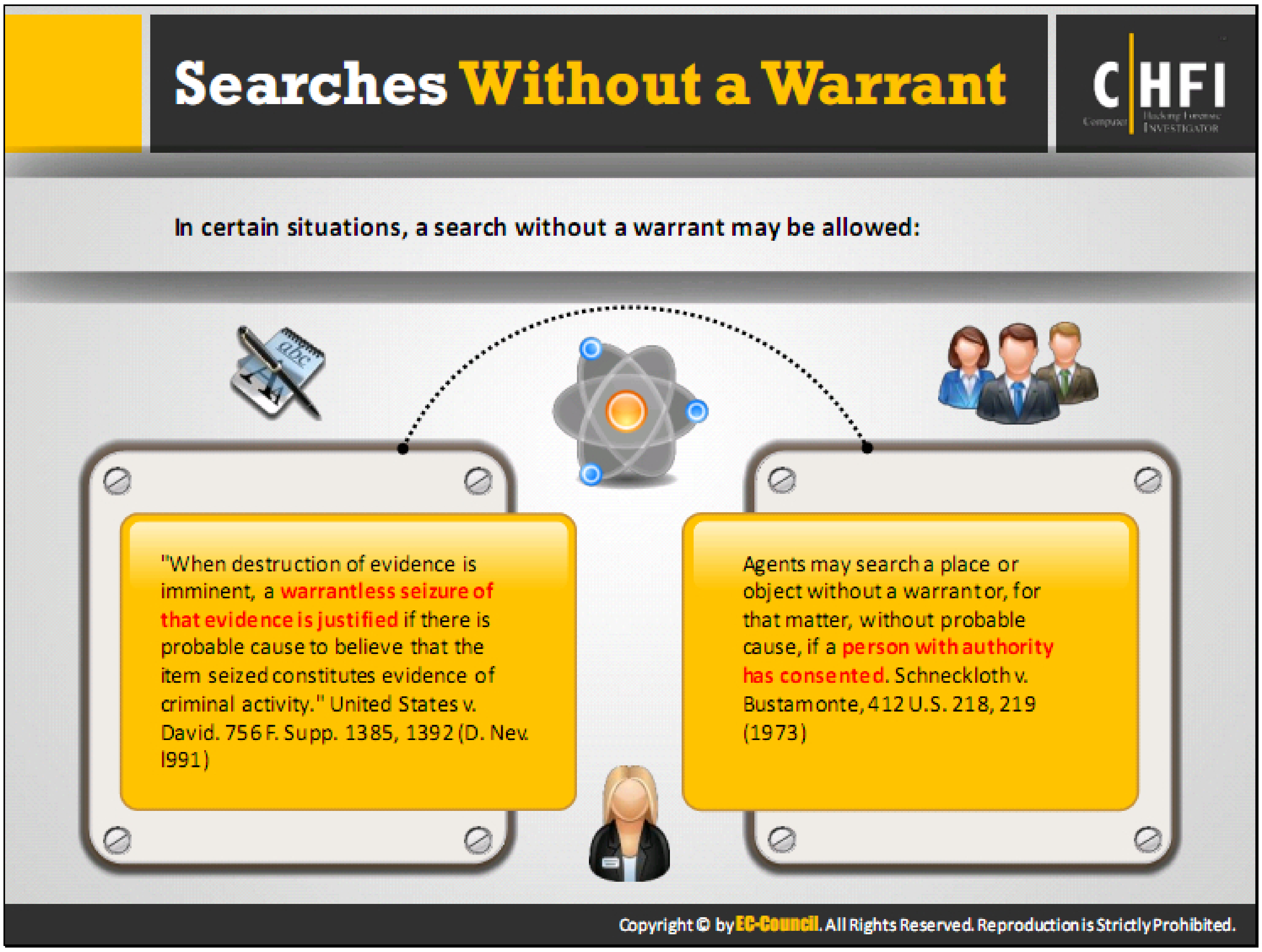
civilian scenes of crime officers.

to enter the said premises on one occasion within one month of the issue of this warrant and to search for the articles or persons in respect of which the above application is made

CERTIFIED TRUE COPY

Justice of the Peace

OCCUPIER'S COPY
Warrant to enter and search premises



Searches Without a Warrant

CHFI
Computer Hacking Forensic Investigator

In certain situations, a search without a warrant may be allowed:

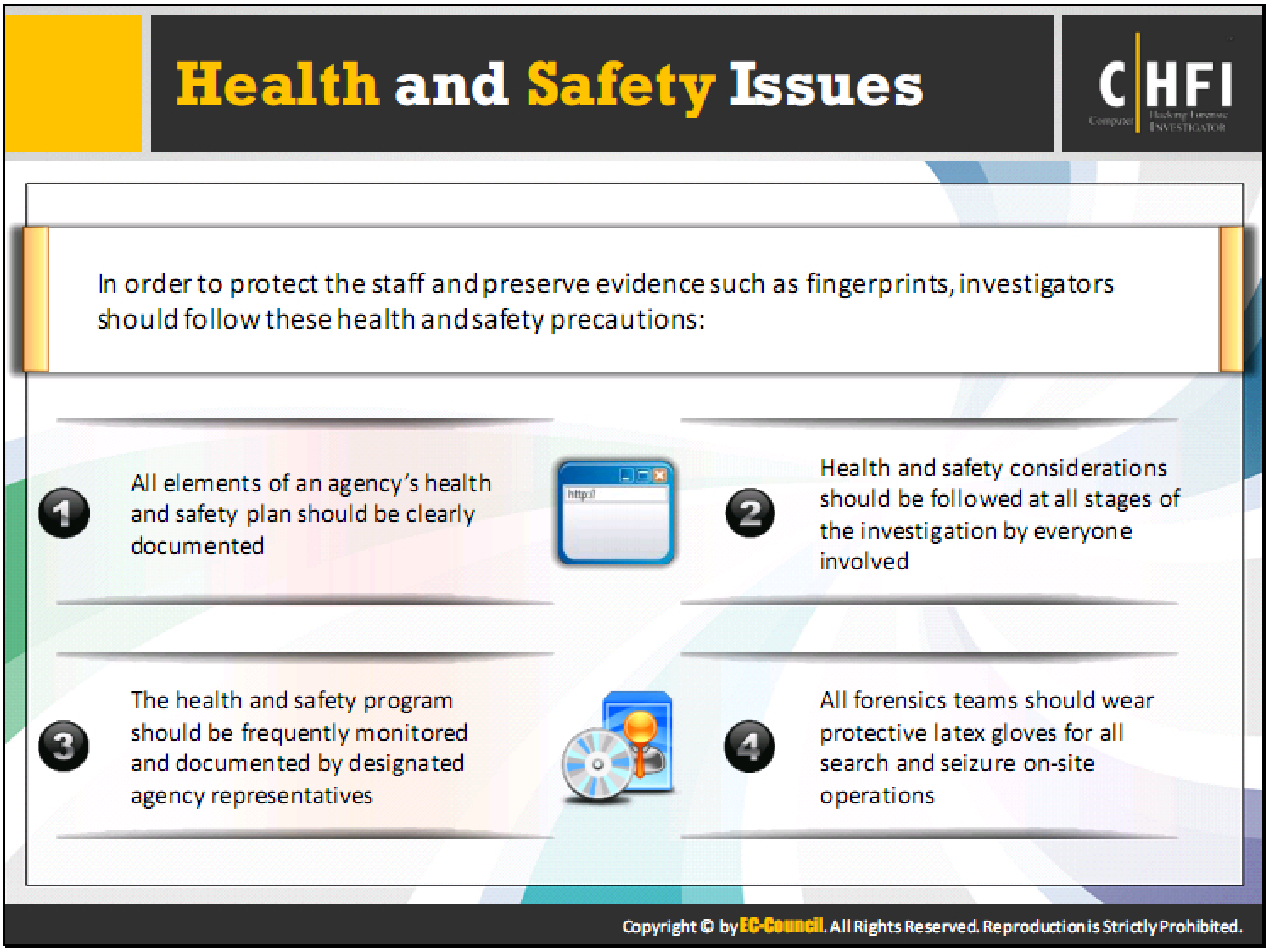
"When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity." United States v. David. 756 F. Supp. 1385, 1392 (D. Nev. I991)

Agents may search a place or object without a warrant or, for that matter, without probable cause, if a person with authority has consented. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)

The court of law has allowed the investigators to perform searches without a warrant, but under certain circumstances, such as when the delay in obtaining a warrant may lead to the destruction or manipulation of evidence and hamper the investigation process. The following pronouncements of different U.S. courts have set the precedents for searches without a warrant:

“When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity.” United States v. David, 756 F. Supp. 1385, 1392 (D. Nev. I991).

Agents may search a place or object without a warrant or probable cause, if a person with authority has consented. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).



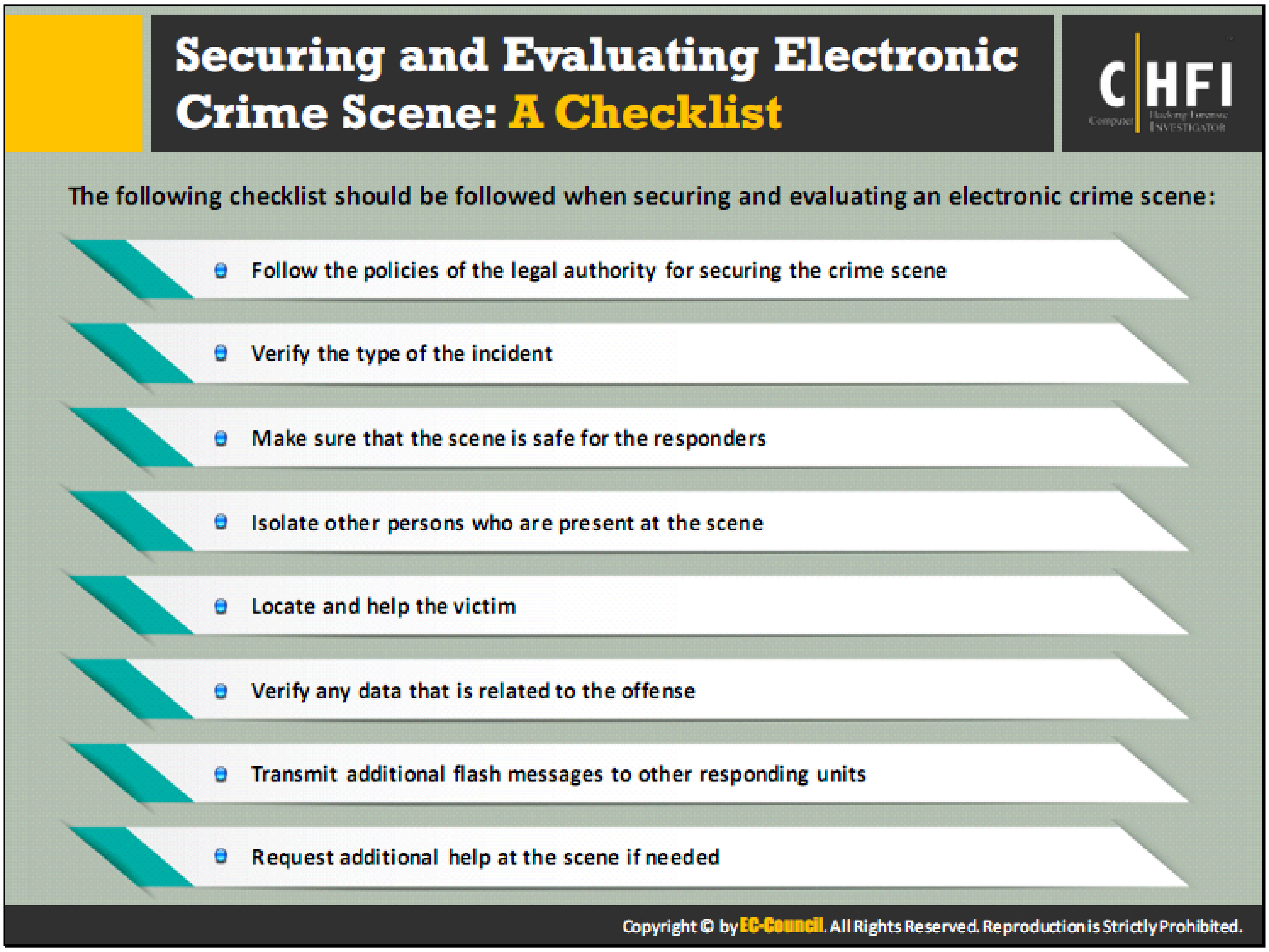
Health and Safety Issues

In order to protect the staff and preserve evidence such as fingerprints, investigators should follow these health and safety precautions:

1. All elements of an agency's health and safety plan should be clearly documented
2. Health and safety considerations should be followed at all stages of the investigation by everyone involved
3. The health and safety program should be frequently monitored and documented by designated agency representatives
4. All forensics teams should wear protective latex gloves for all search and seizure on-site operations

The health and safety issues are:

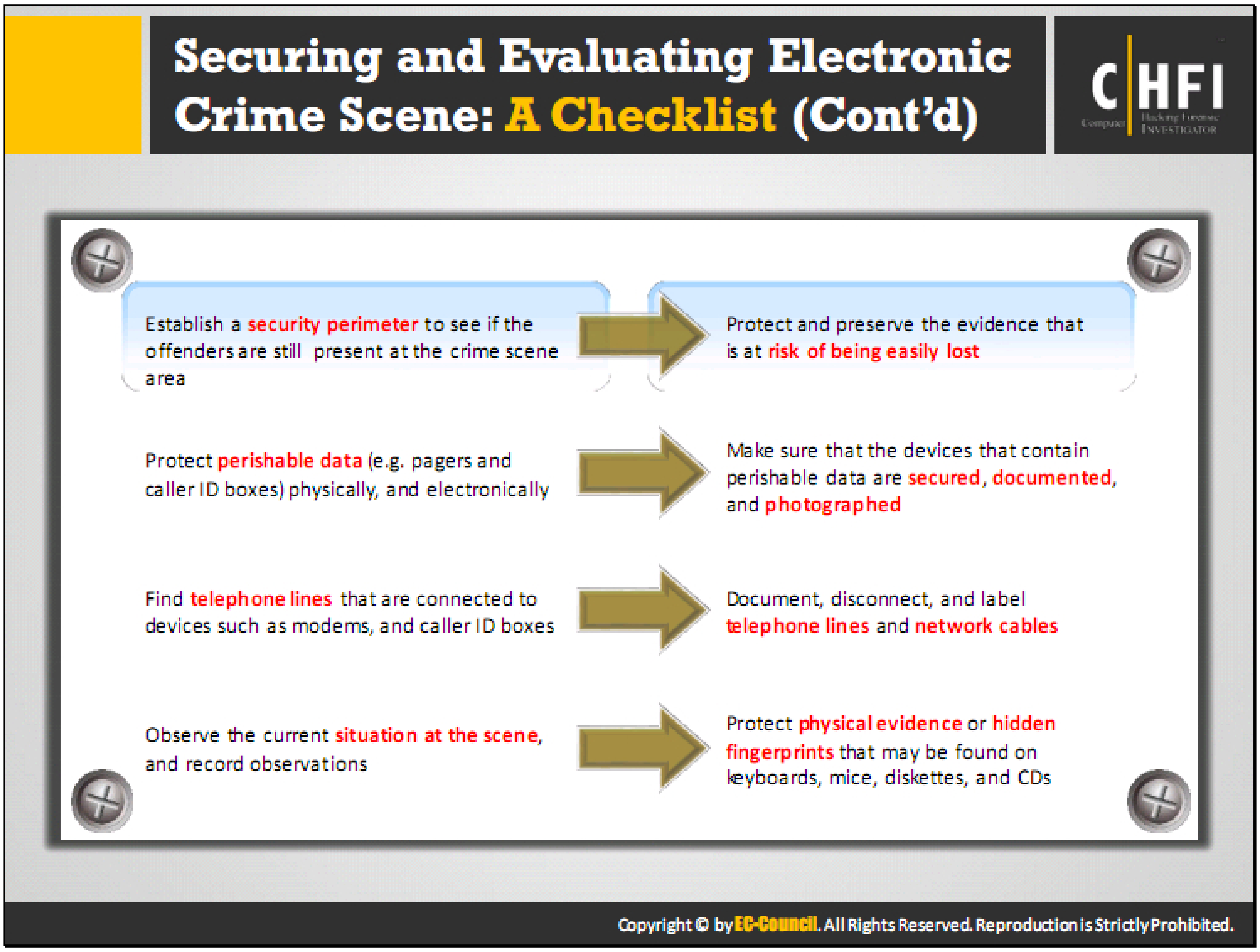
- Clearly document all elements of an agency's health and safety plan.
- Designated agency representatives should frequently monitor and document the health and safety program.
- Health and safety issues are important in all of the work carried out in all phases of the forensic procedures performed by the forensic analysts.
- Persons engaged in the inspection of different types of digital evidence should work according to the rules and policies of the agency.
- All forensic teams should wear protective latex gloves for all searching and seizing operations onsite. This is to both protect the staff and preserve any fingerprints that may come handy in future.



Securing and Evaluating Electronic Crime Scene: A Checklist

The following checklist should be followed when securing and evaluating an electronic crime scene:

- Follow the policies of the legal authority for securing the crime scene
- Verify the type of the incident
- Make sure that the scene is safe for the responders
- Isolate other persons who are present at the scene
- Locate and help the victim
- Verify any data that is related to the offense
- Transmit additional flash messages to other responding units
- Request additional help at the scene if needed



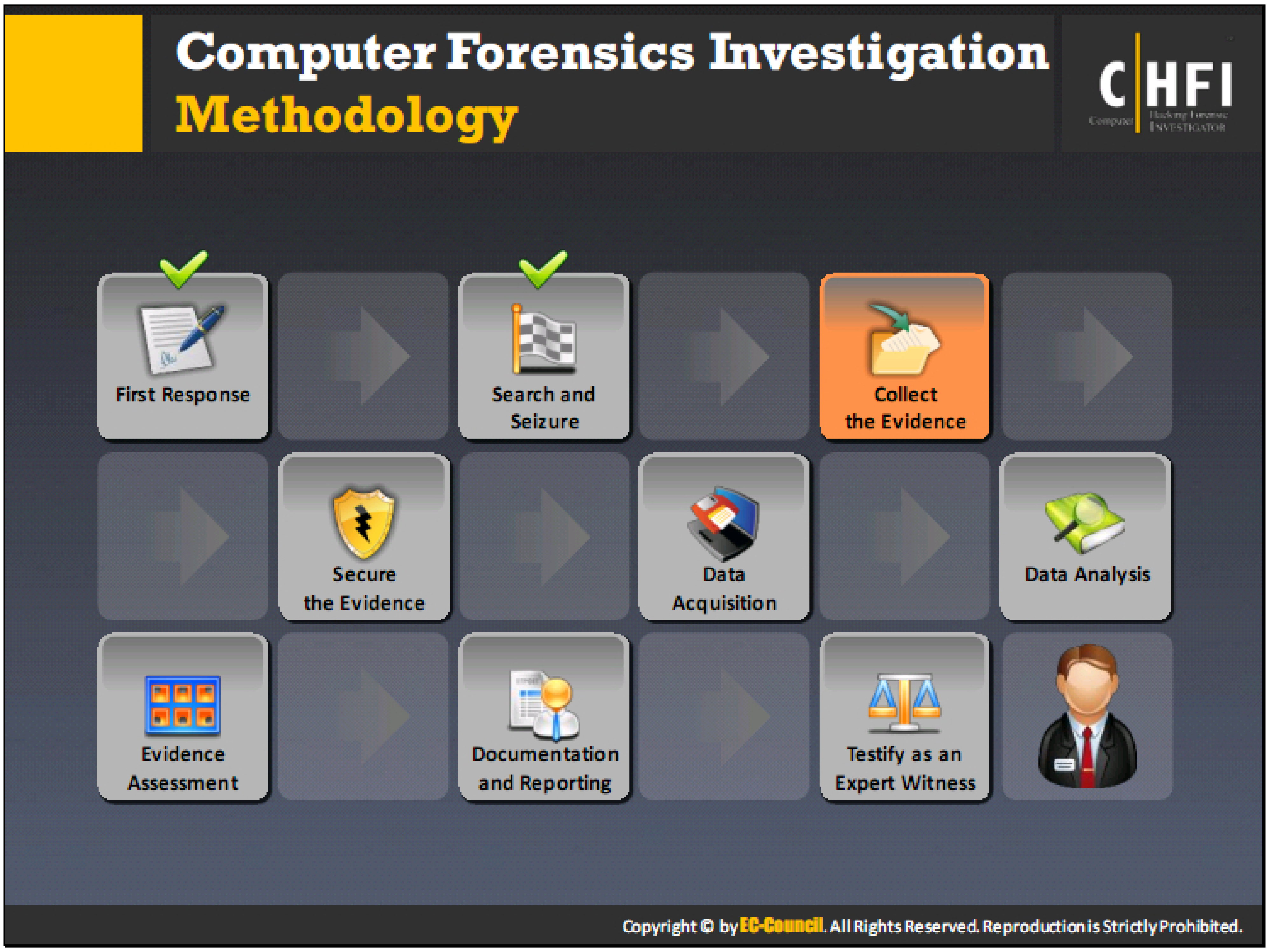
Securing and Evaluating Electronic Crime Scene: A Checklist (Cont'd)

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 → Make sure that the devices that contain perishable data are secured, documented, and photographed

Find 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 CDs



Computer Forensics Investigation Methodology

First Response

Search and Seizure

Collect the Evidence

Secure the Evidence

Data Acquisition

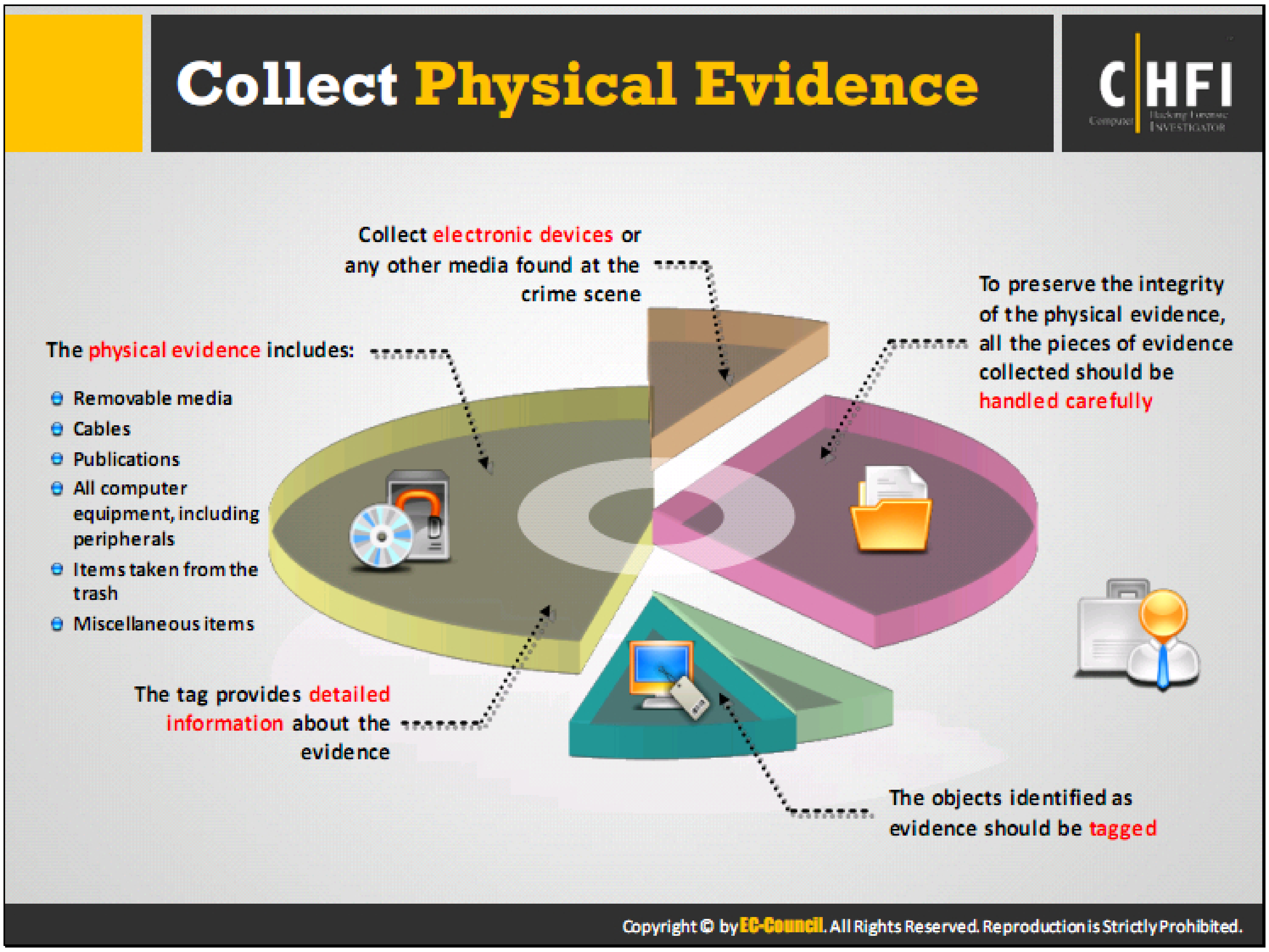
Data Analysis

Evidence Assessment

Documentation and Reporting

Testify as an Expert Witness

Evidence is the crucial data that can help investigators in understanding the process of attack and tracing the attacker. Therefore, the investigators should know where they can find the evidence and how to gather it. This section will discuss the process of collecting evidence from various devices and media.



Collect Physical Evidence

Collect electronic devices or any other media found at the crime scene

To preserve the integrity of the physical evidence, all the pieces of evidence collected should be handled carefully

The physical evidence includes:

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

The tag provides detailed information about the evidence

The objects identified as evidence should be tagged

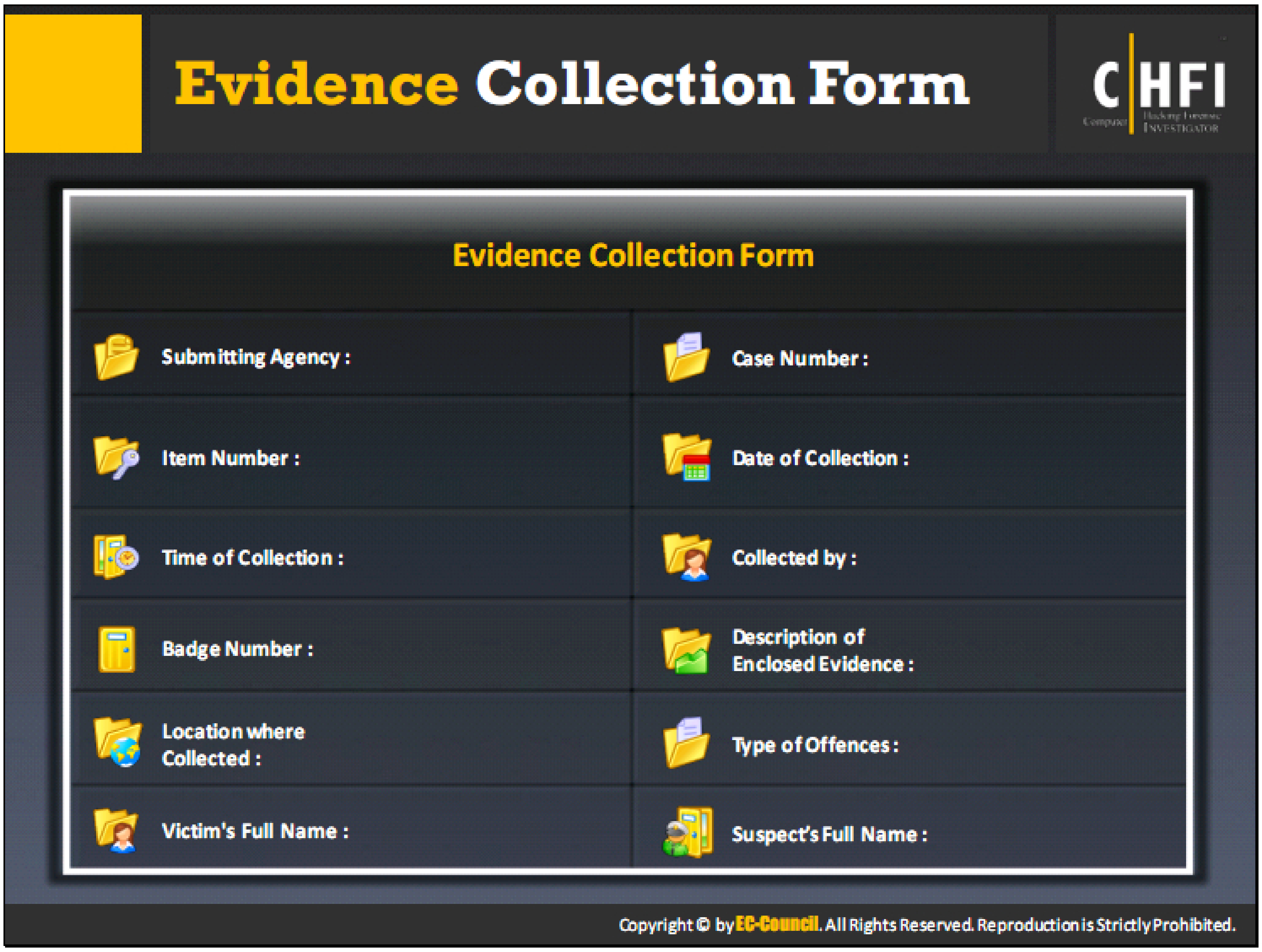
The victim computer and its elements are vital evidence sources in a computer forensic investigation. Collect all the electronic devices or any other media found at the crime scene. Seize storage devices like hard drives, memory cards, and removable media as they can have stored information. Handheld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

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 time, date, investigator's name, and control number.

The physical evidence should include:

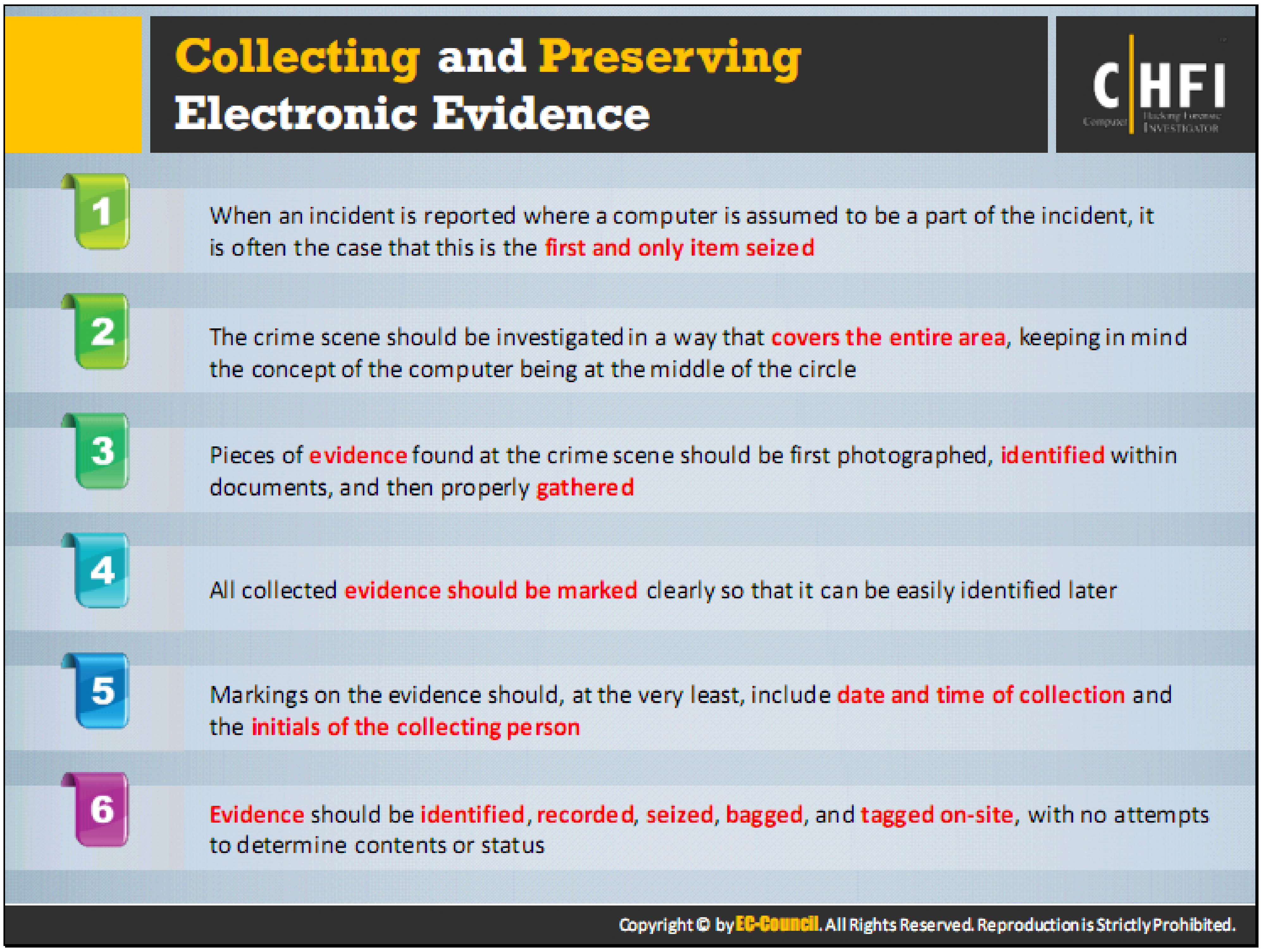
- Removable media
- Cables
- Publications
- All computer equipment including peripherals
- Items taken from the trash
- Miscellaneous items



Evidence Collection Form

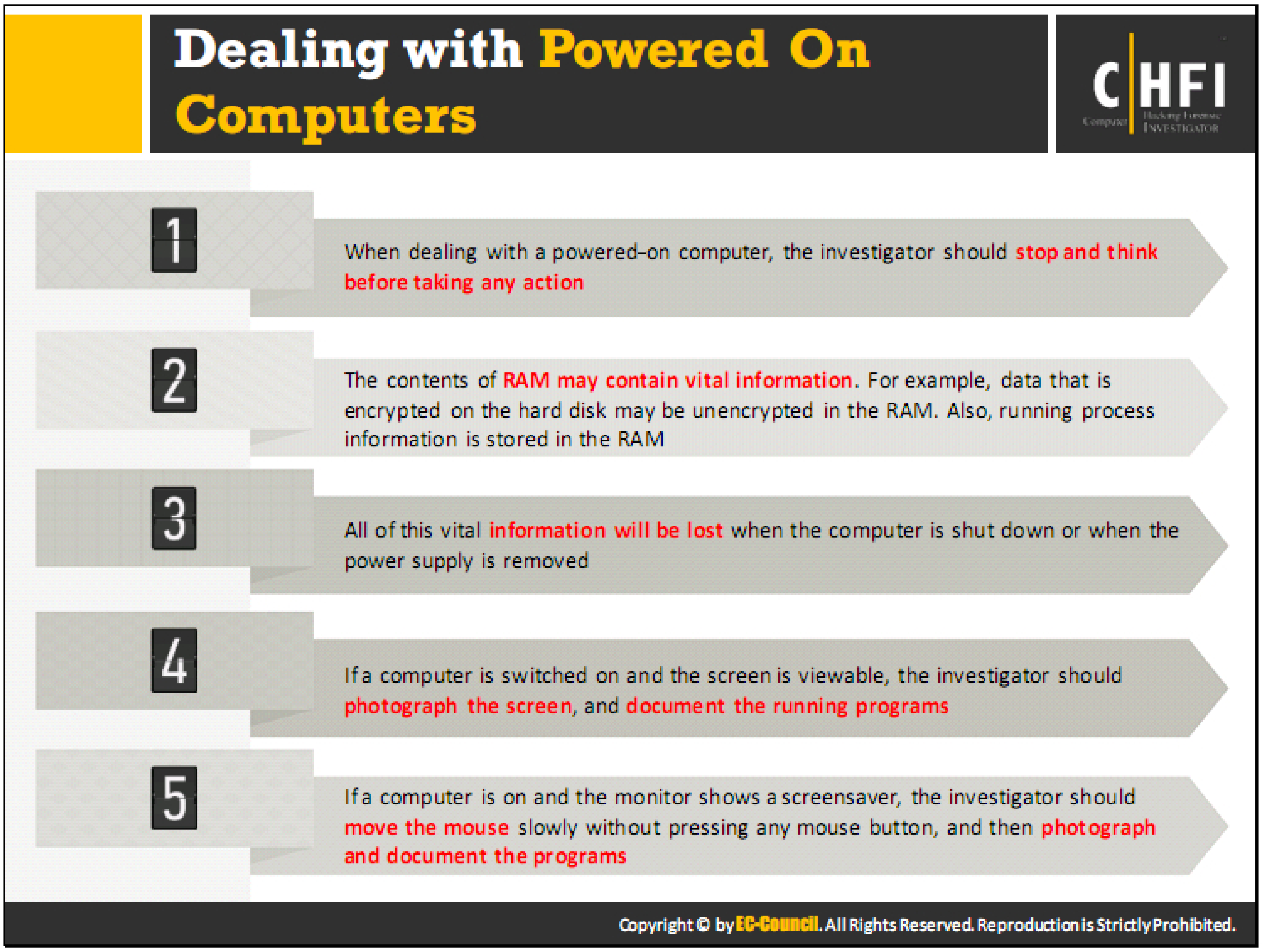
Evidence Collection Form

Submitting Agency :	Case Number :
Item Number :	Date of Collection :
Time of Collection :	Collected by :
Badge Number :	Description of Enclosed Evidence :
Location where Collected :	Type of Offences :
Victim's Full Name :	Suspect's Full Name :



Collecting and Preserving Electronic Evidence

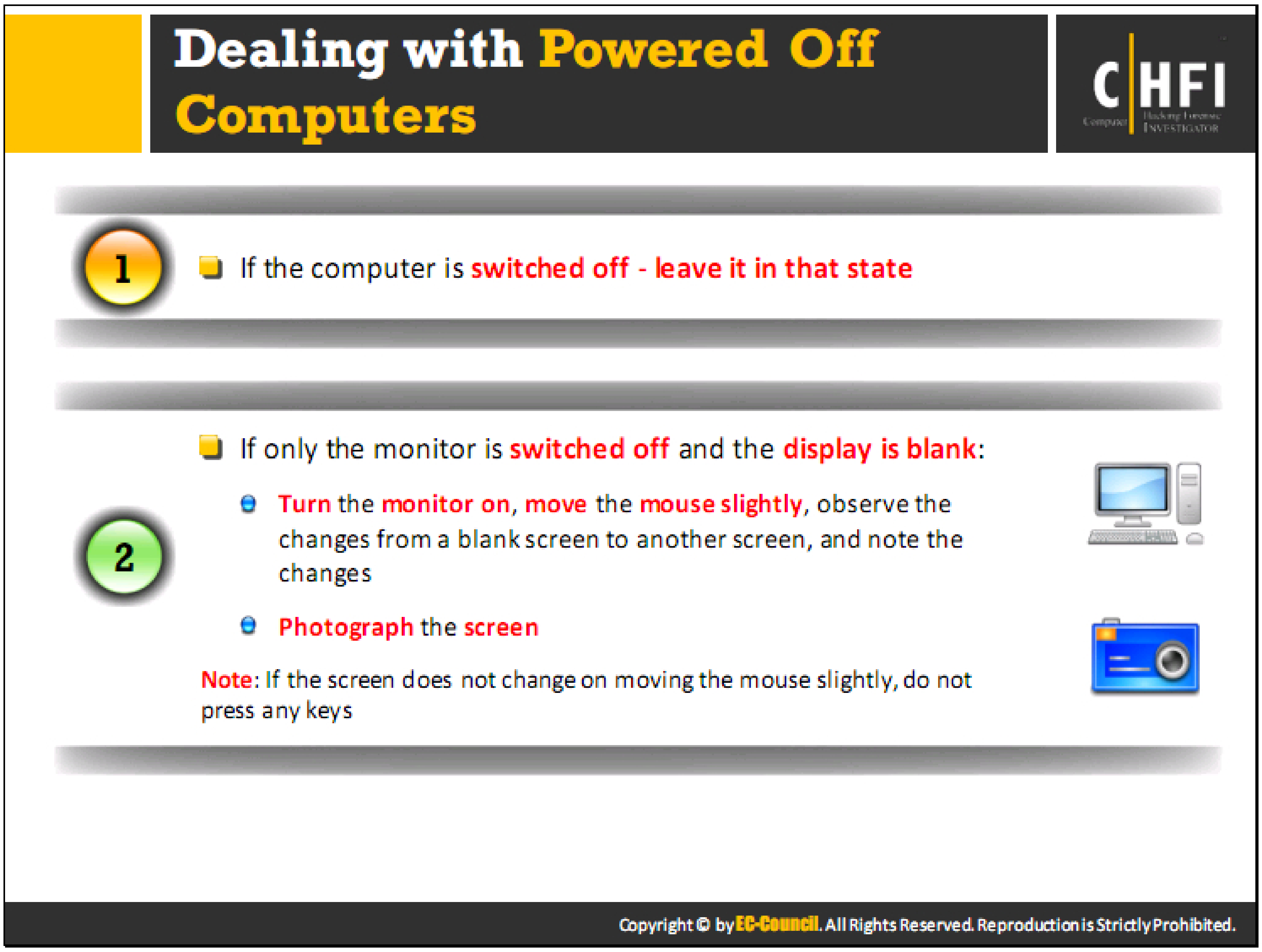
1. When an incident is reported where a computer is assumed to be a part of the incident, it is often the case that this is the **first and only item seized**
2. The crime scene should be investigated in a way that **covers the entire area**, keeping in mind the concept of the computer being at the middle of the circle
3. Pieces of **evidence** found at the crime scene should be first photographed, **identified** within documents, and then properly **gathered**
4. All collected **evidence should be marked** clearly so that it can be easily identified later
5. Markings on the evidence should, at the very least, include **date and time of collection** and the **initials of the collecting person**
6. **Evidence** should be **identified**, **recorded**, **seized**, **bagged**, and **tagged on-site**, with no attempts to determine contents or status



Dealing with Powered On Computers

1. When dealing with a powered-on computer, the investigator should stop and think before taking any action
2. The contents of RAM may contain vital information. For example, data that is encrypted on the hard disk may be unencrypted in the RAM. Also, running process information is stored in the RAM
3. All of this vital information will be lost when the computer is shut down or when the power supply is removed
4. If a computer is switched on and the screen is viewable, the investigator should photograph the screen, and document the running programs
5. If a computer is on and the monitor shows a screensaver, the investigator should move the mouse slowly without pressing any mouse button, and then photograph and document the programs

Electronic evidence is versatile in nature and easily broken during collection, preservation, and analysis. Therefore, act with caution to prevent damage.



