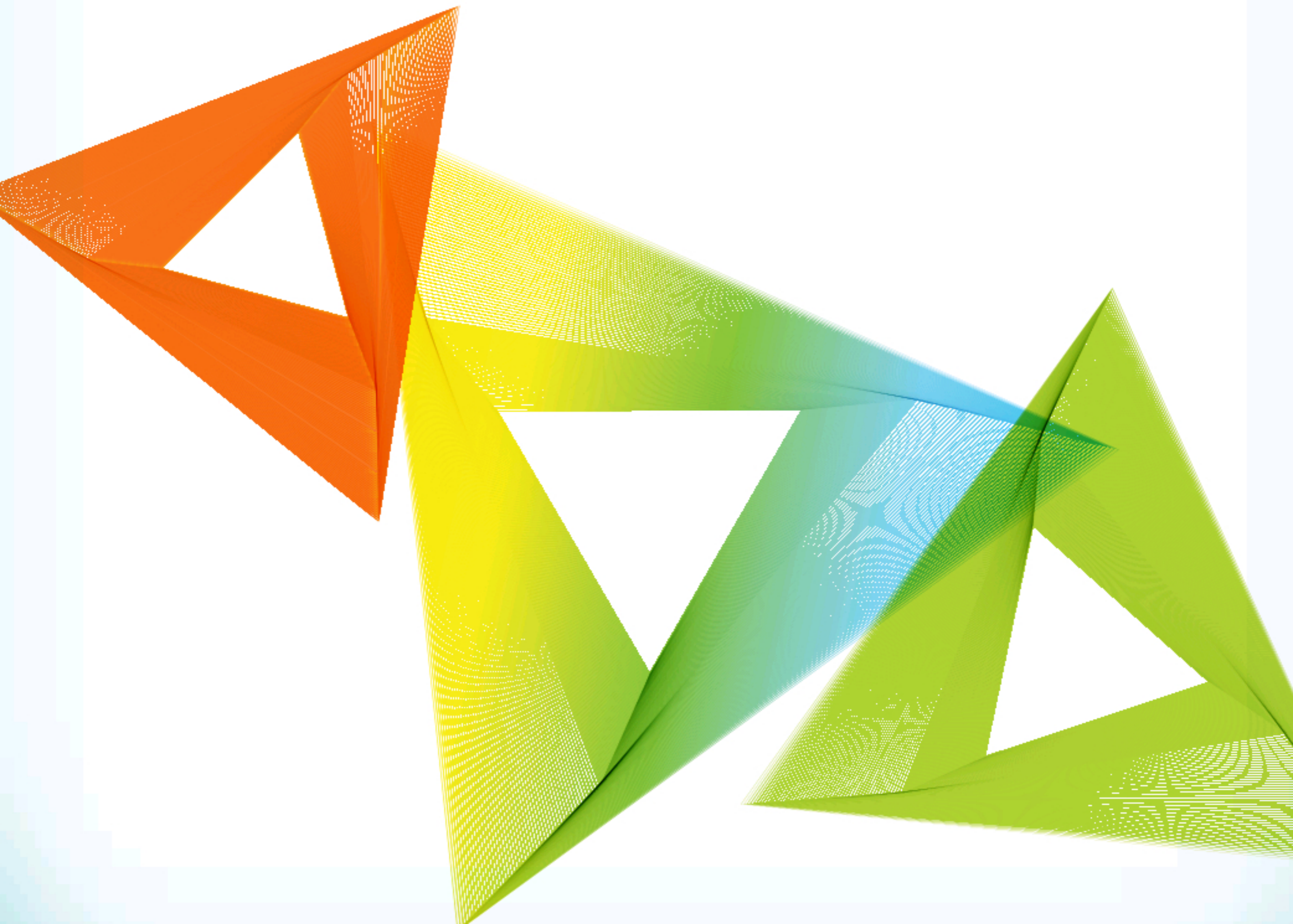


Data Acquisition and Duplication

Module 04






Computer Hacking Forensic Investigator v9

Module 04: Data Acquisition and Duplication

Exam 312-49

Module Objectives




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

- 1 Understand data acquisition and its importance
- 2 Understand live data acquisition
- 3 Understand static data acquisition
- 4 Review data acquisition and duplication steps
- 5 Choose the steps required to keep the device unaltered
- 6 Determine the best acquisition method and select appropriate data acquisition tool
- 7 Perform the data acquisition on Windows and Linux Machines
- 8 Summarize data acquisition best practices

