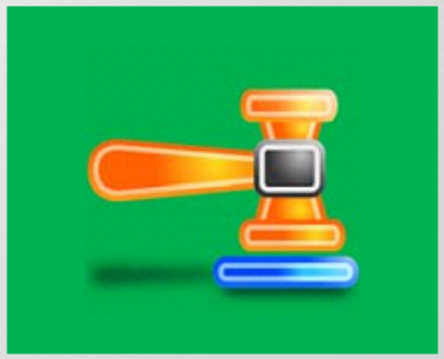
Computer Forensics Investigation Process

Module 02

Designed by Cyber Crime Investigators. Presented by Professionals.



Module Objectives

C|HFI Computer Hacking Forensic Investigator

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

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

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

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

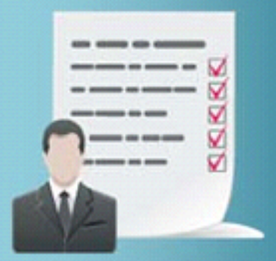
Phases Involved in the Computer Forensics Investigation Process

Pre-investigation Phase:

- Deals with tasks to be performed prior to the commencement of **actual investigation**
- Involves setting up a **computer forensics lab**, building a forensics workstation, developing an investigation toolkit, setting up an investigation team, getting approval from the relevant authority, etc.

Investigation Phase:

- Considered as the **main phase** of the computer forensics investigation process
- Involves acquisition, preservation, and analysis of **evidentiary data** to identify the **source of crime** and the culprit 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

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

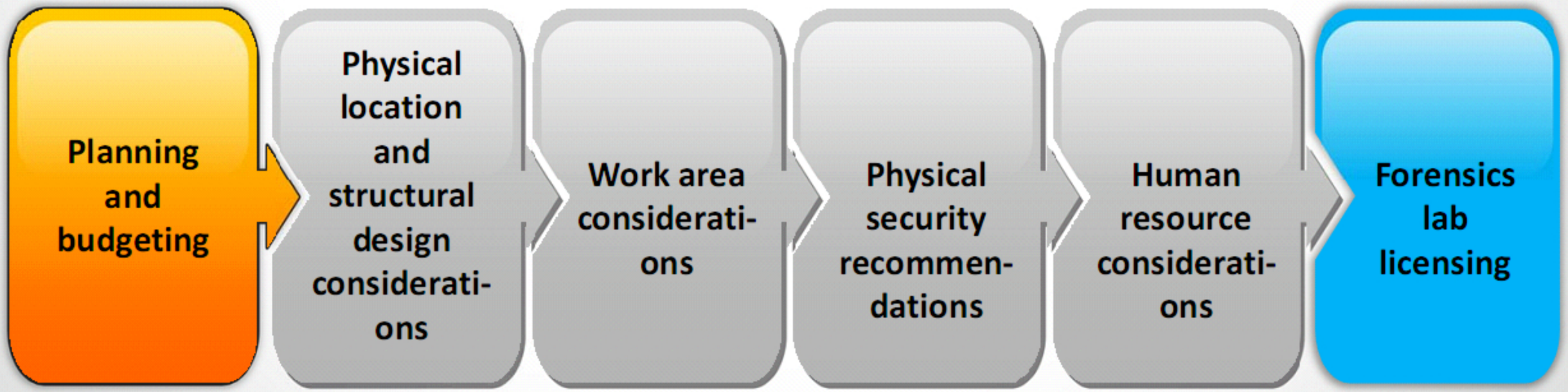
Pre-investigation Phase

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

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:



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

Planning and Budgeting

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

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

Physical Location and Structural Design Considerations

C|HFI Computer Hacking Forensic Investigator

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

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

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**

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

Physical Security Recommendations

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

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

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**

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

Evidence Locker Recommendations

C|HFI Computer Hacking Forensic Investigator

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

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

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**

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

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

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

Building a Forensics Workstation

C|HFI Computer Hacking Forensic Investigator

- 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

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

Basic Workstation Requirements in a Forensics Lab

C|HFI Computer Hacking Forensic Investigator

Hardware requirements for a basic forensic workstation are as follows:

Processor with high computing speed

8 GB RAM for satisfying minimum processing requirements

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

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

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

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

For emergencies, a spare RAM and hard disk

Tape drive, USB drive, and removal drive bays

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

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

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

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

Forensics Hardware

C|HFI Computer Hacking Forensic Investigator

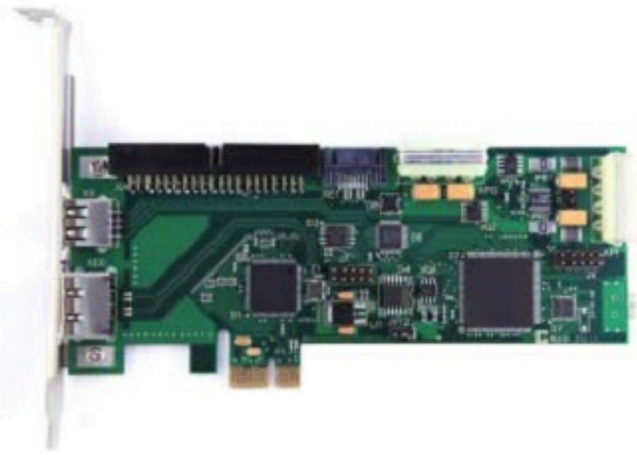
Paraben's First Responder Bundle

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

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

Forensics Hardware (Cont'd)

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

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

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

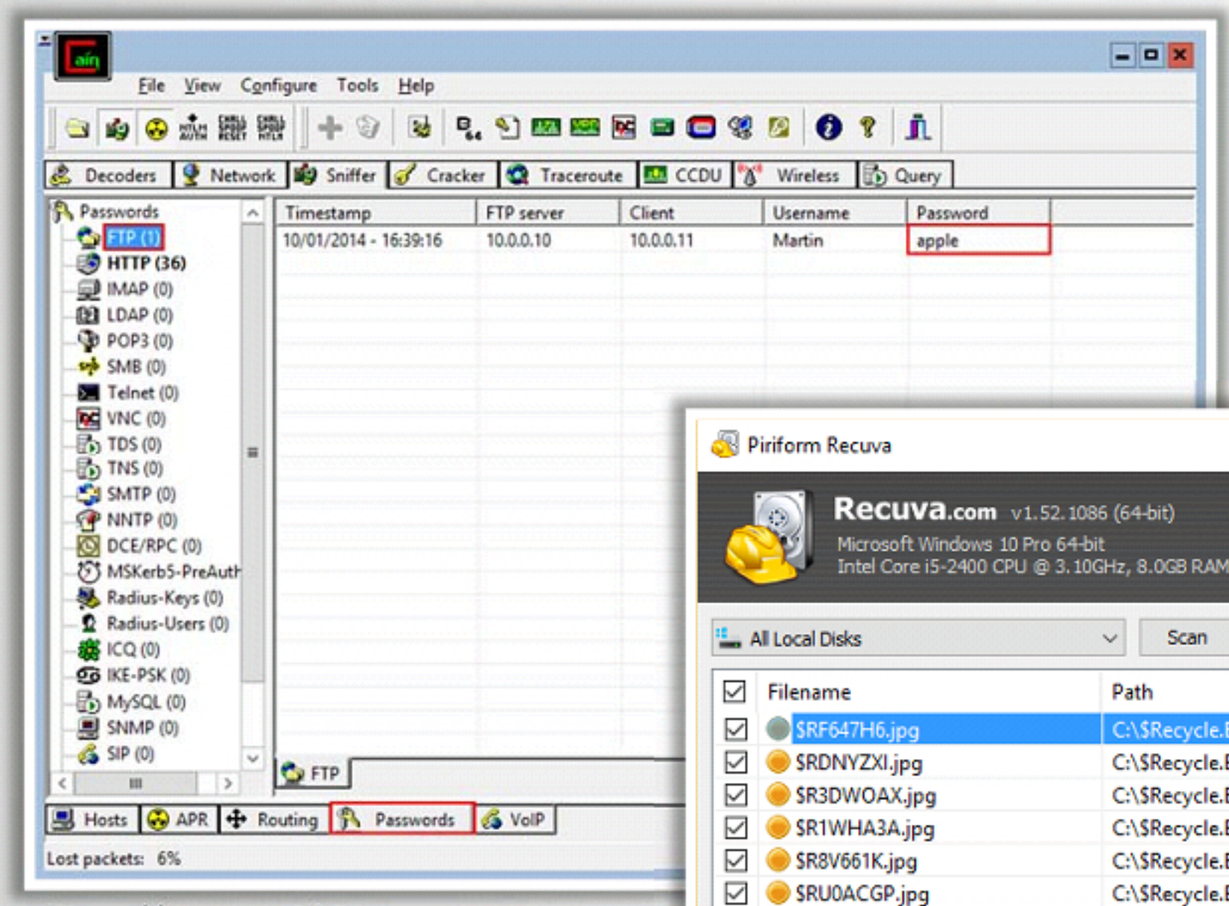
Shadow 3
http://www.voomtech.com

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

Forensics Software

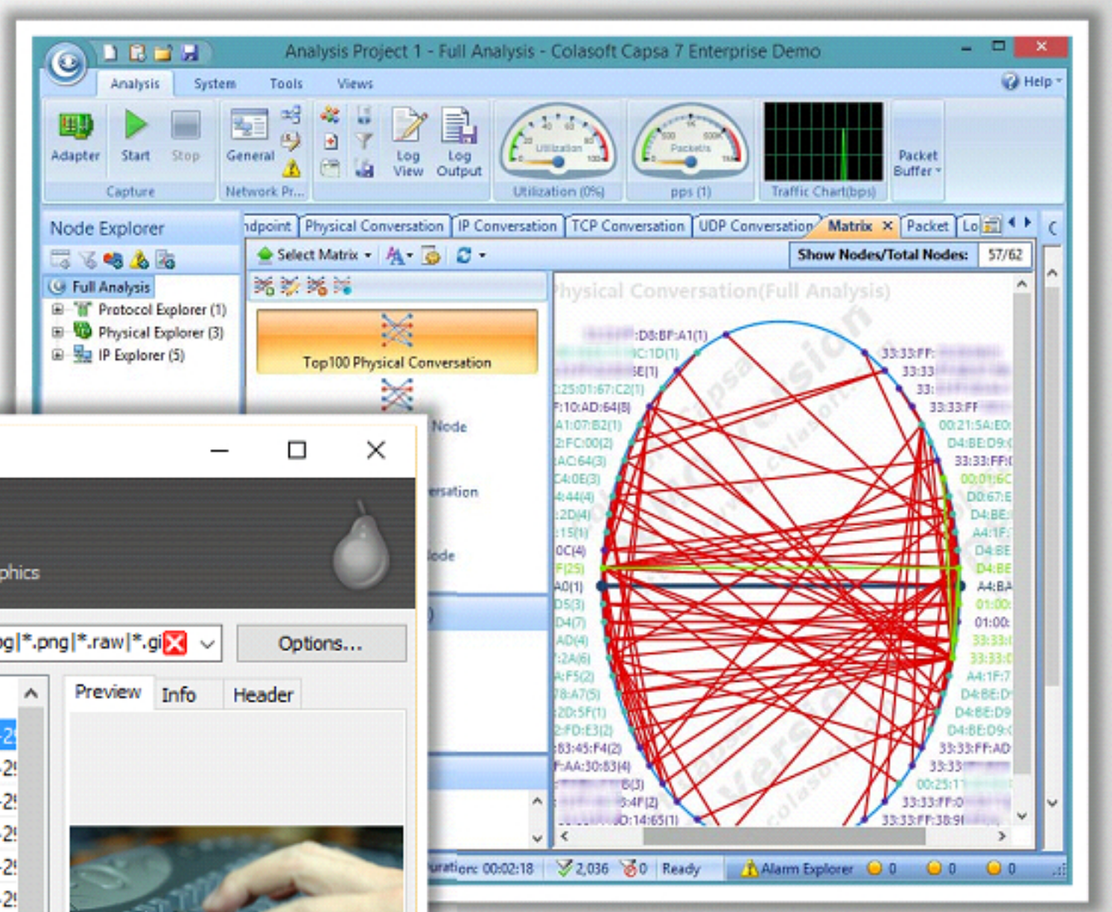
C|HFI Computer Hacking Forensic Investigator