Dealing with Powered Off Computers

1 If the computer is switched off - leave it in that state

2 If only the 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

Note: If the screen does not change on moving the mouse slightly, do not press any keys

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

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

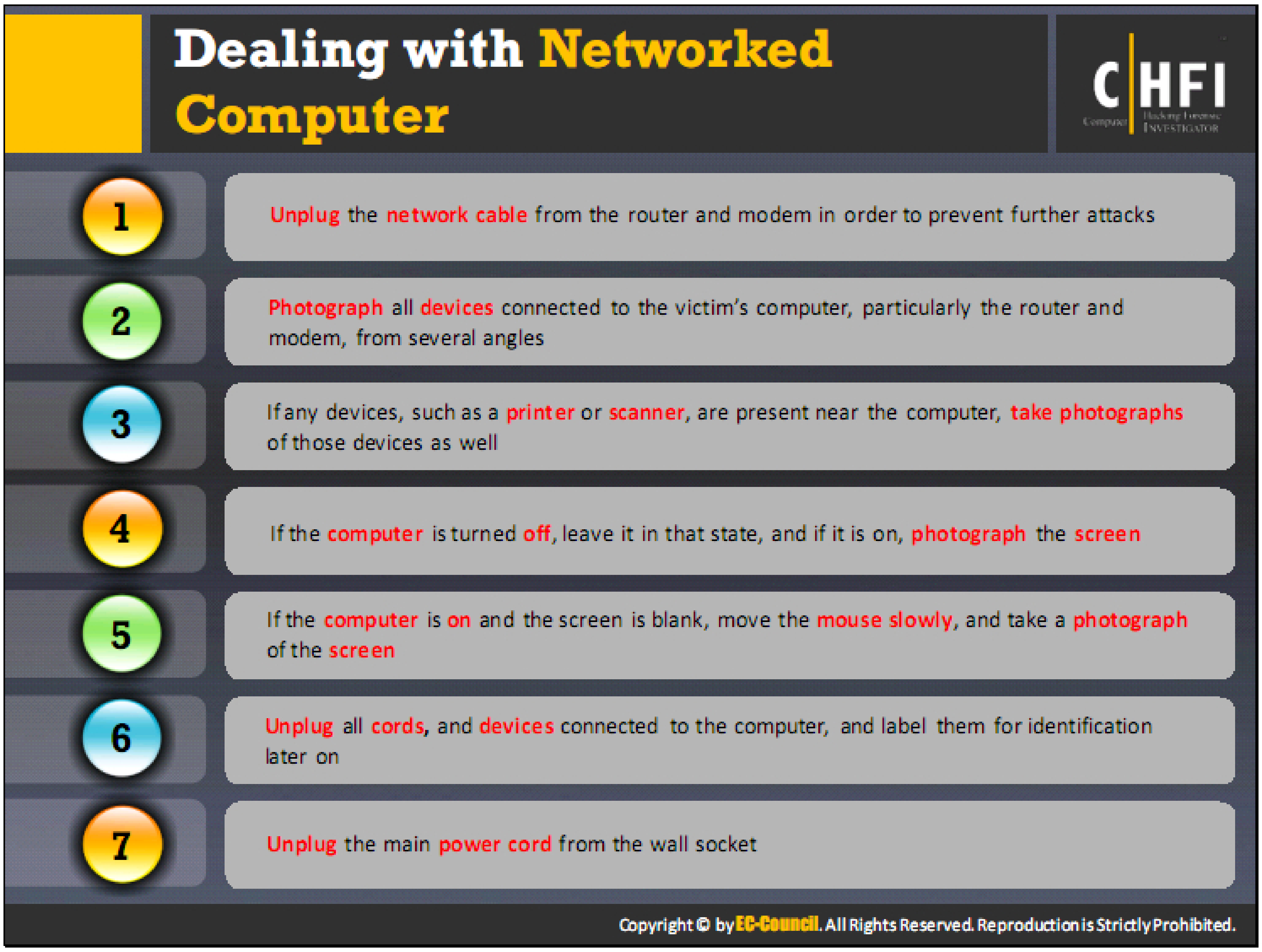
- If it is switched OFF, leave it OFF

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, do not perform any other keystroke.
- Photograph the screen.



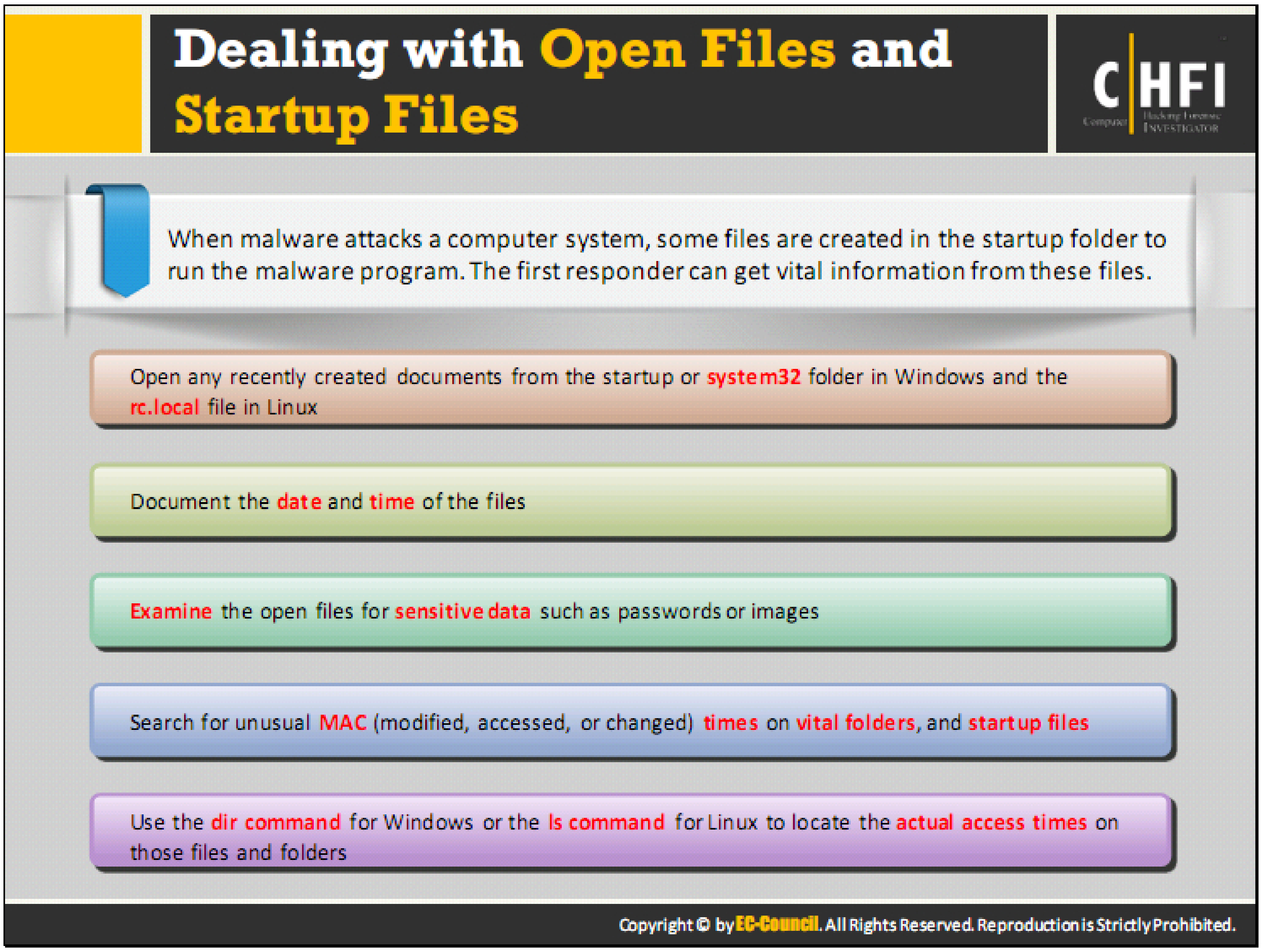
Dealing with Networked Computer

1. Unplug the network cable from the router and modem in order to prevent further attacks
2. Photograph all devices connected to the victim's computer, particularly the router and modem, from several angles
3. If any devices, such as a printer or scanner, are present near the computer, take photographs of those devices as well
4. If the computer is turned off, leave it in that state, and if it is on, photograph the screen
5. If the computer is on and the screen is blank, move the mouse slowly, and take a photograph of the screen
6. Unplug all cords, and devices connected to the computer, and label them for identification later on
7. Unplug the main power cord from the wall socket

If the victim's computer has an Internet connection, the first responder must follow the following procedure in order to protect the evidence:

- Unplug the network cable from the router and modem because the internet connection can make it vulnerable to further attack.
- 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 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 OFF, leave it OFF.
- If the computer is ON, take a photograph of the screen.
- If the computer is ON and the screen is blank, move the mouse slowly and take a photograph of the screen.
- Unplug all the cords and devices connected to the computer and label them for later 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.

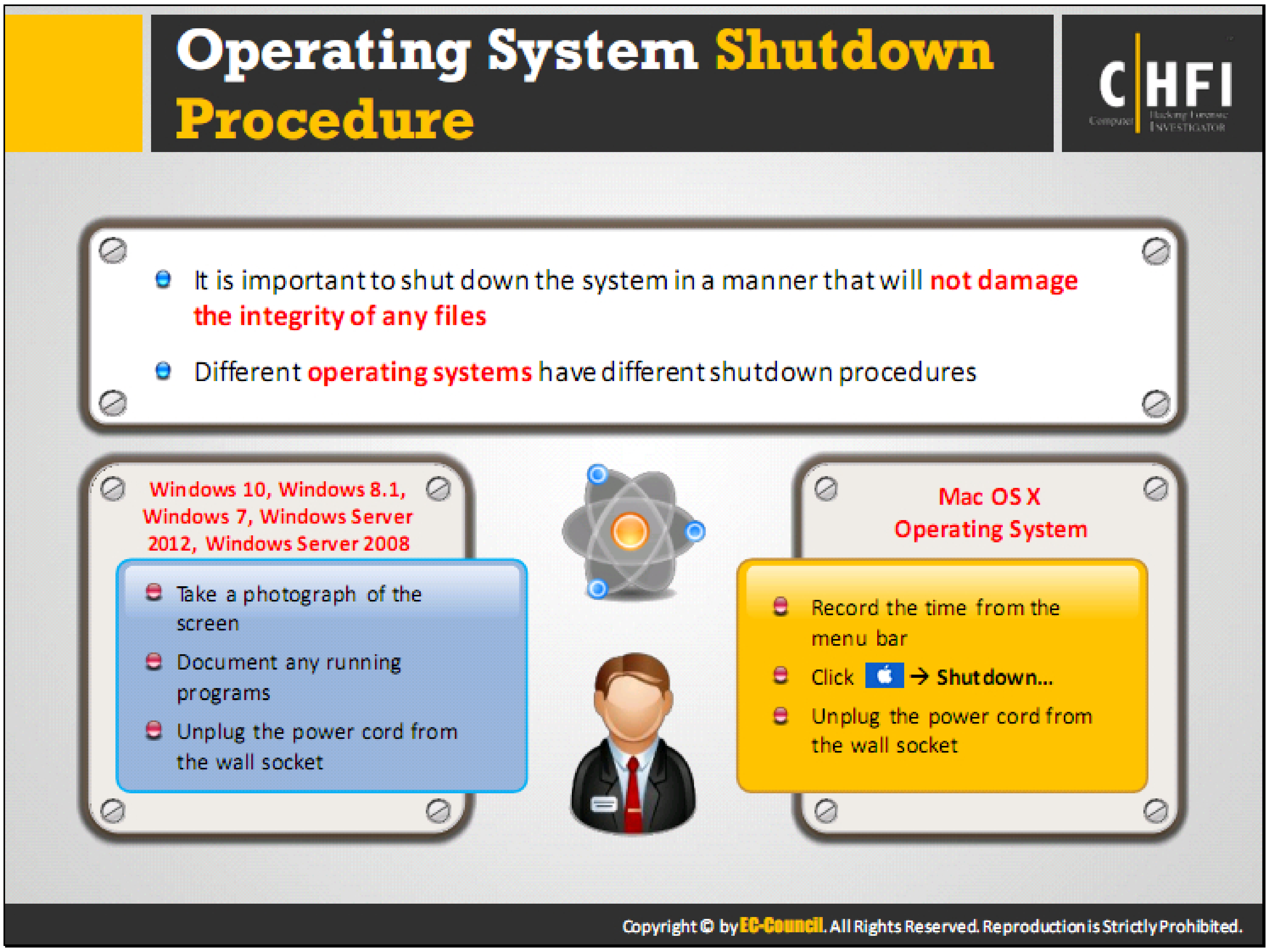


Dealing with Open Files and Startup Files

When malware attacks a computer system, some files are created in the startup folder to run the malware program. The first responder can get vital information from these 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 (modified, accessed, or changed) 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

When a computer crime occurs through malware attack, the malware creates some files. To run the malicious code, the malware creates some files in the startup folders for Windows operating systems and in the rc.local file folder for Linux operating systems. First responders can get vital information from these files. Use the ls command for the Linux operating system.



Operating System Shutdown Procedure

- It is important to shut down the system in a manner that will **not damage the integrity of any files**
- Different **operating systems** have different shutdown procedures

Windows 10, Windows 8.1, Windows 7, Windows Server 2012, Windows Server 2008

- Take a photograph of the screen
- Document any running programs
- Unplug the power cord from the wall socket

Mac OS X Operating System

- Record the time from the menu bar
- Click → **Shutdown...**
- Unplug the power cord from the wall socket

First responders have to make a vital decision at the time of 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 most cases, the type of operating system is a key in making this decision. Different operating systems have different shutdown procedures. Some of the operating systems directly shut down by simply unplugging the power cord from the wall socket without losing any files. However, for some operating systems, first responders have to follow the predefined shutdown procedure; otherwise, data may be lost or the hard drives may crash.

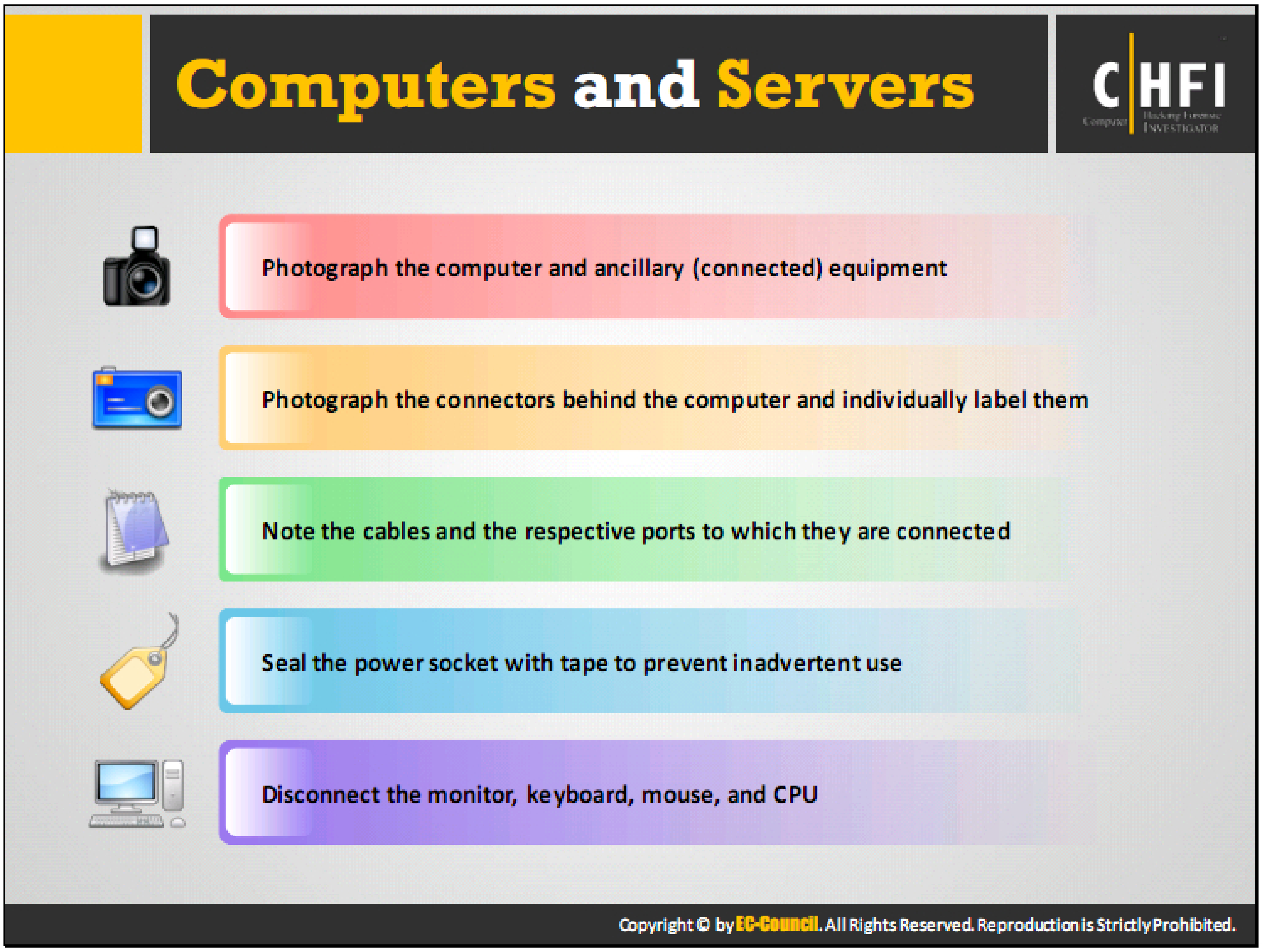
The first responder must follow the following procedures to shut down the operating system:

Windows 7, Windows XP, Windows Vista, Windows Server 2008, Windows Server 2003 operating system:

- Take a photograph of the screen
- If any program is running, give a brief explanation
- Unplug the power cord from the wall socket

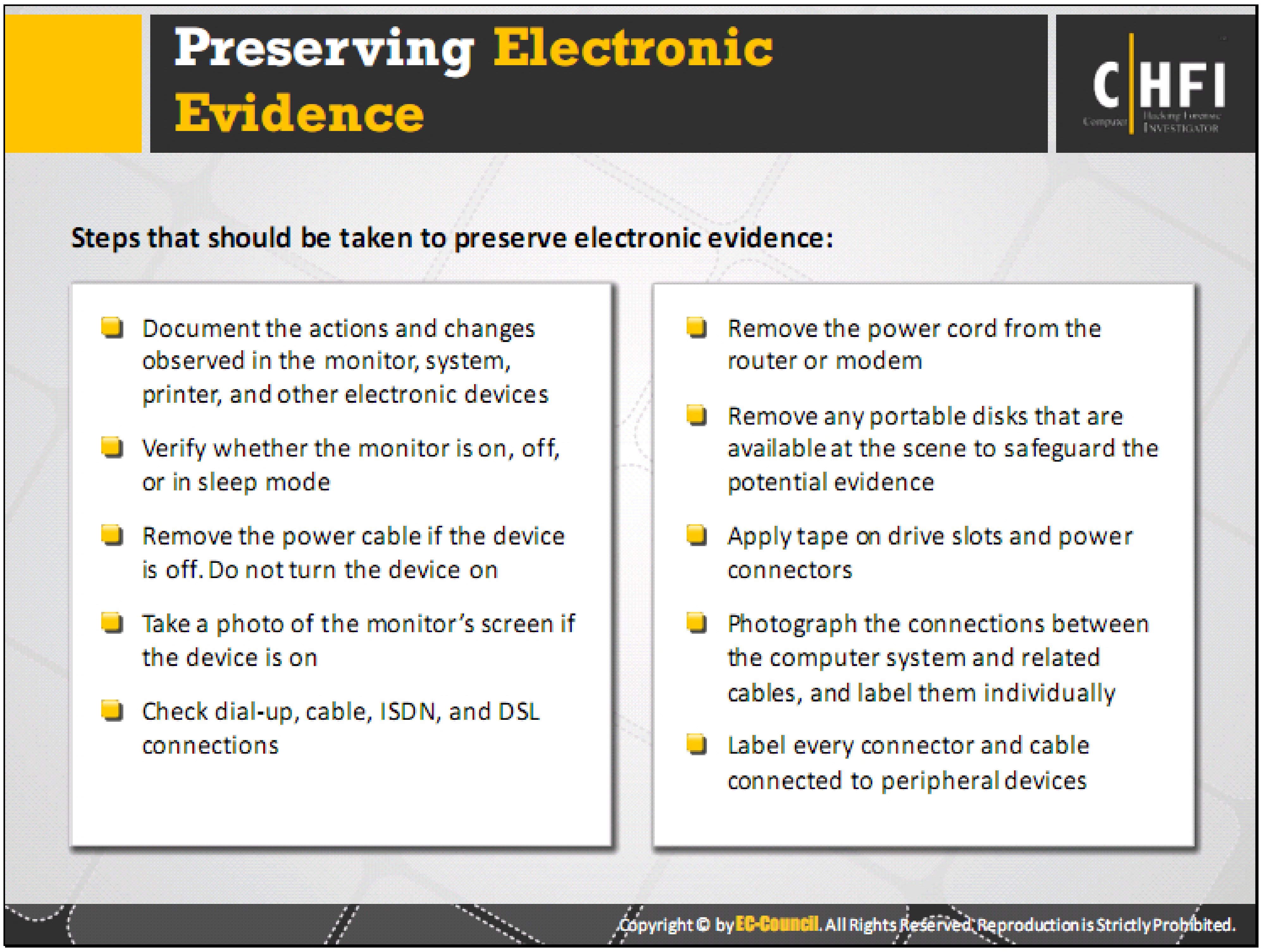
MAC OS X Operating System:

- Record the time from the menu bar
- Click Special Shutdown
- Unplug the power cord from the wall socket



Computers and Servers

- Photograph the computer and ancillary (connected) equipment
- Photograph the connectors behind the computer and individually label them
- Note the cables and the respective ports to which they are connected
- Seal the power socket with tape to prevent inadvertent use
- Disconnect the monitor, keyboard, mouse, and CPU



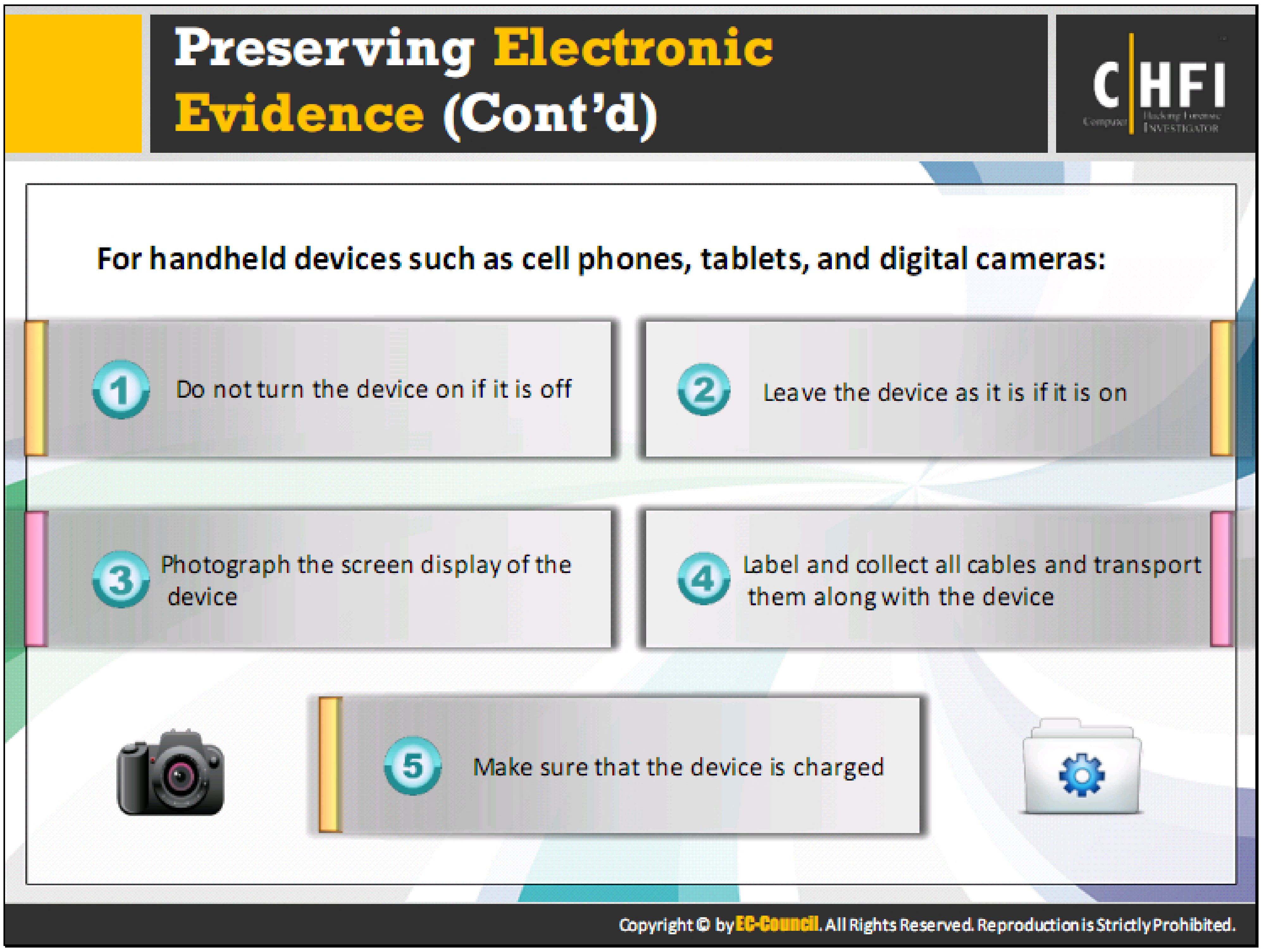
Preserving Electronic Evidence

Steps that should be taken to preserve electronic evidence:

- Document the actions and changes observed in the monitor, system, printer, and other electronic devices
- Verify whether the monitor is on, off, or in sleep mode
- Remove the power cable if the device is off. Do not turn the device on
- Take a photo of the monitor's screen if the device is on
- Check dial-up, cable, ISDN, and DSL connections
- Remove the power cord from the router or modem
- Remove any portable disks that are available at the scene to safeguard the potential evidence
- Apply tape on drive slots and power connectors
- Photograph the connections between the computer system and related cables, and label them individually
- Label every connector and cable connected to peripheral devices

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, i.e., 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.

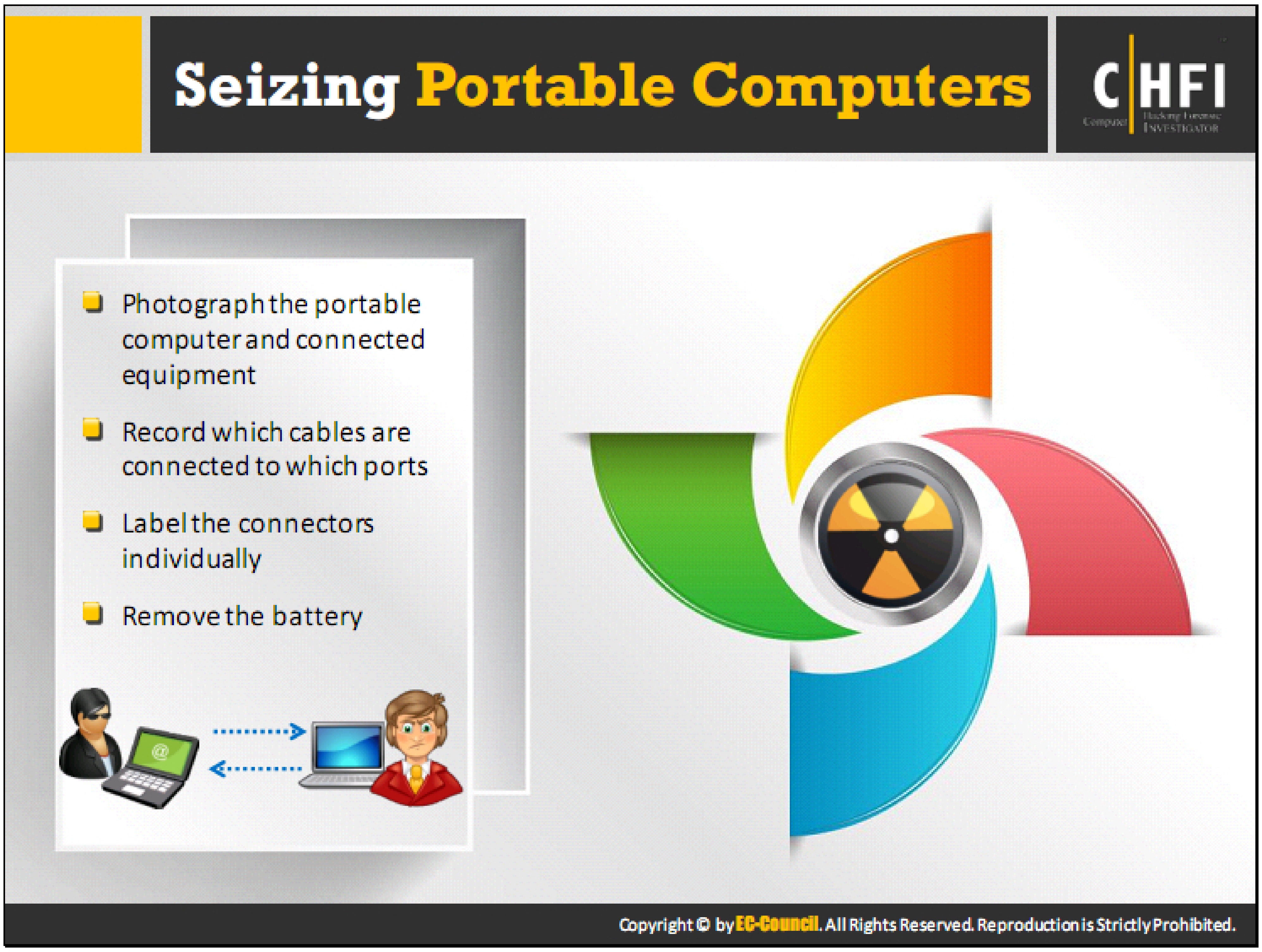


Preserving Electronic Evidence (Cont'd)

CHFI
Computer Hacking Forensic INVESTIGATOR

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

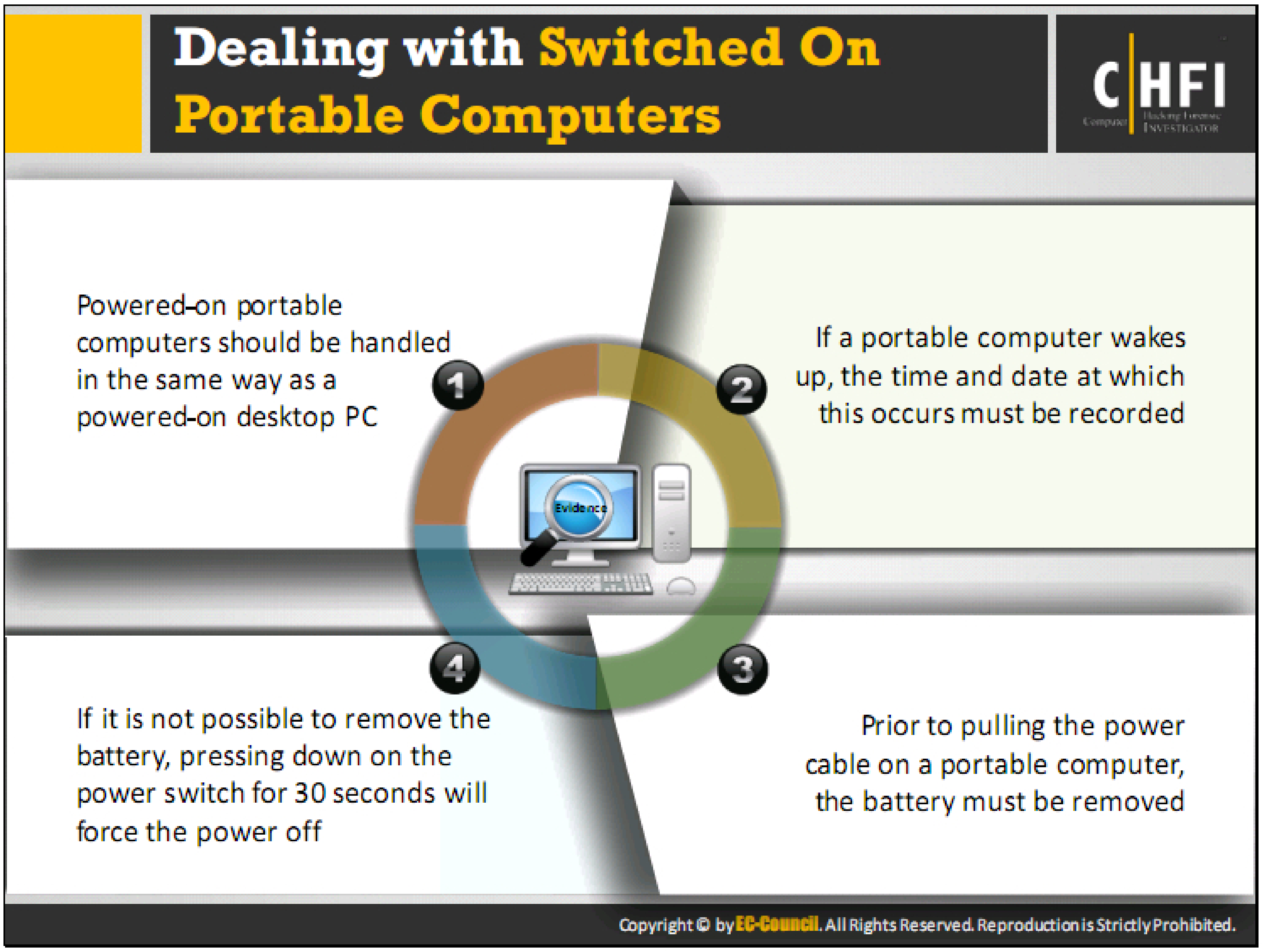
1. Do not turn the device on if it is off
2. Leave the device as it is if it is on
3. Photograph the screen display of the device
4. Label and collect all cables and transport them along with the device
5. Make sure that the device is charged



Seizing Portable Computers

CHFI
Computer Hacking Forensic INVESTIGATOR

- Photograph the portable computer and connected equipment
- Record which cables are connected to which ports
- Label the connectors individually
- Remove the battery