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

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

Understanding Data Acquisition



- Data acquisition is the use of established methods to **extract the Electronically Stored Information (ESI)** from suspect computer or storage media to gain insight into a crime or an incident
- It is one of the **most critical steps of digital forensics** as improper acquisition may alter data in evidence media, and render it inadmissible in the court of law
- Investigators should be able to verify the accuracy of acquired data, and the complete **process should be auditable and acceptable to the court**

Types of Data Acquisition

Live Data Acquisition

Involves collecting **volatile information** that resides in registries, cache, and RAM

Static Data Acquisition

Acquisition of data that **remains unaltered** even if the system is powered off

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

Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value. With the progress of technology, the process of data acquisition has become more accurate, simple, and versatile. It uses many types of electronic equipment, ranging from small sensors to sophisticated computers. Following are the two categories of data acquisition:

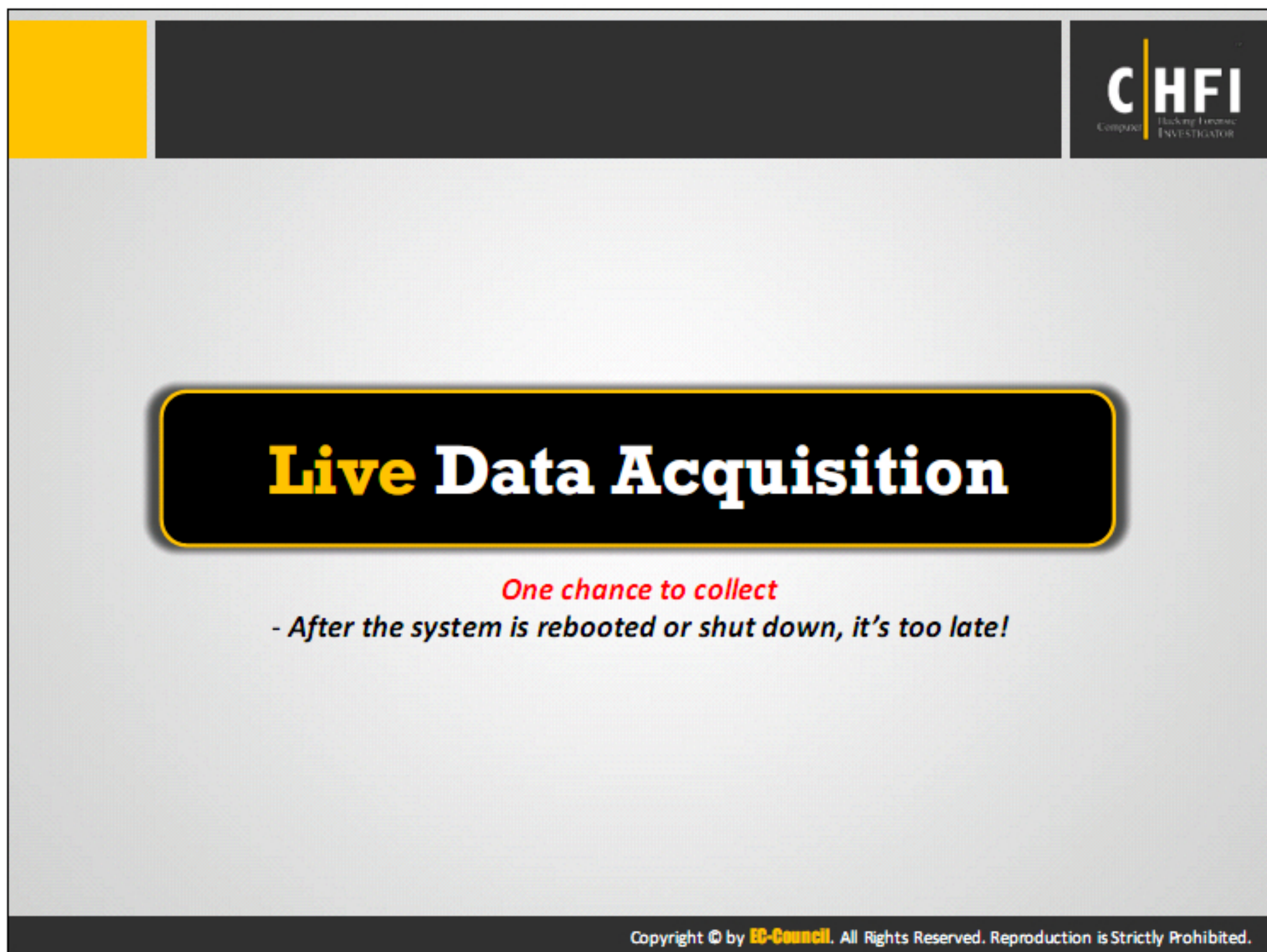
Live Data Acquisition

It is the process of acquiring volatile data from a working computer (either locked or in sleep condition) that is already powered on. Volatile data is fragile and lost when the system loses power or the user switches it off. Such data reside in registries, cache, and RAM. Since RAM and other volatile data are dynamic, a collection of this information should occur in real time.

Static Data Acquisition

It is the process of acquiring the non-volatile or unaltered data remains in the system even after shutdown. Investigators can recover such data from hard drives as well as from slack space, swap files, and unallocated drive space. Other sources of non-volatile data include CD-ROMs, USB thumb drives, smartphones, and PDAs.

The static acquisition is usually applicable for the computers the police had seized during the raid and include an encrypted drive.

A presentation slide with a grey background. At the top left is a yellow square. At the top right is a dark grey rectangle containing the 'CHFI' logo, which includes the text 'Computer Hacking Forensic Investigator'. In the center, a dark rounded rectangle contains the title 'Live Data Acquisition' in yellow and white. Below the title, the text 'One chance to collect' is in red, followed by '- After the system is rebooted or shut down, it's too late!' in black. At the bottom, a dark grey bar contains the copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'


CHFI
Computer Hacking Forensic Investigator

Live Data Acquisition

One chance to collect
- After the system is rebooted or shut down, it's too late!

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

Live Data Acquisition



- As RAM and other volatile data are **dynamic**, collection of this information should occur in real time
- Potential evidence may be lost or destroyed even** by simply looking through files on a running computer or by booting up the computer to “look around” or playing games on it