Password Cracking Tool: Cain & Abel

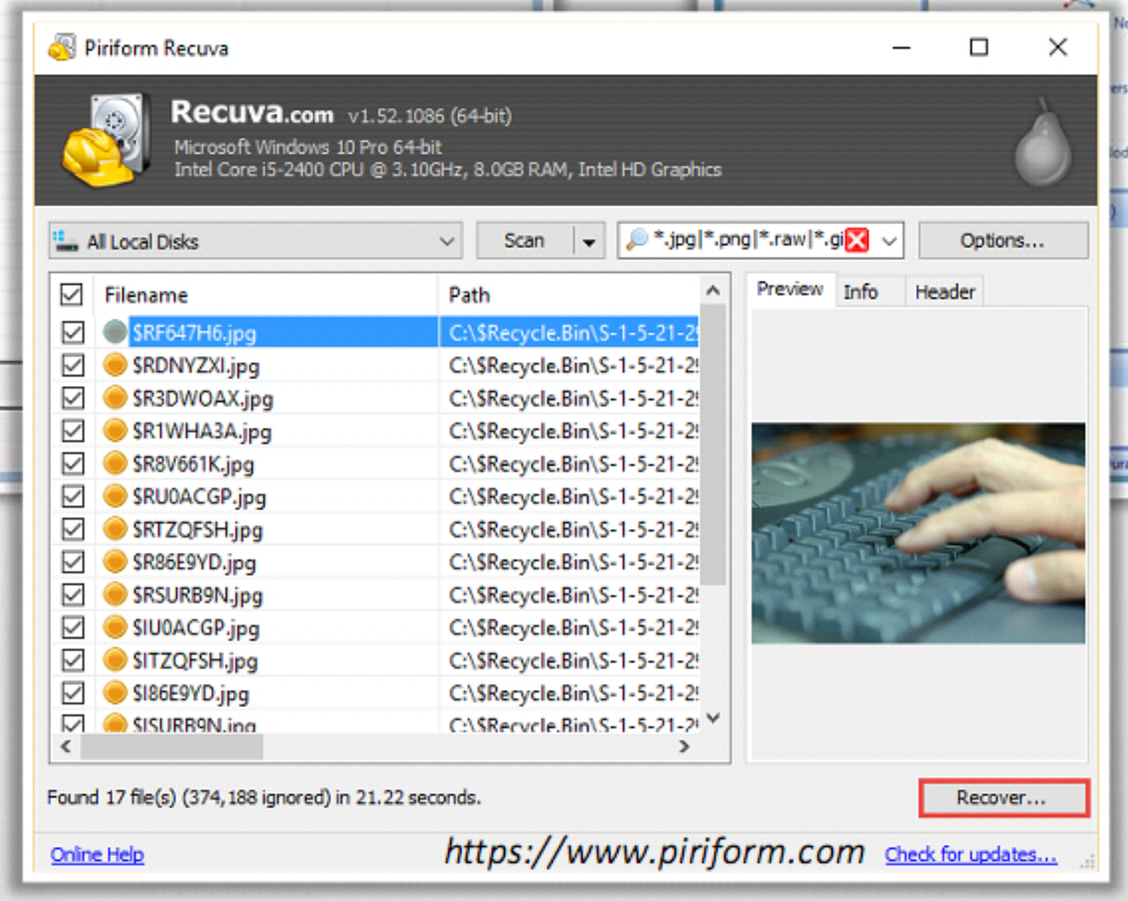


http://www.oxid.it

Network Traffic Analysis Tool: Capsa Network Analyzer



http://www.colasoft.com



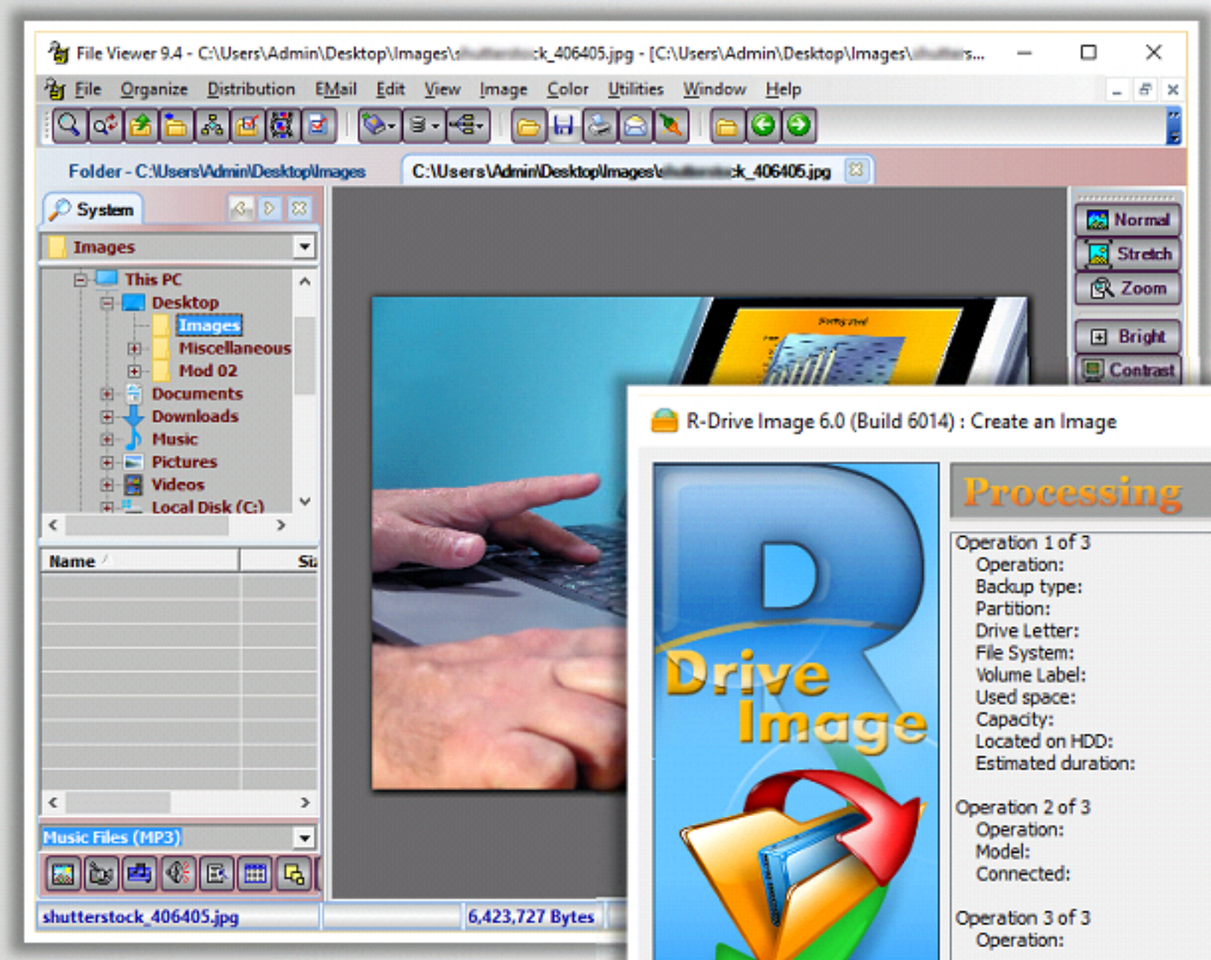
Data Recovery Tool: Recuva

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

Forensics Software (Cont'd)

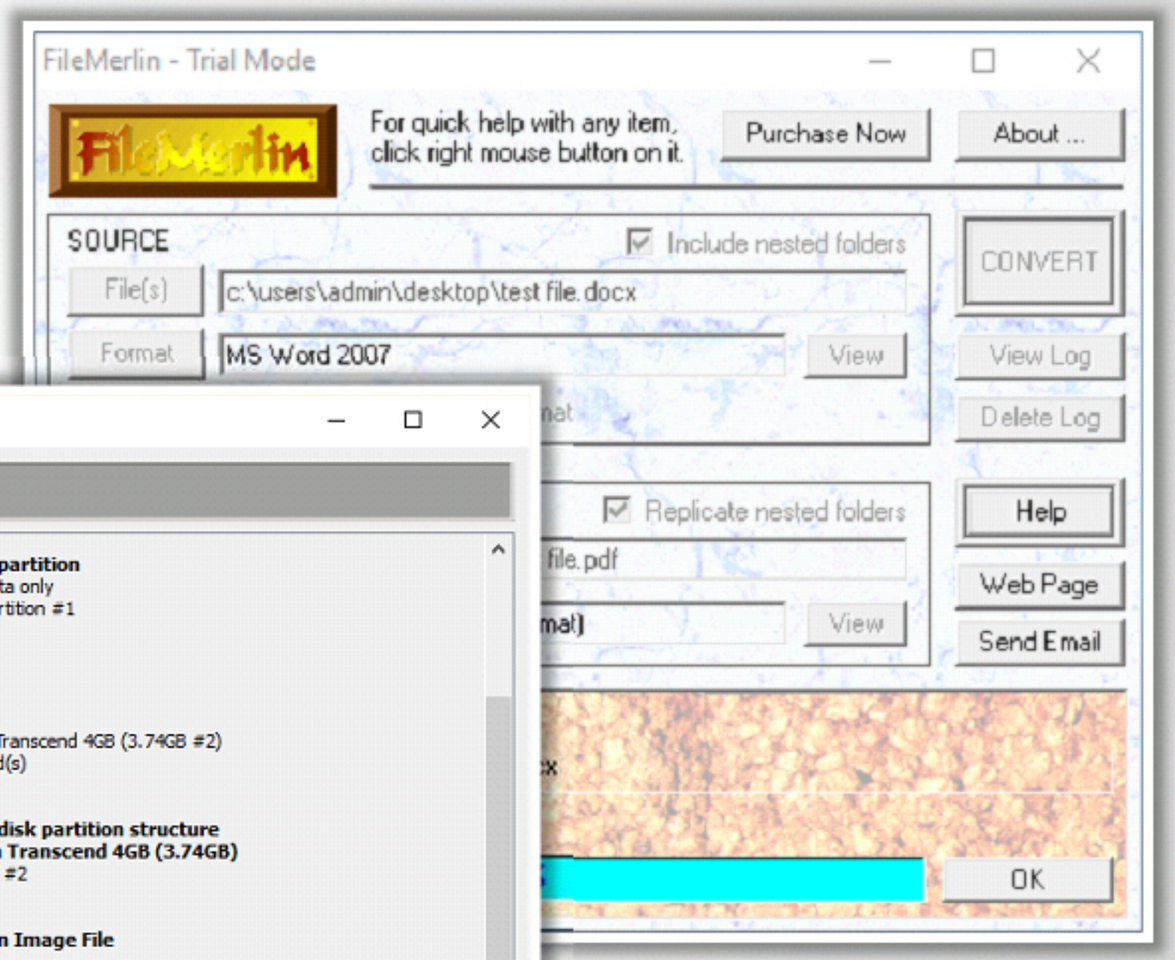
C|HFI Computer Hacking Forensic Investigator

File Viewing Software: File Viewer



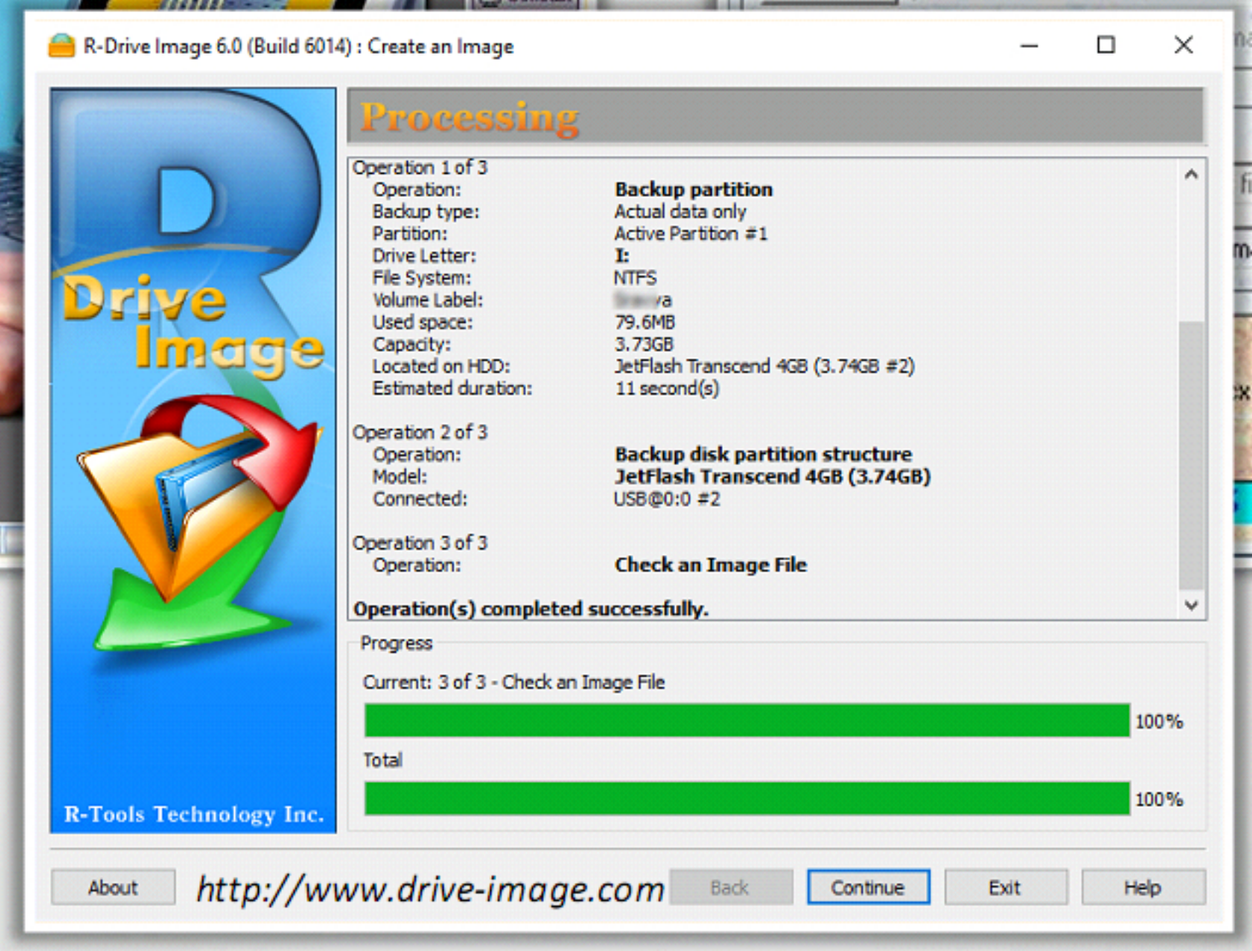
http://www.accessoryware.com

File Type Conversion Software: FileMerlin



http://www.file-convert.com

Imaging Tool: R-Drive Image



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

Forensics Software (Cont'd)

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

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

Forensics Software (Cont'd)

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

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

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

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

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**

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

Review Policies and Laws

C|HFI Computer Hacking Forensic Investigator

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

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

Forensics Laws

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

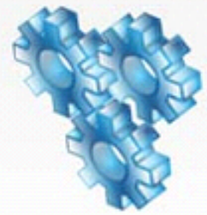
- **18 USC §1029** - Fraud and related activity in connection with access devices
- **18 USC §1030** - Fraud and related activity in connection with computers
- **18 USC §1361-2** - Prohibits malicious mischief
- **Rule 402** - General Admissibility of Relevant Evidence
- **Rule 901** - Authenticating 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

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

Establish Quality Assurance Processes

An investigator implements various tools and techniques to **retrieve** and **analyze data** of evidentiary value. However, the **standalone procedure** he/she follows may affect the resultant evidence and the case outcome.