C|HFI
Computer Hacking Forensic INVESTIGATOR
Evidence

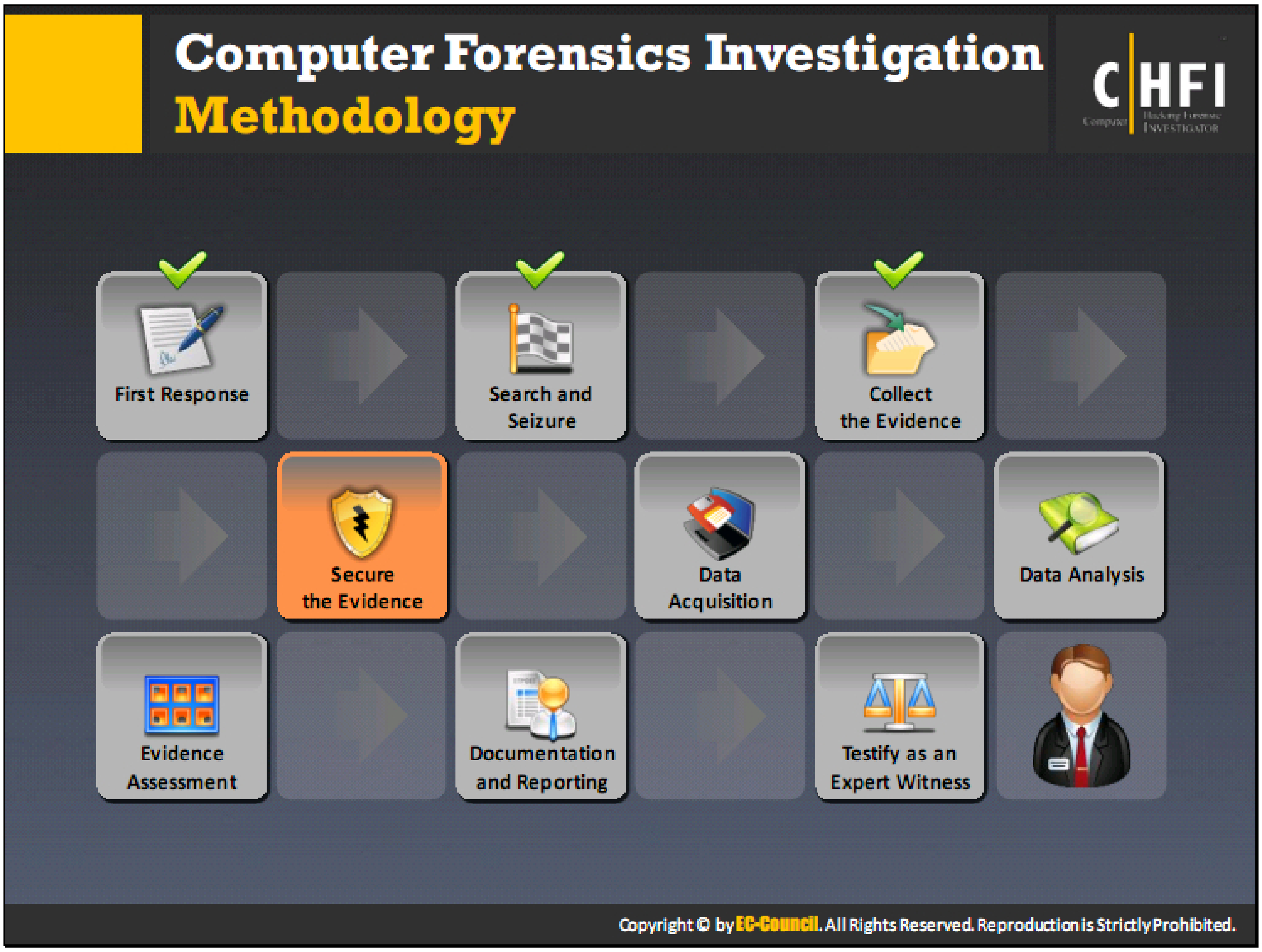
Dealing with Switched On Portable Computers

1. Powered-on portable computers should be handled in the same way as a powered-on desktop PC

2. If a portable computer wakes up, the time and date at which this occurs must be recorded

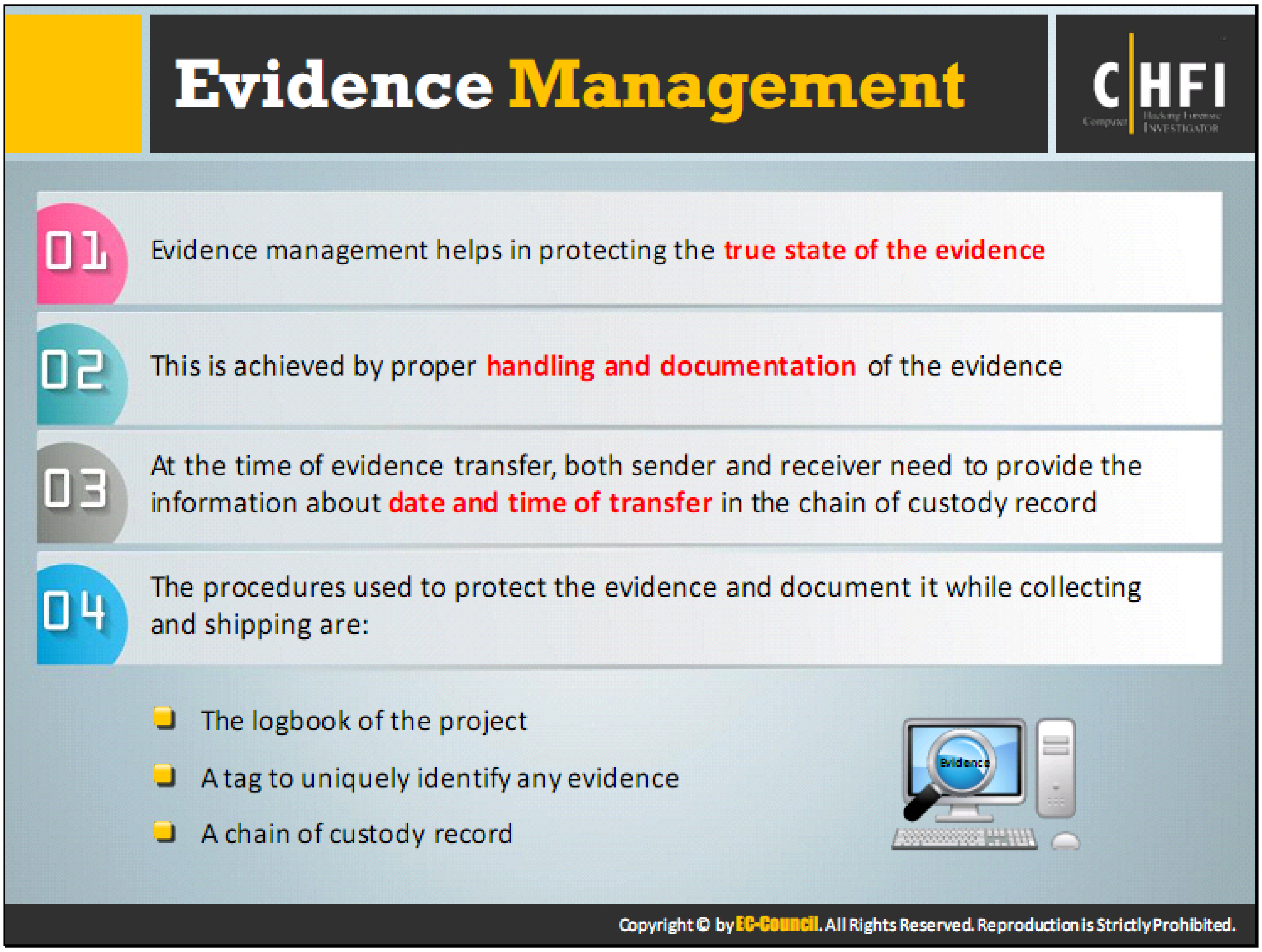
3. Prior to pulling the power cable on a portable computer, the battery must be removed

4. If it is not possible to remove the battery, pressing down on the power switch for 30 seconds will force the power off



Computer Forensics Investigation
Methodology
CHFI Computer Hacking Forensic Investigator
First Response
Search and Seizure
Collect the Evidence
Secure the Evidence
Data Acquisition
Data Analysis
Evidence Assessment
Documentation and Reporting
Testify as an Expert Witness
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence is fragile data that is easy to manipulate, alter, and destroy. Therefore, attackers are always looking for ways to damage it in every possible way. This section will discuss the process of storing the evidence in a secure manner.


CHFI
Computer Hacking Forensic Investigator
Evidence

Evidence Management

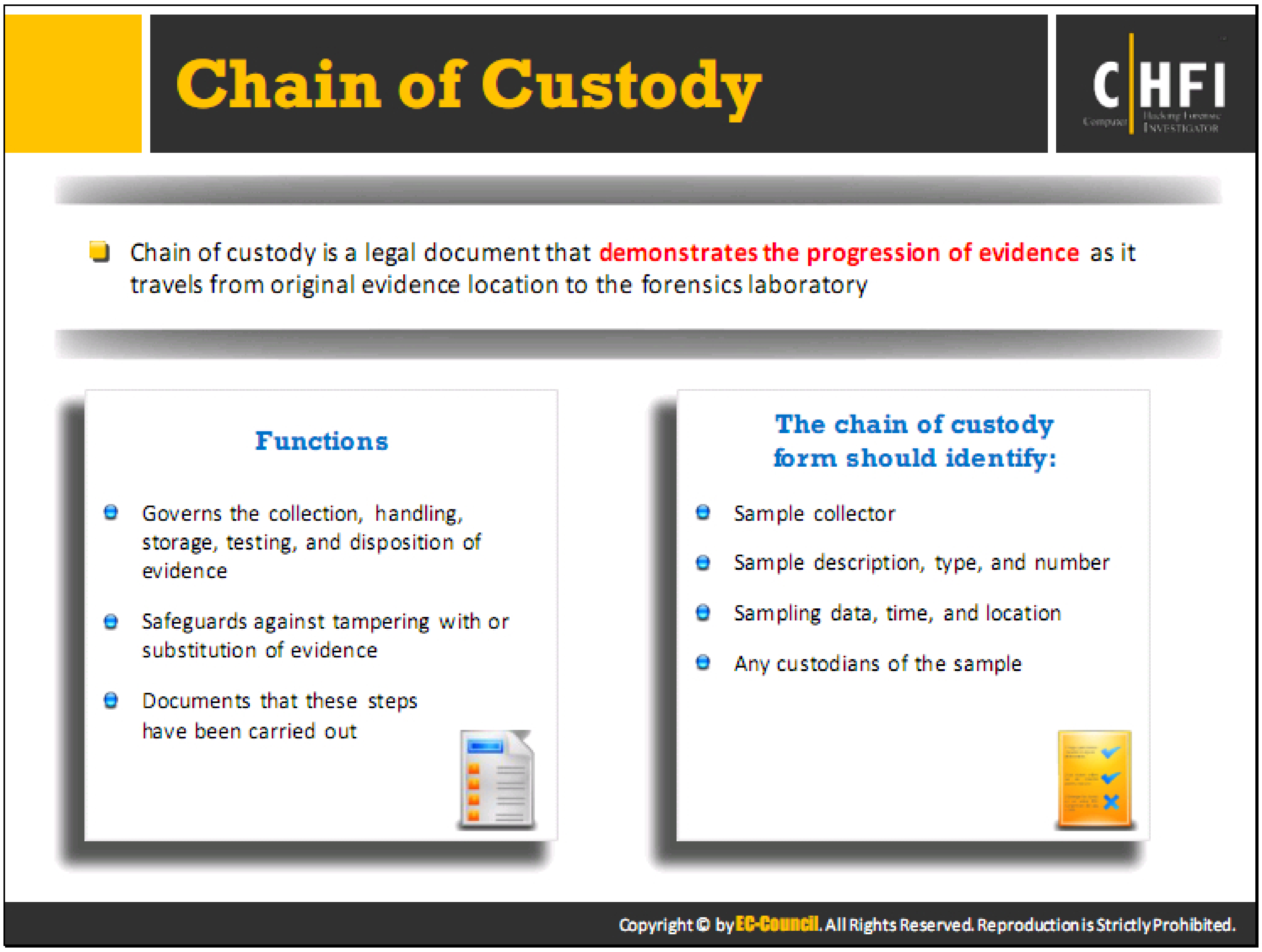
01 Evidence management helps in protecting the **true state of the evidence**

02 This is achieved by proper **handling and documentation** of the evidence

03 At the time of evidence transfer, both sender and receiver need to provide the information about **date and time of transfer** in the chain of custody record

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

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



Chain of Custody

- Chain of custody is a legal document that demonstrates the progression of evidence as it travels from original evidence location to the forensics laboratory

Functions

- Governs the collection, handling, storage, testing, and disposition of evidence
- Safeguards against tampering with or substitution of evidence
- Documents that these steps have been carried out

The chain of custody form should identify:

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

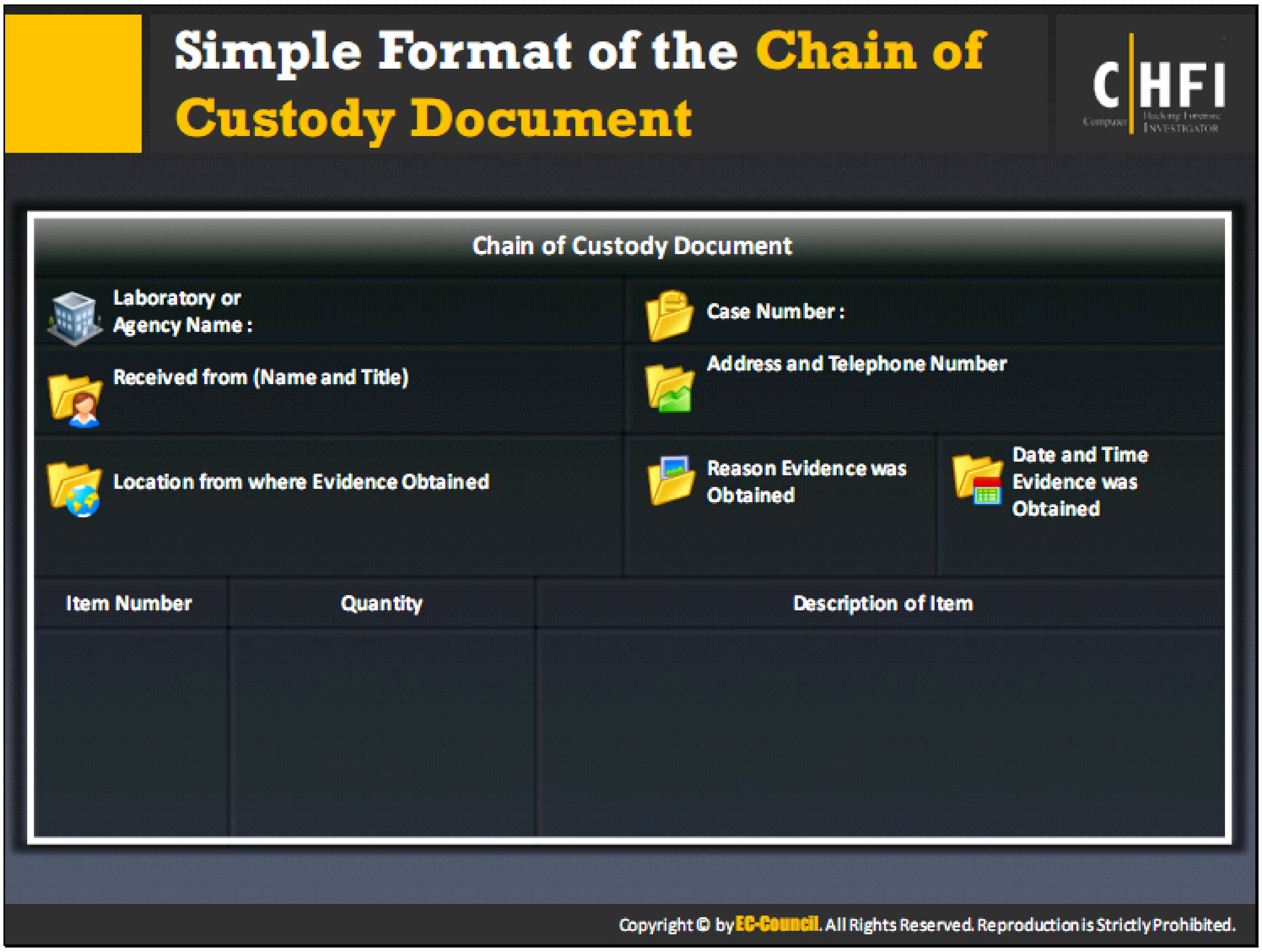
Chain of custody is a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory. It is a roadmap that shows how investigators collected, analyzed, and preserved the evidence. The investigators need to present this document in 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 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 important significance. The forensic investigator needs to document each step taken during the period of collecting the evidence. It is important that the investigators clarify the source, date of recovery, method of recovery, and nature of the digital evidence.



Simple Format of the Chain of Custody Document

CHFI
Computer Hacking Forensic INVESTIGATOR

Chain of Custody Document

Laboratory or Agency Name :

Case Number :

Received from (Name and Title)

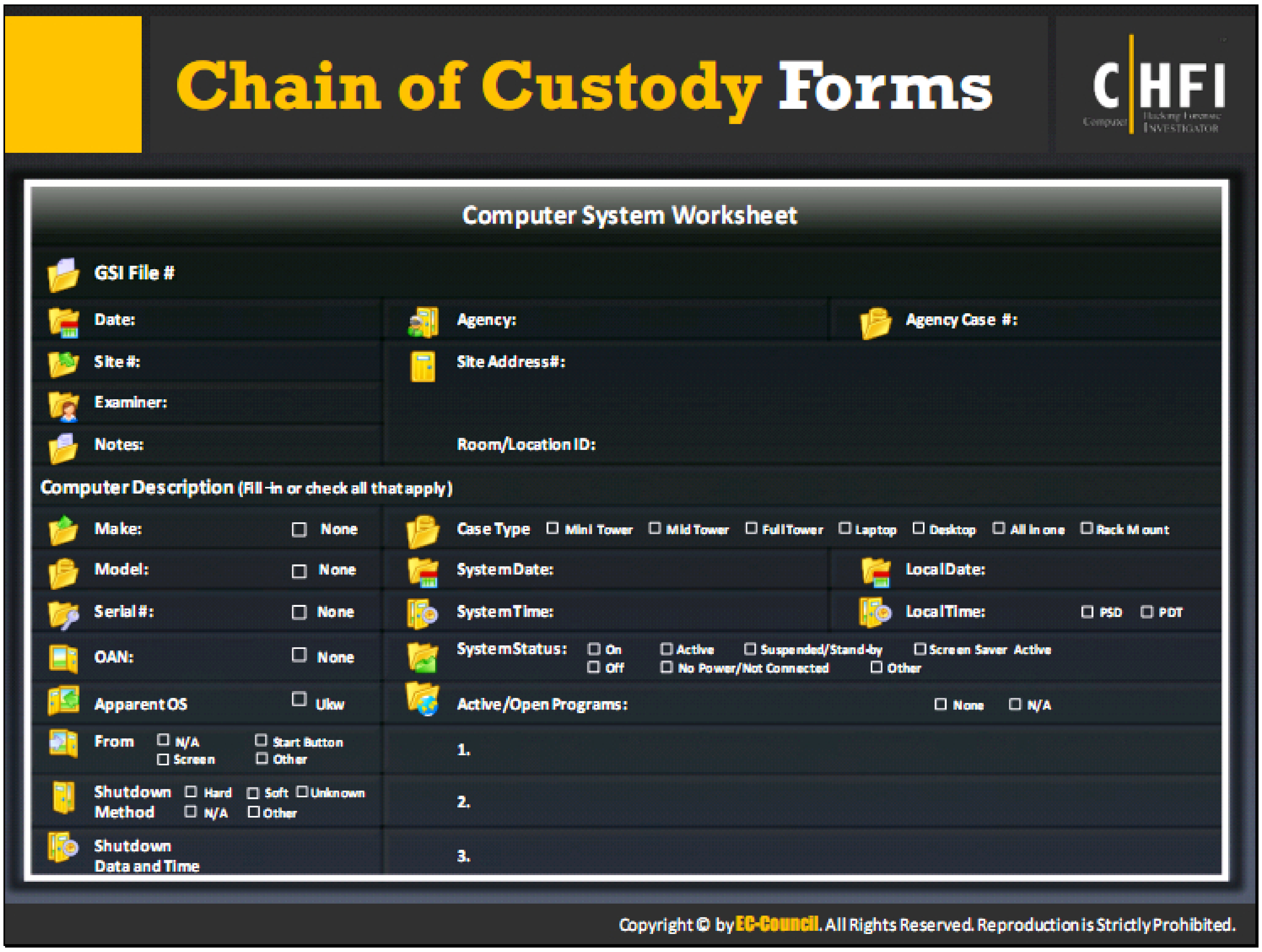
Address and Telephone Number

Location from where Evidence Obtained

Reason Evidence was Obtained

Date and Time Evidence was Obtained

Item Number	Quantity	Description of Item



Chain of Custody Forms

CHFI
Computer Hacking Forensic INVESTIGATOR

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 □ Off □ Active □ No Power/Not Connected □ Suspended/Stand-by □ Other □ Screen Saver Active

Apparent OS □ Ukw

Active/Open Programs: □ None □ N/A

From □ N/A □ Screen □ Start Button □ Other

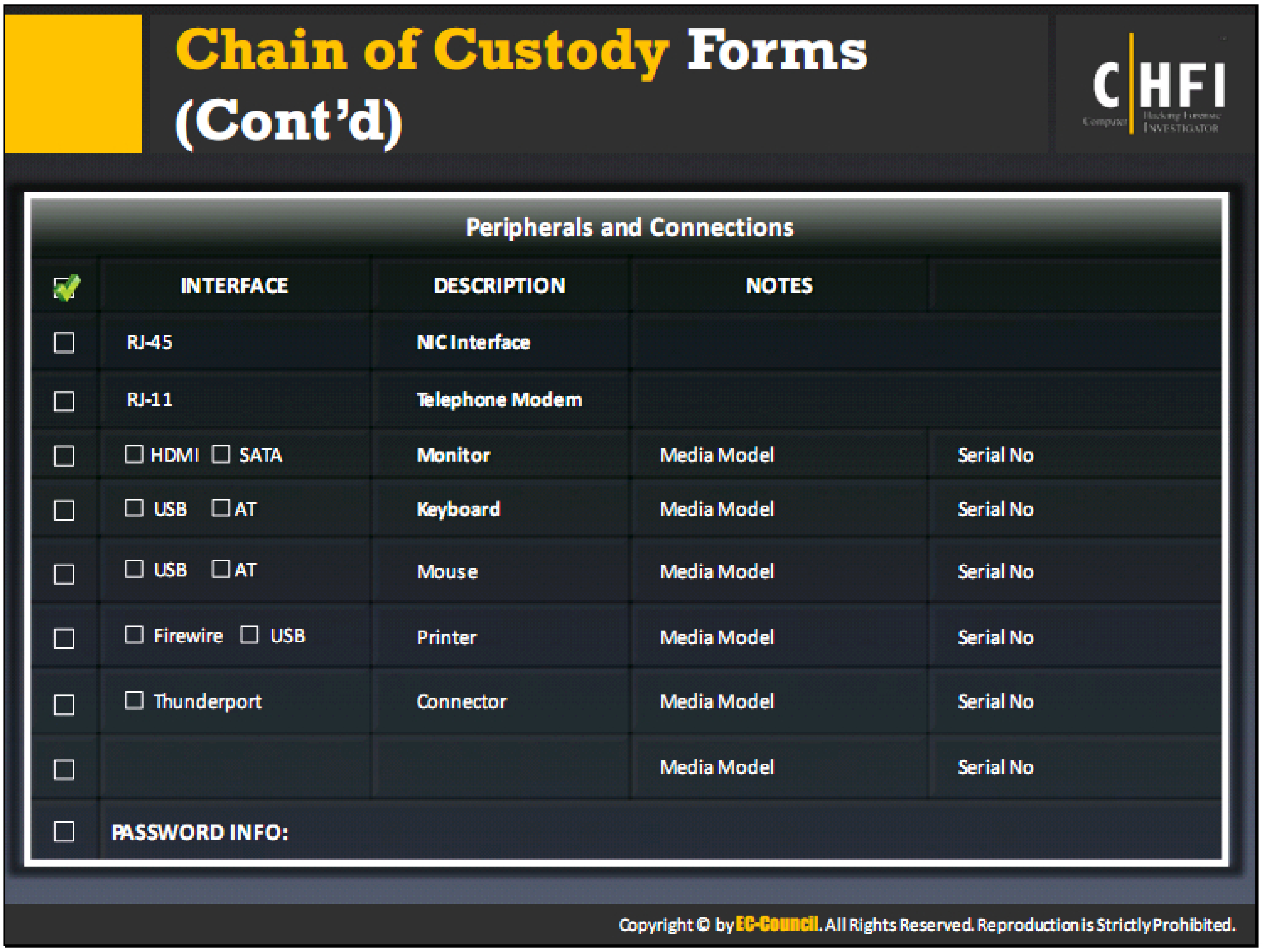
1.

Shutdown Method □ Hard □ N/A □ Soft □ Other □ Unknown

2.

Shutdown Data and Time

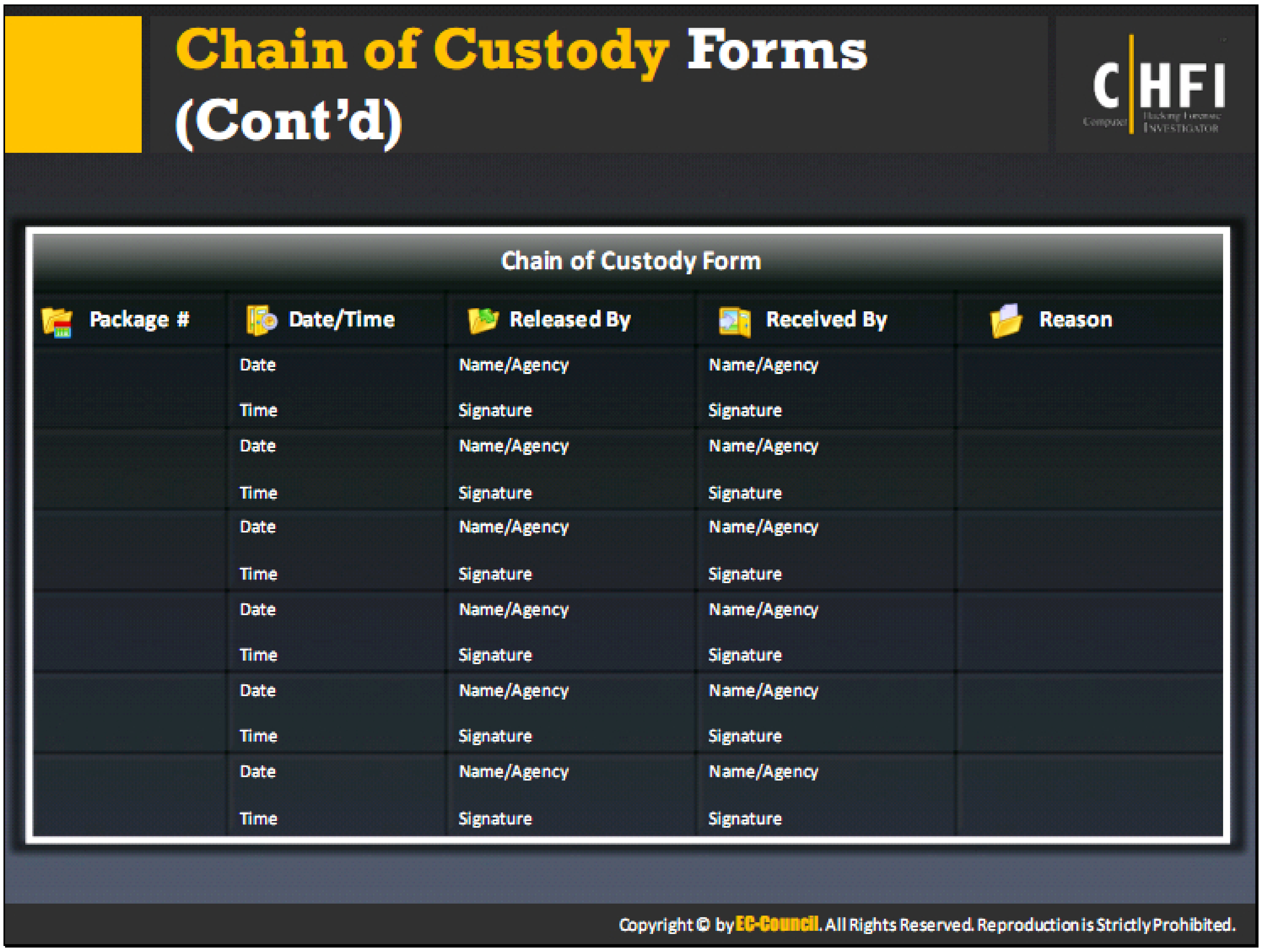
3.



Chain of Custody Forms (Cont'd)

Peripherals and Connections

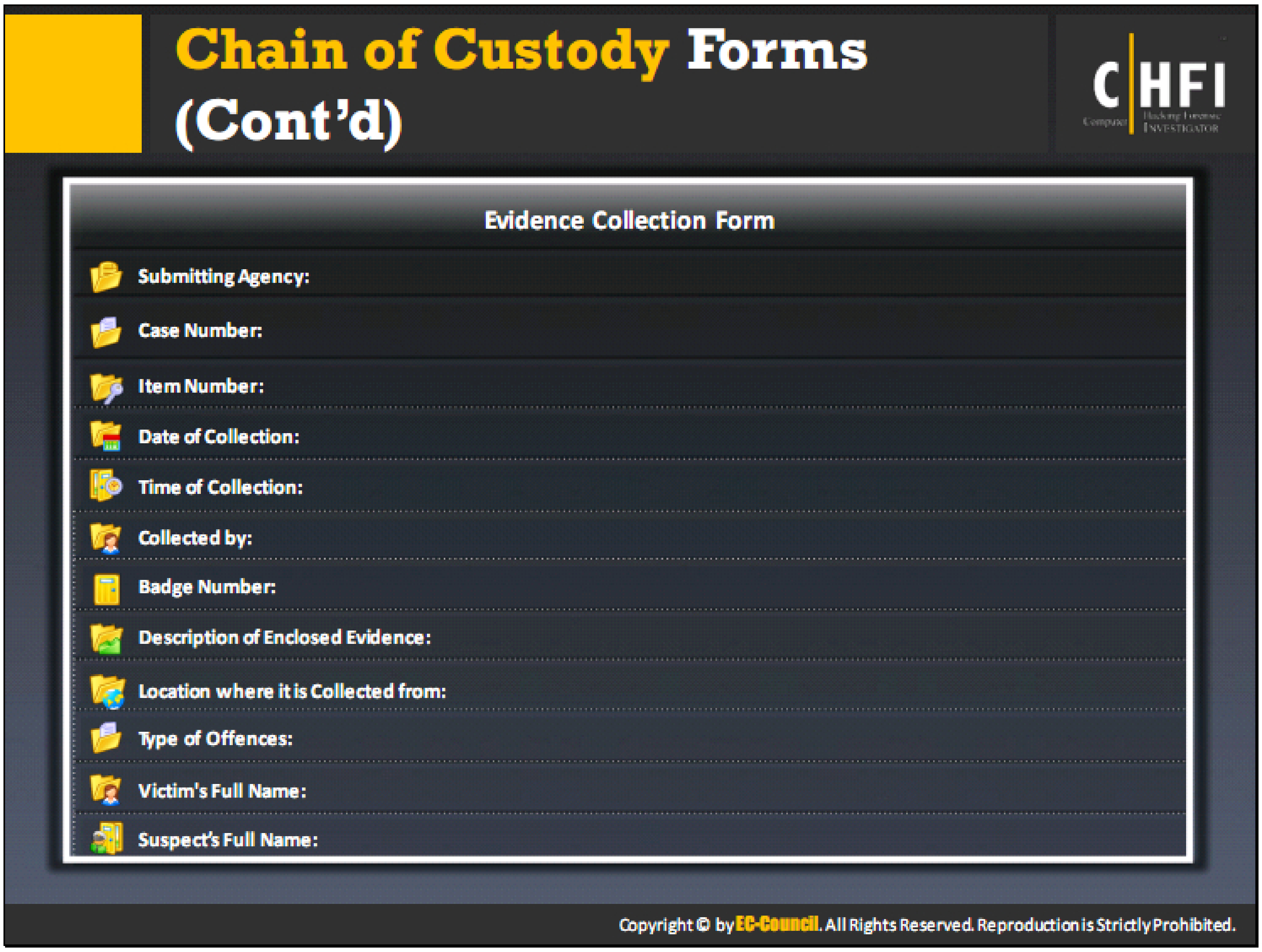
☑	INTERFACE	DESCRIPTION	NOTES	
□	RJ-45	NIC Interface		
□	RJ-11	Telephone Modem		
□	□ HDMI □ SATA	Monitor	Media Model	Serial No
□	□ USB □ AT	Keyboard	Media Model	Serial No
□	□ USB □ AT	Mouse	Media Model	Serial No
□	□ Firewire □ USB	Printer	Media Model	Serial No
□	□ Thunderport	Connector	Media Model	Serial No
□			Media Model	Serial No
□	PASSWORD INFO:			



Chain of Custody Forms (Cont'd)

Chain of Custody Form

Package #	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	



Chain of Custody Forms (Cont'd)

CHFI Computer Hacking Forensic Investigator

Evidence Collection Form

Submitting Agency:

Case Number:

Item Number:

Date of Collection:

Time of Collection:

Collected by:

Badge Number:

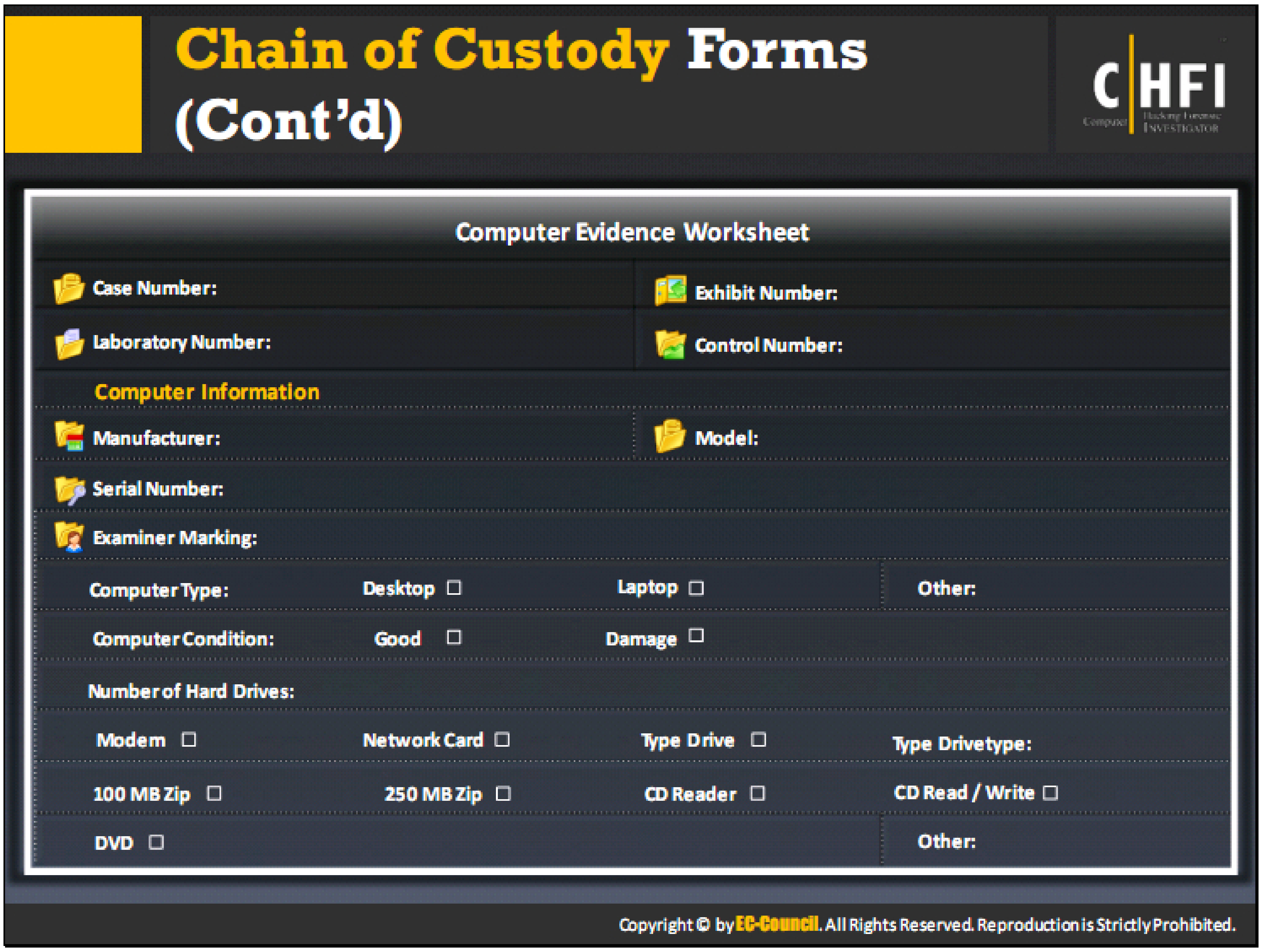
Description of Enclosed Evidence:

Location where it is Collected from:

Type of Offences:

Victim's Full Name:

Suspect's Full Name:

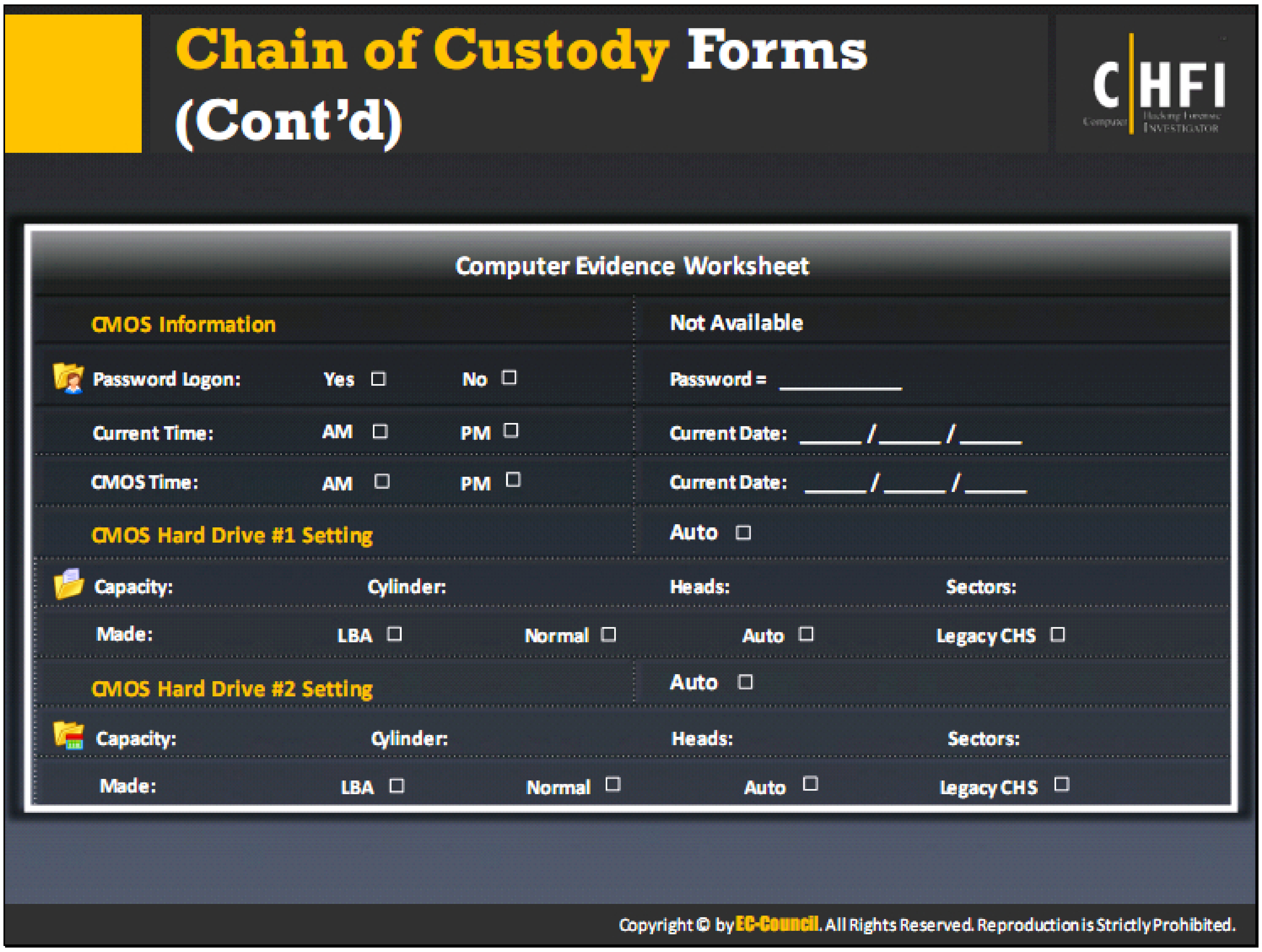


Chain of Custody Forms (Cont'd)

CHFI Computer Hacking Forensic Investigator

Computer Evidence Worksheet

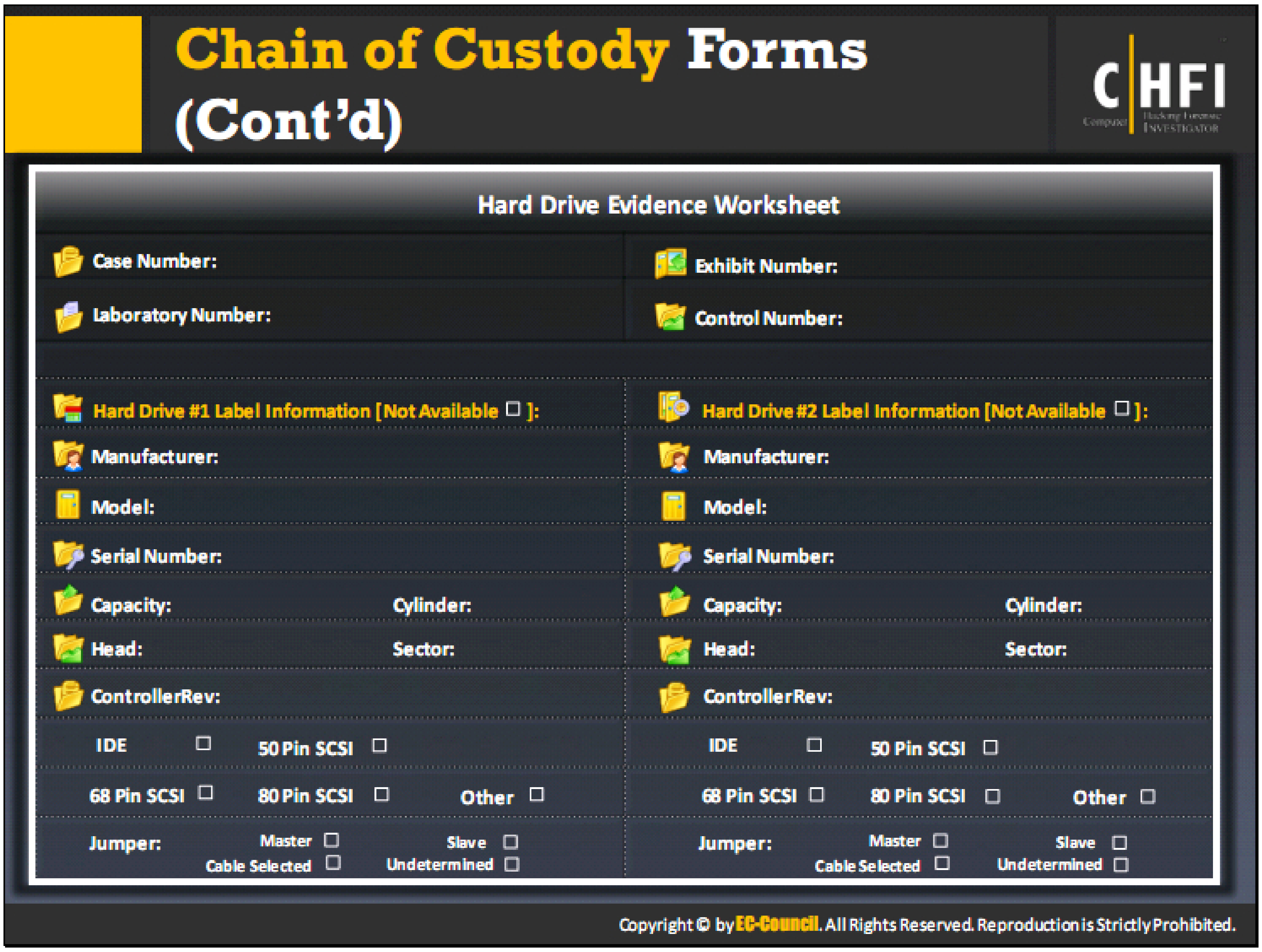
Case Number:		Exhibit Number:	
Laboratory Number:		Control Number:	
Computer Information			
Manufacturer:		Model:	
Serial Number:			
Examiner Marking:			
Computer Type:	Desktop □	Laptop □	Other:
Computer Condition:	Good □	Damage □	
Number of Hard Drives:			
Modem □	Network Card □	Type Drive □	Type Drivetype:
100 MB Zip □	250 MB Zip □	CD Reader □	CD Read / Write □
DVD □			Other:



Chain of Custody Forms (Cont'd)

Computer Evidence Worksheet

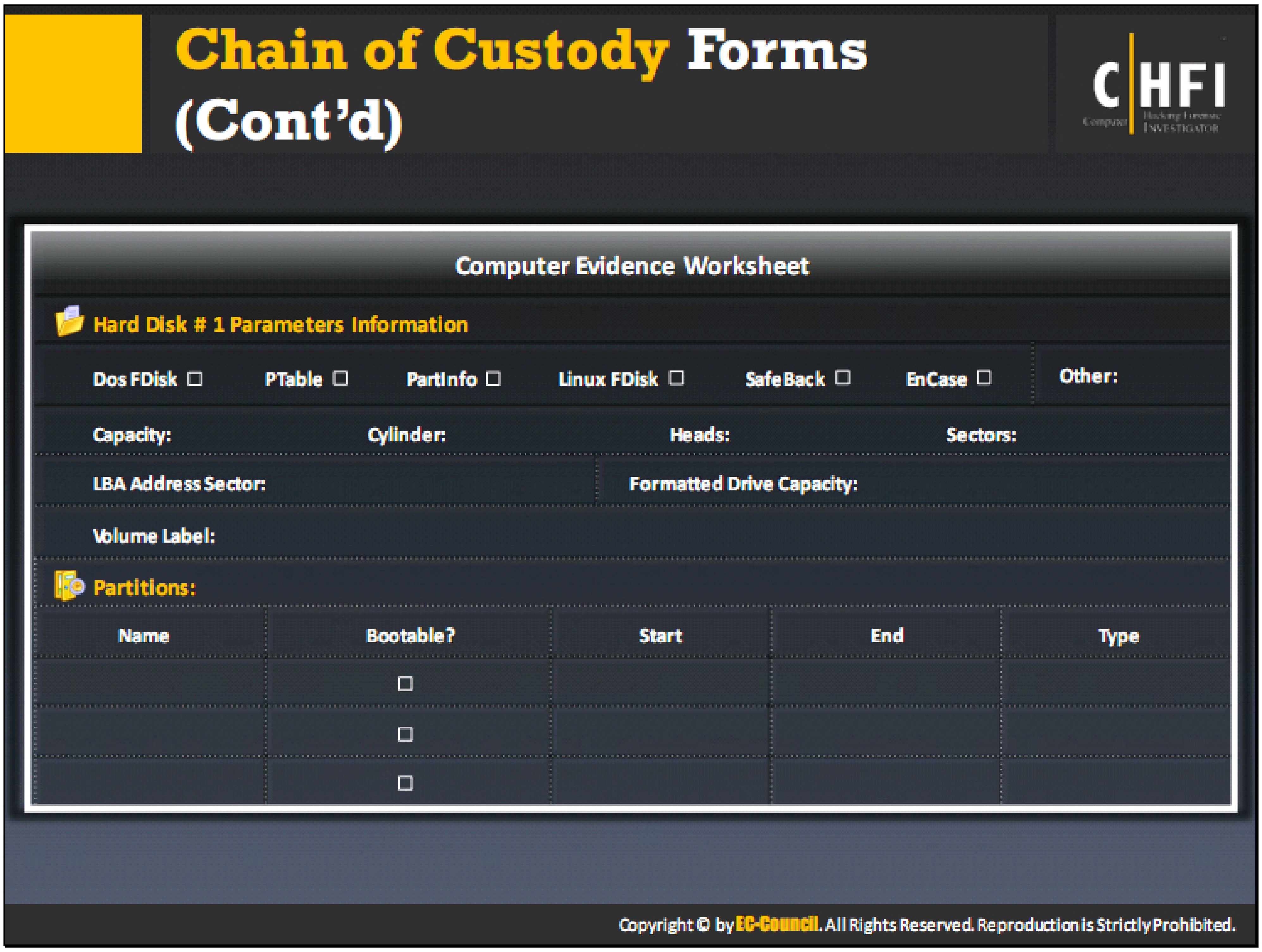
CMOS Information			Not Available	
Password Logon:	Yes □	No □	Password = ________	
Current Time:	AM □	PM □	Current Date: _____/_____/_____	
CMOS Time:	AM □	PM □	Current Date: _____/_____/_____	
CMOS Hard Drive #1 Setting			Auto □	
Capacity:		Cylinder:	Heads:	Sectors:
Made:	LBA □	Normal □	Auto □	Legacy CHS □
CMOS Hard Drive #2 Setting			Auto □	
Capacity:		Cylinder:	Heads:	Sectors:
Made:	LBA □	Normal □	Auto □	Legacy CHS □



Chain of Custody Forms (Cont'd)

Hard Drive Evidence Worksheet

Case Number:	Exhibit Number:
Laboratory Number:	Control Number:
Hard Drive #1 Label Information [Not Available □]:	Hard Drive #2 Label Information [Not Available □]:
Manufacturer:	Manufacturer:
Model:	Model:
Serial Number:	Serial Number:
Capacity: Cylinder:	Capacity: Cylinder:
Head: Sector:	Head: Sector:
ControllerRev:	ControllerRev:
IDE □ 50 Pin SCSI □	IDE □ 50 Pin SCSI □
68 Pin SCSI □ 80 Pin SCSI □ Other □	68 Pin SCSI □ 80 Pin SCSI □ Other □
Jumper: Master □ Slave □ Cable Selected □ Undetermined □	Jumper: Master □ Slave □ Cable Selected □ Undetermined □



Chain of Custody Forms (Cont'd)

Computer Evidence Worksheet

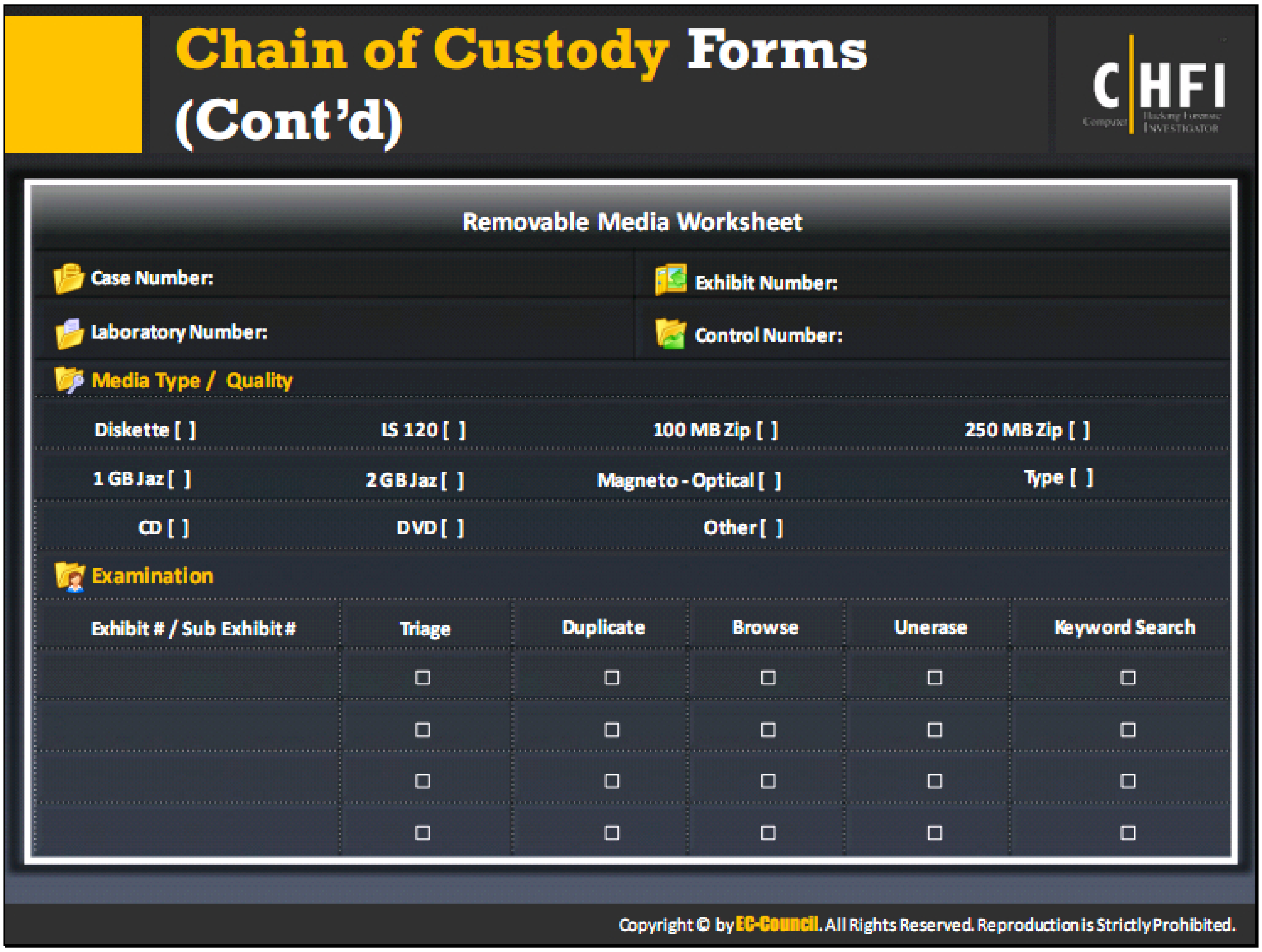
Hard Disk # 1 Parameters Information

Dos FDisk □	PTable □	PartInfo □	Linux FDisk □	SafeBack □	EnCase □	Other:

Capacity:	Cylinder:	Heads:	Sectors:
LBA Address Sector:	Formatted Drive Capacity:		
Volume Label:			

Partitions:

Name	Bootable?	Start	End	Type
	□			
	□			
	□			



Chain of Custody Forms (Cont'd)

Removable Media Worksheet

Case Number:	Exhibit Number:
Laboratory Number:	Control Number:

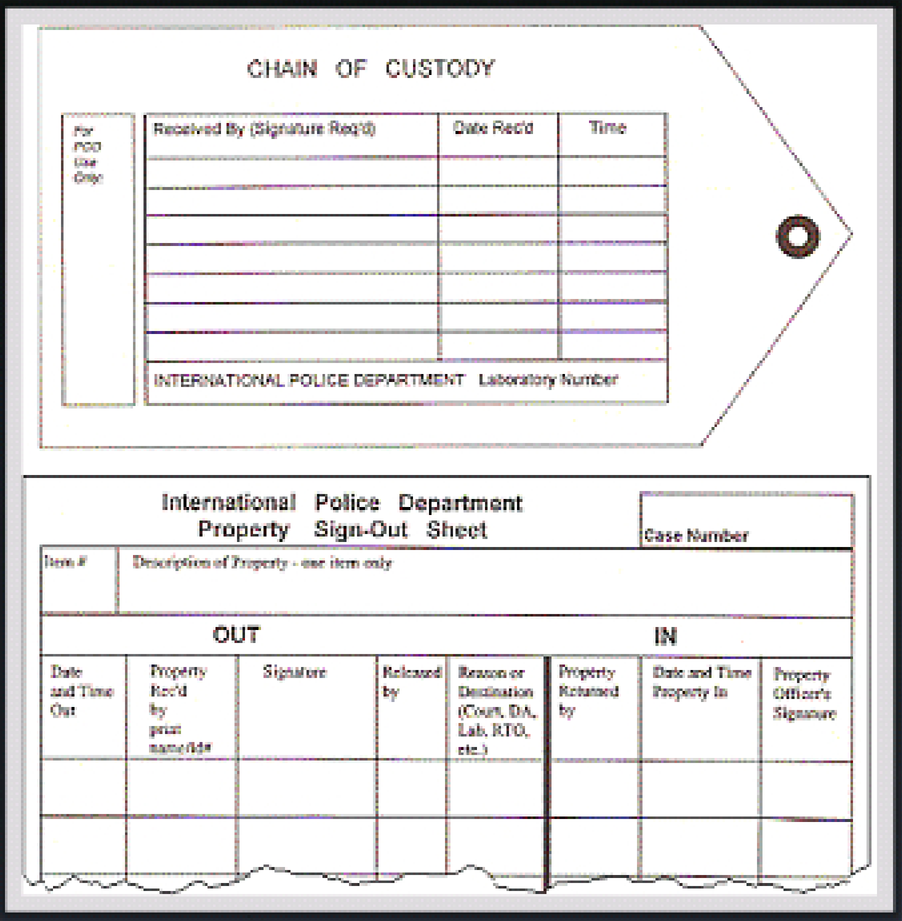
Media Type / Quality

Diskette [ ]	LS 120 [ ]	100 MB Zip [ ]	250 MB Zip [ ]
1 GB Jaz [ ]	2 GB Jaz [ ]	Magneto - Optical [ ]	Type [ ]
CD [ ]	DVD [ ]	Other [ ]	

Examination

Exhibit # / Sub Exhibit #	Triage	Duplicate	Browse	Unerase	Keyword Search
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□
	□	□	□	□	□

Chain of Custody on Property Evidence Envelope/Bag and Sign-out Sheet



CHAIN OF CUSTODY

For PCO Use Only

Received By (Signature Req'd)	Date Rec'd	Time

INTERNATIONAL POLICE DEPARTMENT Laboratory Number

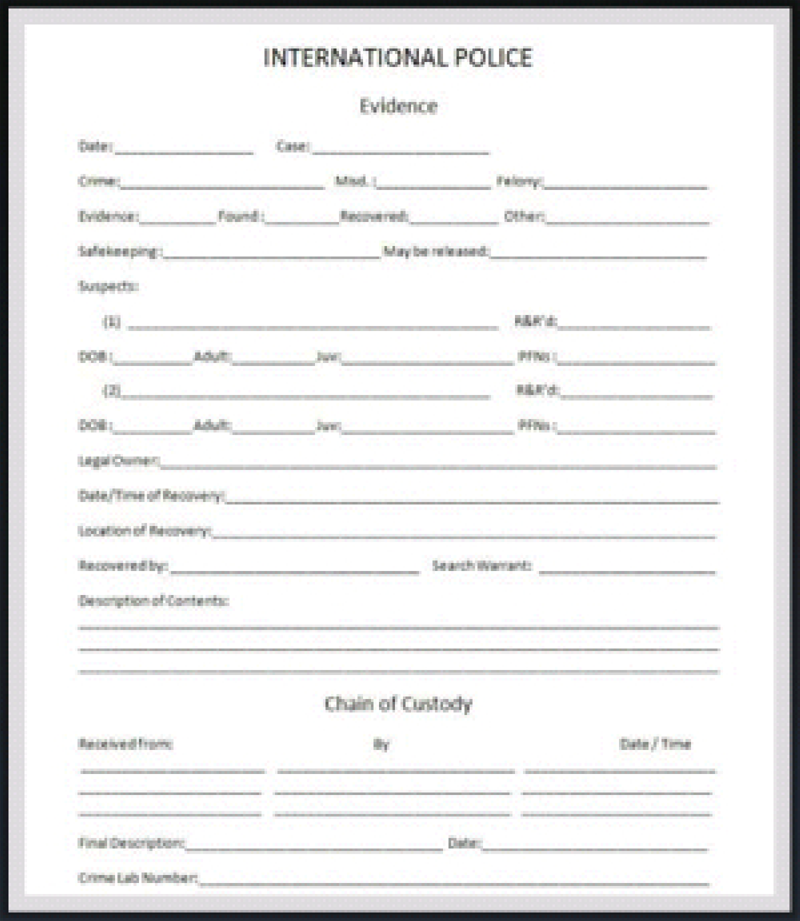
International Police Department
Property Sign-Out Sheet

Case Number

Item #

Description of Property - one item only

OUT					IN		
Date and Time Out	Property Rec'd by print name/Id#	Signature	Released by	Reason or Destination (Court, DA, Lab, RTO, etc.)	Property Returned by	Date and Time Property In	Property Officer's Signature



INTERNATIONAL POLICE

Evidence

Date: ____________ Case: ________________

Crime: ____________________ Misd. : __________ Felony: ______________

Evidence: ________ Found : ________ Recovered: __________ Other: ______________

Safekeeping: ____________________ May be released: ____________________

Suspects:

(1) __________________________________ R&R'd: ______________

DOB : ________ Adult: ________ Juv: ________________ PFNs : ______________

(2) __________________________________ R&R'd: ______________

DOB : ________ Adult: ________ Juv: ________________ PFNs : ______________

Legal Owner: ____

Date/Time of Recovery: ____________________________________

Location of Recovery: _____________________________________

Recovered by: ______________________ Search Warrant: ______________

Description of Contents:

Chain of Custody

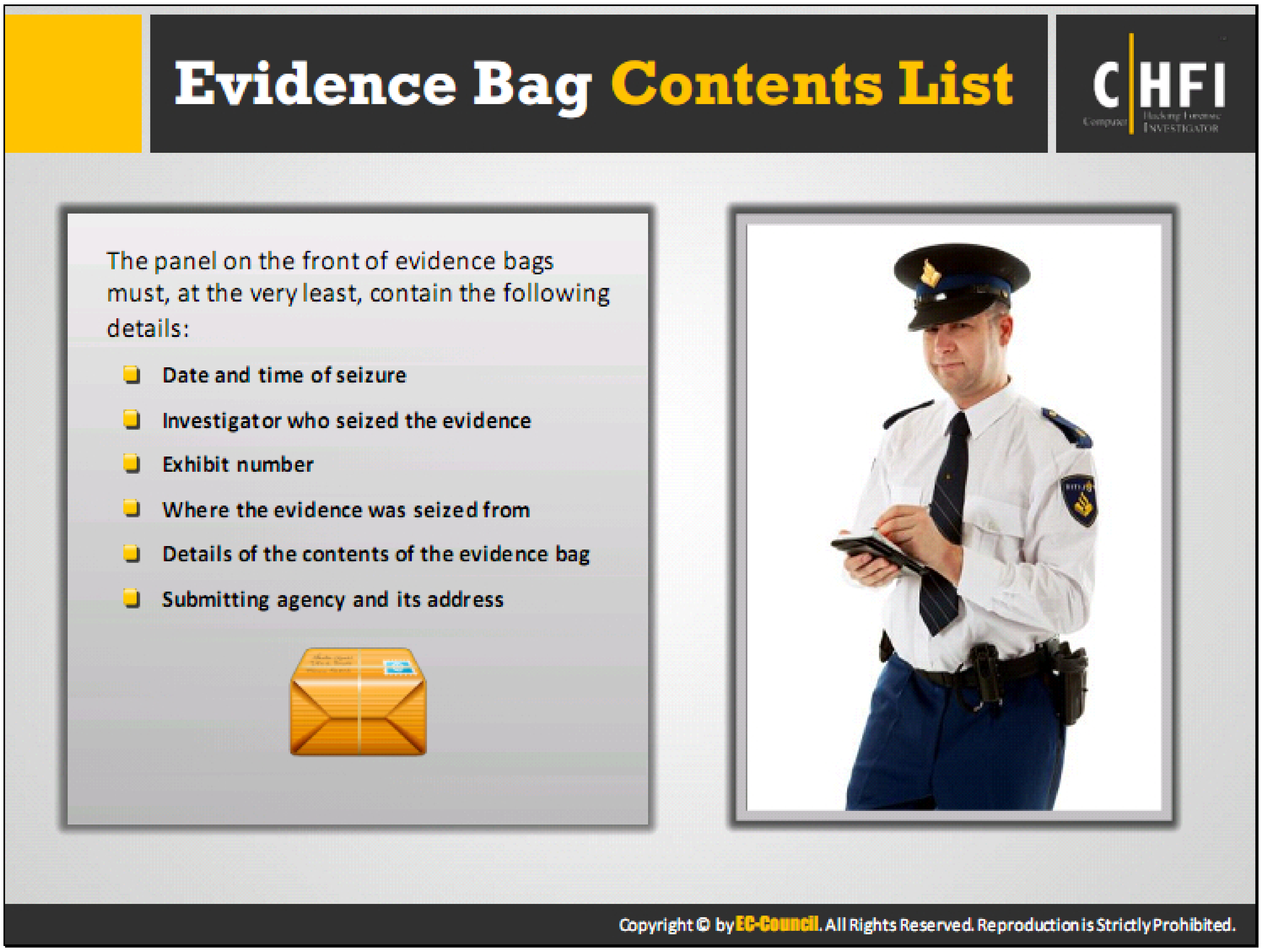
Received from:	By	Date / Time

Final Description: ______________________ Date: ____________________

Crime Lab Number: ______________________________________

Packaging and Transporting Electronic Evidence

Investigators 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 to the court. This section will make you aware of the processes that can help in packaging and transporting the digital evidence in a safe and secure manner.



Evidence Bag **Contents List**

The panel on the front of evidence bags must, at the very least, contain the following details:

- Date and time of seizure
- Investigator 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 name of the officers who took photographs or prepared a scene sketch, sites where individual items were found, and names of the suspects, if any.

Packaging Electronic Evidence

- Make sure the gathered electronic evidence is correctly **documented**, **labeled**, and **listed before packaging**
- Pay special attention to **hidden or trace evidence**, and take necessary actions to safeguard it
- Pack magnetic media in **antistatic packaging**
- Do not use materials such as plastic bags for packaging because they may produce static electricity
- Avoid **folding** and **scratching** storage devices such as diskettes, DVDs, and tapes
- Make sure that all containers that contain evidence are **labeled in the appropriate way**

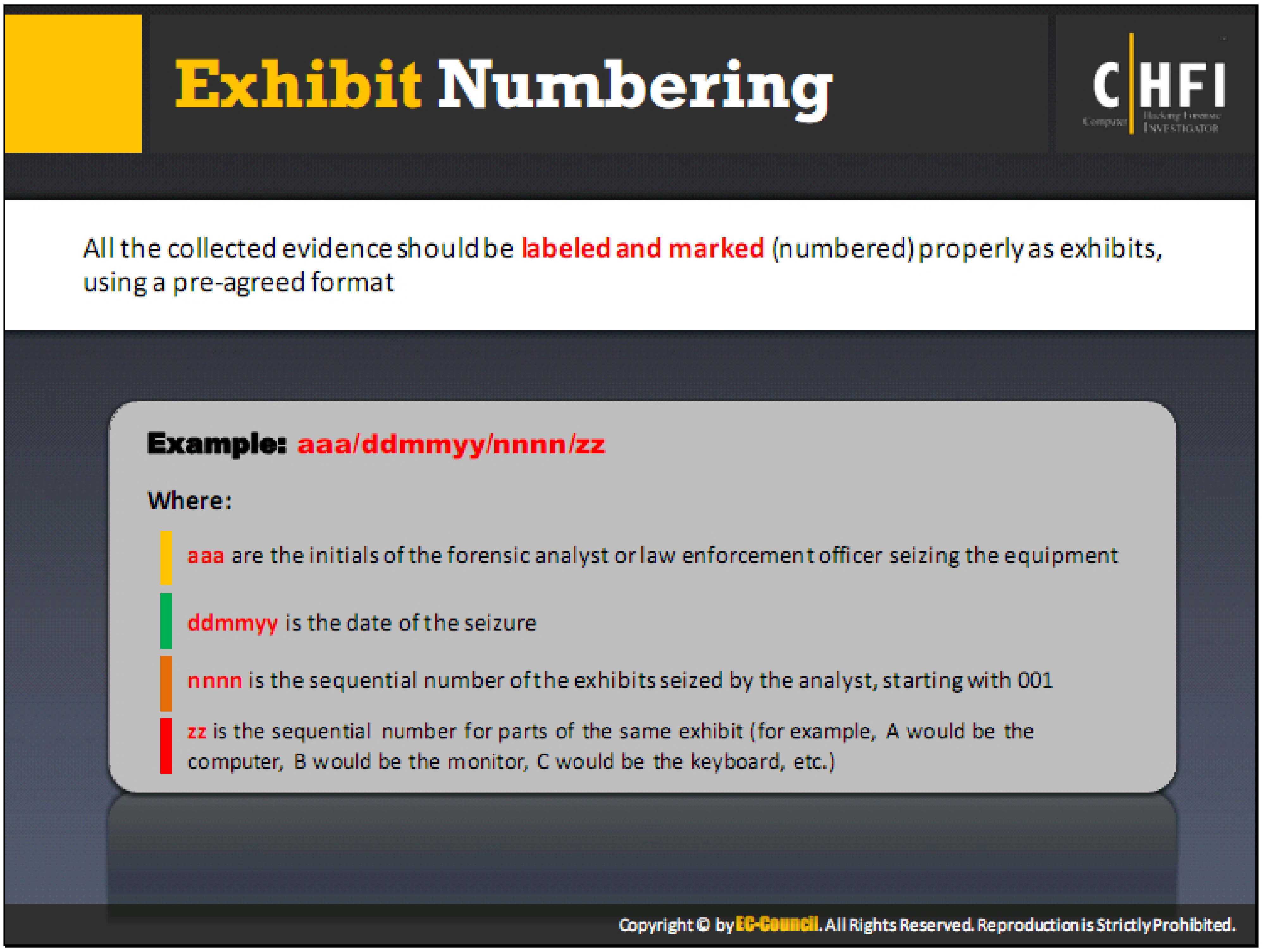


Exhibit Numbering

All the collected evidence should be **labeled and marked** (numbered) properly as exhibits, using a pre-agreed format

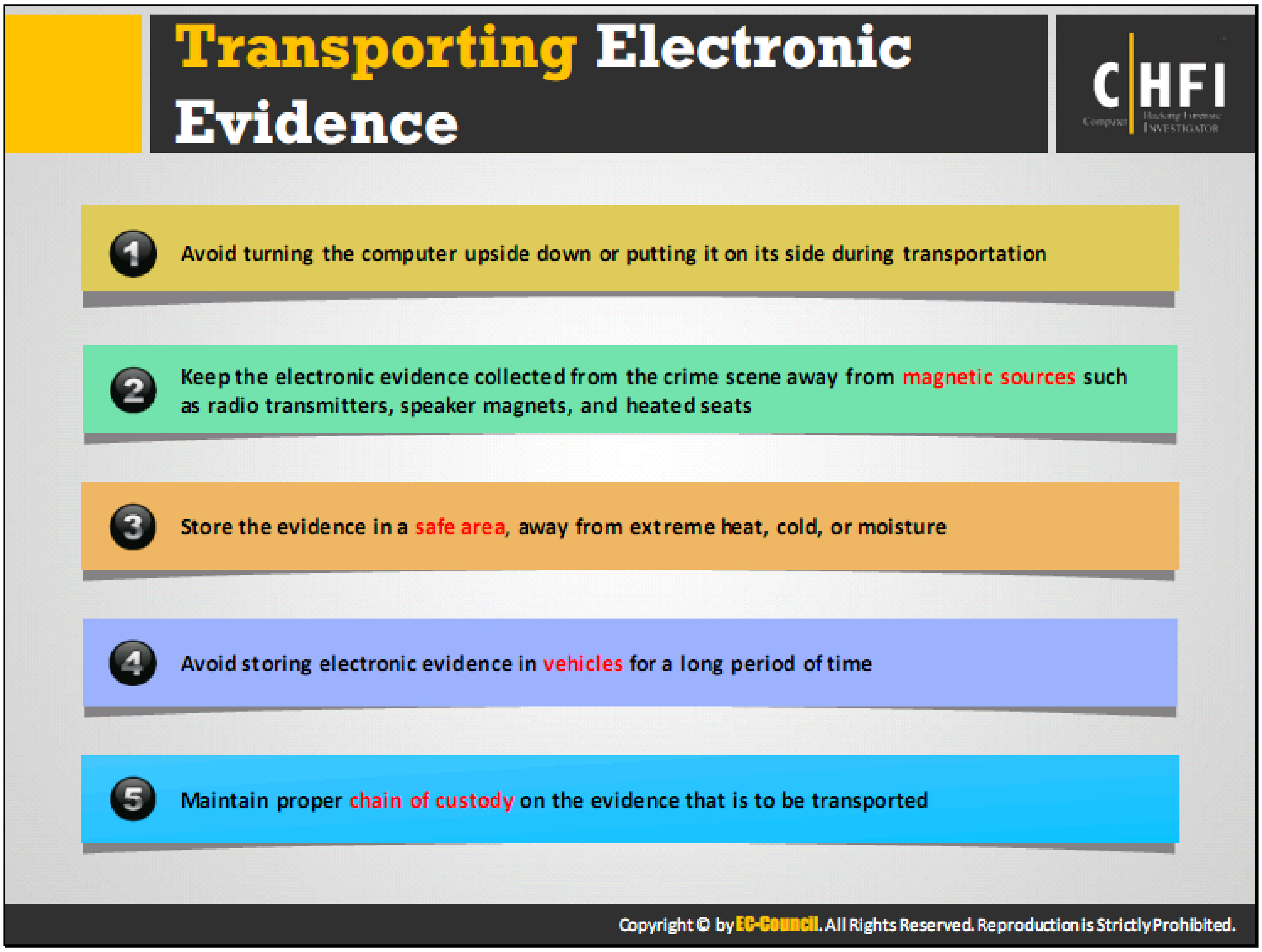
Example: aaa/ddmmyy/nnnn/zz

Where:

- aaa are the initials of the forensic analyst or law enforcement officer seizing the equipment
- ddmmyy is the date of the seizure
- nnnn is the sequential number of the exhibits seized by the analyst, starting with 001
- zz is the sequential number for parts of the same exhibit (for example, A would be the computer, B would be the monitor, C would be the keyboard, etc.)

Exhibit numbering or exhibit labeling refers to the process of tagging evidence with sequential number, which includes case and evidence details. This will allow the investigator to easily identify the evidence and know its details. The investigators should mark all the evidence in a pre-agreed format, such as: aaa/ddmmyy/nnnn/zz. Where:

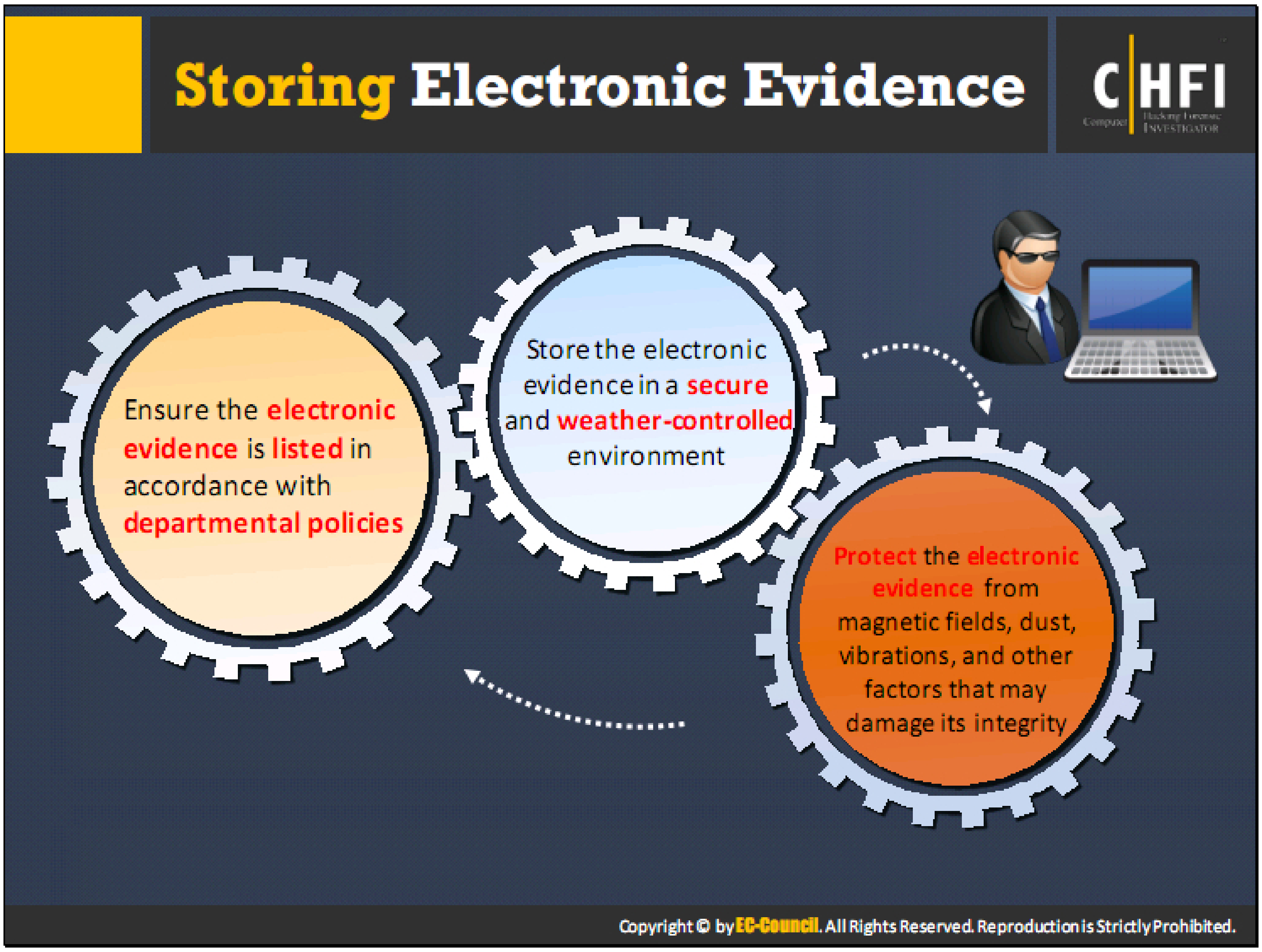
- **aaa** are the initials of the forensic analyst or law enforcement officer seizing the equipment.
- **dd/mm/yy** is the date of seizure.
- **nnnn** is the sequential number of the exhibits seized by aaa, starting with 001 and going to nnnn.
- **zz** is the sequence number for parts of the same exhibit (e.g., ‘A’ could be the CPU, ‘B’ the monitor, ‘C’ the keyboard, etc.)