- In volatile data collection, **contamination is harder to control** because tools and commands may change file access dates and times, use shared libraries or DLLs, trigger the execution of malicious software (malware), or—in the worst case—**force a reboot** and lose all volatile data
- Volatile information assists in determining a logical timeline of the security incident, and the possible users responsible

Types of volatile data

System Information

- Collection of information about the current configuration and running state of the suspicious computer
- Volatile system information includes system profile (details about configuration), current system date and time, command history, current system uptime, running processes, open files, start up files, clipboard data, logged on users, and DLLs or shared libraries

Network Information

- Collection of information about the network state of the suspicious computer
- Volatile network information includes open connections and ports, routing information and configuration, and ARP cache

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

Live data acquisition is the process of extracting volatile information present in the registries, cache, and RAM of digital devices through its normal interface. The volatile information is dynamic in nature and changes with time, therefore, the investigators should collect the data in real time.

Simple actions such as looking through the files on a running computer or booting up the computer have the potential to destroy or modify the available evidence data, as it is not write-protected. Additionally, contamination is harder to control because the tools and commands may change file access dates and times, use shared libraries or DLLs, trigger the execution of malicious software (malware), or—worst case—force a reboot that results in losing of all volatile data. Therefore, the investigators must be very careful while performing the live acquisition process. Volatile information assists in determining a logical timeline of the security incident, network connections, command history, processes running, connected peripherals and devices, as well as the users, logged onto the system.

Depending on the source, there are the following two types of volatile data:

System Information


System information is the information related to a system that can act as evidence in a criminal or security incident. This information includes the current configuration and running state of the suspicious computer. Volatile system information includes system profile (details about configuration), login activity, current system date and time, command history, current system uptime, running processes, open files, startup files, clipboard data, logged on users, DLLs, or

shared libraries. The system information also includes critical data stored in slack spaces of hard disk drive.

Network Information

Network information is the network related information stored in the suspicious system and connected network devices. Volatile network information includes open connections and ports, routing information and configuration, ARP cache, shared files, services accessed, etc.