Thus, there is a need for a forensics unit to establish and follow a **well-documented systematic process** for investigating a case that ensures quality assurance



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

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

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

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

General Quality Assurance in the Digital Forensic Process

C|HFI Computer Hacking Forensic Investigator

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
10. Review, update, and document policy and standards annually

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

Quality Assurance Practices:
Laboratory Software and Hardware

C|HFI Computer Hacking Forensic Investigator

- 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.

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

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

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)

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

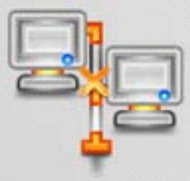
Risk Assessment

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

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

Risk Assessment Matrix

Likelihood	Consequences				
	Insignificant (Minor problem easily handled 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

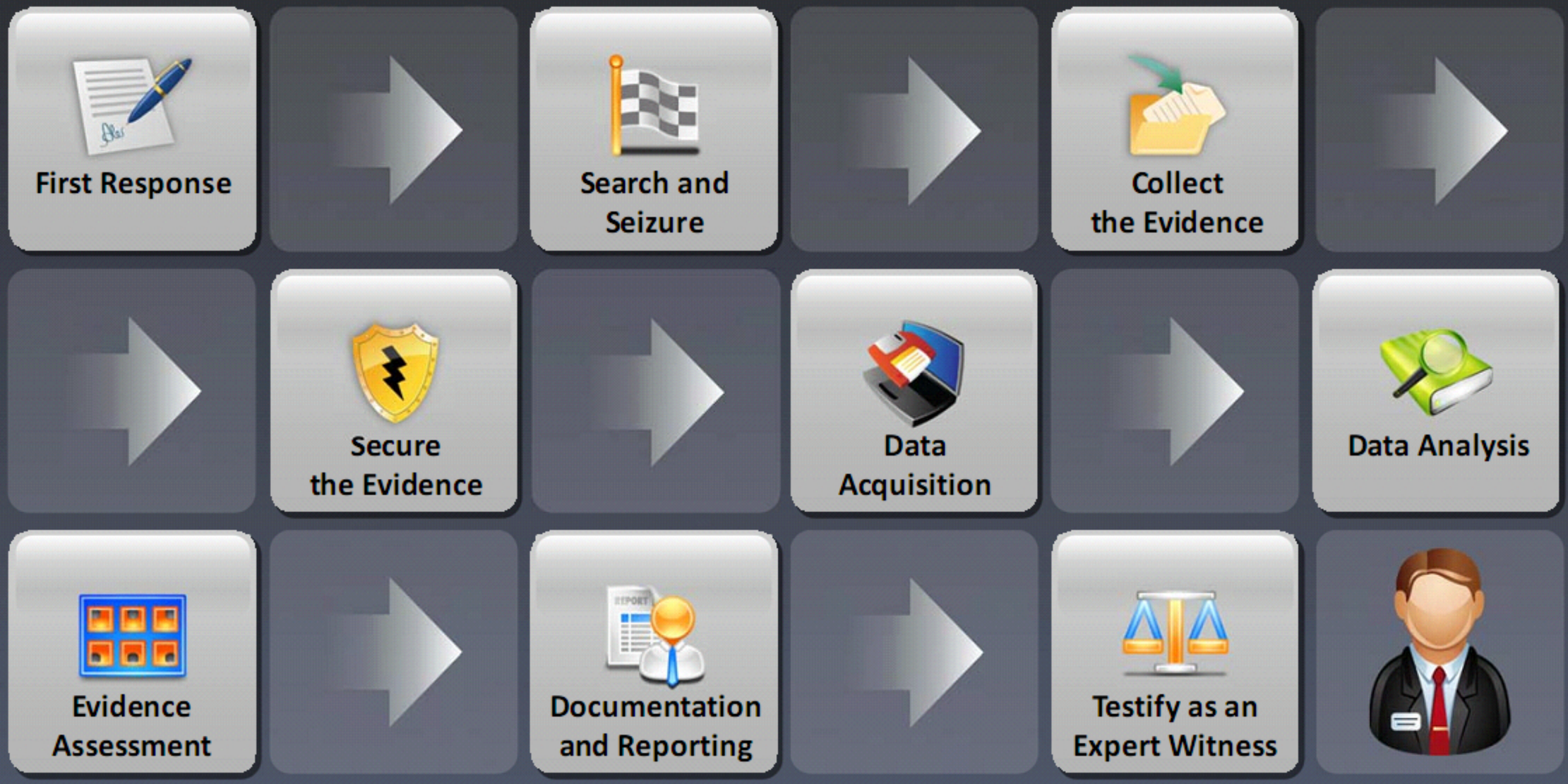
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigation Phase

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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic Investigator



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

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

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

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

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

Investigation Process (Cont'd)

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**

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

Questions to Ask When a Client Calls the 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?

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

Checklist to Prepare for a Computer Forensics Investigation

C|HFI Computer Hacking Forensic INVESTIGATOR

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

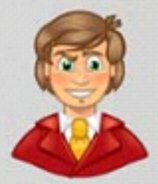
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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

Notify Decision Makers and Acquire Authorization

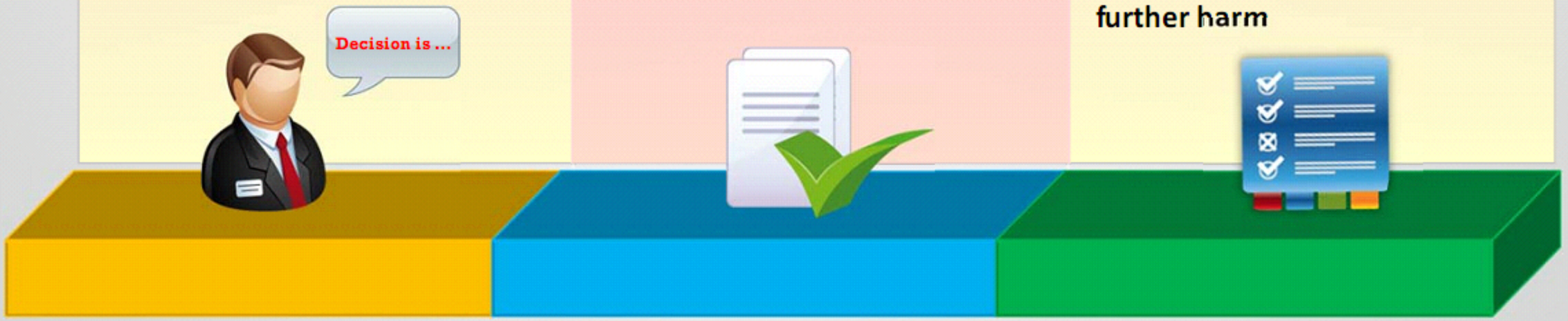
- Decision makers are the people who **implement policies and procedures for handling an incident**
- Notify the decision maker for authorization when the written incident response policies and procedures do not exist
- After the authorization, **assess the situation** and **define the course of action**

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

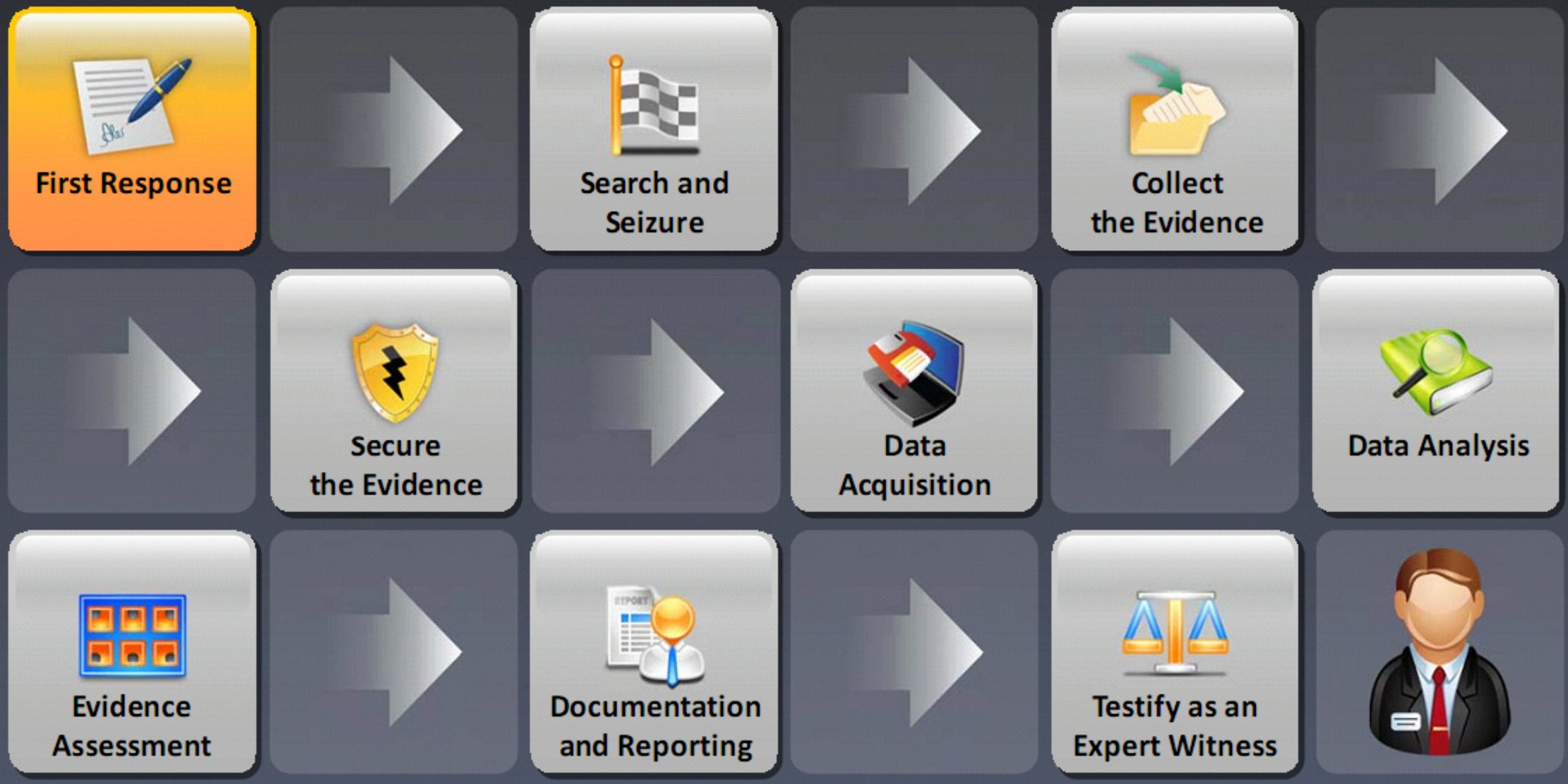
Depending on the scope of the incident and presence of any national security issues or life safety issues, the first priority is to protect the organization from further harm



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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic Investigator