Transporting Electronic Evidence

CHFI
Computer Hacking Forensic INVESTIGATOR

1. Avoid turning the computer upside down or putting it on its side during transportation
2. Keep the electronic evidence collected from the crime scene away from magnetic sources such as radio transmitters, speaker magnets, and heated seats
3. Store the evidence in a safe area, away from extreme heat, cold, or moisture
4. Avoid storing electronic evidence in vehicles for a long period of time
5. Maintain proper chain of custody on the evidence that is to be transported



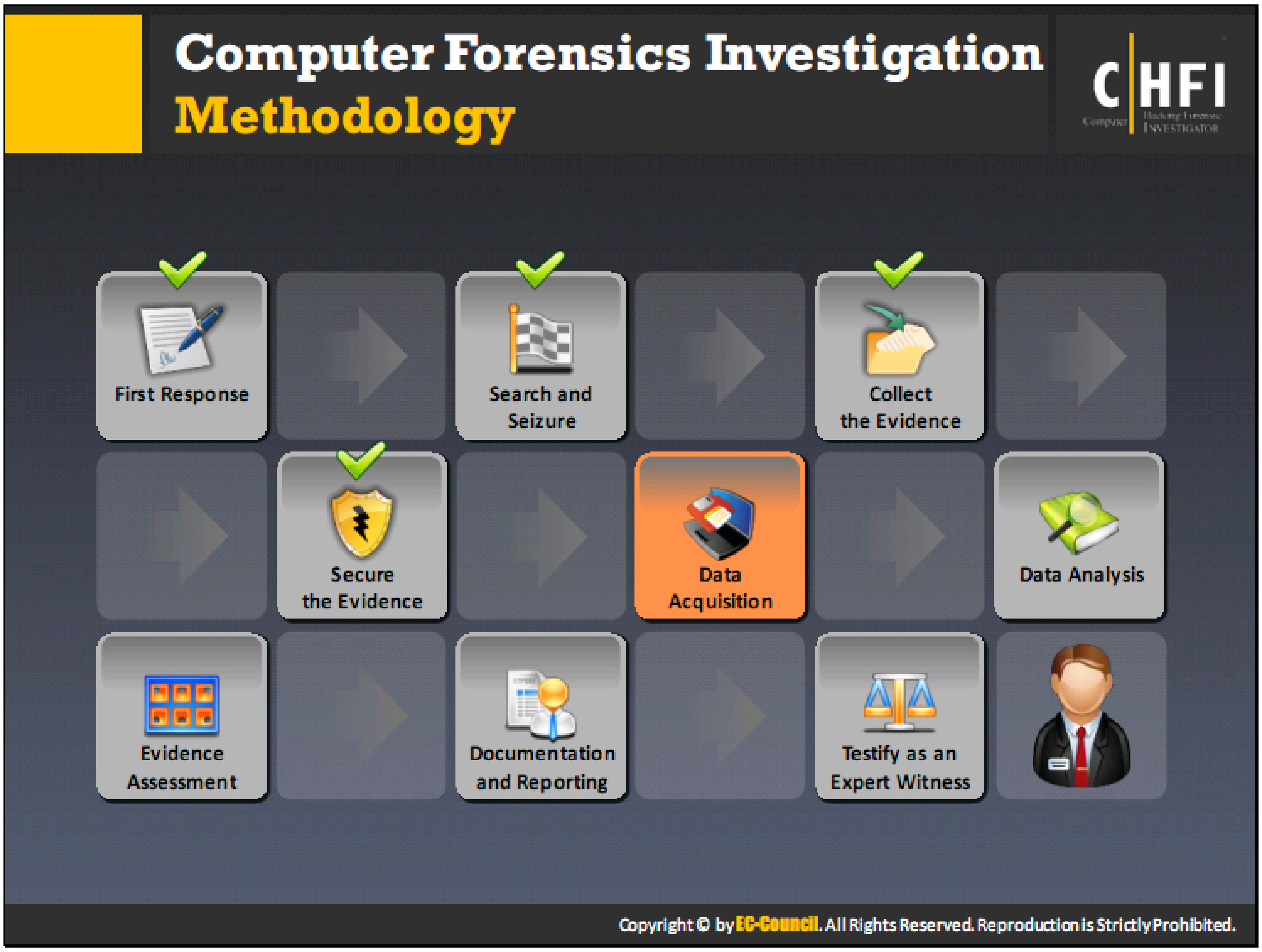
Storing Electronic Evidence

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

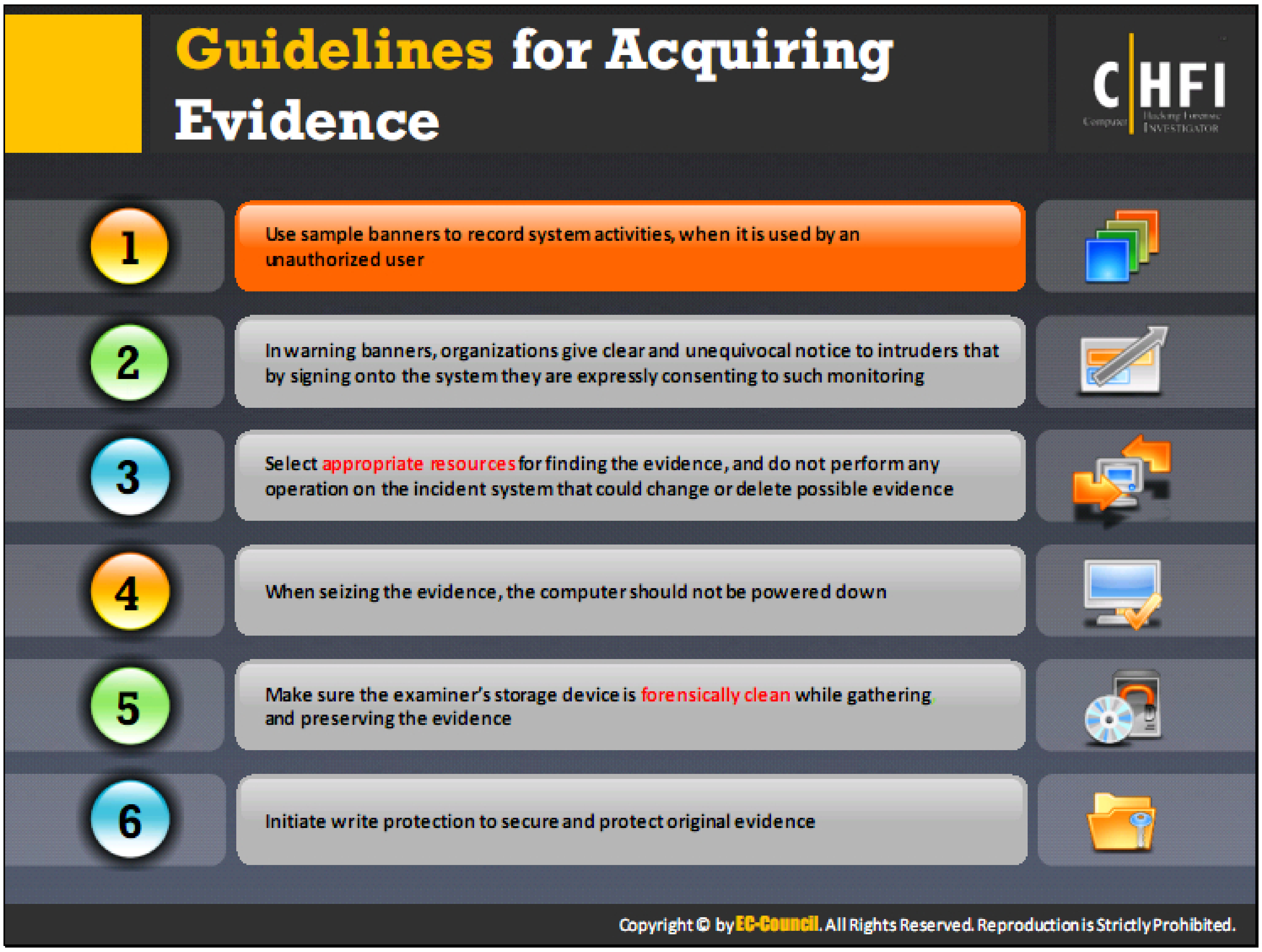
Electronic devices contain digital information that may be potential evidence such as system date, time, and configuration. They lose this potential evidence because of improper and prolonged storage. Digital/electronic evidence is fragile in nature. Therefore, first responders should follow the practices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



Computer Forensics Investigation Methodology

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

During the investigation of digital devices, all the evidence may be present in the form of data. Therefore, the investigators should have expertise in acquiring the data stored across various devices in different forms. This section will describe how the investigators can acquire such data.



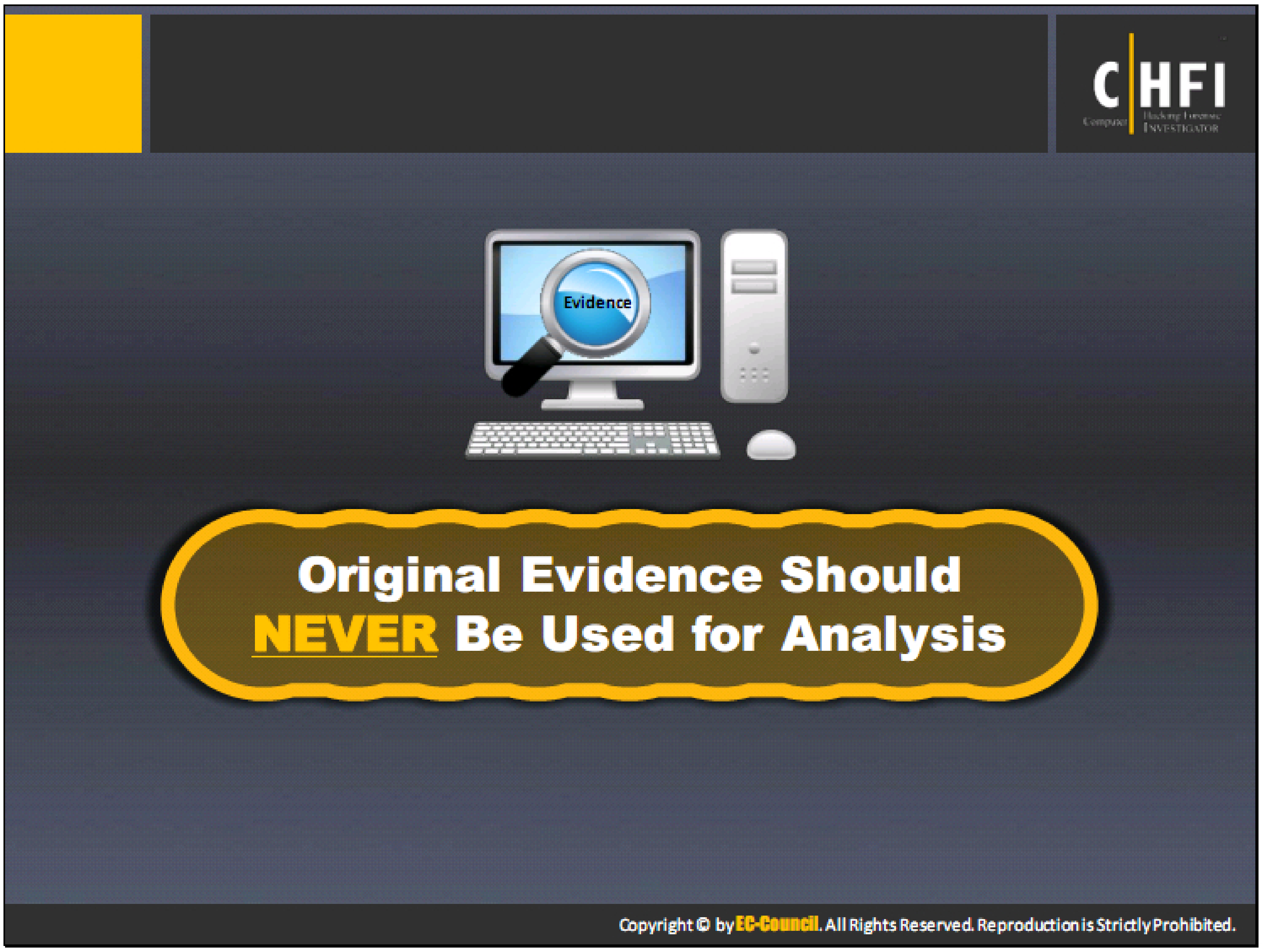
Guidelines for Acquiring Evidence

CHFI
Computer Hacking Forensic INVESTIGATOR

1. Use sample banners to record system activities, when it is used by an unauthorized user
2. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
3. Select appropriate resources for finding the evidence, and do not perform any operation on the incident system that could change or delete possible evidence
4. When seizing the evidence, the computer should not be powered down
5. Make sure the examiner's storage device is forensically clean while gathering and preserving the evidence
6. Initiate write protection to secure and protect original evidence

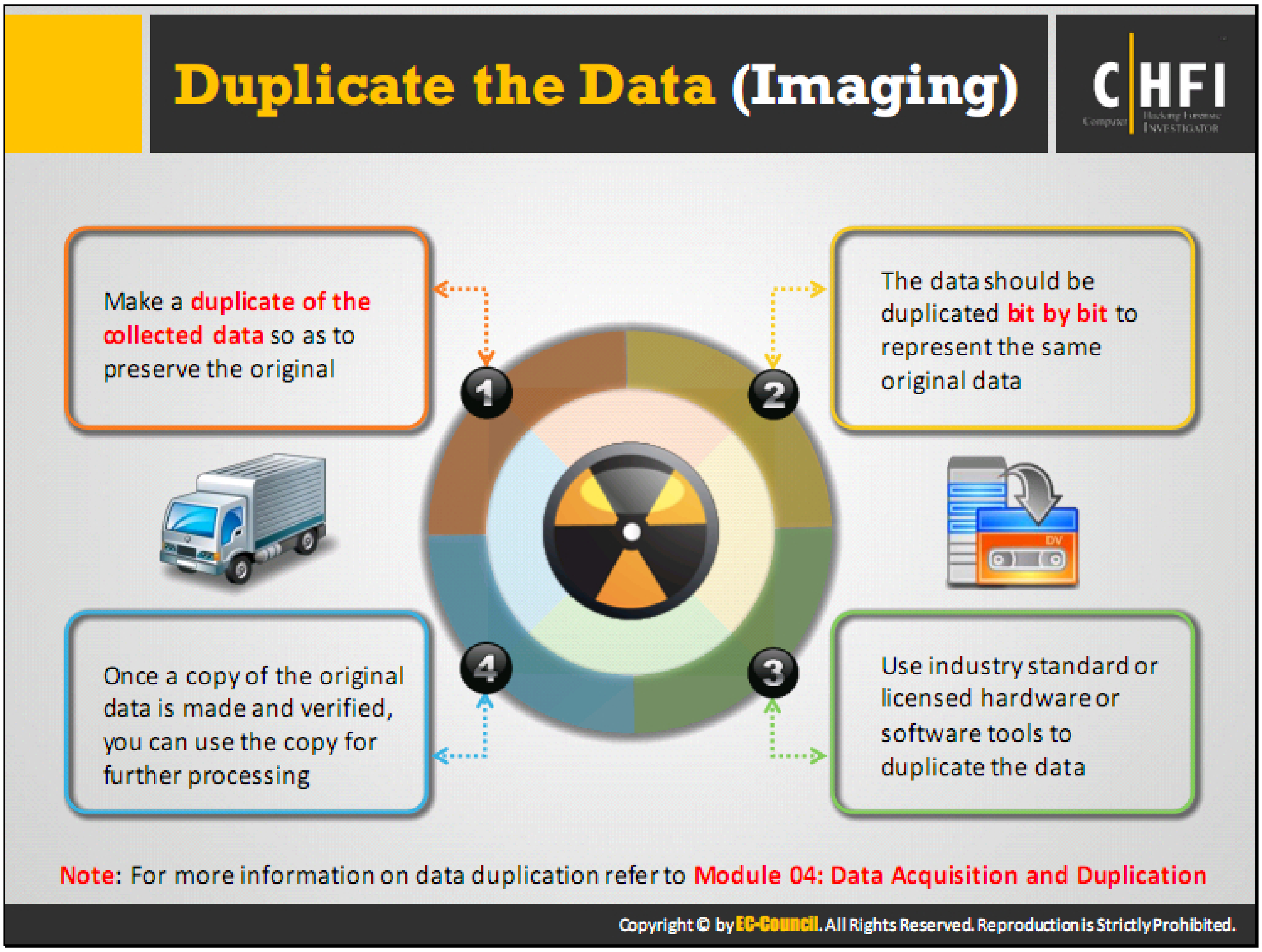
Acquiring evidence is a critical step in the investigation. It changes the scenario of the case, as there can be a large amount of information that helps to solve the case. The guidelines for acquiring the evidence are:

- Select the appropriate resources for finding the evidence.
- Do not perform any operation on the incident system that could change or delete possible evidence.
- Create a duplicate for the evidence and perform forensics on it.
- If the devices carrying evidences are necessary to keep the business running or if the investigators cannot transport the device, copy or image the evidence.
- Use sample banners to record system activities, when used by an unauthorized user.
- Seize any equipment that can act as evidence.
- When seizing the evidence, do not power down the computer.
- Make sure the examiner's storage device is forensically clean while gathering and preserving the evidence.
- Initiate write protection to secure and protect original evidence.
- In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring.



Original Evidence Should **NEVER** Be Used for Analysis

Investigation and analysis processes can have both positive and negative impact over the evidential data, and sometimes these processes can alter this data in such a way that it is no longer acceptable in a court of law. Therefore, the investigators should make copies of the evidence and work on it to avoid damage to the original data in case of accidents or mishaps. This section will discuss the procedures that the investigators should follow to avoid damage of evidence files.



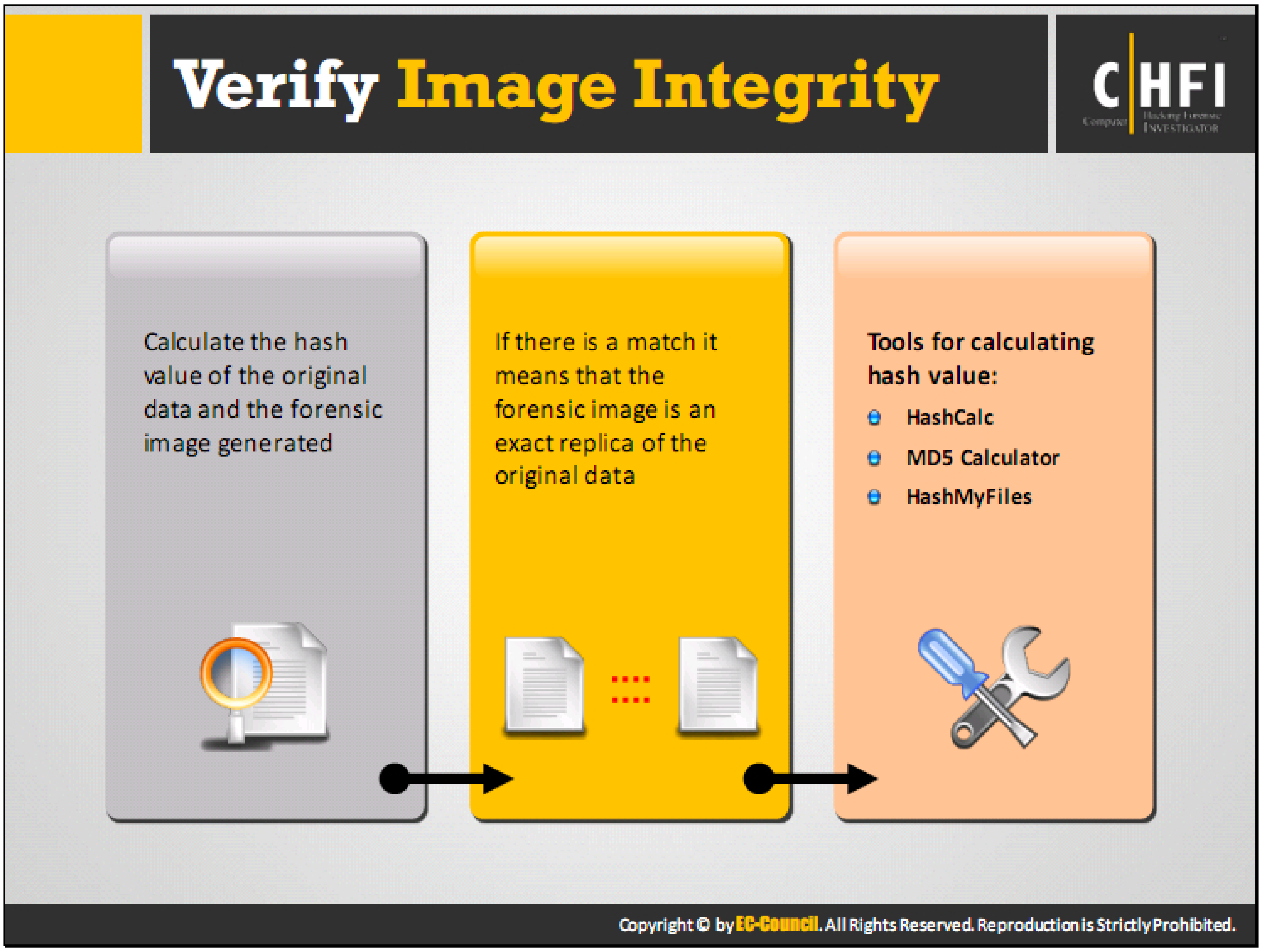
Duplicate the Data (Imaging)

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

Note: For more information on data duplication refer to **Module 04: Data Acquisition and Duplication**

Performing the investigation on the original evidence can misdirect the investigation 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.



Verify Image Integrity

Calculate the hash value of the original data and the forensic image generated

If there is a match it means that the forensic image is an exact replica of the original data

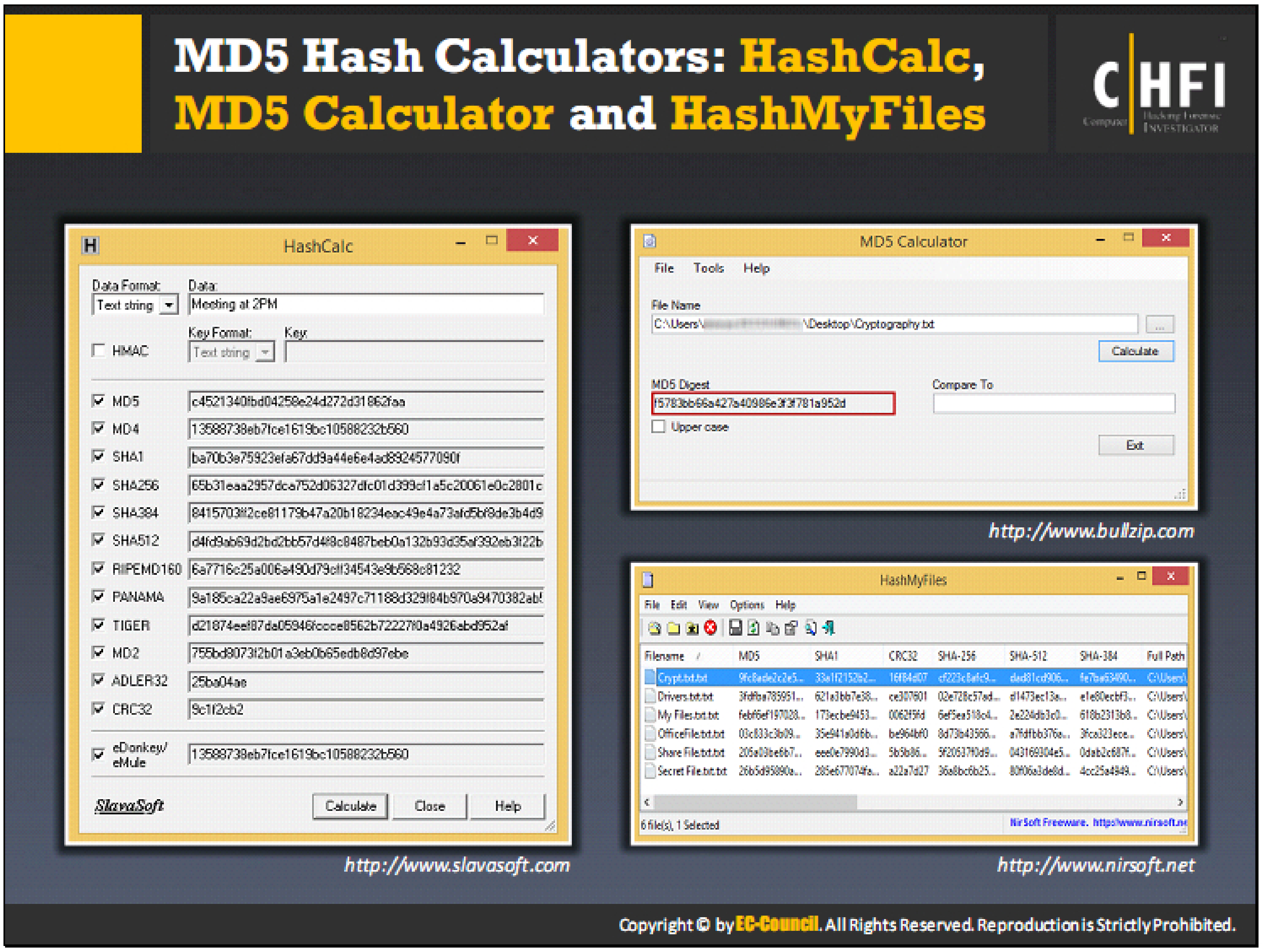
Tools for calculating hash value:

- **HashCalc**
- **MD5 Calculator**
- **HashMyFiles**

Hash values are equivalent to data fingerprints. No two files contain the same hash values. The hash algorithms used in forensics are MD5 and SHA. Calculate and match the MD5 hash for the original evidence and the forensic image. The same hash values show that the image is the same as the evidence.

Tools for calculating hash value are:

- **HashCalc:** HashCalc is a calculator that allows computing message digest checksums and HMACs for files, as well as for text and hex strings.
- **MD5 Calculator:** The MD5 Calculator is a program that will enable you to calculate the MD5 value of the selected file.
- **HashMyFiles:** HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system.



MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles

HashCalc

Data Format: Text string
Data: Meeting at 2PM
□ HMAC
Key Format: Text string
Key:

☑ MD5	c4521340fbd04258e24d272d31862faa
☑ MD4	13588738eb7fce1619bc10588232b560
☑ SHA1	ba70b3e75923efa67dd9a44e6e4ad8924577090f
☑ SHA256	65b31eaa2957dca752d06327dfc01d399cf1a5c20061e0c2801c
☑ SHA384	8415703ff2ce81179b47a20b18234eac49e4a73afd5bf8de3b4d9
☑ SHA512	d4fd9ab69d2bd2bb57d4f8c8487beb0a132b93d35af392eb3f22b
☑ RIPEMD160	6a7716c25a006a490d79cff34543e9b568c81232
☑ PANAMA	9a185ca22a9ae6975a1e2497c71188d329f84b970a9470382ab!
☑ TIGER	d21874eef87da05946fccce8562b72227f0a4926abd952af
☑ MD2	755bd8073f2b01a3eb0b65edb8d97ebe
☑ ADLER32	25ba04ae
☑ CRC32	9c1f2cb2
☑ eDonkey/ eMule	13588738eb7fce1619bc10588232b560

http://www.slavasoft.com

MD5 Calculator

File Name: C:\Users\[redacted]\Desktop\Cryptography.txt

MD5 Digest: f5783bb66a427a40986e3f3f781a952d
Compare To:
□ Upper case

http://www.bullzip.com

HashMyFiles

Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	Full Path
Crypt.txt.txt	9fc8ade2c2e5...	33a1f2152b2...	16f84d07	cf223c8afc9...	dad81cd906...	fe7ba63490...	C:\Users\
Drivers.txt.txt	3fdfba785951...	621a3bb7e38...	ce307601	02e728c57ad...	d1473ec13a...	e1e80ecbf3...	C:\Users\
My Files.txt.txt	febf6ef197028...	173ecbe9453...	0062f5fd	6ef5ea518c4...	2e224db3c0...	618b2313b8...	C:\Users\
OfficeFile.txt.txt	03c833c3b09...	35e941a0d6b...	be964bf0	8d73b43566...	a7fdfbb376a...	3fca323ece...	C:\Users\
Share File.txt.txt	205a03be6b7...	eee0e7990d3...	5b5b86...	9f20637f0d9...	043169304e5...	0dab2c687f...	C:\Users\
Secret File.txt.txt	26b5d95890a...	285e677074fa...	a22a7d27	36a8bc6b25...	80f06a3de8d...	4cc25a4949...	C:\Users\

6 file(s), 1 Selected

http://www.nirsoft.net

HashCalc

Source: http://www.slavasoft.com

HashCalc allows computing message digest checksums and HMACs for files, as well as for text and hex strings. It offers a choice of 13 hash and checksum algorithms for calculations.

Features:

- Support for 12 well-known and documented hash and checksum algorithms: MD2, MD4, MD5, SHA-1, SHA-2 (256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, and CRC32
- Support for a custom hash algorithm (MD4-based) used in eDonkey and eMule applications
- Support for 2 modes of calculations: HASH/CHECKSUM and HMAC
- Support for 3 input data formats: files, text strings, and hex strings
- Works with large size files (tested on file sizes up to 15 GB)
- Drag-and-drop support
- Quick and easy installation
- Calculates hash/checksum and HMAC for files of any type: music, audio, sound, video, image, icon, text, compression, etc., with the extensions: .mp3, .wav, .avi, .mpg, .midi,

.mov, .dvd, .ram, .zip, .rar, .ico, .gif, .pif, .pic, .tif, .tiff, .txt, .doc, .pdf, .wps, .dat, .dll, .hex, .bin, .iso, .cpp, .dss, .par, .pps, .cue, .ram, .md5, .sfv, etc.

MD5 Calculator

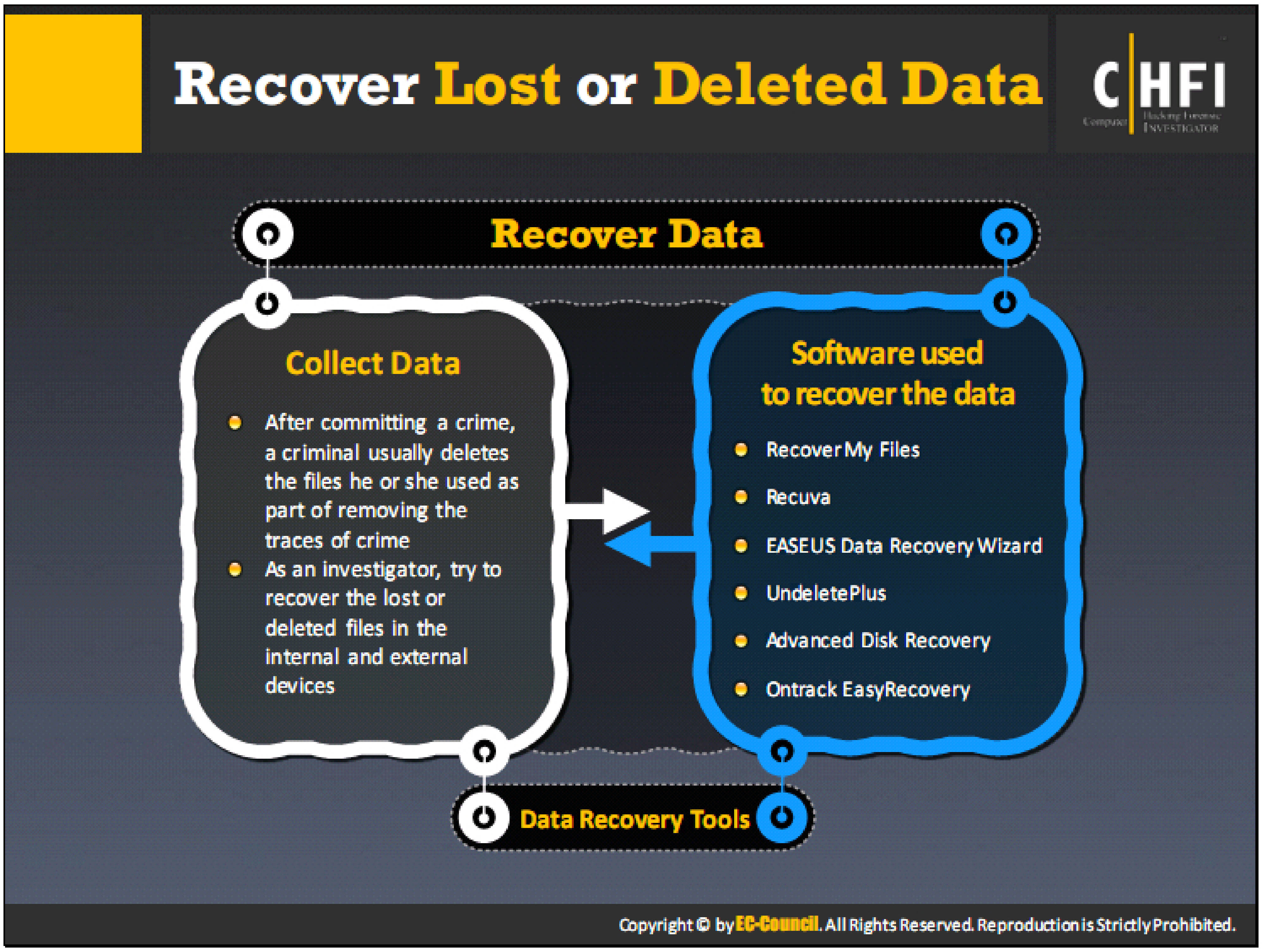
Source: *http://www.bullzip.com*

The MD5 Calculator is a program that will enable you to right-click any file and select "MD5 Calculator" from the context menu. This will calculate the MD5 value of the selected file. You can compare the calculated value to a value given to you by another person or from a website.

HashMyFiles

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

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system. HashMyFiles can also be launched from the context menu of Windows Explorer and display the MD5/SHA1 hashes of the selected file or folder. HashMyFiles does not require any installation process or additional DLL files.



Recover Lost or Deleted Data

Recover Data

Collect Data

- After committing a crime, a criminal usually deletes the files he or she used as part of removing the traces of crime
- As an investigator, try to recover the lost or deleted files in the internal and external devices

Software used to recover the data

- Recover My Files
- Recuva
- EASEUS Data Recovery Wizard
- UndeletePlus
- Advanced Disk Recovery
- Ontrack EasyRecovery

Data Recovery Tools

Modern operating systems make it difficult to delete a file completely from a system. When a file is deleted unintentionally, stop using the system. Collect the lost or deleted data for evidence on the internal and external devices.

Software used to recover the data

Examples of software used to recover lost or deleted data:

Recover My Files

Source: http://www.recovermyfiles.com

Recover My Files data recovery software will recover deleted files emptied from the Windows Recycle Bin, or lost because of the format or corruption of a hard drive, virus or Trojan infection, and unexpected system shutdown or software failure.

Recuva

Source: https://www.piriform.com

Recuva can recover pictures, music, documents, videos, emails or any other file type that are lost. It can recover from any rewriteable media like memory cards, external hard drives, USB sticks etc.

EASEUS Data Recovery Wizard

Source: http://www.easeus.com

It is hard drive data recovery software to recover data lost from PCs, laptops, or other storage media because of deleting, formatting, partition loss, OS crash, virus attack etc.