Order of Volatility



- When collecting evidence, the collection should proceed from the **most volatile to the least volatile**
- The list below is the order of volatility for a typical system:

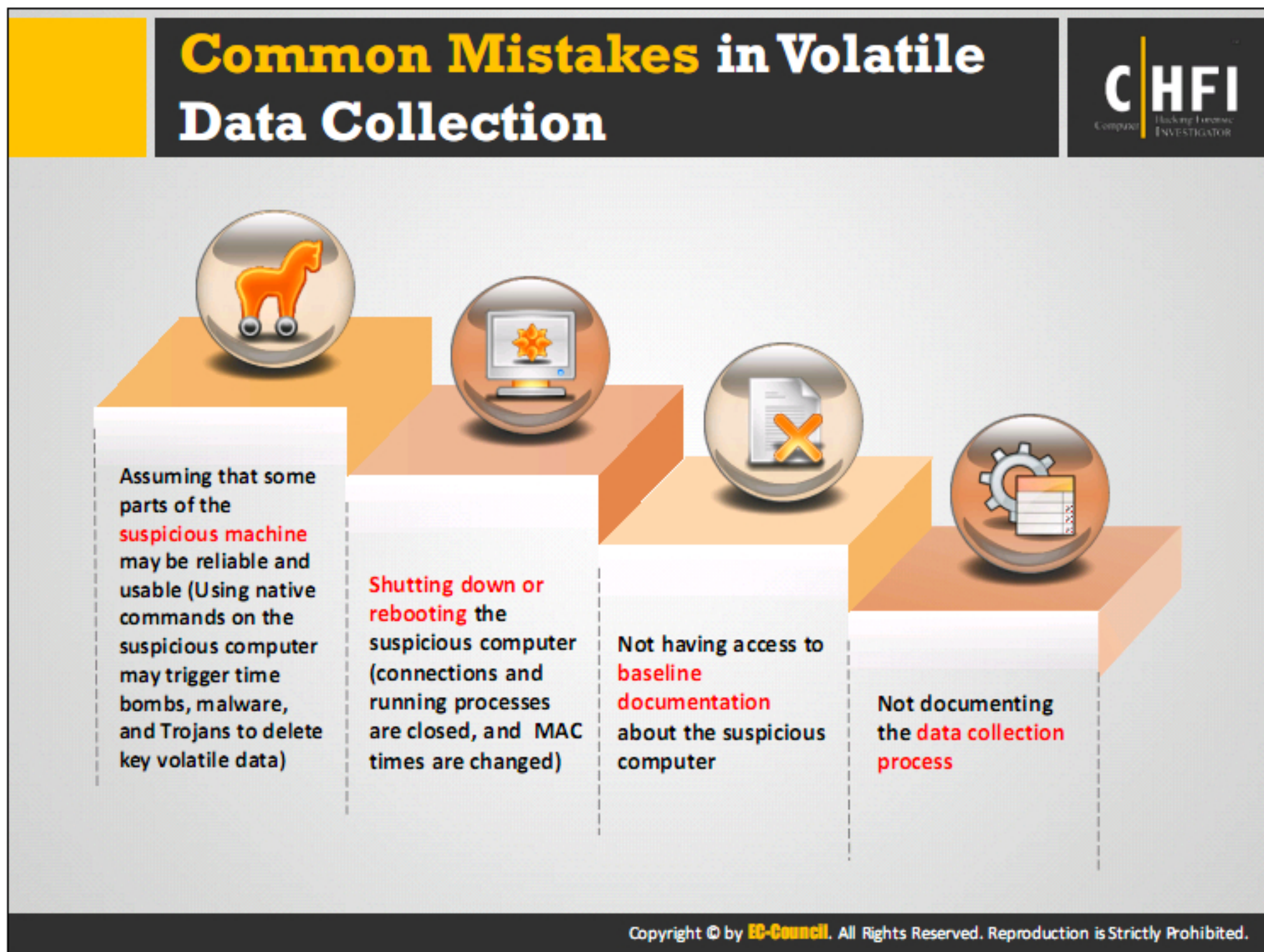
- 1 Registers, and cache
- 2 Routing table, process table, kernel statistics, and memory
- 3 Temporary file systems
- 4 Disk or other storage media
- 5 Remote logging and monitoring data that is relevant to the system in question
- 6 Physical configuration, and network topology
- 7 Archival media

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

Investigators should always remember that the entire data do not have the same level of volatility and collect the most volatile data at first, during live acquisitions. The order of volatility for a typical computer system is as follows:

- **Registers, cache:** The information in the registers or the processor cache on the computer exists around for a matter of nanoseconds. They are always changing and are the most volatile data.
- **Routing table, process table, kernel statistics, and memory:** A routing table, ARP cache, kernel statistics information is in the ordinary memory of the computer. These are a bit less volatile than the information in the registers, with the life span of ten nanoseconds.
- **Temporary file systems:** Temporary file systems tend to be present for a longer time on the computer compared to routing tables, ARP cache, etc. These systems are eventually over written or changed, sometimes in seconds or minutes later.
- **Disk or other storage media:** Anything stored on a disk stays for a while. However, sometimes, things could go wrong and erase or write over that data. Therefore, disk data are also volatile with a lifespan of some minutes.
- **Remote logging and monitoring data related to the target system:** The data that goes through a firewall generates logs in a router or in a switch. The system might store these logs somewhere else. The problem is that these logs can over write themselves, sometimes a day later, an hour later, or a week later. However, generally they are less volatile than a hard drive.

- **Physical configuration, network topology:** Physical configuration and network topology are less volatile and have more life span than some other logs.
- **Archival media:** A DVD-ROM, a CD-ROM or a tape can have the least volatile data because the digital information is not going to change in such data sources automatically any time unless damaged under a physical force.



The investigators should collect the volatile data carefully because any mistake would result in permanent data loss.



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

The step-by-step procedure of the volatile data collection methodology:

Step 1: Incident Response Preparation

Eliminating or anticipating every type of security incident or threat is not possible practically. However, to collect all kinds of volatile data, responders can be prepared to react to the security incident successfully.

The following should be ready before an incident occurs:

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

Step 2: Incident Documentation

Ensure to store the logs and profiles in organized and readable format. For e.g., use naming conventions for forensic tool output, record time stamps of log activities and include the identity of the forensic investigator. Document all the information about the security incident


needs and maintain a logbook to record all actions during the forensic collection. Using the first responder toolkit logbook helps to choose the best tools for the investigation.

Step 3: Policy Verification

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

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

Volatile Data Collection Methodology (Cont'd)



Step 4

Volatile Data Collection Strategy

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

Step 5

Volatile Data Collection Setup

- **Establish a trusted command shell**
Do not open, or use a command shell or terminal from the suspicious system. This minimizes the footprint on the suspicious system and restricts the triggering of any kinds of malware that have been installed on the system
- **Establish the transmission and storage method**
Identify and record how the data could be transmitted from the live suspicious computer to a remote data collection system as there will not be enough space on the response disk to collect forensics tools' output
EX: Netcat and Cryptcat that transmit data remotely via a network
- **Ensure the integrity of forensic tool output**
Compute an MD5 hash of forensics tools' output to ensure the integrity and admissibility

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

Step 4: Volatile Data Collection Strategy

Security incidents are not similar. The first responder toolkit logbook and the questions from the graphic to create the volatile data collection strategy that suits the situation and leaves a negligible amount of footprint on the suspicious system should be used.

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

Step 5: Volatile Data Collection Setup

- **Establish a trusted command shell:** Do not open or use a command shell or terminal of the suspicious system. This action minimizes the footprint on the suspicious system and stops any kind of malware to trigger on the system.
- **Establish the transmission and storage method:** Identify and record the data transmission process from the live suspicious computer to the remote data collection system, as there will not be enough space on the responsive disk to collect forensic tool output. For e.g., Netcat and Cryptcat can transmit data remotely via a network.
- **Ensure the integrity of forensic tool output:** Compute an MD5 hash of the forensic tool output to ensure the integrity and admissibility.

CHFI
Computer Hacking Forensic Investigator



- Do not shut down or restart a system under investigation until all relevant volatile data has been recorded
- Maintain a log of all actions performed on the running machine
- Photograph the screen of the running system to document its state
- Identify the operating system running on the suspect machine
- Note system date, time and command history, if shown on screen, and compare with the current actual time
- Check the system for the use of whole disk or file encryption
- Do not use the administrative utilities on the compromised system during an investigation, and be cautious particularly when running diagnostic utilities
- As you execute each forensics tool or command, generate the date and time to establish an **audit trail**
- Dump the RAM from the system to a forensically sterile removable storage device
- Collect other volatile operating system data and save to a removable storage device
- Determine evidence seizure method (of hardware and any additional artifacts on the hard drive that may be determined to be of evidentiary value)
- Complete a full report documenting all steps and actions taken