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

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**

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

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

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

First Response Basics

C|HFI 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

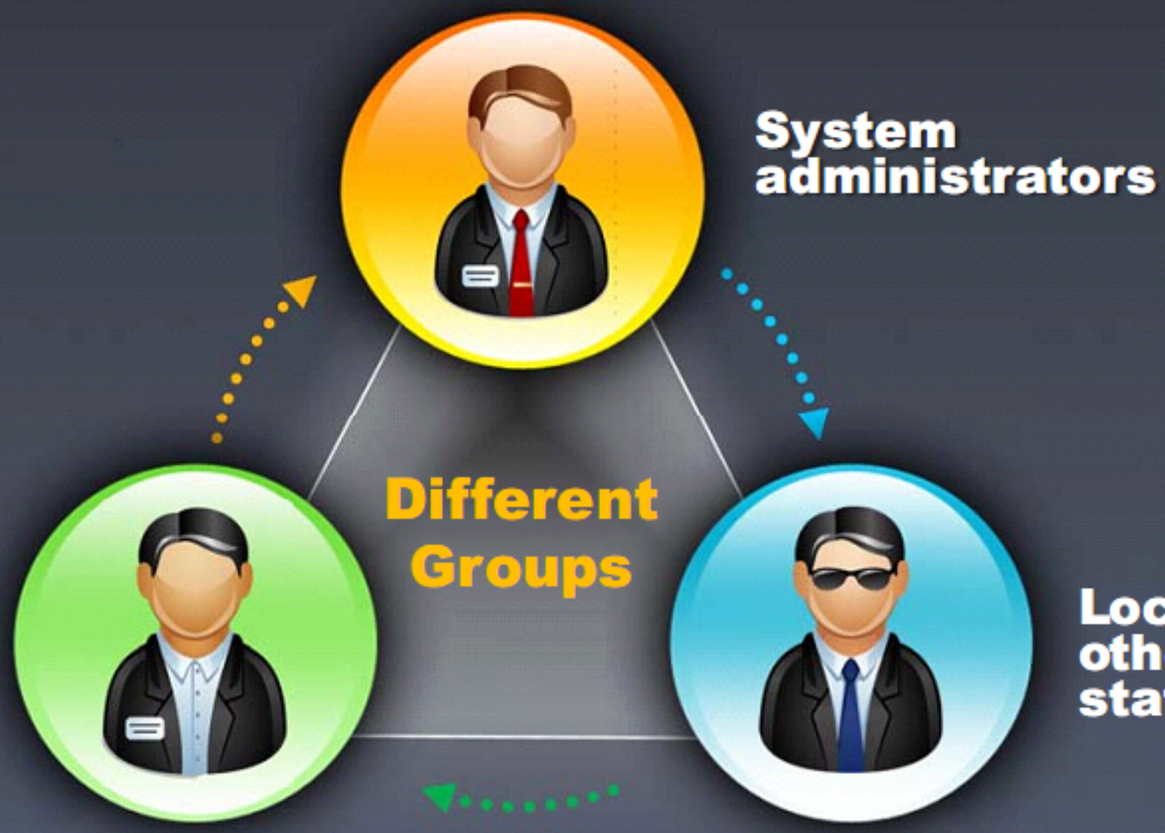
03 Any information present inside the collected electronic devices is potential evidence and should be treated accordingly

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

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

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



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

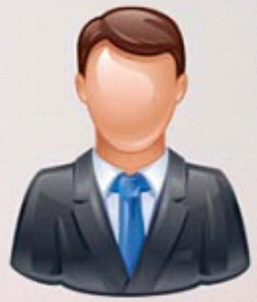
First Response by System Administrators

The system administrator plays an important role in ensuring network protection and maintenance, as well as playing a **vital role in the investigation**

1

Once a system administrator discovers an incident, it must be **reported** according to the current organizational incident reporting procedures

2



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

3

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

First Response by Non-forensics Staff

C|HFI Computer Hacking Forensic Investigator

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

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

First Response by Laboratory Forensics Staff

C|HFI Computer Hacking Forensic Investigator

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
- Initial interviews

03 Documenting the Electronic Crime Scene

- Photograph the scene
- Sketch the scene

04 Collecting and Preserving the Electronic Evidence

- Collect evidence
- Exhibit numbering
- 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

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

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**

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

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

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

Photographing the Scene

C|HFI 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

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

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

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

Note Taking Checklist

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

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

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

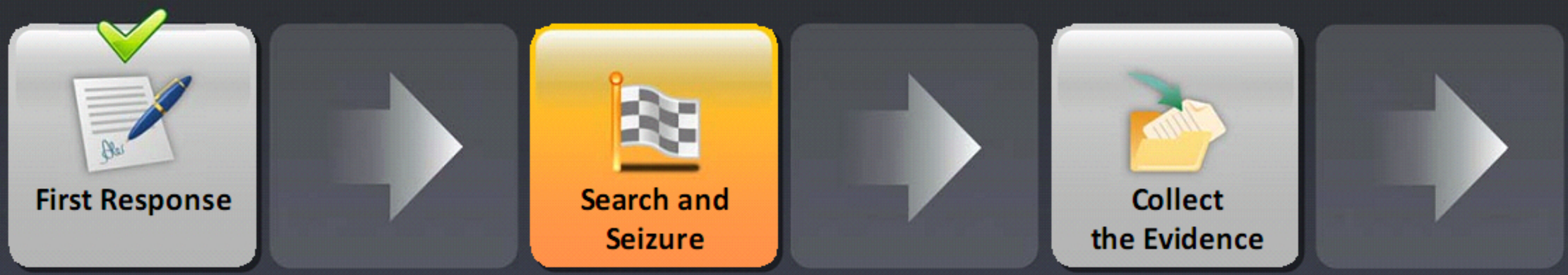
Crime Scene Checklist

  - – 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

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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic Investigator



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

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

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

Sample of Consent Search Form

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_____

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

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

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

Witness Statement Checklist

C|HFI Computer Hacking Forensic Investigator

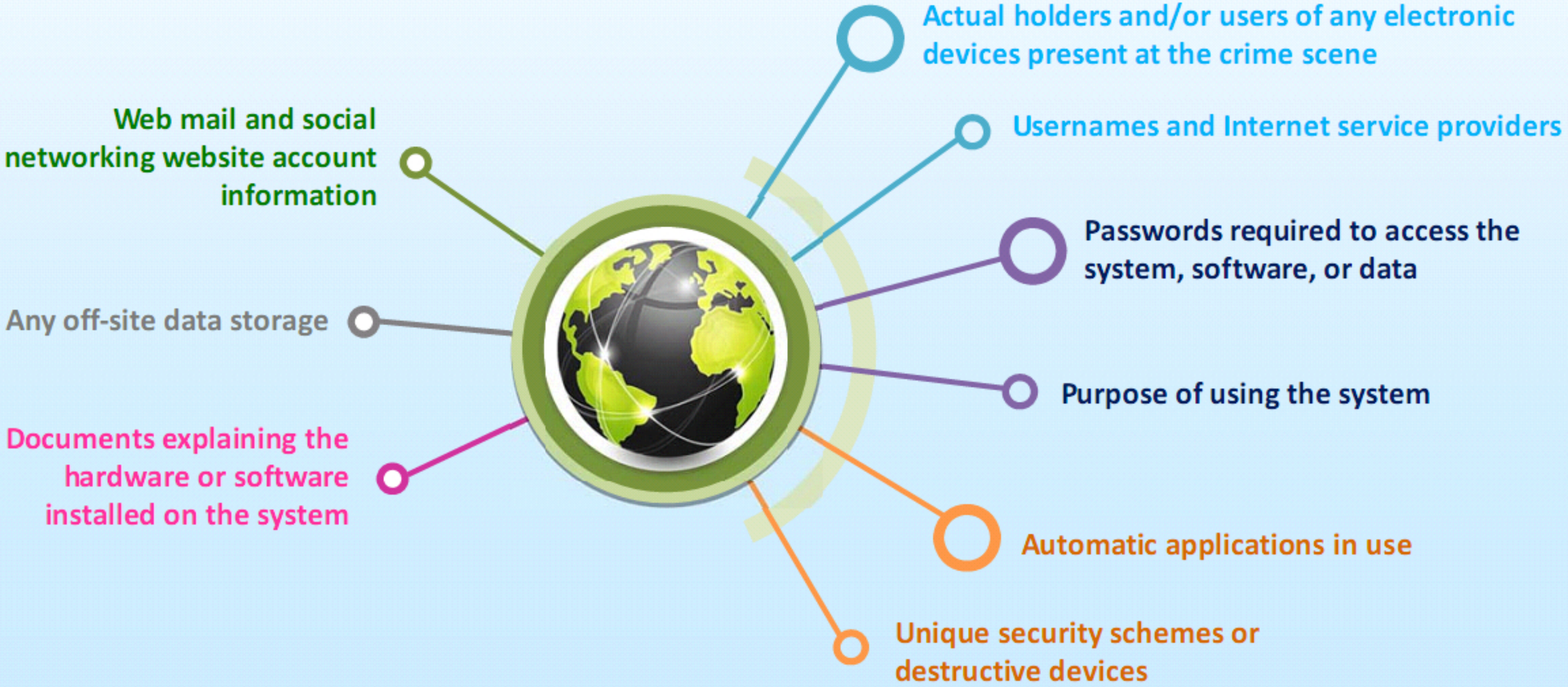
ACTIONS	CHECK IF PERFORMED WELL
1. Sets the person at ease • explains reason for taking statement • explains what may be required of witness • explains the importance of telling the truth • respects the legal rights of the individual being interviewed	 — — — —
2. Ensures the environment is appropriate 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	—

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

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 :



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

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**

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

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?

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

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

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

Initial Search of the Scene

C|HFI Computer Hacking Forensic INVESTIGATOR

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

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

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.

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

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?

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**

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

Where will this search be **conducted**?

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

Example of Search Warrant

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

AO 106 (Rev. 5/85) Affidavit for Search Warrant

United States District Court

WESTERN DISTRICT OF WASHINGTON

MAR 2 8 1997

CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
DEPUTY

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 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, 1505, 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

ISSUED No. 9602582

1

BRISTOL MAGISTRATES' COURT — (1013)

Date :- 21 MAY 1999 and time :- 10.02

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 :- 9 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

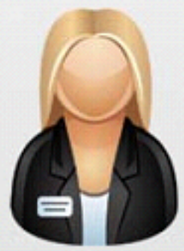
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Searches Without a Warrant

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. l991)

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)



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

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

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

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

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

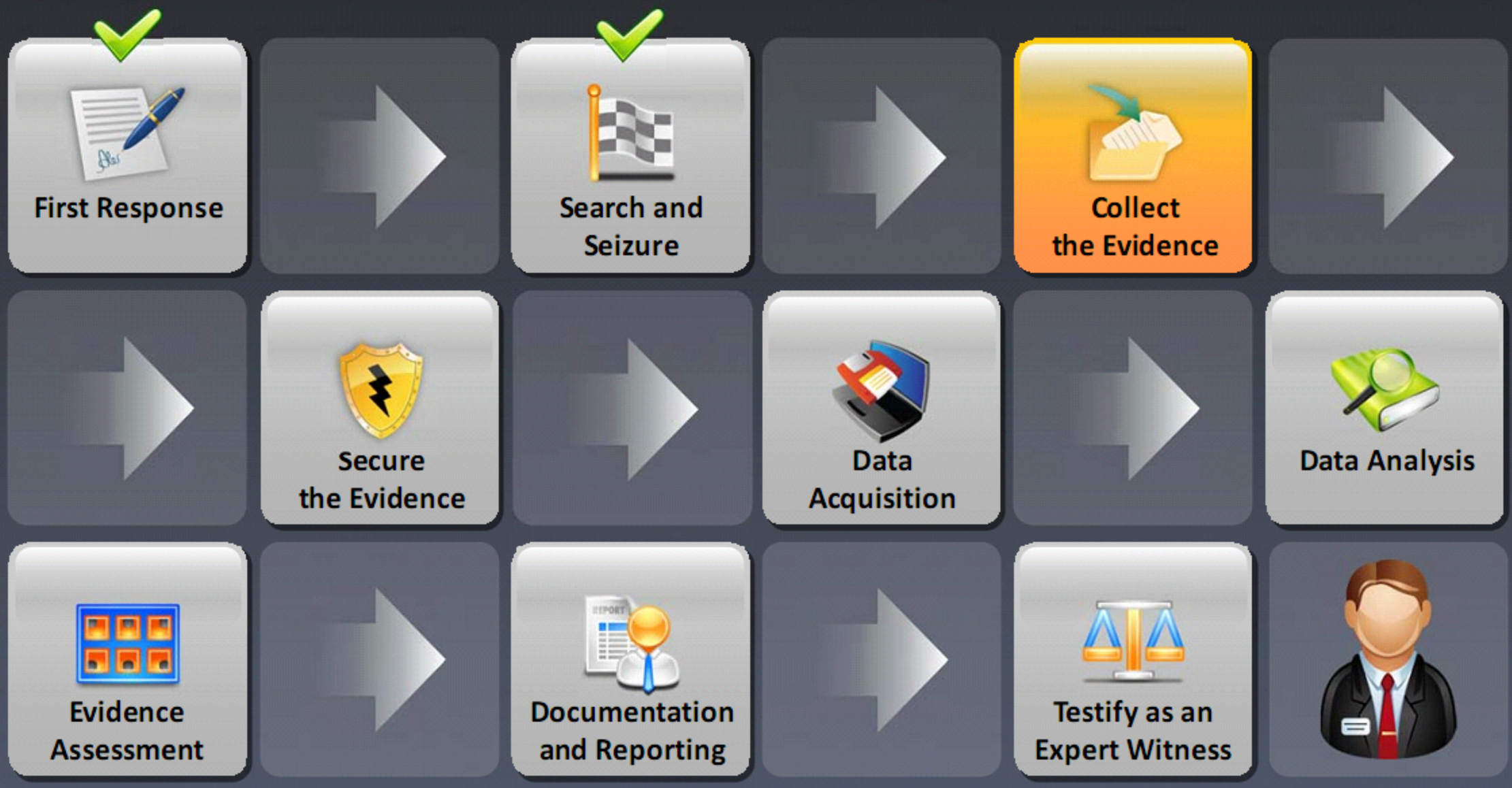
Securing and Evaluating Electronic Crime Scene: A Checklist (Cont'd)