Advanced Disk Recovery

Source: http://www.systweak.com

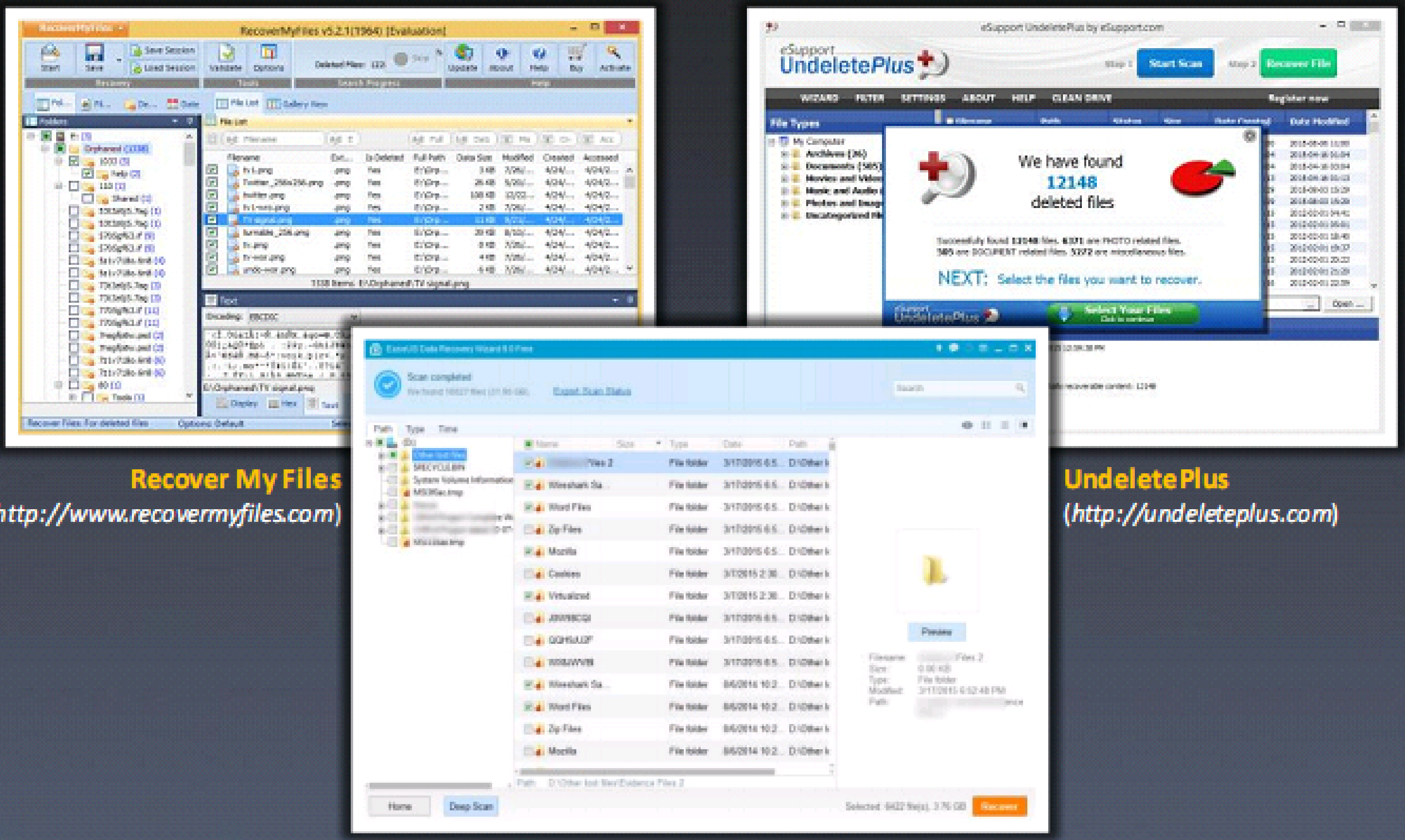
Advanced Disk Recovery scans the entire system for deleted files and folders and provides an opportunity to recover them. Hard drives, partitions, external devices, and even CDs and DVDs can be scanned for recoverable files using Advanced Disk Recovery. The software offers two types of scans. The Quick Scan uses the Master File Table to find all files with the same filename. The Deep Scan uses file signatures to search for deleted files or folders. After either type of scan, one can preview the deleted files and folders, and restore any or all of them to the location of choice. With just a few clicks, one can locate and restore most of the deleted files.

Ontrack EasyRecovery

Source: https://www.krollontrack.com

Ontrack EasyRecovery is a data recovery software ready to retrieve missing files. It recovers data and also protects it.

Data Recovery Software



We have found
12148
deleted files

Successfully found 12148 files. 6371 are PHOTO related files. 505 are DOCUMENT related files. 5272 are miscellaneous files.

NEXT: Select the files you want to recover.

Recover My Files (*http://www.recovermyfiles.com*)

UndeletePlus (*http://undeleteplus.com*)

EASEUS Data Recovery Wizard (*http://www.easeus.com*)

Recover My Files

Source: http://www.recovermyfiles.com

Recover My Files data recovery software will recover deleted files emptied from the Windows Recycle Bin, or lost because of formatting or corruption of a hard drive, virus or Trojan infection, and unexpected system shutdown or software failure. Recover My Files can preview the data "on-the-fly" while searching.

Features:

- Recover files even if they are emptied from the Recycle Bin.
- Recover files after accidental format, even if you have reinstalled Windows.
- Recover disks after a hard disk crash.
- Get back files after a partitioning error.
- Get data back from RAW hard drives.
- Recover documents, photos, video, music, and email.
- Recover from a hard drive, camera card, USB, Zip, floppy disk, iPod, and other media.

UndeletePlus

Source: http://www.undeleteplus.com

- Recovers documents, photos, video, music, and email.
- Recover files - even those emptied from the Recycle Bin.
- File recovery after accidental format - even if one has reinstalled Windows.
- Recover files from hard drives, USB thumb drives, camera media cards, floppy disks, and other storage devices.

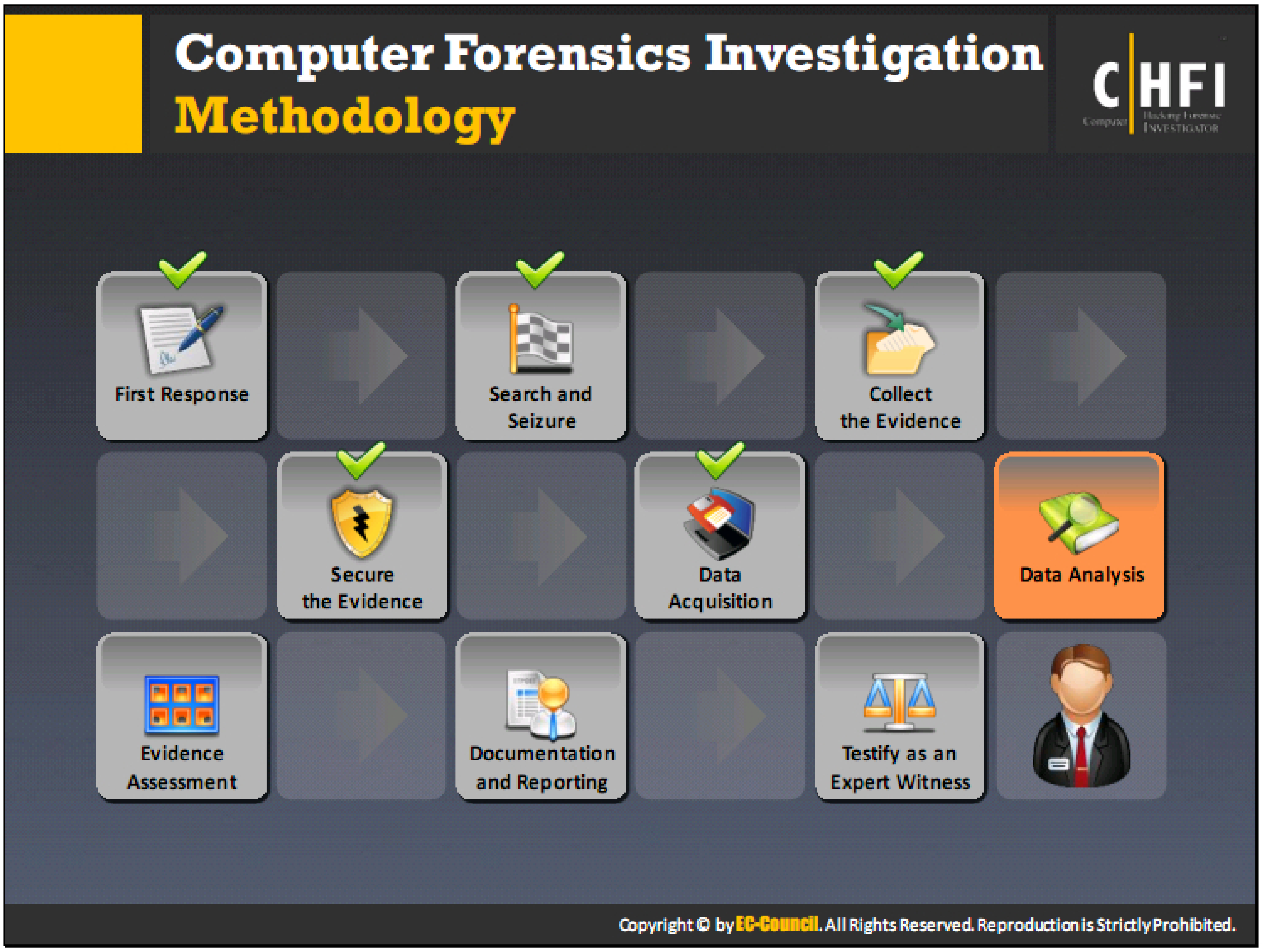
EASEUS Data Recovery Wizard

Source: http://www.easeus.com

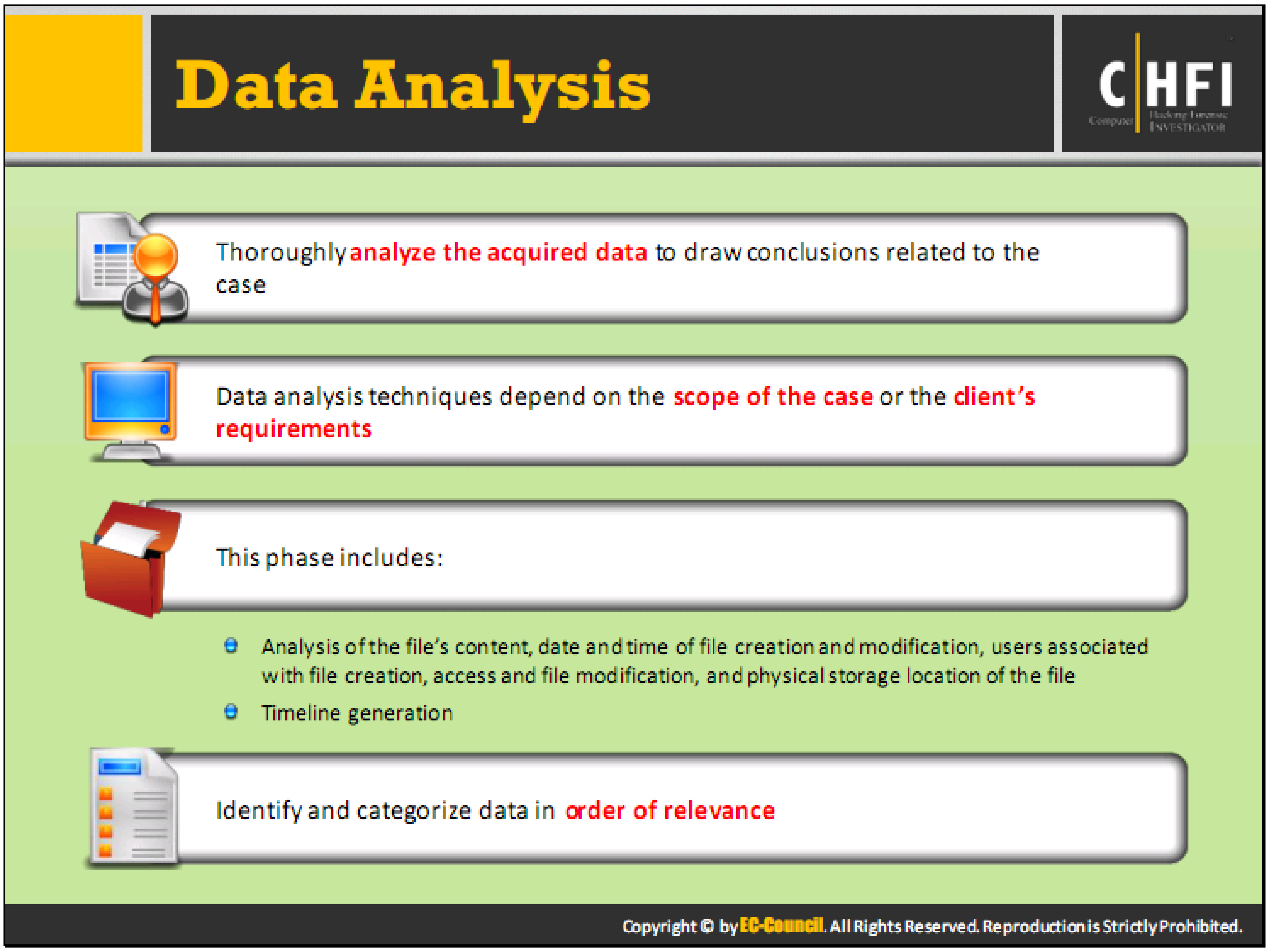
It is a hard drive data recovery software that provides a reliable data recovery solution to save all kinds of data loss scenarios. It enables you to recover different files from PC/laptop, hard drive, lost or raw partition, USB drive, memory card, digital camera, music player or other storage devices because of deleting, formatting, partition loss, partition inaccessibility, virus attack or other unknown reasons.

Features:

- Supports large hard disk.
- Specify your recovery file types before scanning for precise searching results.
- Filter your search by file name, type, and date to find files.
- Preview the files to check their details and quality before you decide to recover them.


Computer Forensics Investigation
Methodology
CHFI Computer Hacking Forensic Investigator
First Response
Search and Seizure
Collect the Evidence
Secure the Evidence
Data Acquisition
Data Analysis
Evidence Assessment
Documentation and Reporting
Testify as an Expert Witness
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data analysis refers to the process of going through the data and finding the relevant evidential data and its relevance to the crime. This section will explain the process of analyzing the data in order to use it for proving the crime and the perpetrator.



Data Analysis

CHFI

Thoroughly **analyze the acquired data** to draw conclusions related to the case

Data analysis techniques depend on the **scope of the case** or the **client's requirements**

This phase includes:

- Analysis of the file's content, date and time of file creation and modification, users associated with file creation, access and file modification, and physical storage location of the file
- Timeline generation

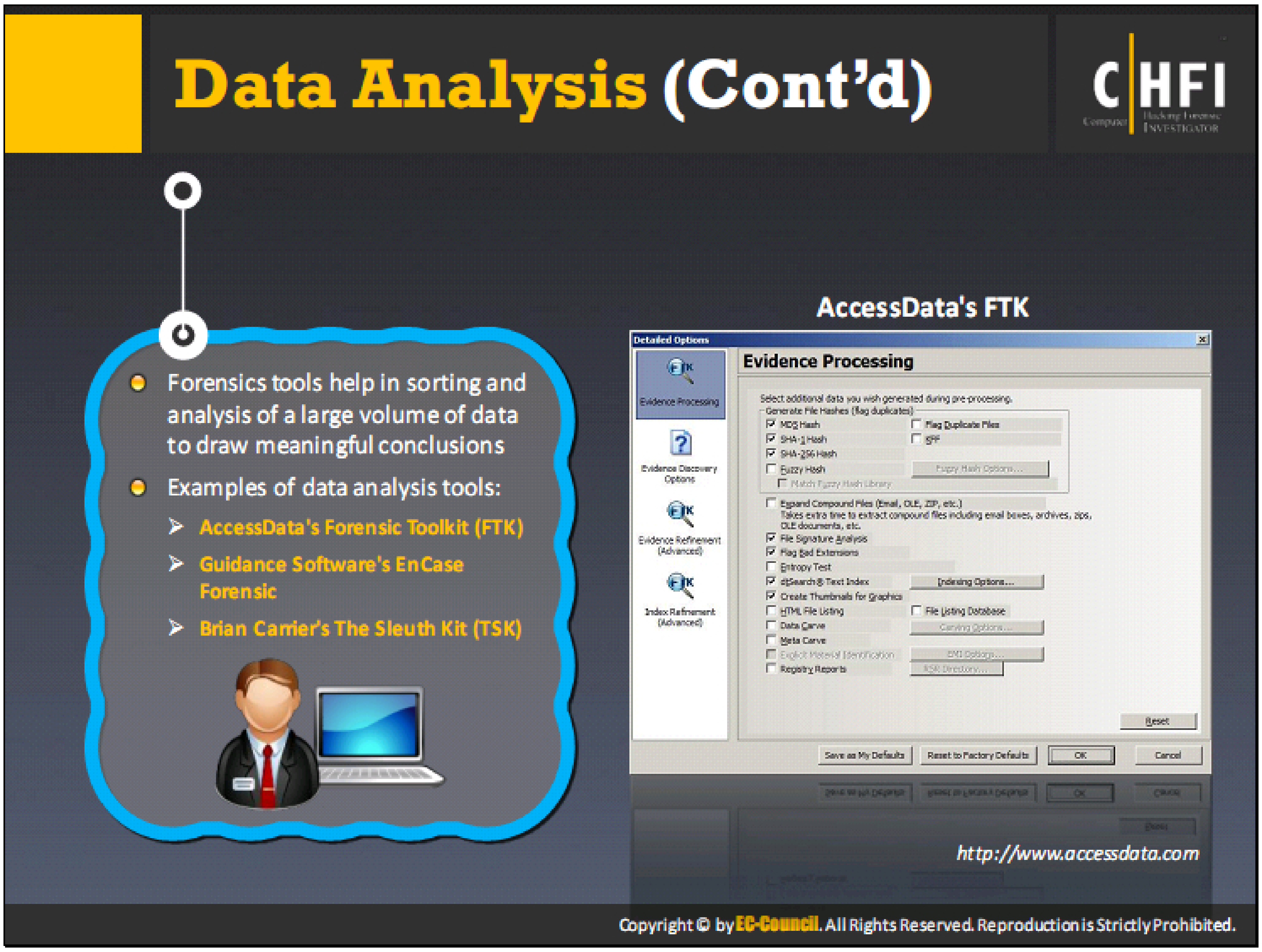
Identify and categorize data in **order of relevance**

Data analysis refers to the process of examining, identifying, separating, converting, and modeling data to isolate useful information. In forensic investigation, the data analysis helps in gathering and examining data to find its relevance with the incident in order to submit the findings to an authority for conclusions and decision-making.

Thoroughly analyze the acquired data to draw conclusions related to the case. Data analysis techniques depend on the scope of the case or client's requirements, and the type of evidence. This phase includes:

- Analyzing the file content for data usage
- Analyzing the date and time of file creation and modification
- Users associated with file creation, access, and file modification
- Physical storage location of the file
- Timeline generation

Identify and categorize data in order of relevance to the case, such that the most relevant data serves as the most important evidence to the case.



Data Analysis (Cont'd)

- Forensics tools help in sorting and analysis of a large volume of data to draw meaningful conclusions
- Examples of data analysis tools:
  - **AccessData's Forensic Toolkit (FTK)**
  - **Guidance Software's EnCase Forensic**
  - **Brian Carrier's The Sleuth Kit (TSK)**

AccessData's FTK

Detailed Options

Evidence Processing

Select additional data you wish generated during pre-processing.

Generate File Hashes (flag duplicates)

☑ MD5 Hash
☐ Flag Duplicate Files
☑ SHA-1 Hash
☐ KFF
☑ SHA-256 Hash
☐ Fuzzy Hash
☐ Match Fuzzy Hash Library

☐ Expand Compound Files (Email, OLE, ZIP, etc.)
Takes extra time to extract compound files including email boxes, archives, zips, OLE documents, etc.
☑ File Signature Analysis
☑ Flag Bad Extensions
☐ Entropy Test
☑ dtSearch® Text Index
☑ Create Thumbnails for Graphics
☐ HTML File Listing
☐ File Listing Database
☐ Data Carve
☐ Meta Carve
☐ Explicit Material Identification
☐ Registry Reports

CHFI
Computer Hacking Forensic Investigator
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Fuzzy Hash Options...
Indexing Options...
Carving Options...
EMI Options...
RSR Directory...
Reset
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

http://www.accessdata.com

AccessData's FTK

Source: http://www.accessdata.com

FTK Imager is a data preview and imaging tool that enables 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.

EnCase® Forensic

Source: https://www.guidancesoftware.com

EnCase is a popular multi-purpose forensic platform that includes many useful tools to support several areas of the digital forensic process. This tool can collect a lot of data from many devices and extract potential evidence. It also generates an evidence report.

EnCase Forensic can help investigators 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.

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

- GREP
- Conditional
- Boolean
- Word searches

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

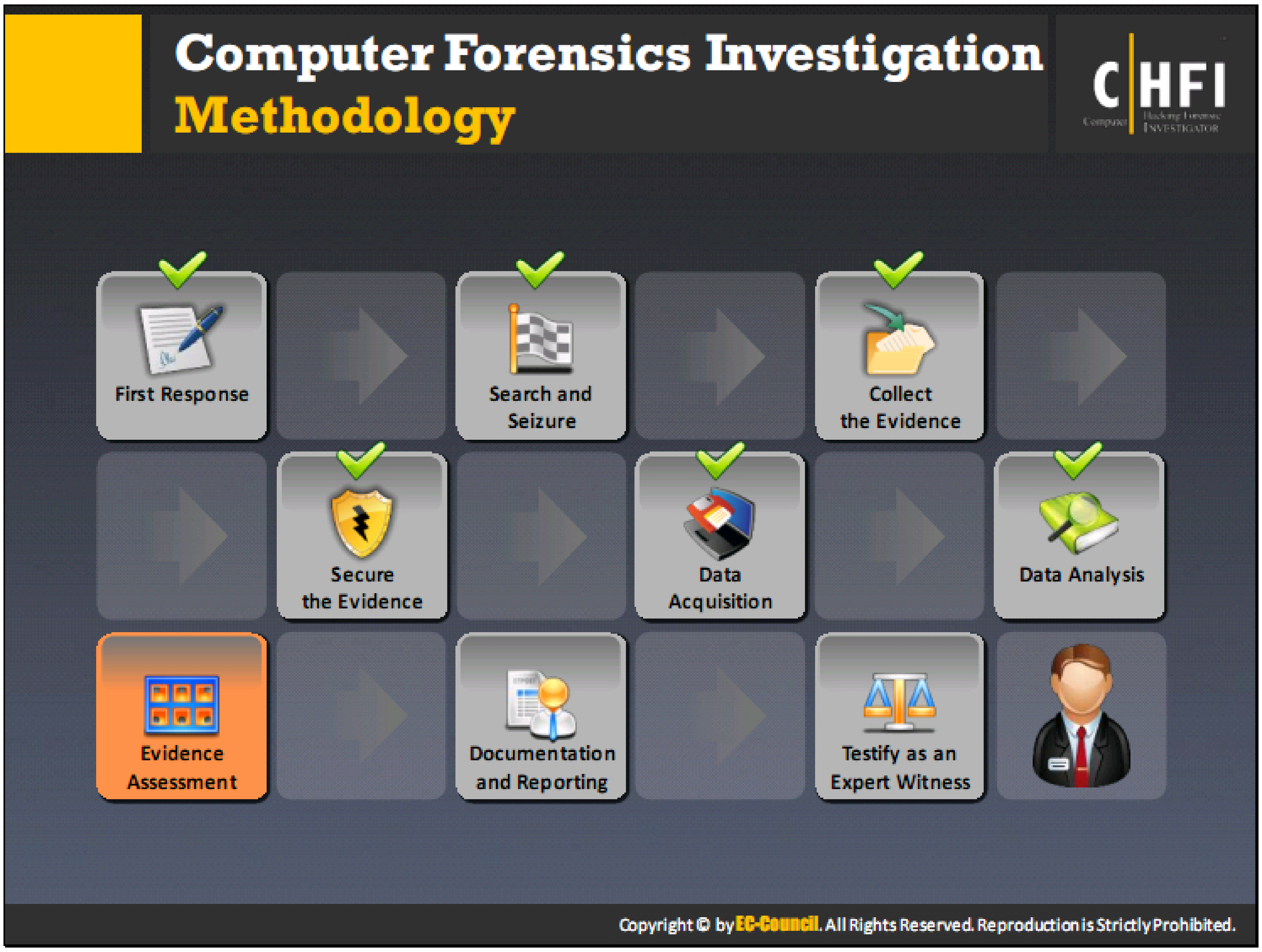
The Sleuth Kit (TSK)

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

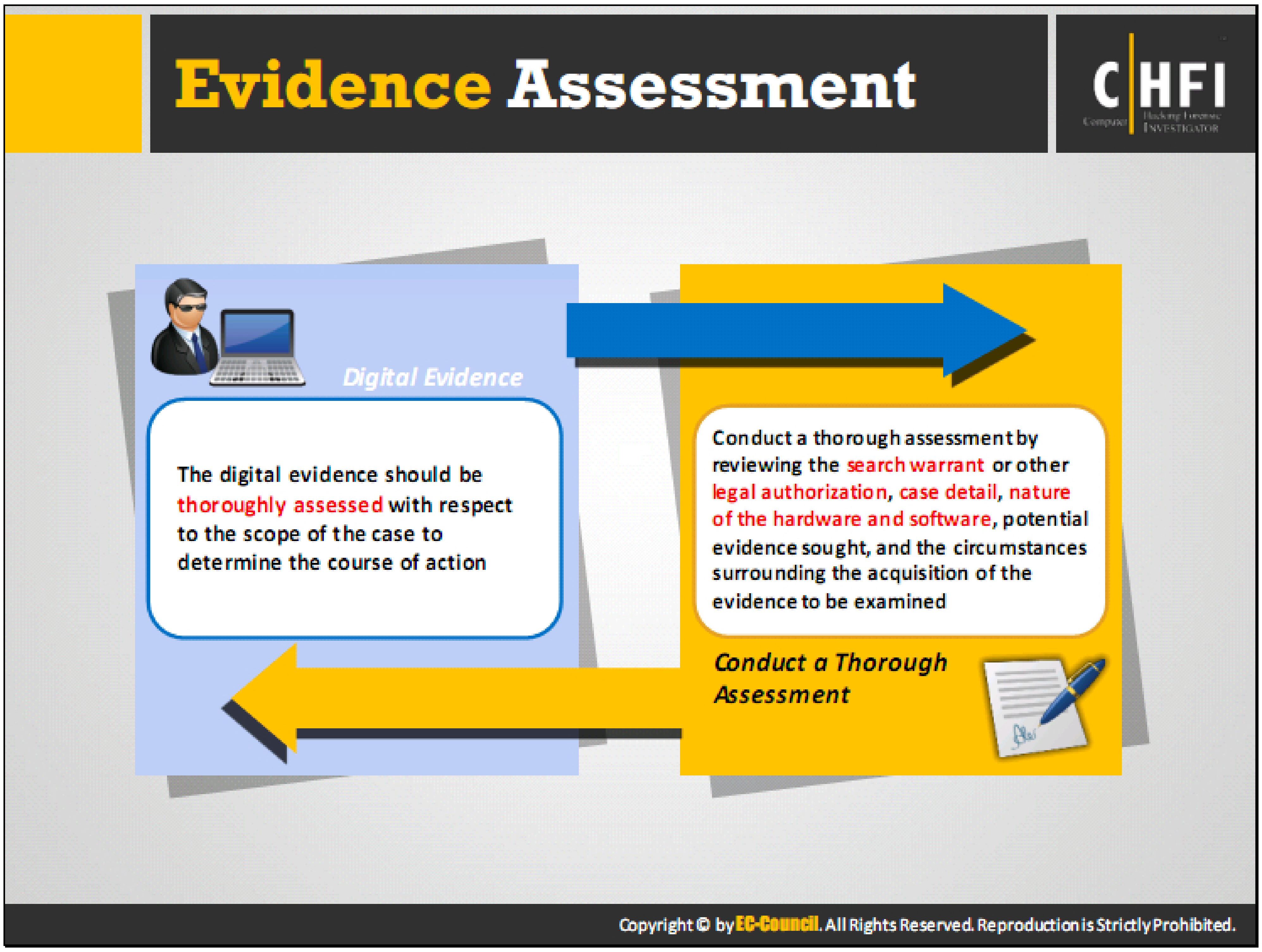
The Sleuth Kit (TSK) is a library and collection of command line tools that allows investigating disk images. The core functionality of TSK allows analyzing volume and filing system data. The plug-in framework also allows incorporating additional modules to analyze file contents and build automated systems. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.

Post-investigation Phase

The responsibility of the investigators does not end with finding the evidence data and analyzing it, but they should also be able to explain how they arrived at the conclusion to the prosecutors, attorneys, and judges. This section will provide knowledge on assessing the data, documenting it in an easily understandable manner, and creating easy to read reports.


Computer Forensics Investigation
Methodology
CHFI
Computer Hacking Forensic Investigator
First Response
Search and Seizure
Collect the Evidence
Secure the Evidence
Data Acquisition
Data Analysis
Evidence Assessment
Documentation and Reporting
Testify as an Expert Witness
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evidence assessment is the process of relating the obtained evidential data to the incident for understanding how the complete incident took place. This section will discuss the process of evidence assessment.



Evidence Assessment

Digital Evidence

The digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action

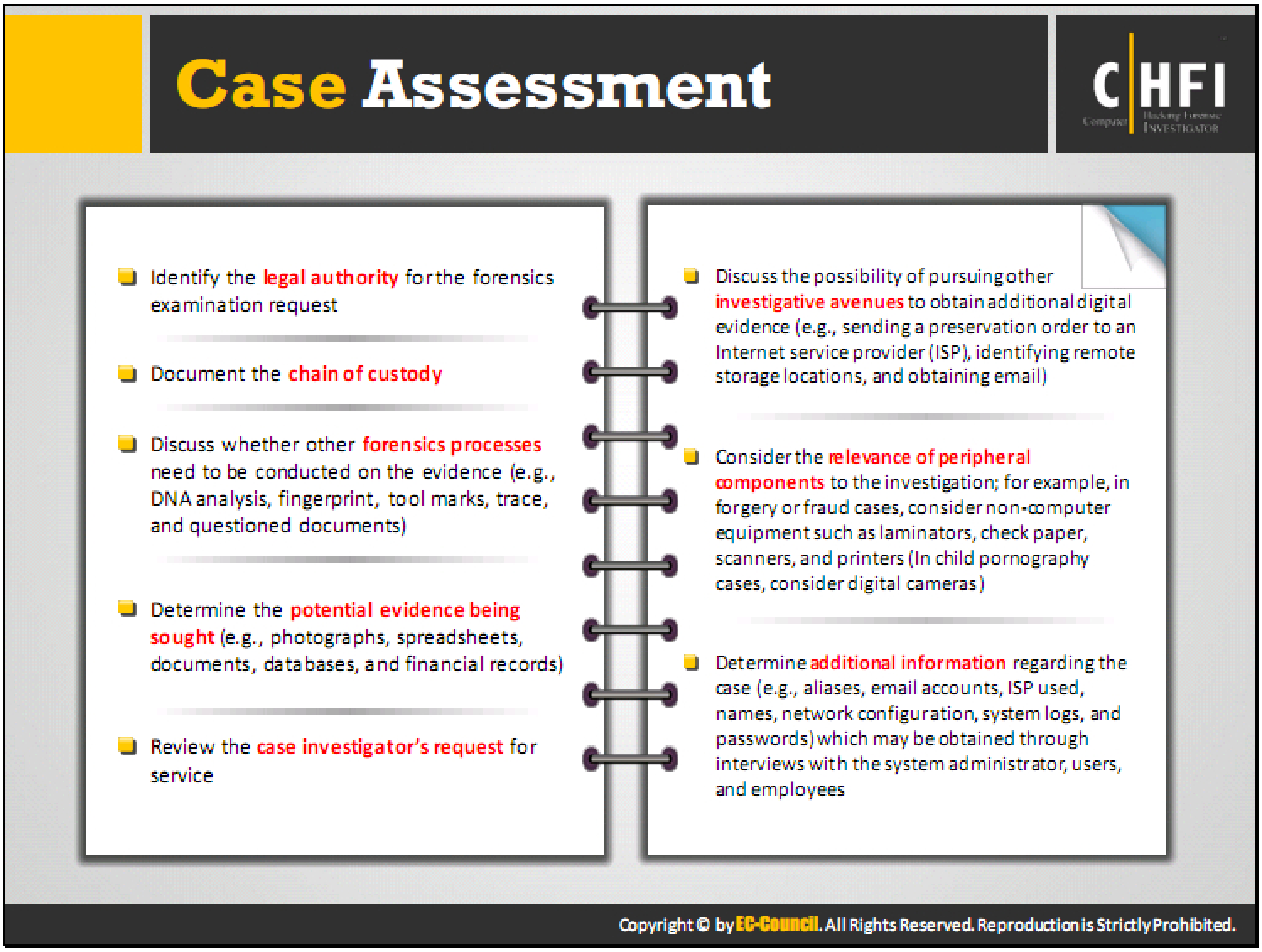
Conduct a thorough assessment by reviewing the search warrant or other legal authorization, case detail, nature of the hardware and software, potential evidence sought, and the circumstances surrounding the acquisition of the evidence to be examined

Conduct a Thorough Assessment

Evidence assessment is about evaluating the evidence and clues related to the incident that can be helpful in solving the case. Assessment of evidence is a crucial stage in the forensics process. Evidence assessment depends on the type of incident, the objectives required to perform the incident, the 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 in order to decide the course of action.

Procedure:

Assess thoroughly by analyzing the search warrant and other legal authorization, such as the case details, the nature of the hardware and software, and the circumstances of evidence acquisition.



Case Assessment

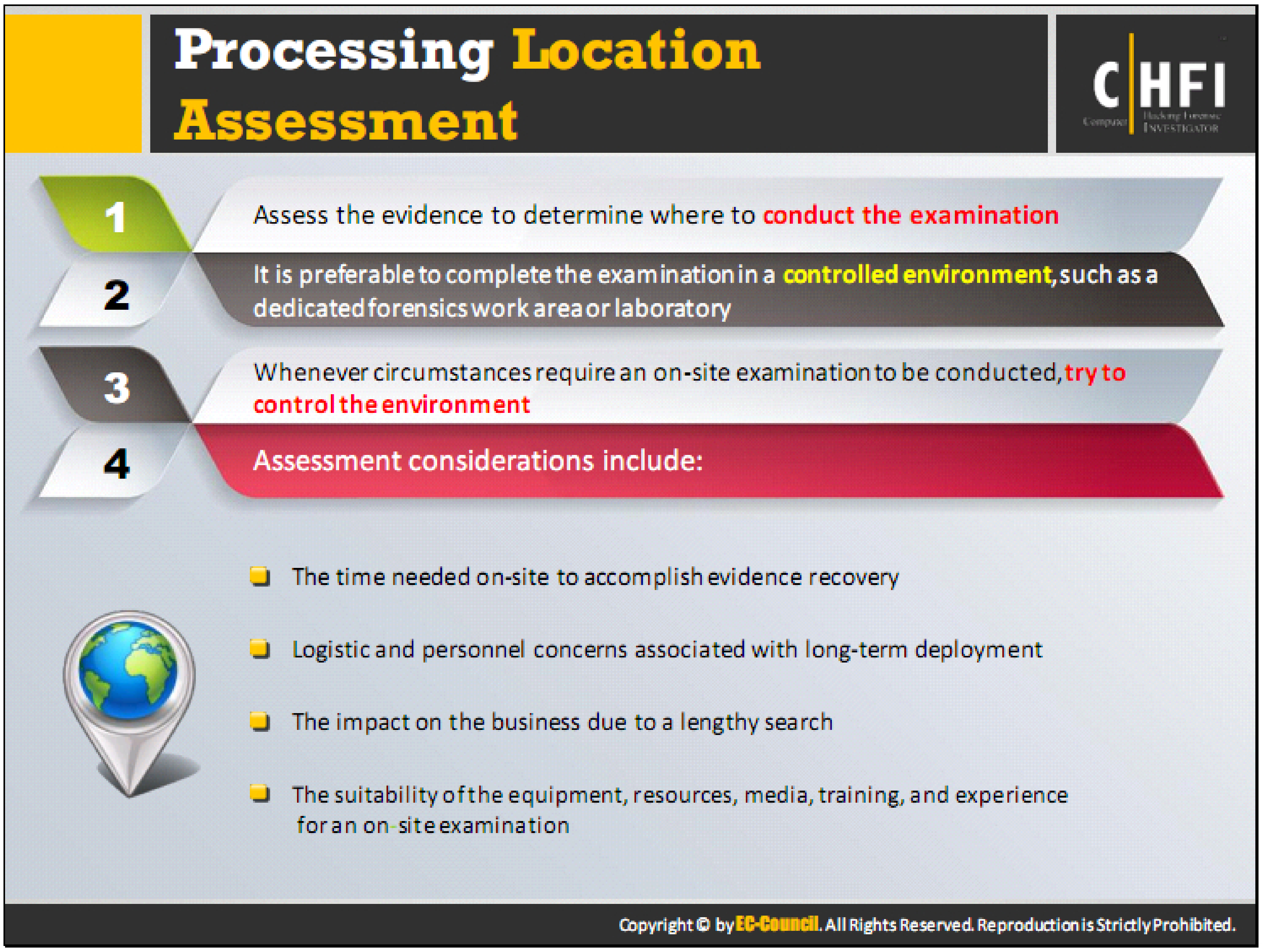
- Identify the legal authority for the forensics examination request
- Document the chain of custody
- Discuss whether other forensics processes need to be conducted on the evidence (e.g., DNA analysis, fingerprint, tool marks, trace, and questioned documents)
- Determine the potential evidence being sought (e.g., photographs, spreadsheets, documents, databases, and financial records)
- Review the case investigator's request for service
- Discuss the possibility of pursuing other investigative avenues to obtain additional digital evidence (e.g., sending a preservation order to an Internet service provider (ISP), identifying remote storage locations, and obtaining email)
- Consider the relevance of peripheral components to the investigation; for example, in forgery or fraud cases, consider non-computer equipment such as laminators, check paper, scanners, and printers (In child pornography cases, consider digital cameras)
- Determine additional information regarding the case (e.g., aliases, email accounts, ISP used, names, network configuration, system logs, and passwords) which may be obtained through interviews with the system administrator, users, and employees

In this phase, the investigator assesses the impact of the incident on the organization, the reasons and the source of the incident, steps required to tackle the incident, the investigating team required to handle the case, the procedure of investigation, and the possible outcome of the forensic process. Case assessment is important to implement a proper plan in handling the case and achieving desired results.

The guidelines for performing case assessment:

- Initially examine the investigator's service request.
- Get the legal authority to obtain a forensic examination request.
- Ensure that the request assignment has sufficient required assistance.
- Provide the complete chain of custody.
- Check if the evidence requires forensic processes, such as analysis of DNA, fingerprints, tool marks, trace evidence, and questioned documents.
- Establish the potential evidence sought.
- Review the case investigator's request for service.
- Check if there is a possibility to follow investigative methods, such as to identify a remote storage location, to send a preservation order to an Internet service provider (ISP), and to obtain email.

- Identify the relevance of various network elements to the crime scene, such as credit cards, check papers, scanners, and cameras.
- Obtain additional details such as email addresses, ISP used, and names.
- Evaluate the skill levels of the users to identify their expertise in destroying or concealing the evidence.
- Set the order of the evidence examination.
- Ascertain the requirement for additional personnel.
- Identify the requirement for additional equipment.