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

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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic INVESTIGATOR



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

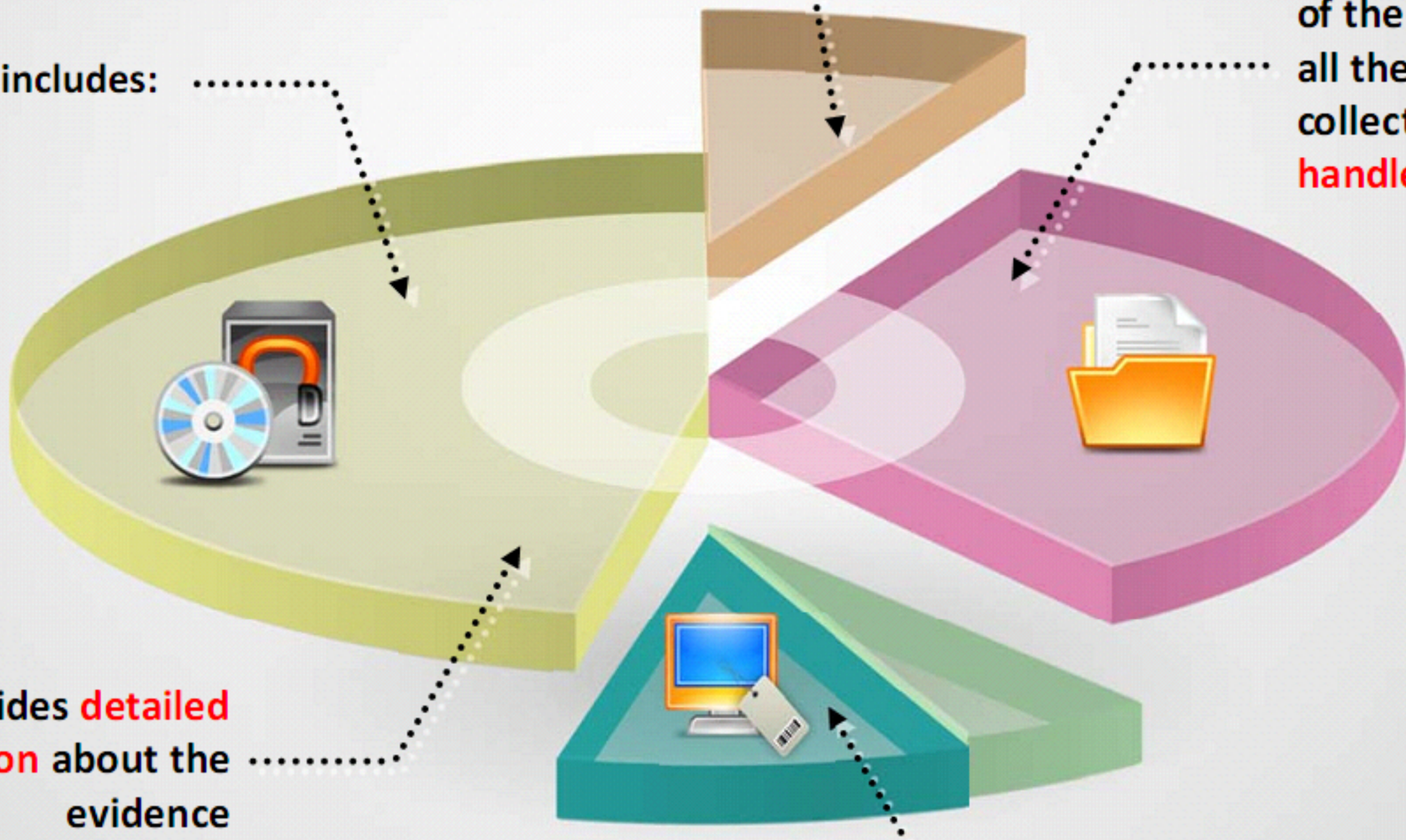
Collect Physical Evidence

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

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

Evidence Collection Form

C|HFI 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 Collected :	Type of Offences :
Victim's Full Name :	Suspect's Full Name :

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

Collecting and Preserving Electronic Evidence

C|HFI Computer Hacking Forensic Investigator

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

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

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**

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

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.

Dealing with Networked Computer

C|HFI Computer Hacking Forensic Investigator

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

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

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

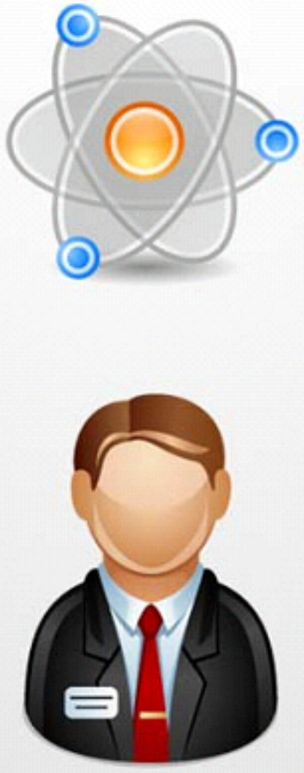
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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

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

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

Preserving Electronic Evidence

C|HFI Computer Hacking Forensic Investigator

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

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

Preserving Electronic Evidence (Cont'd)

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

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

Seizing Portable Computers

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

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

Dealing with Switched On Portable Computers

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

1

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

4

2

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

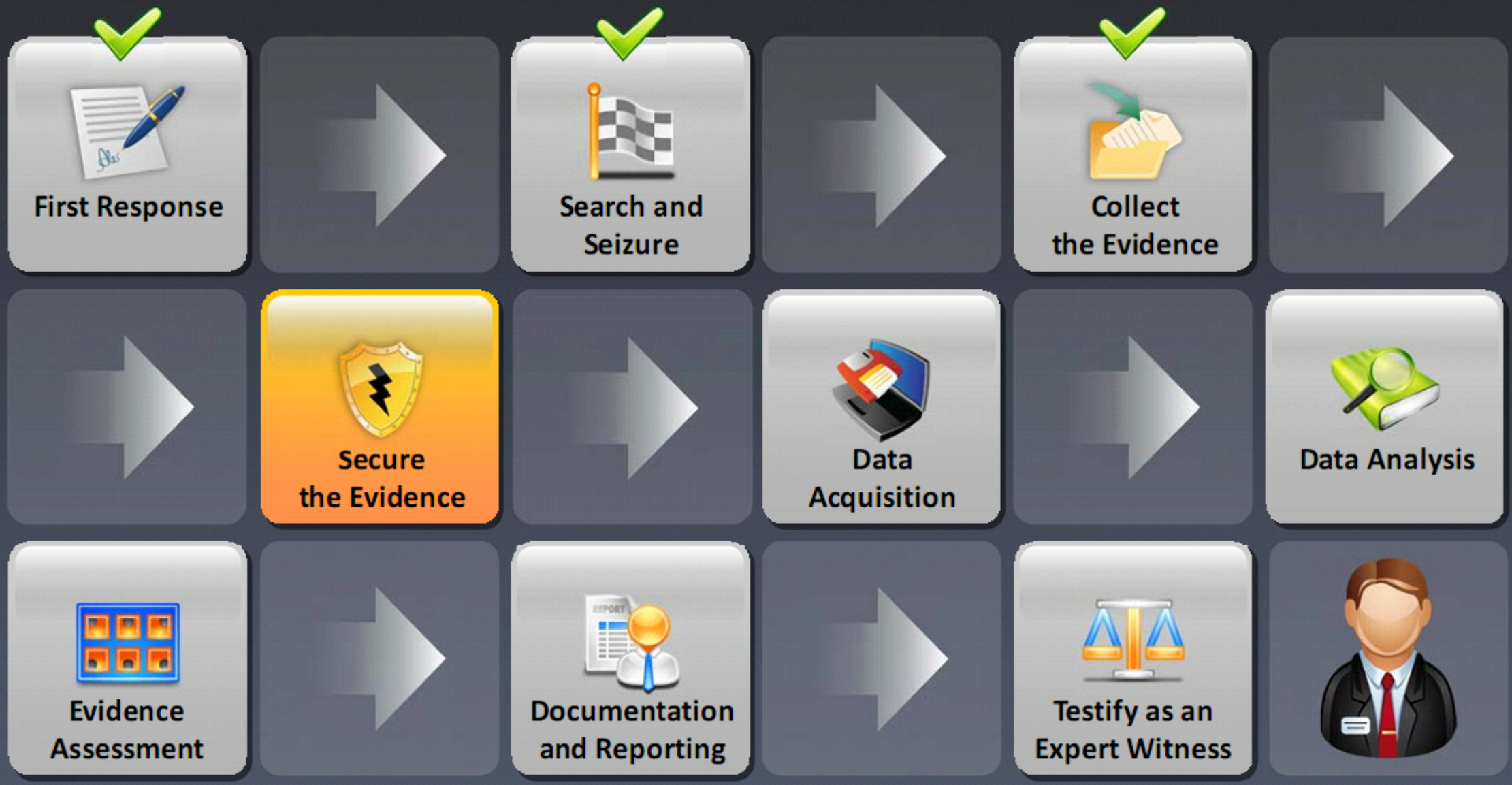
3

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

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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic INVESTIGATOR



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

Evidence Management

C|HFI Computer Hacking Forensic Investigator

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

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

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

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

Simple Format of the Chain of Custody Document

C|HFI 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

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

Chain of Custody Forms

C|HFI 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 ☐ Active ☐ Suspended/Stand-by ☐ Screen Saver Active ☐ Off ☐ No Power/Not Connected ☐ Other

Apparent OS ☐ Ukw

Active/Open Programs: ☐ None ☐ N/A

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

1.

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

2.

Shutdown Data and Time

3.

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

Chain of Custody Forms (Cont'd)

C|HFI Computer Hacking Forensic Investigator

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:**			

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

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	

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

Chain of Custody Forms (Cont'd)

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:

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

Chain of Custody Forms (Cont'd)

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:

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

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 ☐

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

Chain of Custody Forms (Cont'd)

C|HFI Computer Hacking Forensic INVESTIGATOR

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 ☐

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

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
	☐			
	☐			
	☐			

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

Chain of Custody Forms (Cont'd)

C|HFI Computer Hacking Forensic Investigator

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
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

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

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:_____

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

C|HFI Computer Hacking Forensic Investigator

Packaging and Transporting Electronic Evidence

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

C|HFI Computer Hacking Forensic Investigator

Packaging and Transporting Electronic Evidence

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

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**

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

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.)

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

Transporting Electronic Evidence

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

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

Storing Electronic Evidence

Ensure the **electronic evidence** is **listed** in accordance with **departmental policies**

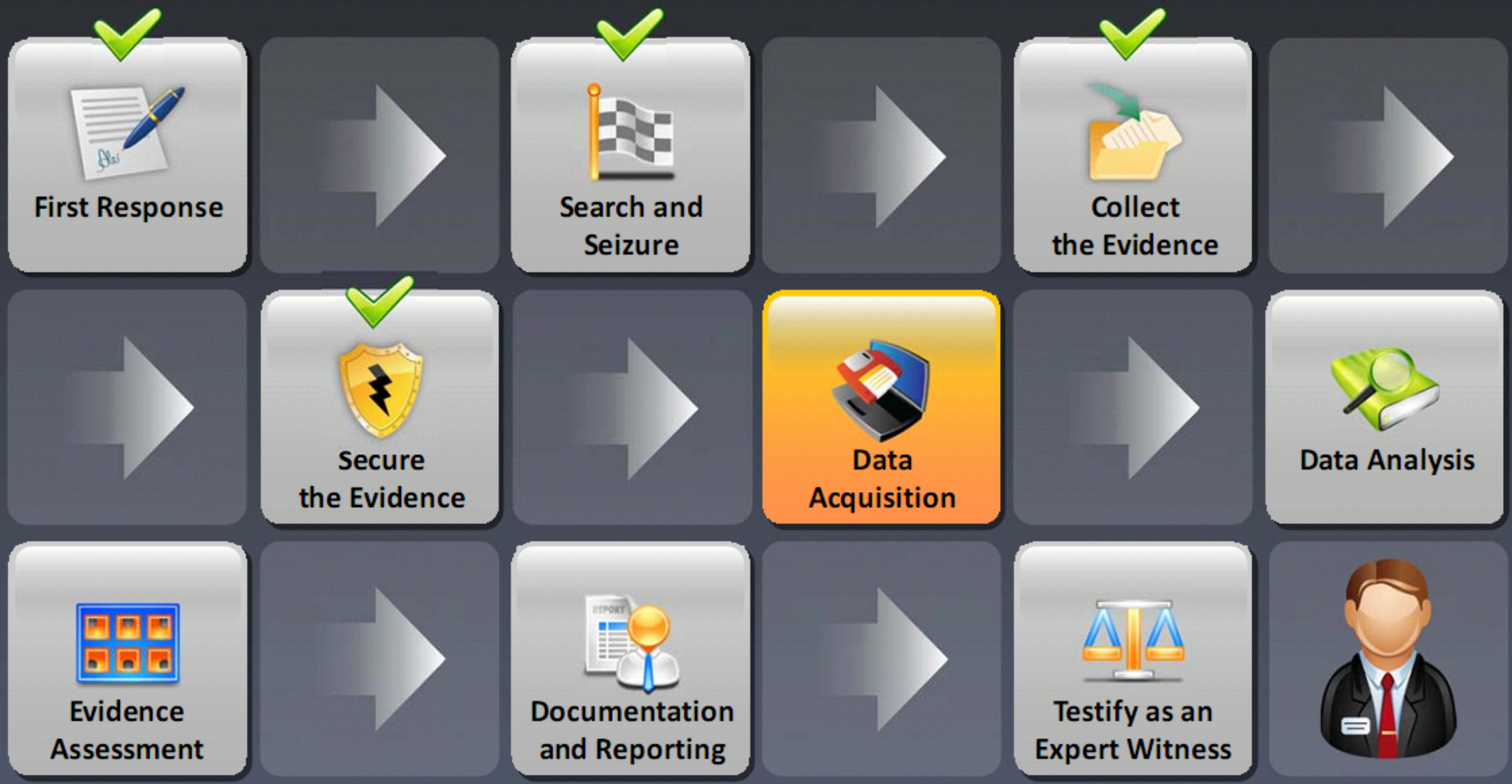
Store the electronic evidence in a **secure** and **weather-controlled** environment