Processing Location Assessment

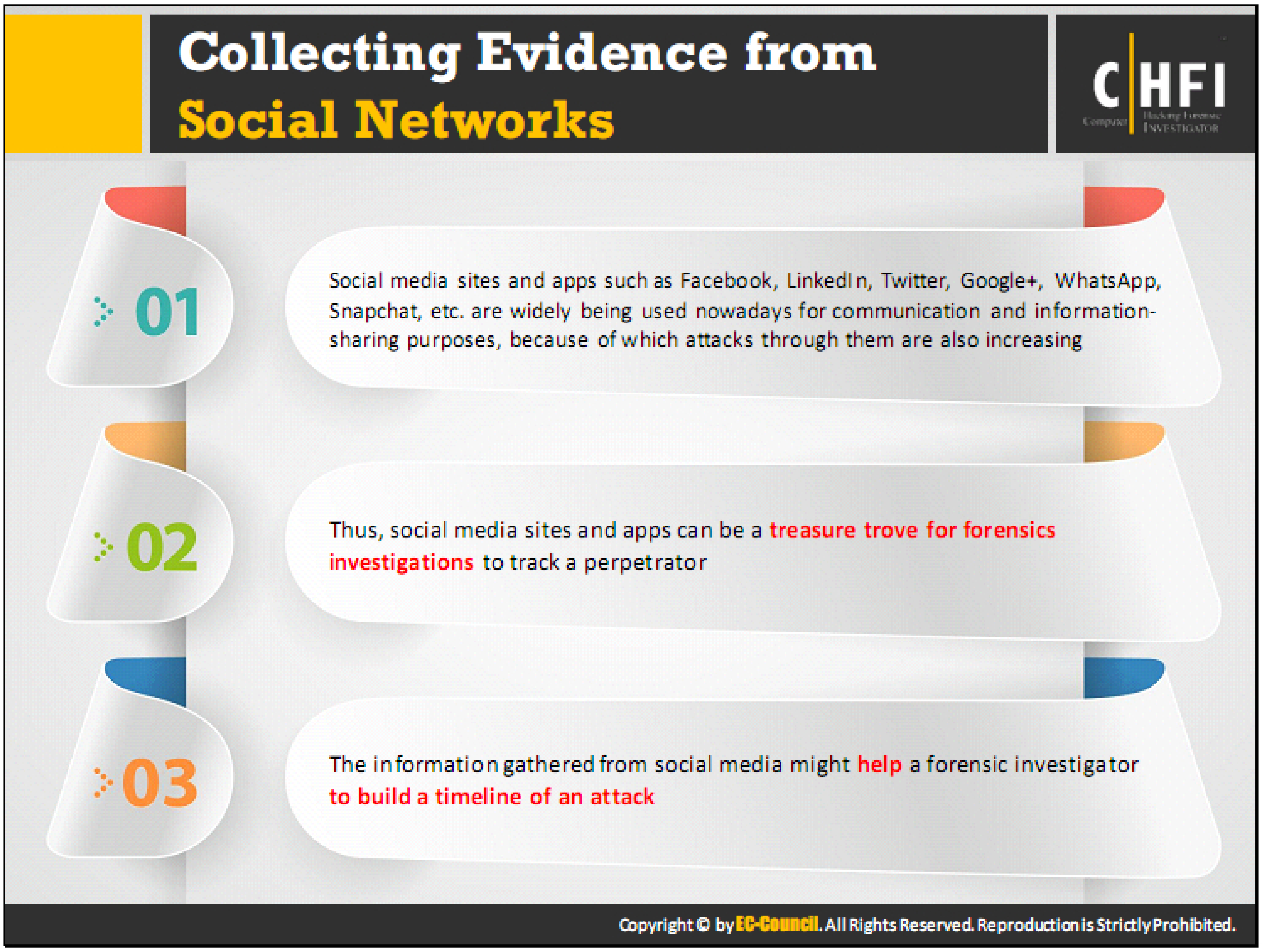
1. Assess the evidence to determine where to **conduct the examination**
2. It is preferable to complete the examination in a **controlled environment**, such as a dedicated forensics work area or laboratory
3. Whenever circumstances require an on-site examination to be conducted, **try to control the environment**
4. Assessment considerations include:

- The time needed on-site to accomplish evidence recovery
- Logistic and personnel concerns associated with long-term deployment
- The impact on the business due to a lengthy search
- The suitability of the equipment, resources, media, training, and experience for an on-site examination

Decide the place to examine the evidence after accessing it. The recommendation for the environment includes a forensic work area or laboratory. It is better to have a controlled environment in case the examination is onsite.

Considerations for the assessment location might include the following:

- The time required to recover the evidence when onsite.
- Logistic and workforce concerns related to long-term deployment.
- Business impact of a time-consuming search.
- Any equipment, resources, media, training, and experience suitable for an onsite examination.



Collecting Evidence from Social Networks

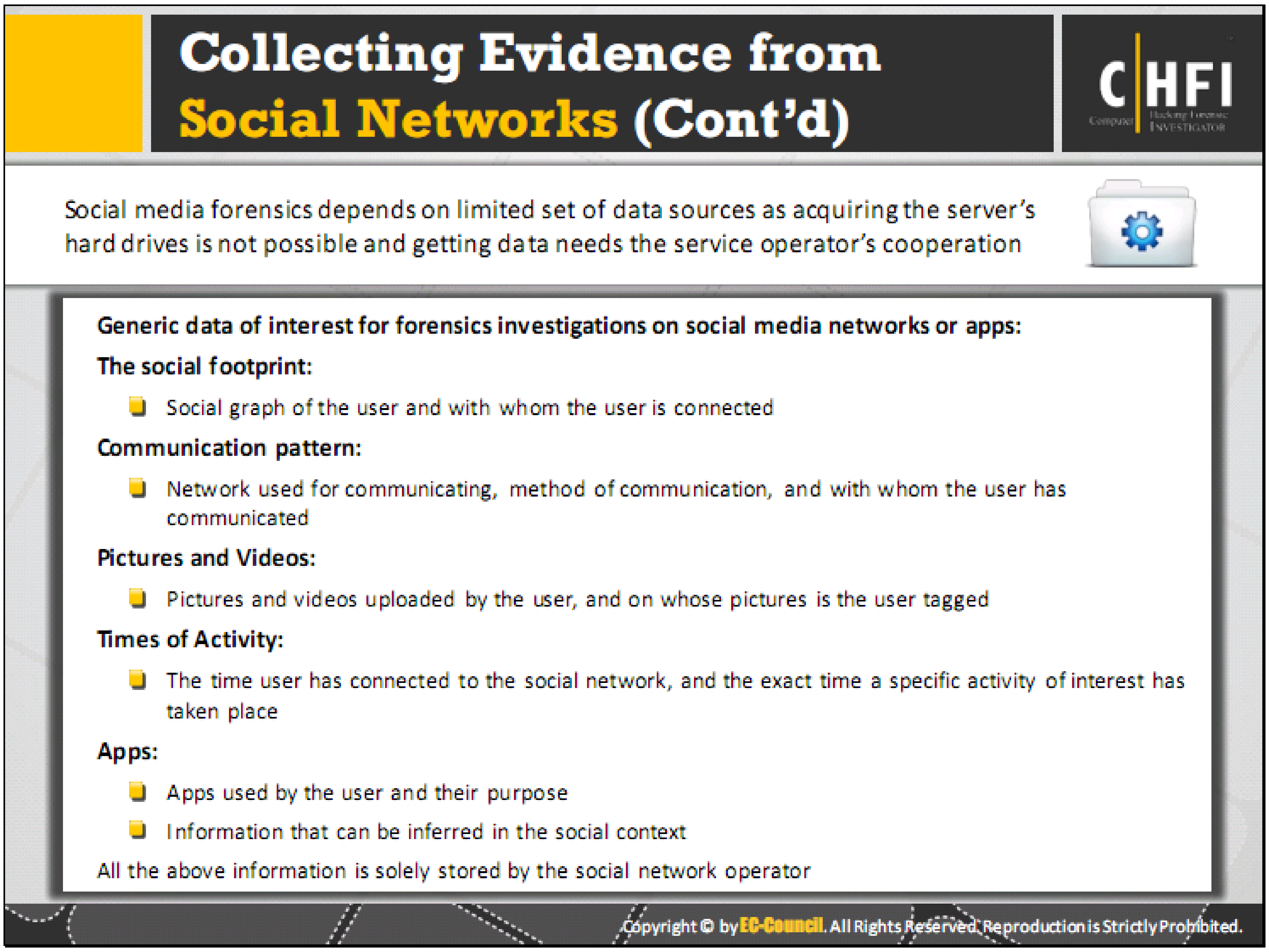
01 Social media sites and apps such as Facebook, LinkedIn, Twitter, Google+, WhatsApp, Snapchat, etc. are widely being used nowadays for communication and information-sharing purposes, because of which attacks through them are also increasing

02 Thus, social media sites and apps can be a **treasure trove for forensics investigations** to track a perpetrator

03 The information gathered from social media might **help** a forensic investigator **to build a timeline of an attack**

Currently, the number of people using social networking sites is increasing rapidly. It has become one of the easiest ways to communicate and share data. This has led cybercriminals to find ways to commit crimes via social networking. Because of 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 of the popular social networking sites are Facebook, WhatsApp, Twitter, LinkedIn, Google+, Snapchat, etc.

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



Collecting Evidence from Social Networks (Cont'd)

CHFI
Computer Hacking Forensic Investigator

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

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

The 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 whose pictures is the user tagged

Times of Activity:

- The time 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

All the above information is solely stored by the social network operator

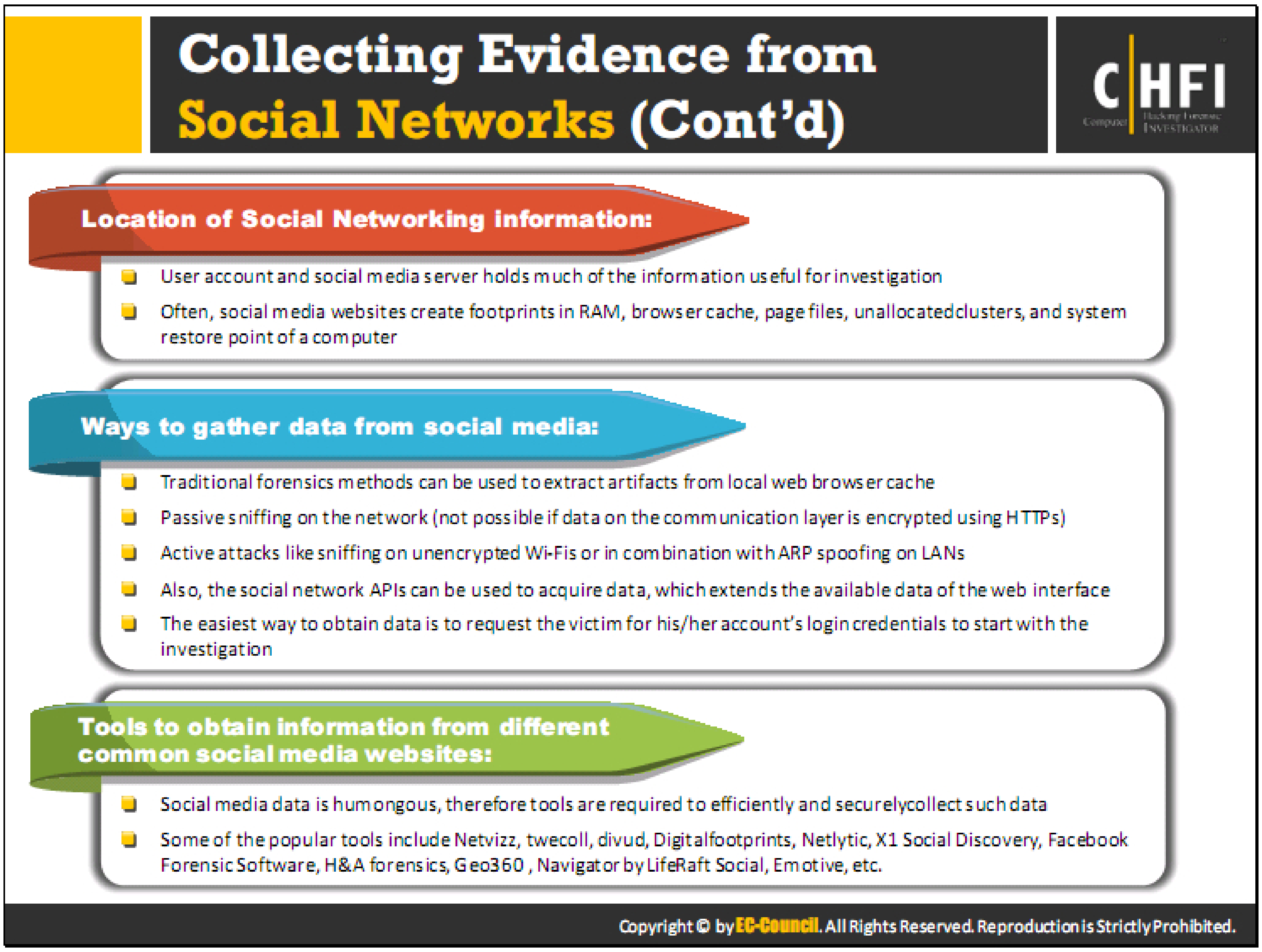
Social media forensics depends on a limited set of data sources as acquiring the server's hard drives is not possible and getting data needs the service operator's cooperation.

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

- **The 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 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
- **Interconnection pattern:** Includes user data like user's friend list, chat messages, group chats etc. This data helps the investigator to know about the user's friends, groups, connections added, etc.
- **Interaction pattern:** The interaction pattern helps users to interact with others through messages and the interaction frequency.

- **Activity Timestamps:** The timeline of the activities of the user on social networking can provide vital information for the investigation. The timestamp of the user communication, data sharing like posting photos, status update etc. reveals information such as a particular user activity.
- **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.

All the above information is solely stored with the social network operator.



Collecting Evidence from Social Networks (Cont'd)

Location of Social Networking information:

- User account and social media server holds much of the information useful for investigation
- Often, social media websites create footprints in RAM, browser cache, page files, unallocatedclusters, and system restore point of a computer

Ways to gather data from social media:

- Traditional forensics methods can be used to extract artifacts from local web browser cache
- Passive sniffing on the network (not possible if data on the communication layer is encrypted using HTTPs)
- Active attacks like sniffing on unencrypted Wi-Fis or in combination with ARP spoofing on LANs
- Also, the social network APIs can be used to acquire data, which extends the available data of the web interface
- The easiest way to obtain data is to request the victim for his/her account's login credentials to start with the investigation

Tools to obtain information from different common social media websites:

- Social media data is humongous, therefore tools are required to efficiently and securelycollect such data
- Some of the popular tools include Netvizz, twecoll, divud, Digitalfootprints, Netlytic, X1 Social Discovery, Facebook Forensic Software, H&A forensics, Geo360 , Navigator by LifeRaft Social, Emotive, etc.

Location of Social Networking information:

- User account and social media server holds much of the information useful for investigation
- Often, social media websites create footprints in RAM, browser cache, page files, unallocated clusters, and system restore point of a computer
- Portable devices such as smartphones also contain important social networking information in the apps. For example, an iPhone can hold the app information in the memory like user profile information, attachments, time stamps, and passwords

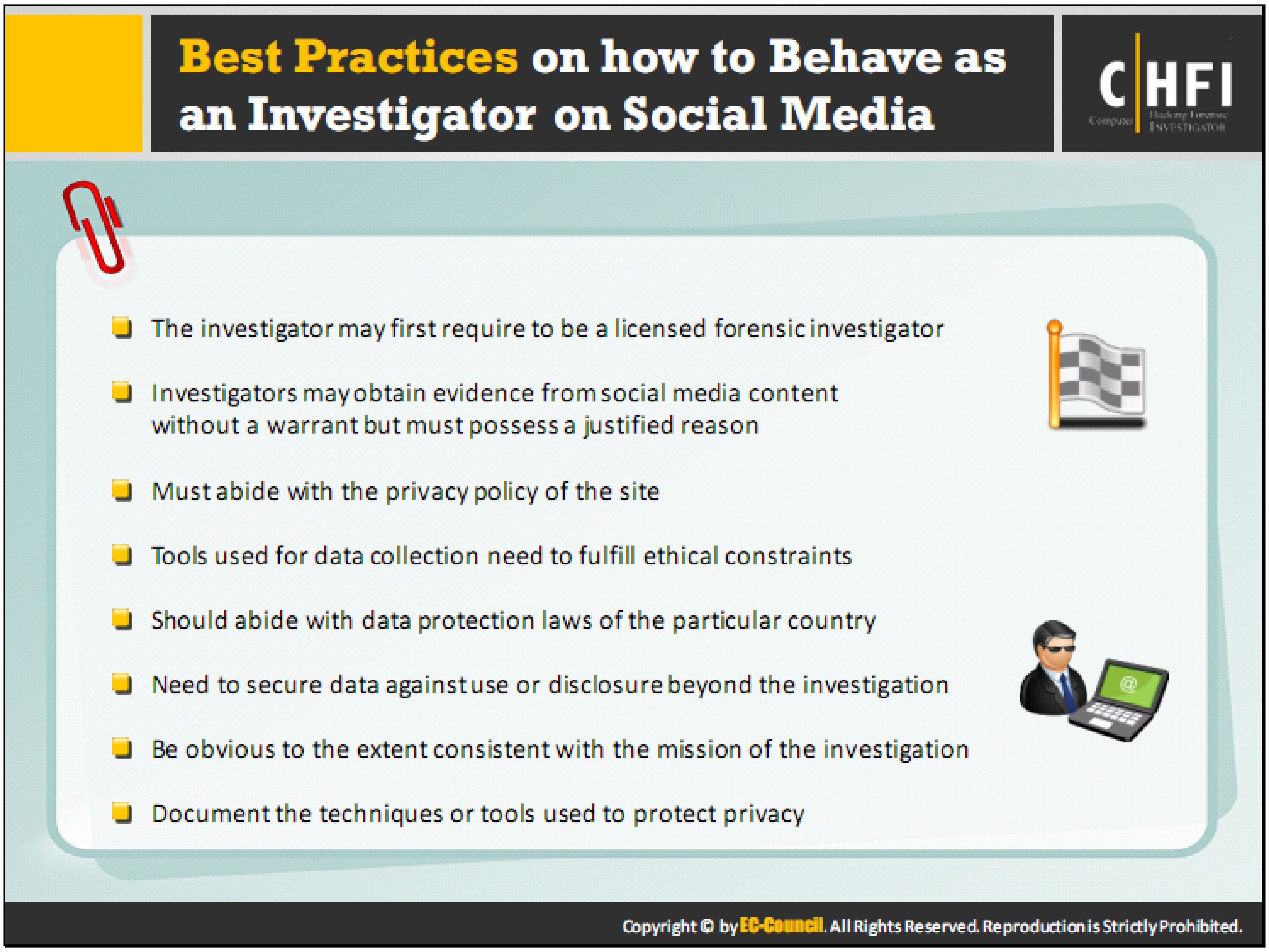
Ways to gather data from social media:

- Traditional forensic methods can be used to extract artifacts from the local web browser cache.
- Passive sniffing on the network (not possible if data on the communication layer is encrypted using HTTPs).
- Active attacks like sniffing on unencrypted Wi-Fi networks or in combination with ARP spoofing on LANs.
- The social network APIs can be used to acquire data, which extends the available data of the web interface.

- The easiest way to obtain data is to request the victim for his/her account's login credentials to start with the investigation.

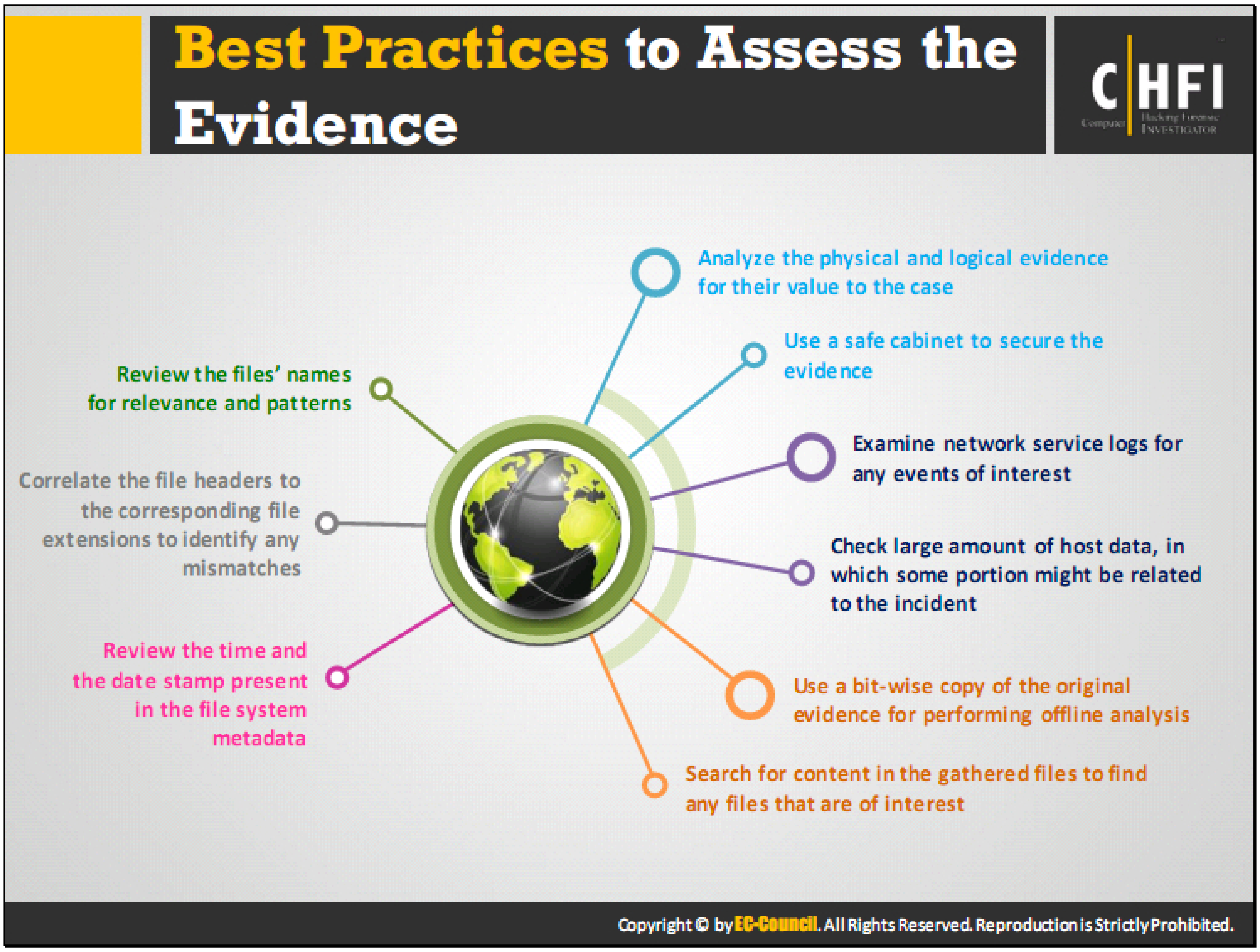
Tools to obtain information from different common social media websites:

- Social media data is enormous, therefore tools are required to efficiently and securely collect social media data.
- Some of the popular tools include Netvizz, twecoll, divud, Digitalfootprints, Netlytic, X1 Social Discovery, Facebook Forensic Software, H&A forensics, Geo360, Navigator by LifeRaft Social, Emotive, etc.



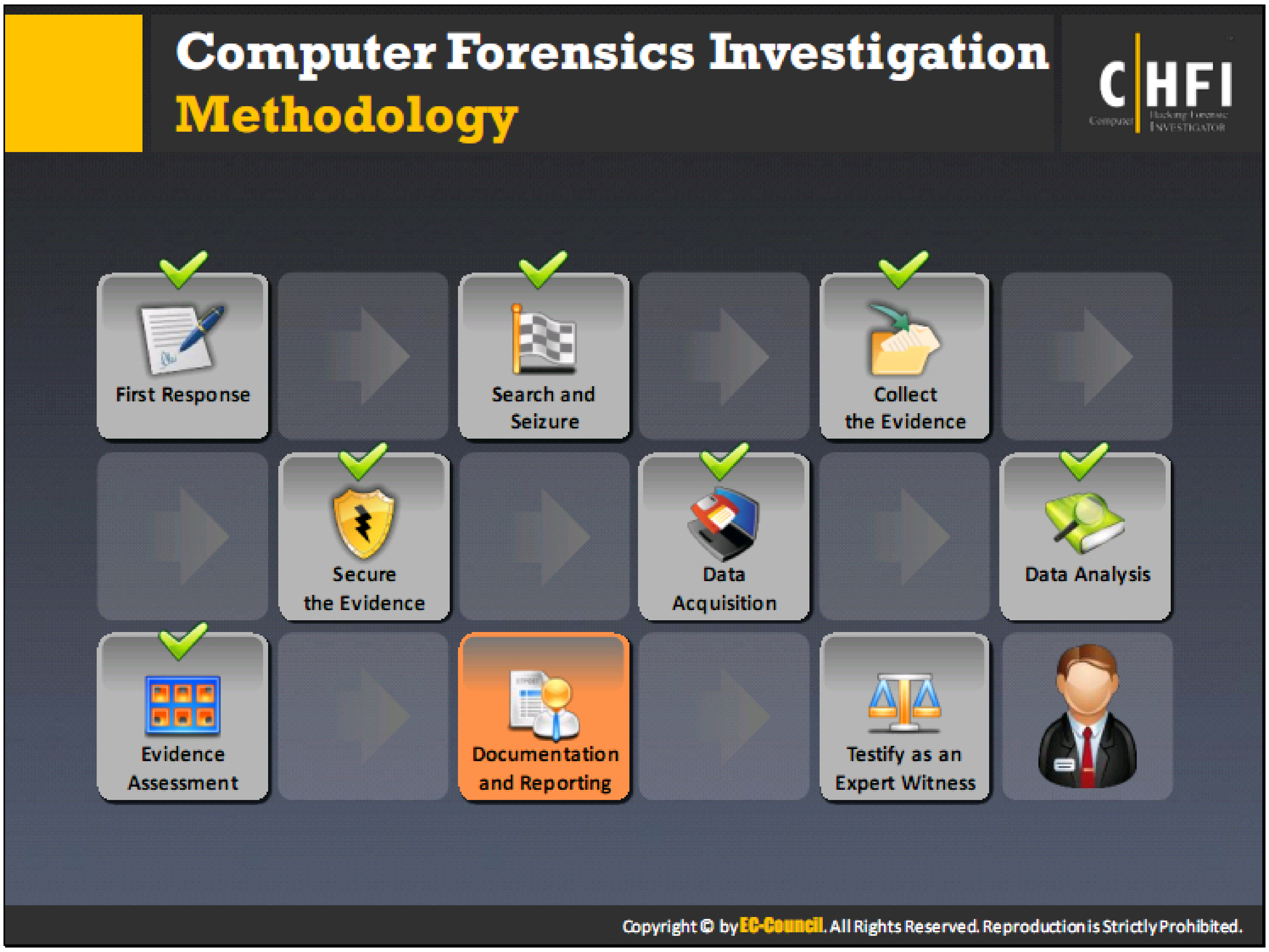
Best Practices on how to Behave as an Investigator on Social Media

- The investigator may first require to be a licensed forensic investigator
- Investigators may obtain evidence from social media content without a warrant but must possess a justified reason
- Must abide with the privacy policy of the site
- Tools used for data collection need to fulfill ethical constraints
- Should abide with data protection laws of the particular country
- Need to secure data against use or disclosure beyond the investigation
- Be obvious to the extent consistent with the mission of the investigation
- Document the techniques or tools used to protect privacy



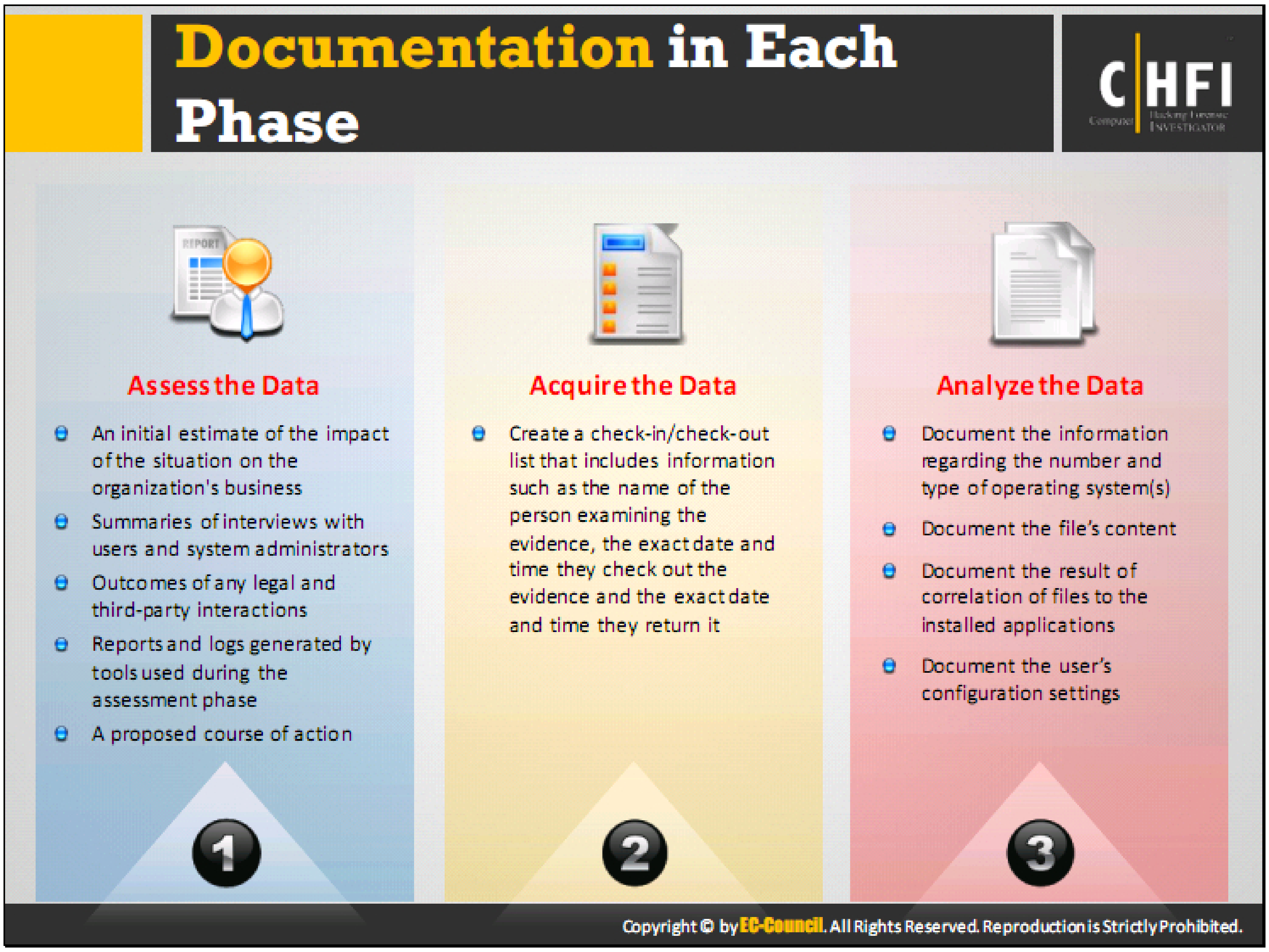
Best Practices to Assess the Evidence

- Analyze the physical and logical evidence for their value to the case
- Use a safe cabinet to secure the evidence
- Examine network service logs for any events of interest
- Check large amount of host data, in which some portion might be related to the incident
- Use a bit-wise copy of the original evidence for performing offline analysis
- Search for content in the gathered files to find any files that are of interest
- Review the time and the date stamp present in the file system metadata
- Correlate the file headers to the corresponding file extensions to identify any mismatches
- Review the files' names for relevance and patterns



Computer Forensics Investigation Methodology

Documenting is the process of writing all the actions the investigators have performed during the investigation to obtain the desired results. The investigators should maintain it in proper order and submit it in court during trial. This section will teach you the process of documenting and reporting.



Documentation in Each Phase

Assess the Data

- An initial estimate of the impact of the situation on the organization's business
- Summaries of interviews with users and system administrators
- Outcomes of any legal and third-party interactions
- Reports and logs generated by tools used during the assessment phase
- A proposed course of action

1

Acquire the Data

- Create a check-in/check-out list that includes information such as the name of the person examining the evidence, the exact date and time they check out the evidence and the exact date and time they return it

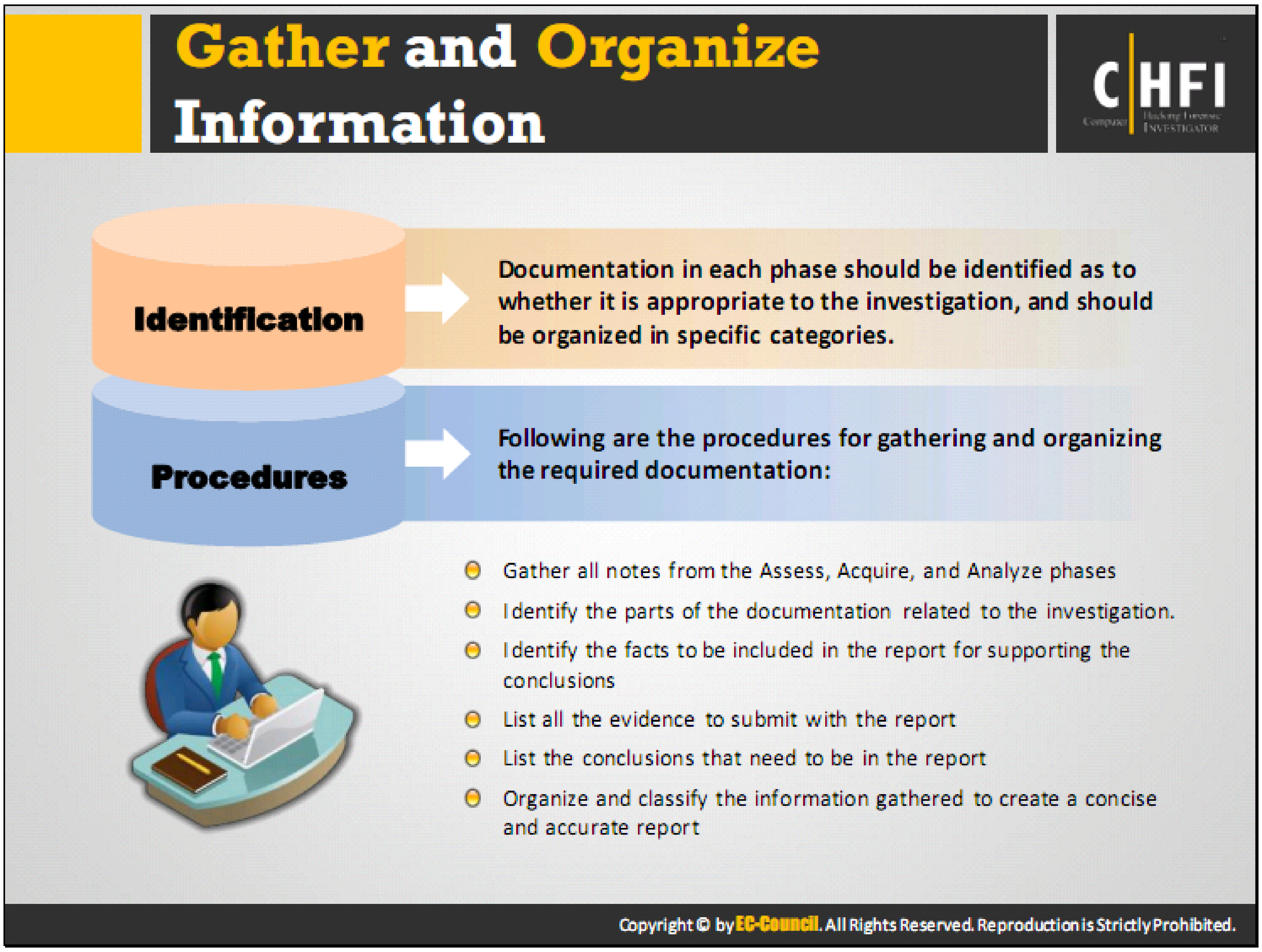
2

Analyze the Data

- Document the information regarding the number and type of operating system(s)
- Document the file's content
- Document the result of correlation of files to the installed applications
- Document the user's configuration settings

3

Investigators need to document all the forensics processes applied to identify, gather, analyze, preserve, and report the evidence in order to offer a good report to a court of law and ease the prosecution.



Gather and Organize Information

Identification

Documentation in each phase should be identified as to whether it is appropriate to the investigation, and should be organized in specific categories.