Protect the **electronic evidence** from magnetic fields, dust, vibrations, and other factors that may damage its integrity

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

Computer Forensics Investigation
Methodology

C|HFI Computer Hacking Forensic Investigator



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

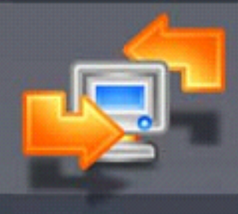
Guidelines for Acquiring Evidence

C|HFI 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

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

Original Evidence Should NEVER Be Used for Analysis

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

Duplicate the Data (Imaging)

Make a **duplicate of the collected data** so as to preserve the original

1

The data should be duplicated **bit by bit** to represent the same original data

2

Once a copy of the original data is made and verified, you can use the copy for further processing

4

Use industry standard or licensed hardware or software tools to duplicate the data

3

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

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

Verify Image Integrity

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

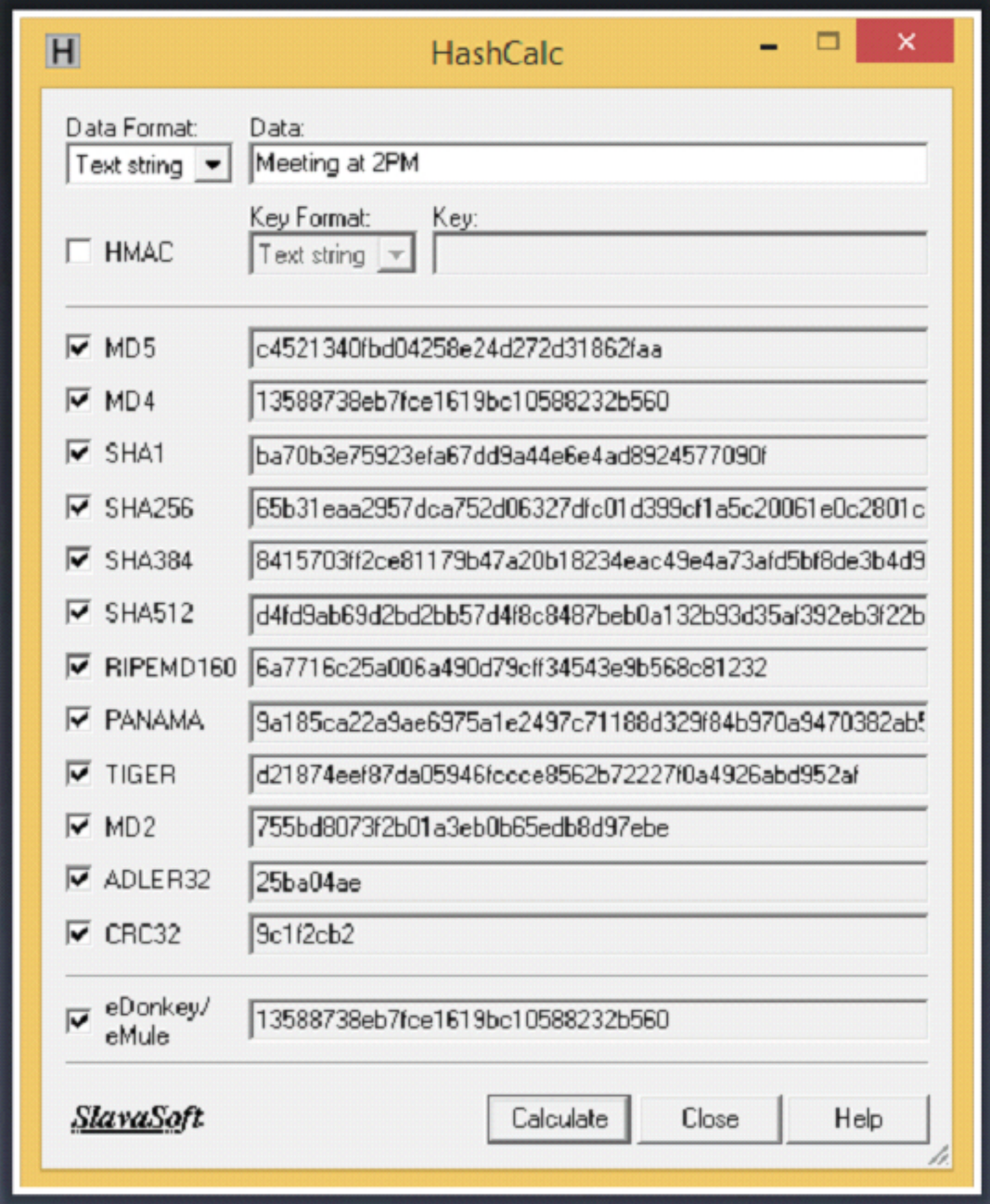
If there is a match it means that the forensic image is an exact replica of the original data

Tools for calculating hash value:

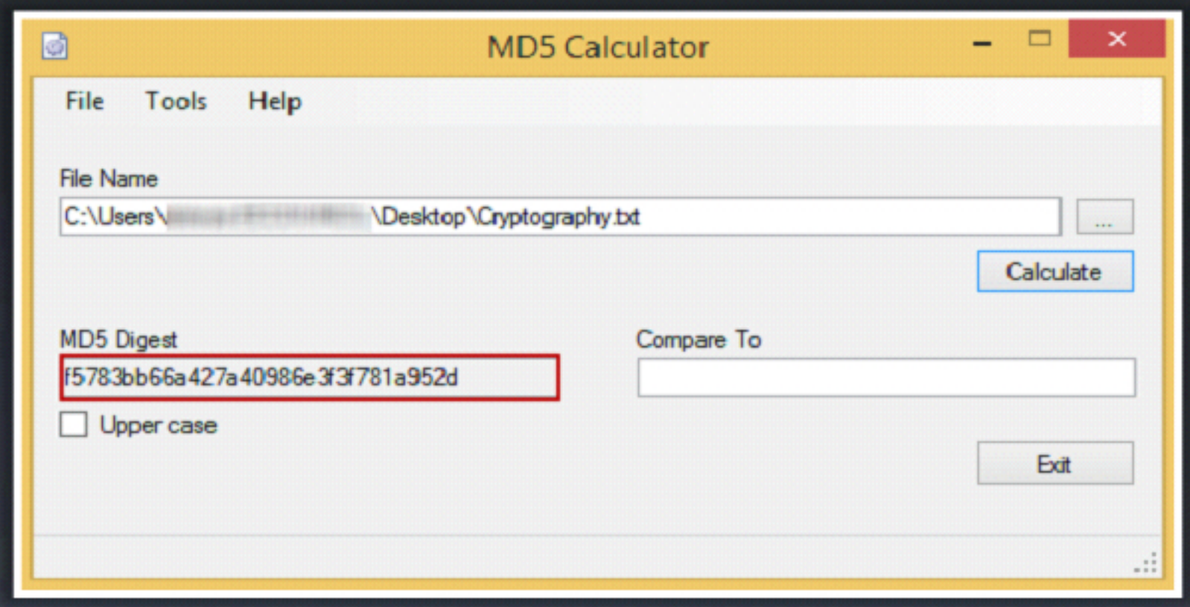
- **HashCalc**
- **MD5 Calculator**
- **HashMyFiles**

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

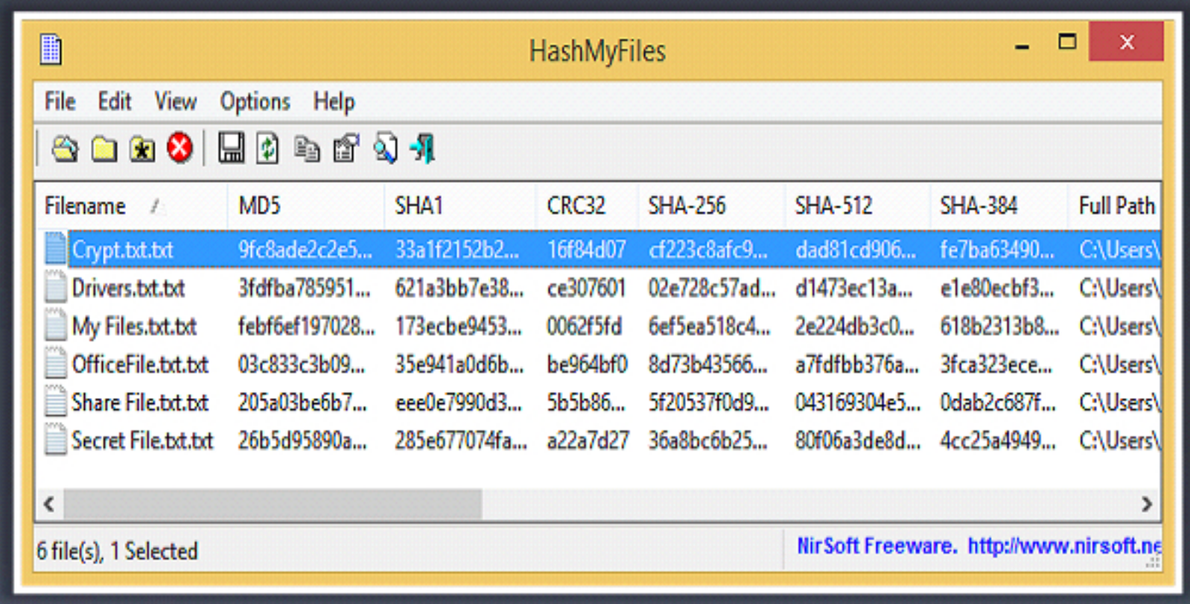
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles



http://www.slavasoft.com



http://www.bullzip.com



http://www.nirsoft.net

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

Recover Lost or Deleted Data

C|HFI Computer Hacking Forensic Investigator

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

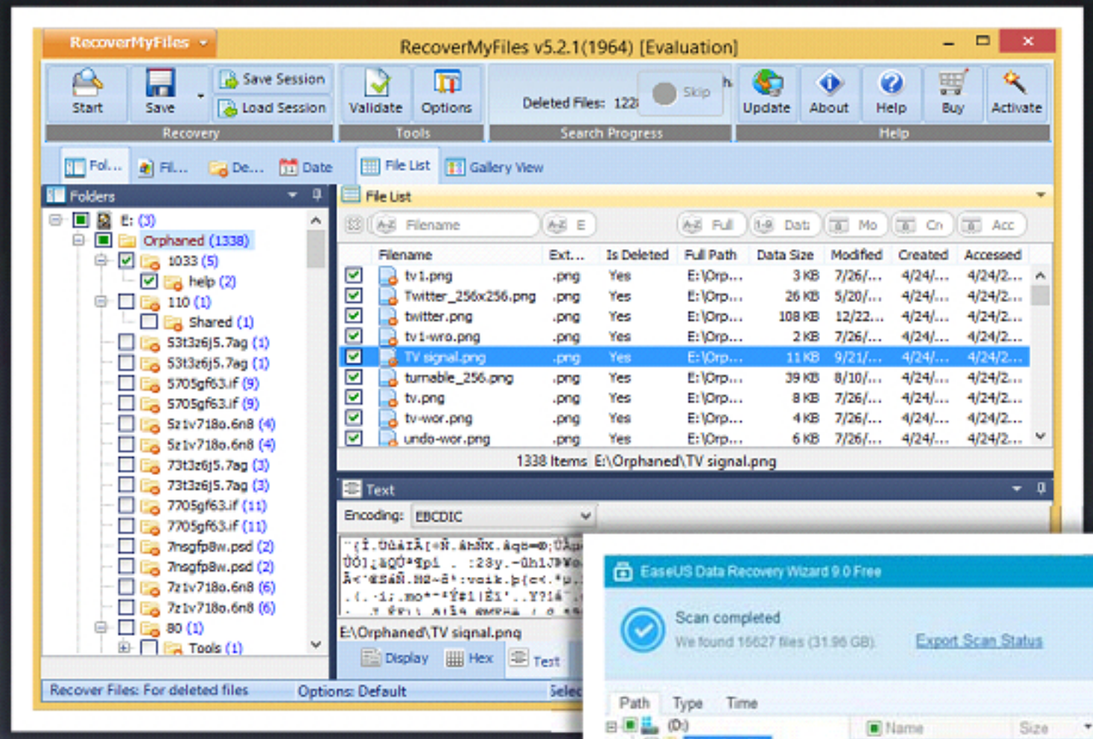
Software used to recover the data

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

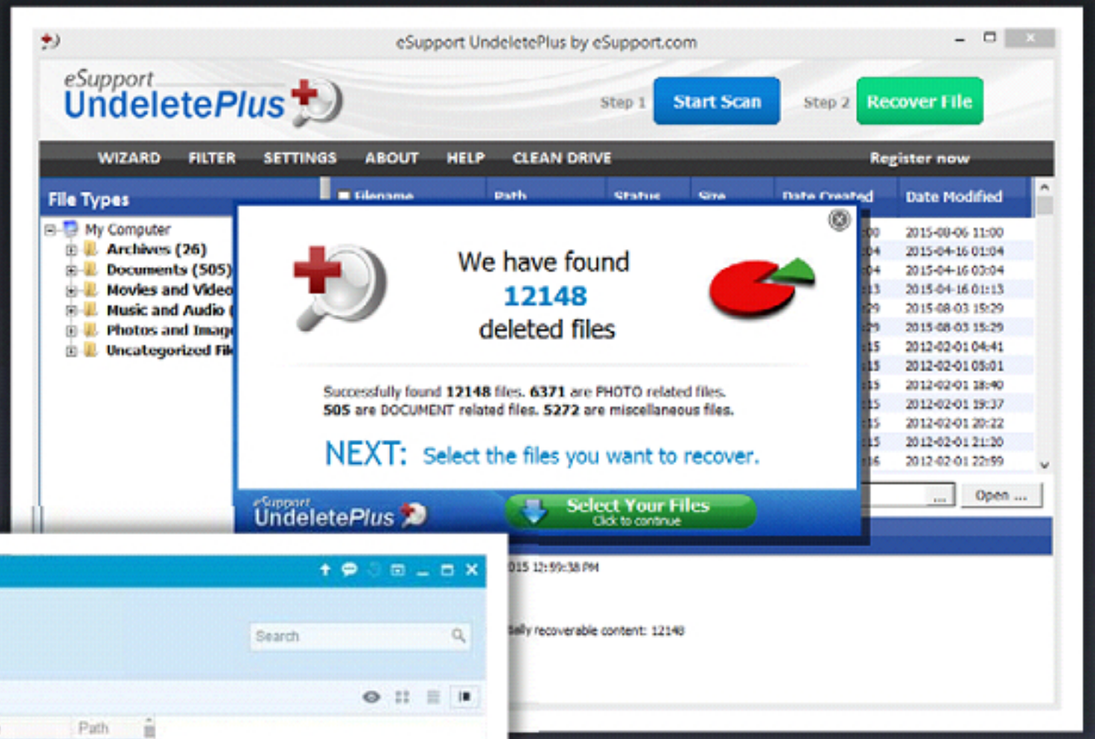
Data Recovery Tools

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

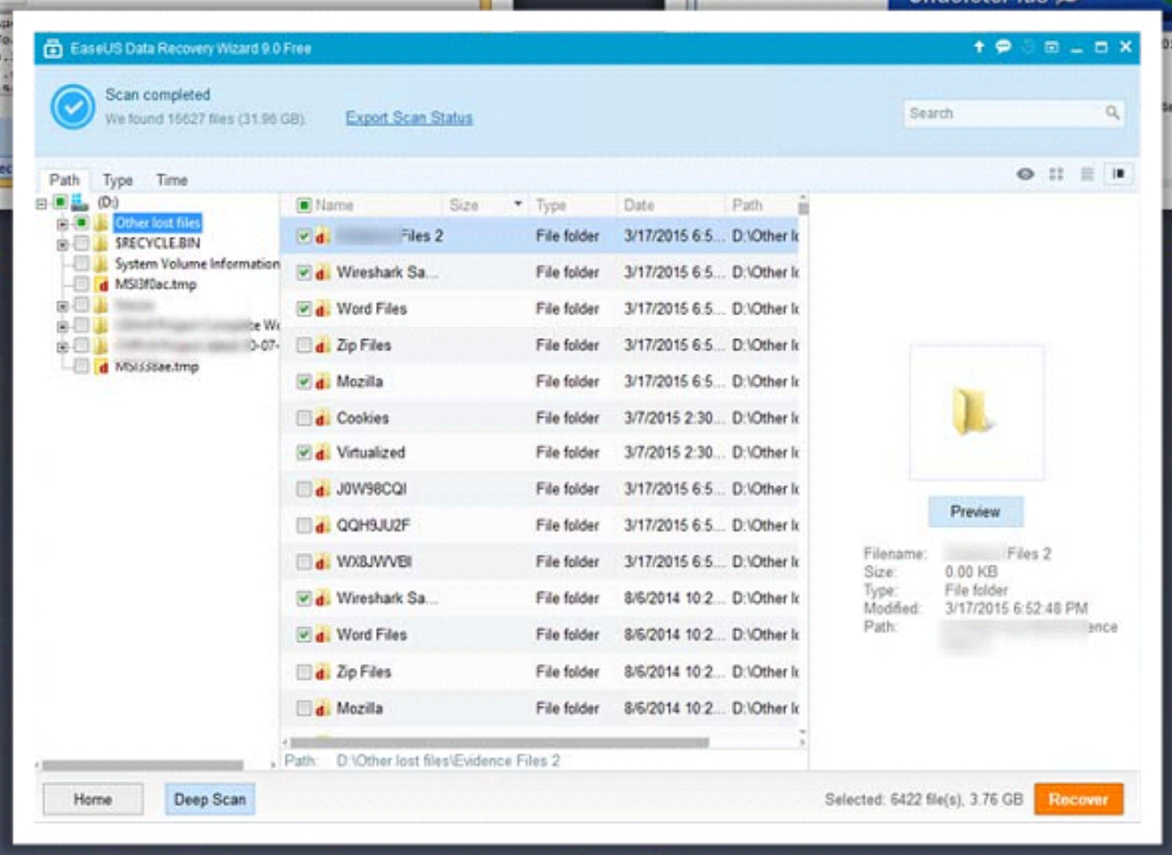
Data Recovery Software



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



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



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

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

Computer Forensics Investigation Methodology

C|HFI 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

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

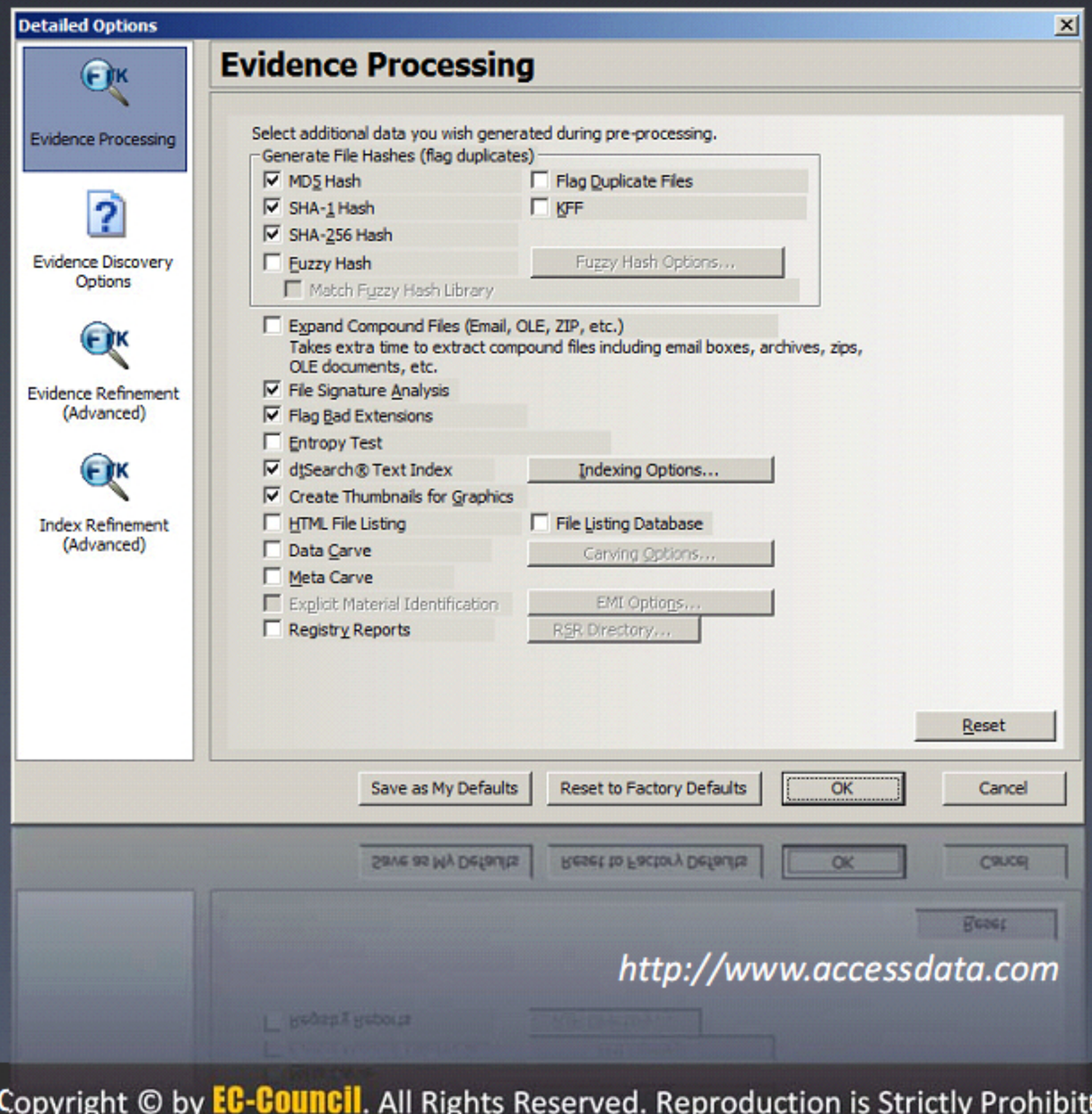
Identify and categorize data in **order of relevance**

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

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



http://www.accessdata.com

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

Post-investigation Phase

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

Computer Forensics Investigation Methodology

C|HFI 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

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

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

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

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

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

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

Collecting Evidence from Social Networks

C|HFI Computer Hacking Forensic Investigator

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**

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

Collecting Evidence from Social Networks (Cont'd)

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

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

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, unallocated clusters, 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 securely collect 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.

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

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

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

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

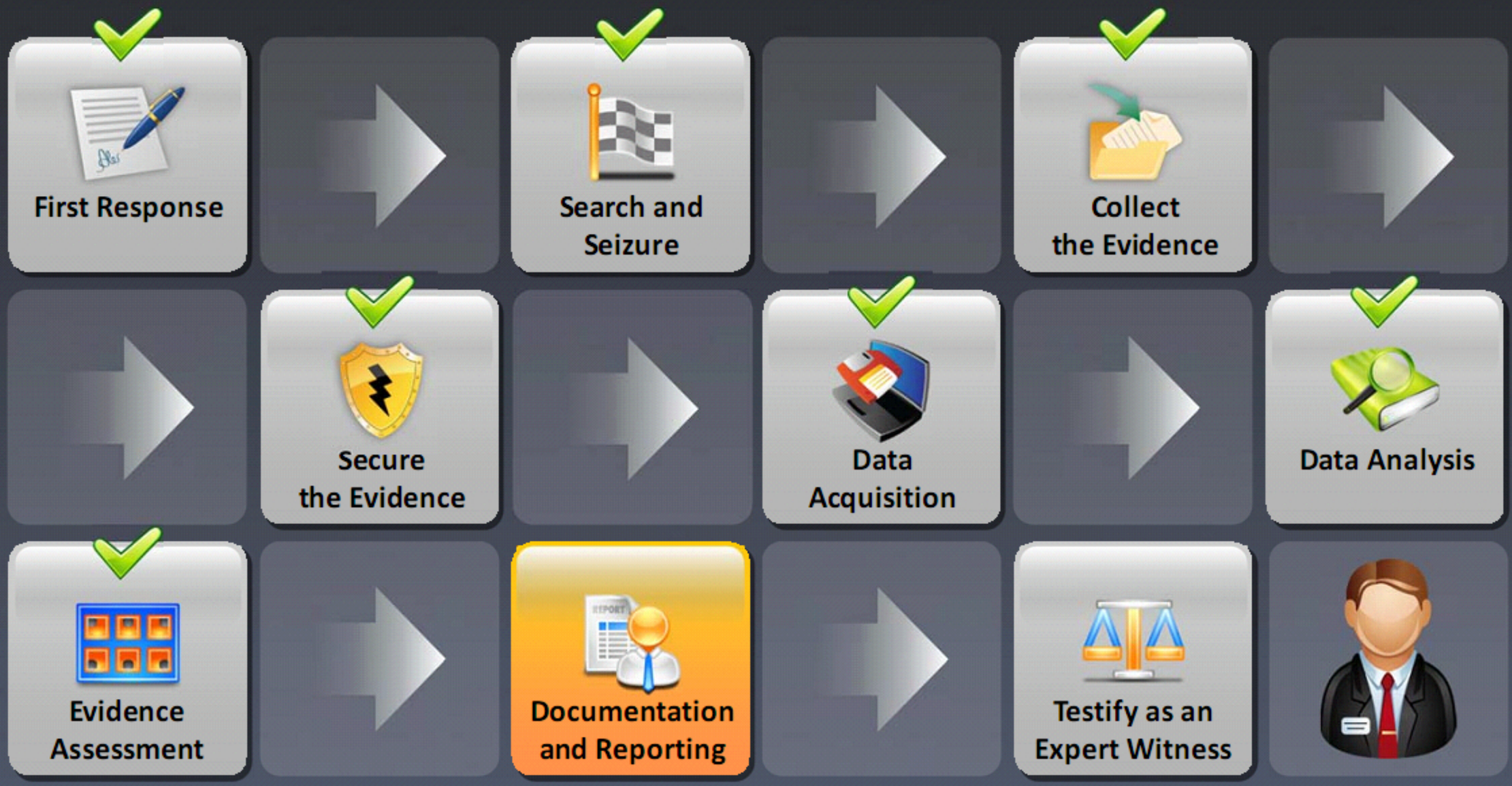
Correlate the file headers to the corresponding file extensions to identify any mismatches

Review the files' names for relevance and patterns

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

Computer Forensics Investigation Methodology

C|HFI Computer Hacking Forensic Investigator



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

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

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

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

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

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

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

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

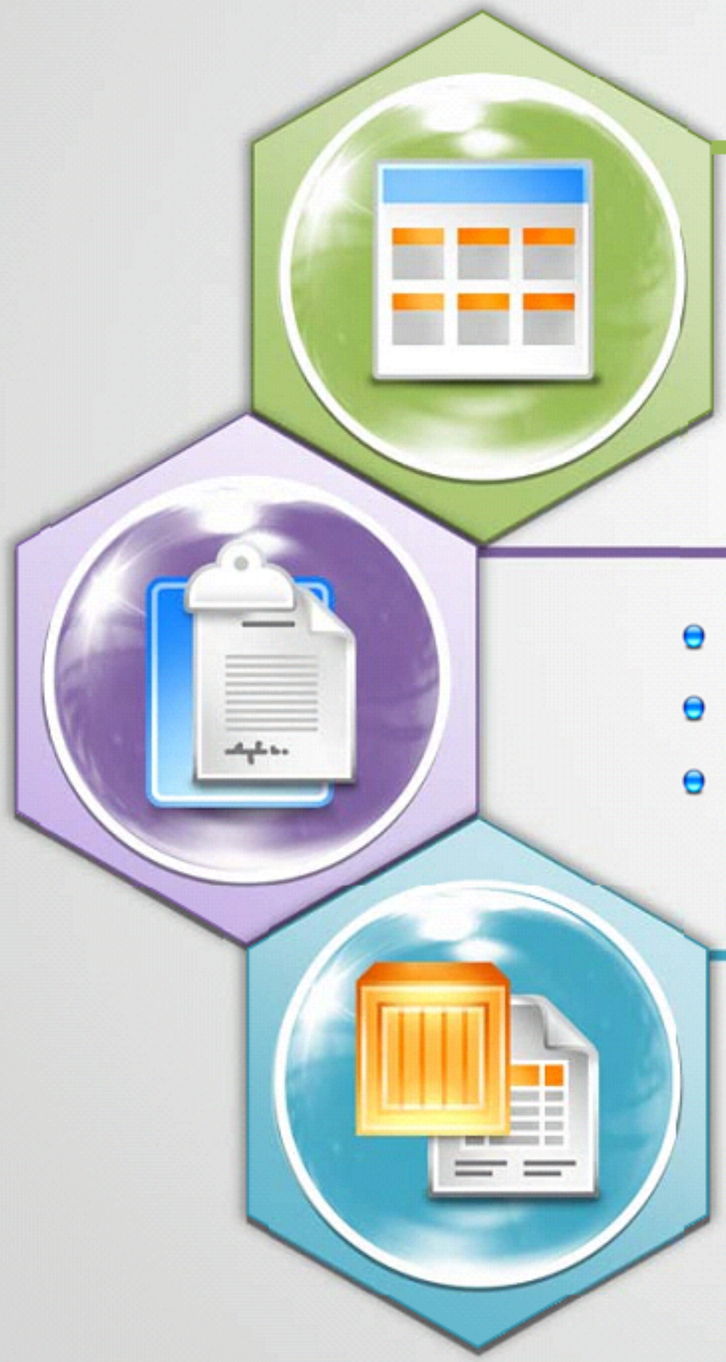
Introduce the incident and explain its impact; the summary should explain clearly what the incident was and how it occurred

Evidence

Provide descriptions of the evidence that was acquired during the investigation

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

Writing the Investigation Report (Cont'd)



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

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

Computer Forensics Investigation Methodology

C|HFI 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

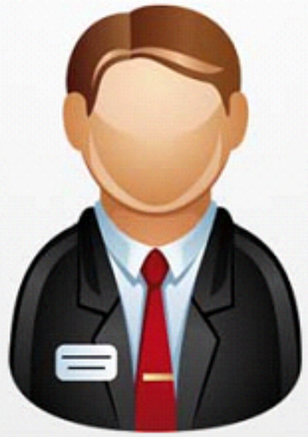
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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



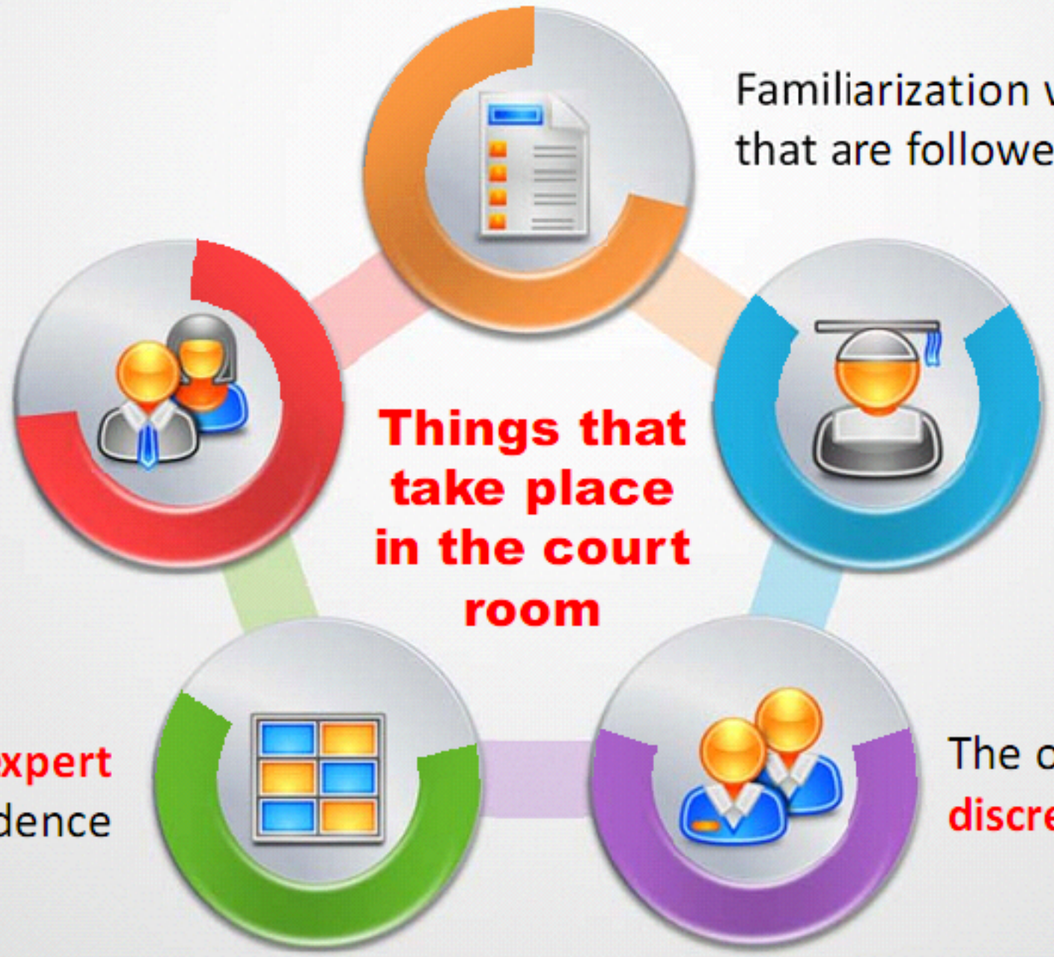
Role of an Expert Witness in Bringing Evidence to Court

- 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

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

Testifying in the Court Room

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



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

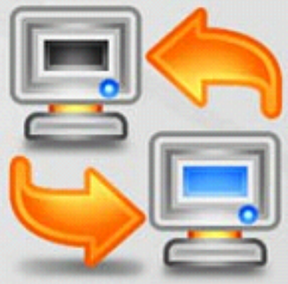
The attorney leads the **expert witness** through the evidence

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

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

Closing the Case

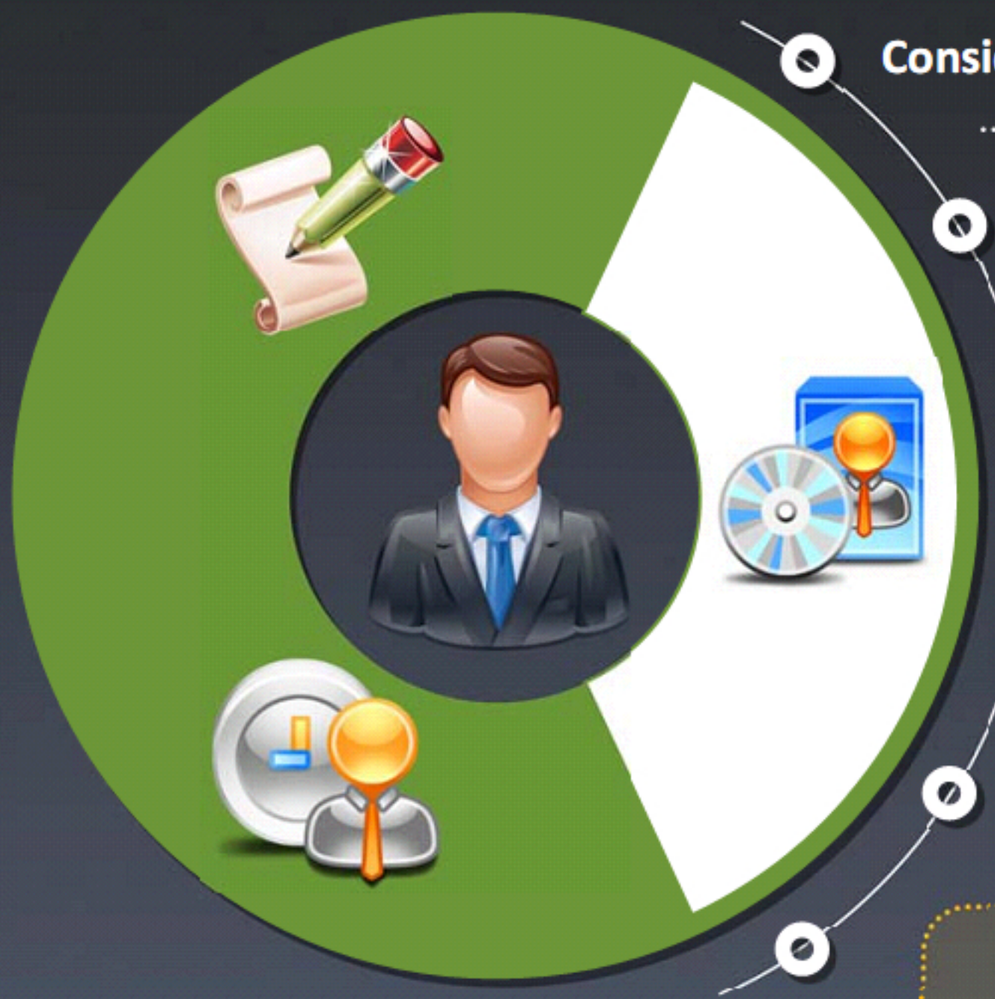
- Final report should **include everything the investigator did** during the course of the investigation, and what he or she found
- Basic **reports** should include: who, what, when, where, and how
- In a **good computing investigation**, the steps are repeatable and always produce the same results
- 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



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

Maintaining Professional Conduct

C|HFI Computer Hacking Forensic Investigator



- 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

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

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

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