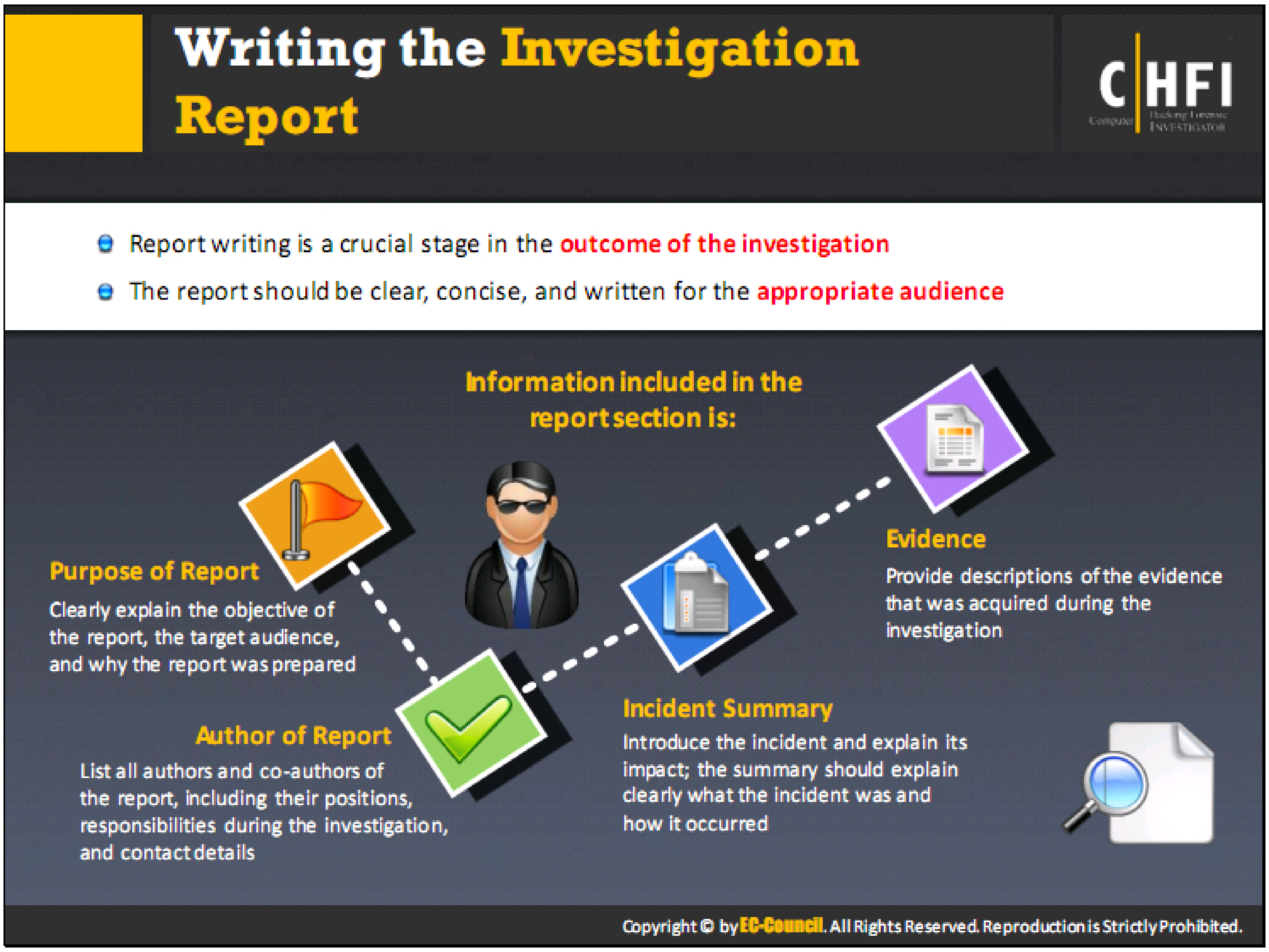
Procedures

Following are the procedures for gathering and organizing the required documentation:

- Gather all notes from the Assess, Acquire, and Analyze phases
- Identify the parts of the documentation related to the investigation.
- Identify the facts to be included in the report for supporting the conclusions
- List all the evidence to submit with the report
- List the conclusions that need to be in the report
- Organize and classify the information gathered to create a concise and accurate report

Identification:

Investigators should identify if the documentation in each phase is appropriate to the investigation and should organize it in specific categories. This will ease the process of searching for a specific piece of evidence from the huge amount data.



Writing the Investigation Report

- Report writing is a crucial stage in the outcome of the investigation
- The report should be clear, concise, and written for the appropriate audience

Information included in the report section is:

Purpose of Report
Clearly explain the objective of the report, the target audience, and why the report was prepared

Author of Report
List all authors and co-authors of the report, including their positions, responsibilities during the investigation, and contact details

Incident Summary
Introduce the incident and explain its impact; the summary should explain clearly what the incident was and how it occurred

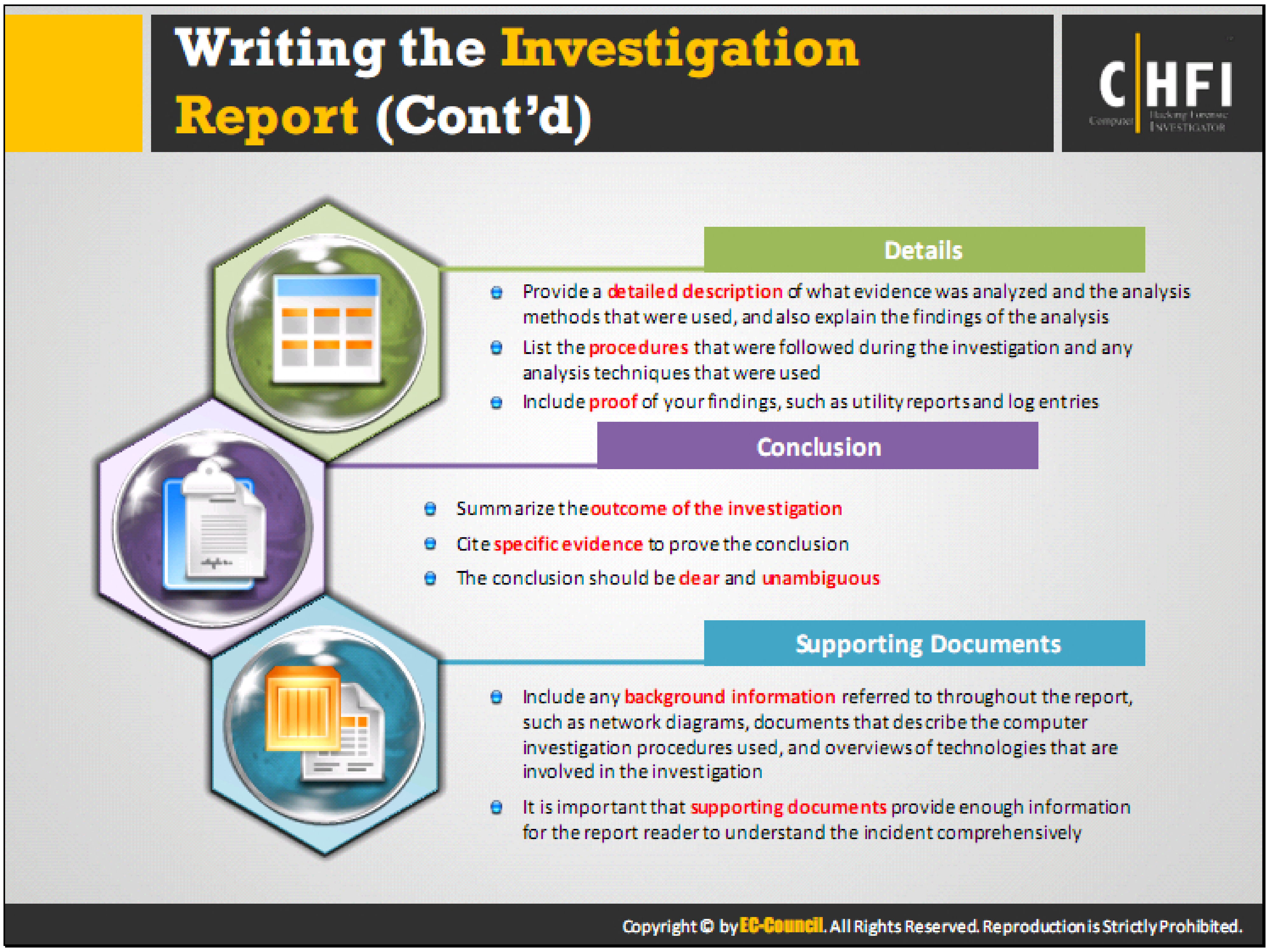
Evidence
Provide descriptions of the evidence that was acquired during the investigation

Report writing is a crucial stage in the outcome of the investigation, as it summarizes all the investigation process into a readable report, presented to a court of law. Based on the accuracy and certainty of this report, the court will prosecute the suspects.

The report should be clear, concise, and written for the appropriate audience. The report should be in local language if necessary and have no jargons. It should include only include the data related to the case and the evidence. Every statement should have a supporting document or evidence.

Information included in the report section is:

- **Purpose of Report:** Explain the objective of the report, the target audience, and the reason for preparing the report clearly. Mention how the evidence supports or denies the claims and provide sufficient backup to the statements.
- **Author of Report:** Include a list of all the authors and co-authors of the report, including their positions, responsibilities during the investigation, and their contact details.
- **Incident Summary:** Introduce the incident and explain its impact; the summary should explain clearly what the incident was and how it occurred.
- **Evidence:** Provide descriptions of the evidence acquired during the investigation, location, status during extraction, extraction procedure, analysis process, tools used, etc. Mention each detail clearly and in such a way that the process is explicable to the people with less or no technical knowledge.



Writing the Investigation Report (Cont'd)

CHFI
Computer Hacking Forensic INVESTIGATOR

Details

- Provide a detailed description of what evidence was analyzed and the analysis methods that were used, and also explain the findings of the analysis
- List the procedures that were followed during the investigation and any analysis techniques that were used
- Include proof of your findings, such as utility reports and log entries

Conclusion

- Summarize the outcome of the investigation
- Cite specific evidence to prove the conclusion
- The conclusion should be clear and unambiguous

Supporting Documents

- Include any background information referred to throughout the report, such as network diagrams, documents that describe the computer investigation procedures used, and overviews of technologies that are involved in the investigation
- It is important that supporting documents provide enough information for the report reader to understand the incident comprehensively

Details

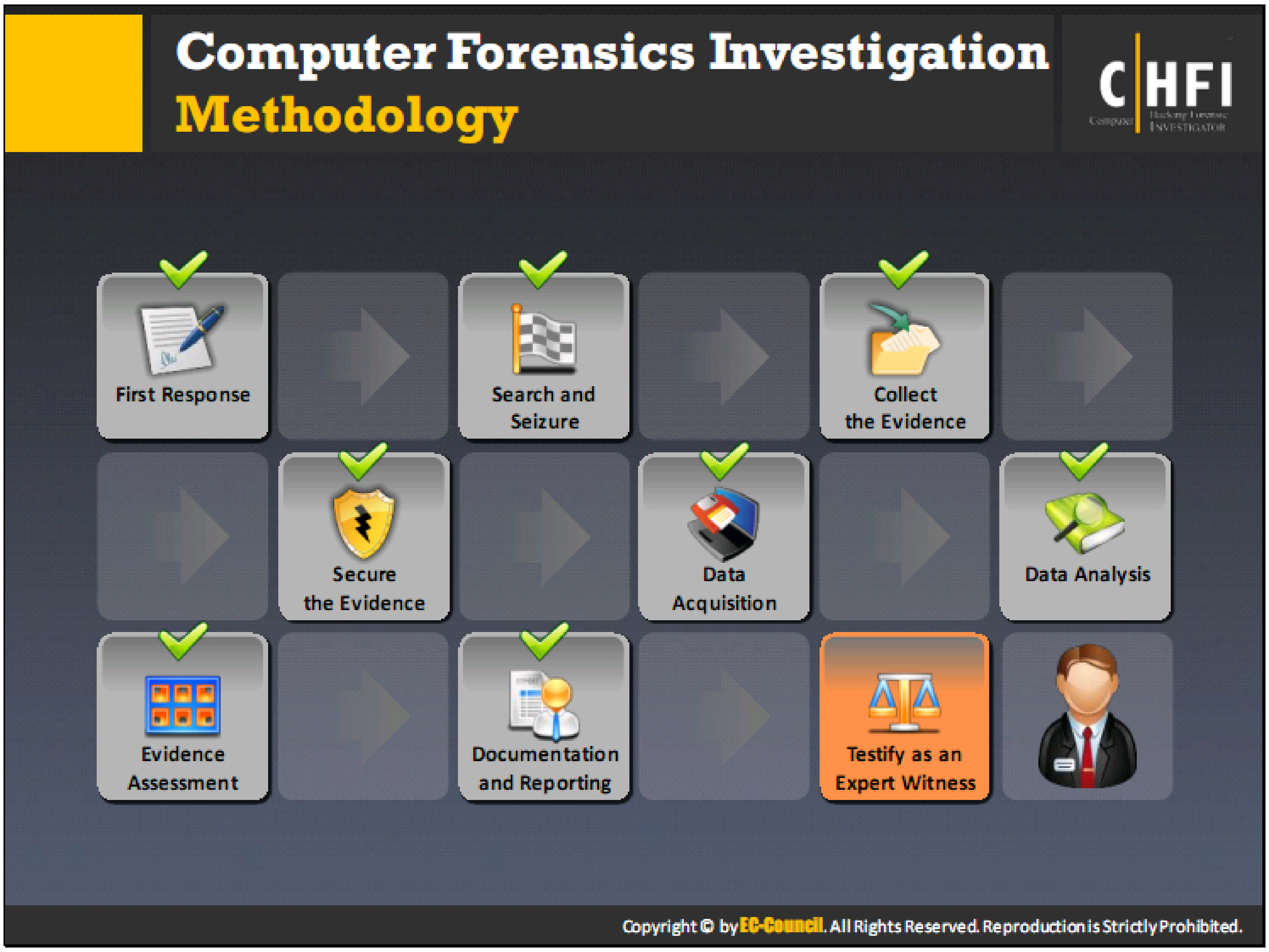
- Provide a detailed description of what evidence was analyzed and the analysis methods that were used and also explain the findings of the analysis.
- List the procedures that were followed during the investigation and any analysis techniques that were used.
- Include proof of your findings, such as utility reports and log entries.

Conclusion

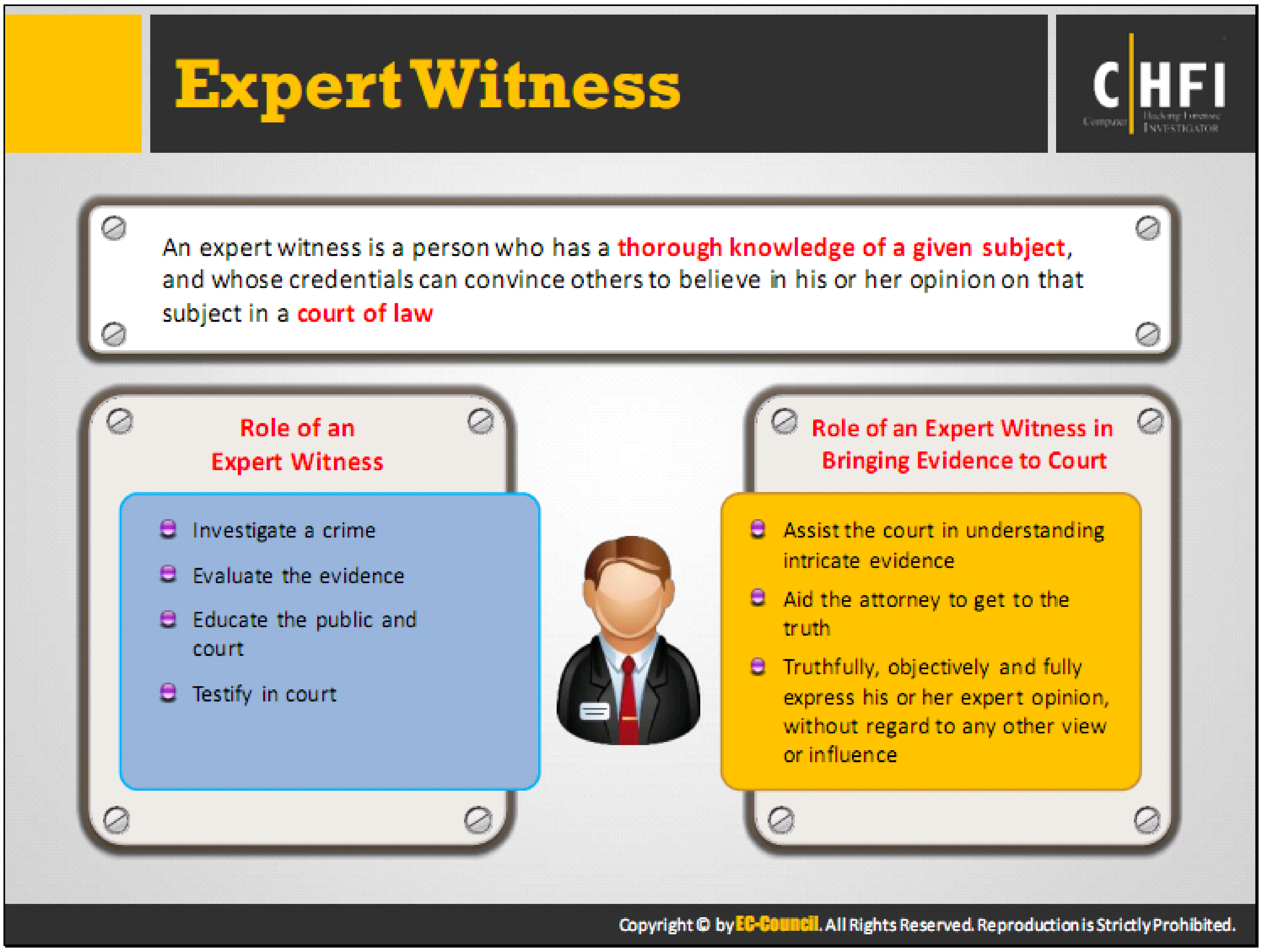
- Summarize the outcome of the investigation.
- Cite specific evidence to prove the conclusion.
- The conclusion should be clear and unambiguous.

Supporting Documents

- Include any background information referred to throughout the report, such as network diagrams, documents that describe the computer investigation procedures used, and overviews of technologies that are involved in the investigation.
- It is important that supporting documents provide enough information for the reader to understand the incident as completely as possible.


Computer Forensics Investigation
Methodology
CHFI
First Response
Search and Seizure
Collect the Evidence
Secure the Evidence
Data Acquisition
Data Analysis
Evidence Assessment
Documentation and Reporting
Testify as an Expert Witness
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

As the attorney, prosecutors, and other panel present in a court of law may be unaware of the technical knowledge regarding the crime, evidence and losses, the investigators should approach authorized personnel who could appear in the court to affirm the accuracy of the process and the data.



Expert Witness

An expert witness is a person who has a **thorough knowledge of a given subject**, and whose credentials can convince others to believe in his or her opinion on that subject in a **court of law**

Role of an Expert Witness

- Investigate a crime
- Evaluate the evidence
- Educate the public and court
- Testify in court

Role of an Expert Witness in Bringing Evidence to Court

- Assist the court in understanding intricate evidence
- Aid the attorney to get to the truth
- Truthfully, objectively and fully express his or her expert opinion, without regard to any other view or influence

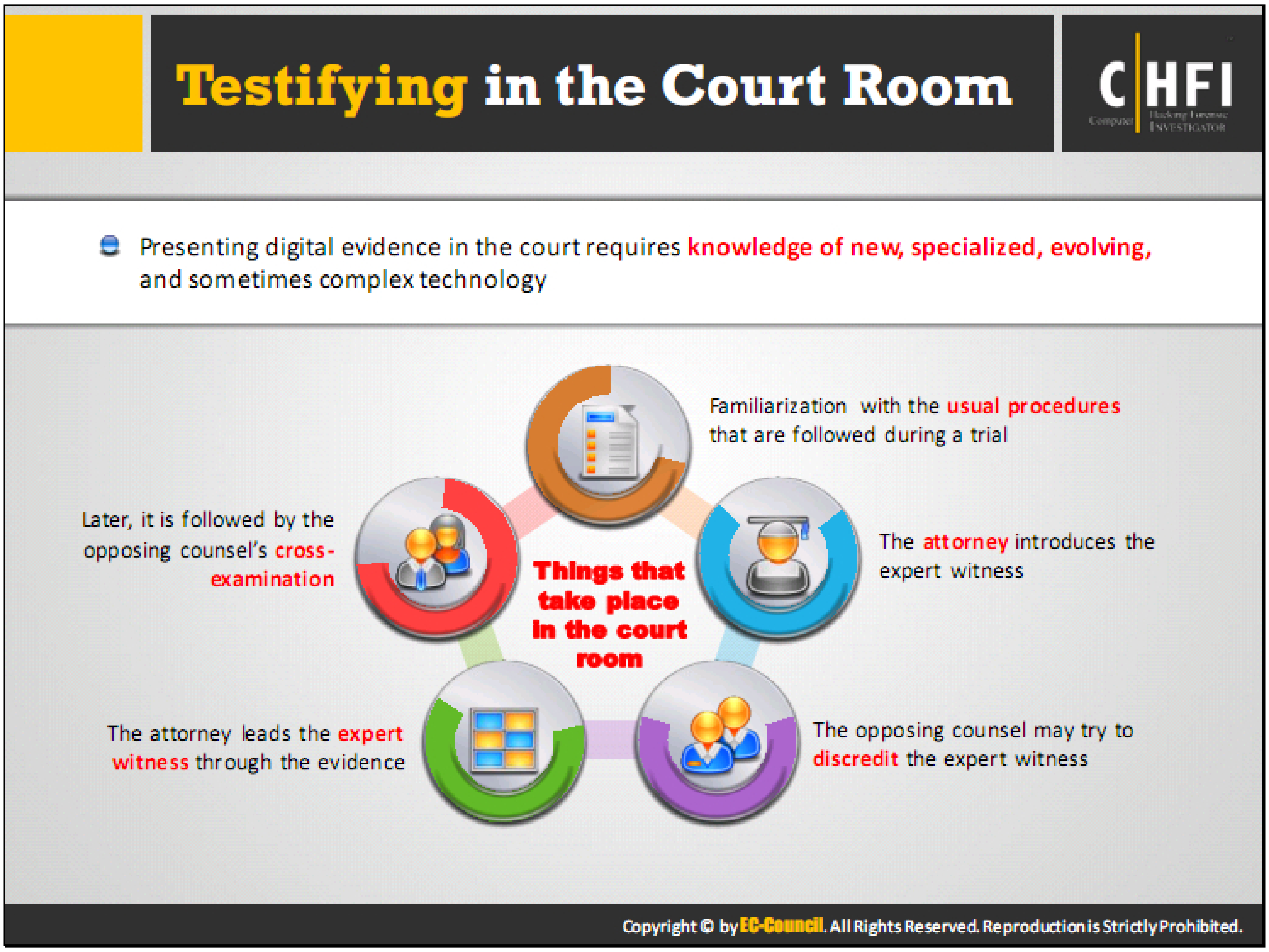
An expert witness is a person who has a thorough knowledge of a subject and whose credentials can convince others to believe his or her opinions on that subject in a court of law. Courts call upon the expert witnesses to authenticate the facts and witnesses during any complex case. Cases involving accidents and deaths often need the help of an expert witness to verify the severity of injuries and mode of death. Whenever there is a case of probability in any criminal case that juries and attorneys cannot understand clearly, they call for the advice of an expert witness, who can clarify the facts and help the court come to a decision. Expert witnesses cross-examine witnesses and evidence, as a normal witness may influence or manipulate the truth under many other factors.

The role of an expert witness is to:

- Investigate a crime
- Evaluate the evidence
- Educate the public and court
- Testify in court
- Conduct investigations on behalf of the court and report the findings back to the court
- Participate in court-appointed expert witness conferences to study any intriguing incident
- Educate the jury, court, and the individuals related to the case about his or her findings

The role of the expert witness in bringing evidence to court is to:

- Assist the court in understanding intricate evidence
- Aid the attorney in determining the truth
- Truthfully express his or her expert opinion, irrespective of others' views and influence



Testifying in the Court Room

- Presenting digital evidence in the court requires **knowledge of new, specialized, evolving,** and sometimes complex technology

Things that take place in the court room

Familiarization with the **usual procedures** that are followed during a trial

The **attorney** introduces the expert witness

The opposing counsel may try to **discredit** the expert witness

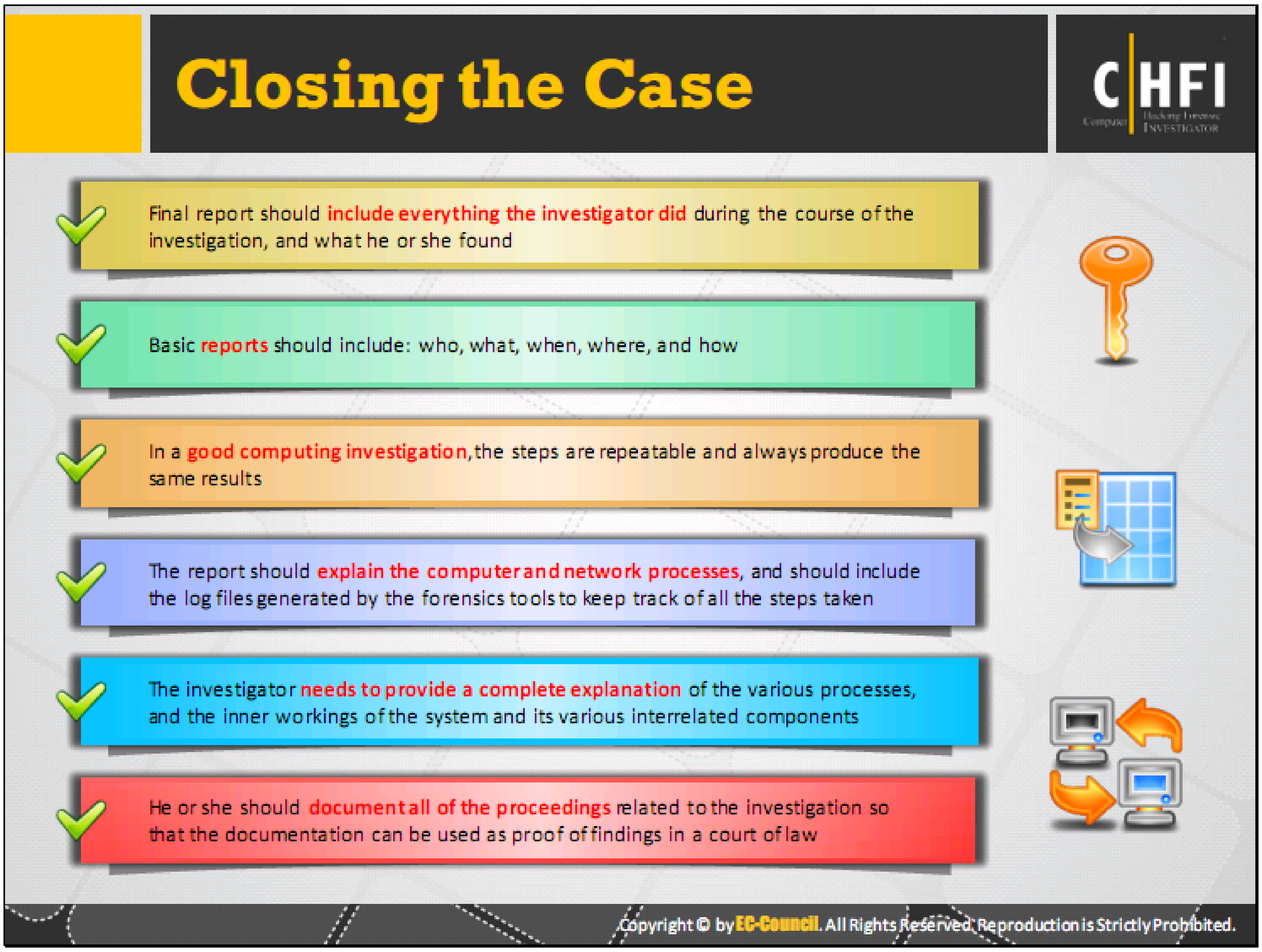
The attorney leads the **expert witness** through the evidence

Later, it is followed by the opposing counsel's **cross-examination**

An expert witness must keep certain factors in mind while testifying in court. The expert witness must have complete information about the usual procedures during a trial. He or she must never question the attorney regarding these matters. The attorney will first introduce the expert witness to the court. The witness will then offer his or her credentials and accomplishments to establish credibility with the jury. Presenting digital evidence to the court requires knowledge of new, specialized, evolving, and sometimes complex technology.

The following things take place in a court room:

- The judge explains the usual procedures followed during a trial
- The attorney introduces the expert witness
- The opposing counsel may try to discredit the expert witness
- The attorney leads the expert witness through the evidence
- Later, the opposing counsel performs a cross-examination



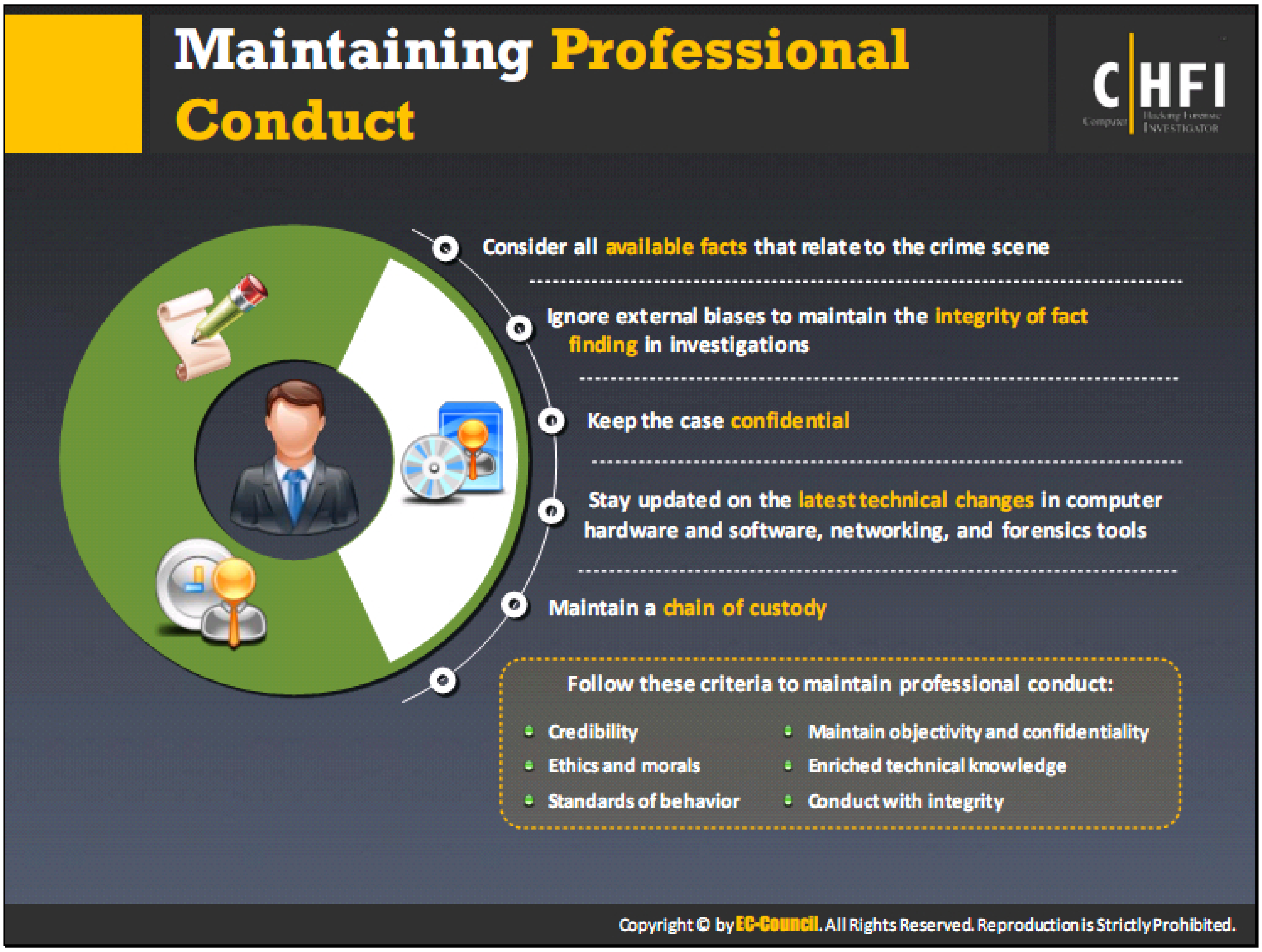
Closing the Case

- ✓ Final report should include everything the investigator did during the course of the investigation, and what he or she found
- ✓ Basic reports should include: who, what, when, where, and how
- ✓ In a good computing investigation, the steps are repeatable and always produce the same results
- ✓ The report should explain the computer and network processes, and should include the log files generated by the forensics tools to keep track of all the steps taken
- ✓ The investigator needs to provide a complete explanation of the various processes, and the inner workings of the system and its various interrelated components
- ✓ He or she should document all of the proceedings related to the investigation so that the documentation can be used as proof of findings in a court of law

After evidence analysis and retrieval, the investigator should prepare a final report, which should include what the investigator did and found. Basic reports should be able to answer questions like who, what, when, where, and how of the evidence. In a good computing investigation, the steps can be repeatable and the results obtained are the same throughout. The report should explain the computer and network processes and the inner working system.

The investigator should document all the proceedings related to the investigation properly, which will help to use the report as proof of findings in a court of law. Since the reader can be a senior personnel manager, a lawyer, or a judge, explanation for various processes provide the inner workings of the system, and its various interrelated components.

Each organization has its predefined template for report writing. Follow the template and understand the organization's needs and requirements while describing the findings. Attach the log files generated by the forensic tool with the formal report, as they keep track of all the steps taken and support the findings of the evidence in court. The narrative part should precede the log in the report based on the fact finding.



Maintaining Professional Conduct

- Consider all available facts that relate to the crime scene
- Ignore external biases to maintain the integrity of fact finding in investigations
- Keep the case confidential
- Stay updated on the latest technical changes in computer hardware and software, networking, and forensics tools
- Maintain a chain of custody

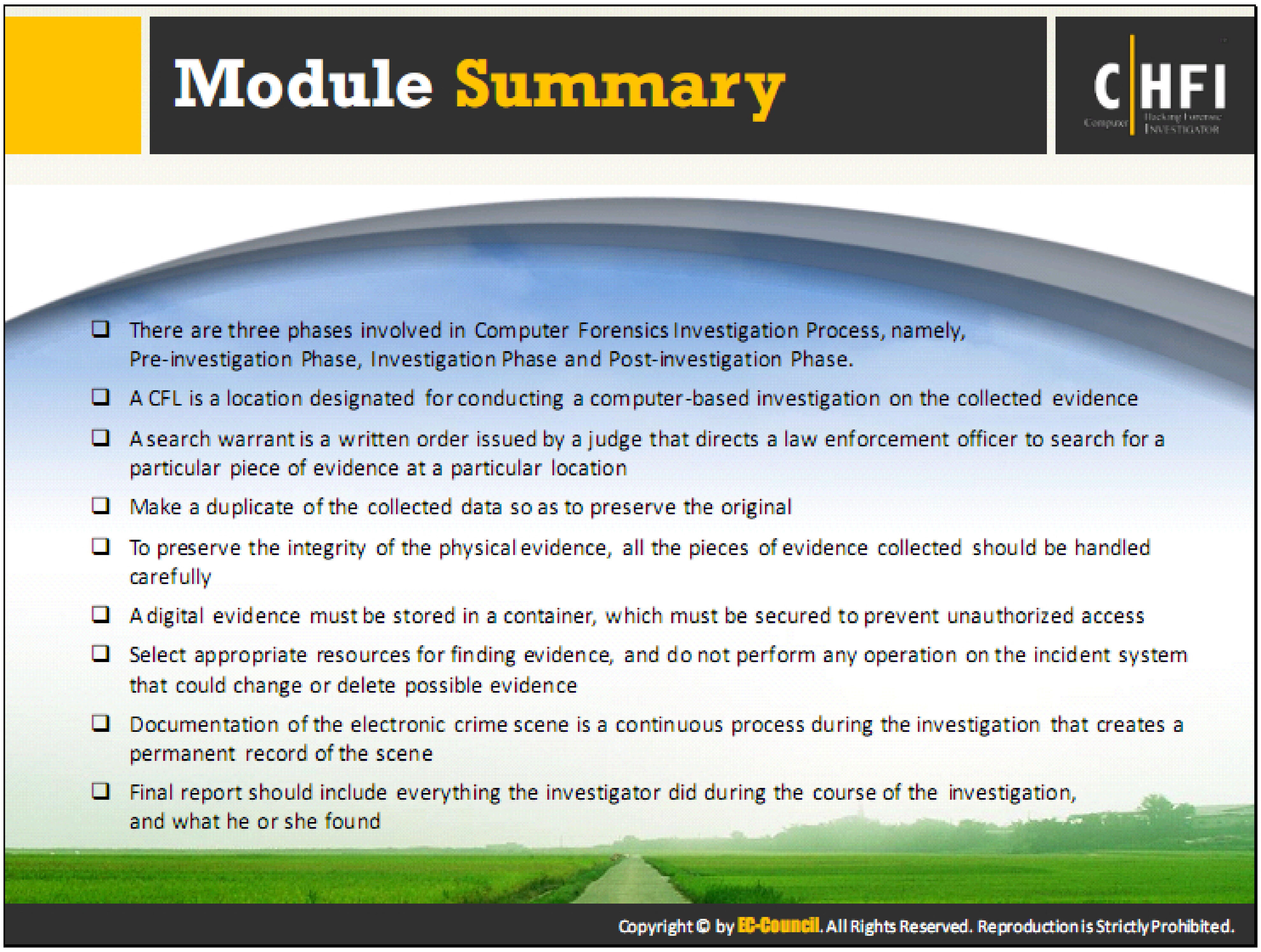
Follow these criteria to maintain professional conduct:

- Credibility
- Ethics and morals
- Standards of behavior
- Maintain objectivity and confidentiality
- Enriched technical knowledge
- Conduct with integrity

The rules that help you maintain professional conduct while investigating a case are:

- Be trustworthy and honest.
- Contribute to society and behave well.
- Avoid harming others.
- Give appropriate credit for intellectual property.
- Be fair and take action not to discriminate.
- Respect the privacy of others.
- Honor confidentiality.
- Honor copyrights, property rights, and patent rights.
- Acquire and maintain professional competence.
- Accept and provide appropriate professional review.
- Consider all the available facts that relate to the crime scene.
- Update software and computer hardware, networking, and forensic tools with the latest technical changes.
- Try to maintain quality, effectiveness, and dignity in the process and products of professional work.

- Keep the case confidential.
- Honor agreements, contracts, and assigned responsibilities.
- Respect the existing laws pertaining to professional work.
- Maintain the chain of custody.
- Avoid external biases to maintain the integrity of fact-finding in all investigations.
- Increase understanding of computers and the consequences of misusing them in public.
- Access computing and communication resources only after getting permission.
- Supervise personnel and resources in order to design and build information systems that improve the quality of working life.
- Support and acknowledge proper and authorized users of an organization's computing and communication resources.
- Conduct sessions in the organization to advise about the principles and limitations of computer systems.



Module Summary

- There are three phases involved in Computer Forensics Investigation Process, namely, Pre-investigation Phase, Investigation Phase and Post-investigation Phase.
- A CFL is a location designated for conducting a computer-based investigation on the collected evidence
- A search warrant is a written order issued by a judge that directs a law enforcement officer to search for a particular piece of evidence at a particular location
- Make a duplicate of the collected data so as to preserve the original
- To preserve the integrity of the physical evidence, all the pieces of evidence collected should be handled carefully
- A digital evidence must be stored in a container, which must be secured to prevent unauthorized access
- Select appropriate resources for finding evidence, and do not perform any operation on the incident system that could change or delete possible evidence
- Documentation of the electronic crime scene is a continuous process during the investigation that creates a permanent record of the scene
- Final report should include everything the investigator did during the course of the investigation, and what he or she found

This module discussed the phases involved in the Computer Forensics Investigation Process, described how a computer forensics lab should be laid out, the search warrant, and duplication of data to preserve the original. The module discussed the role of a first responder, planning search and seizure, chain of custody, and the process of recovering lost data. Additionally, the module described the evidence acquisition and analysis process, documentation, and the process of creating a report.