Step 6: Volatile Data Collection Process


- Record the time, date, and command history of the system
- To establish an audit trail generate dates and times while executing each forensic tool or command
- Start a command history to document all the forensic collection activities. Collect all possible volatile information from the system and network
- Do not shut down or restart a system under investigation until all relevant volatile data has been recorded
- Maintain a log of all actions conducted on a running machine
- Photograph the screen of the running system to document its state
- Identify the operating system (OS) running on the suspect machine
- Note system date, time and command history, if shown on screen, and record with the current actual time
- Check the system for the use of whole disk or file encryption
- Do not use the administrative utilities on the compromised system during an investigation, and particularly be cautious when running diagnostic utilities


- As each forensic tool or command is executed, generate the date and time to establish an audit trail
- Dump the RAM from the system to a forensically sterile removable storage device
- Collect other volatile OS data and save to a removable storage device
- Determine evidence seizure method (of hardware and any additional artifacts on the hard drive that may be determined to be of evidentiary value)
- Complete a full report documenting all steps and actions taken





Static Data Acquisition



- 

1 Static data acquisition is defined as acquiring data that remains **unaltered** when the system is **powered off** or **shutdown**
- 

2 This type of data is termed as **non-volatile** and is usually recovered from hard drives. It can also exist in slack space, swap files and, unallocated drive space
- 

3 Other sources of non-volatile data include **DVD-ROMs**, **USB drives**, **flash cards**, **smart phones**, and **external hard drives**
- 

4 **Examples of static data**: emails, word processing documents, Web activity, spreadsheets, slack space, swap files, unallocated drive space, and various deleted files


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

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

Static data recovered from a hard drive includes:

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

Rules of Thumb



- **Do not work on original digital evidence.** Work on the bit-stream image of a suspicious drive/file to view the static data
- Produce two copies of the original media
 - The first is the **working copy** to be used for analysis
 - The second is the **library/control copy** that is stored for **disclosure** purposes or in the event that the working copy gets corrupt
- If performing a drive-to-drive imaging, use **clean media** to copy to **shrink-wrapped new drives**
- Once duplication of original media is done, verify the **integrity of copies** to the original

The better the quality of evidence, the better the analysis and likelihood of solving the crime

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

Rule of thumb refers to the best practice of a process that helps to ensure a favorable outcome on application. In the case of a digital forensics investigation, “The better the quality of evidence, the better the analysis and likelihood of solving the crime.”


Never perform a forensic investigation or any other process on the original evidence or source of evidence as it may alter the data and leave the evidence ineligible in the court of law. Instead, create a duplicate bit-stream image of a suspicious drive/file to view the static data and work on it. This practice will not only preserve the original evidence, but also provide a chance to recreate a duplicate if something goes wrong.

Always produce two copies of the original media before starting the investigation process for the following purposes:

- One copy is the working copy, for analysis
- One copy is the library/control copy stored for disclosure purposes or in the event that the working copy gets corrupted



If the investigators need to perform a drive-to-drive imaging, use blank media to copy to shrink wrapped new drives. After duplicating the original media, verify the integrity of copies to the original using hash values such as MD5.

Why Create a Duplicate Image?



- The computer/media is a **crime scene** and it should be protected to ensure that the evidence is not **contaminated**
- Duplicate image allows the following:

- Preserves the **original evidence**
- Prevents **inadvertent alteration** of original evidence during examination
- Allows recreation of the **duplicate image** if necessary
- Evidence can be duplicated with no **degradation** from copy to copy




Duplicating

Original Hard Disk

Duplicate Hard Disk


Only One Chance to Do it Right



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


Digital data are more susceptible to loss, damage, and corruption unless the investigators preserve and handle it properly. Prior to examination, the investigators should forensically image or duplicate the electronic device data and keep two or more copies. Forensic investigators should use only the image data for their investigation.

Bit Stream Image Vs. Backups




Bit Stream Image

- Bit stream image (also referred to as mirror image/evidence-grade backups) involves a **bit-by-bit copy** of a physical hard drive or any other storage media
- It **exactly duplicates** all sectors on a given storage device
- This includes **hidden and residual data** (slack, space, swap, unused space, residue, and deleted files)
- Bit stream programs rely **on cyclic redundancy check (CRC) computations** in the validation process



Backups

- Most operating systems pay attention only to the **live file system structure**
- Slack, residue, deleted files, etc., are not **indexed**
- Backups usually do not capture this data, and modify the **timestamps** of data, contaminating the timeline



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

Bit-Stream Image

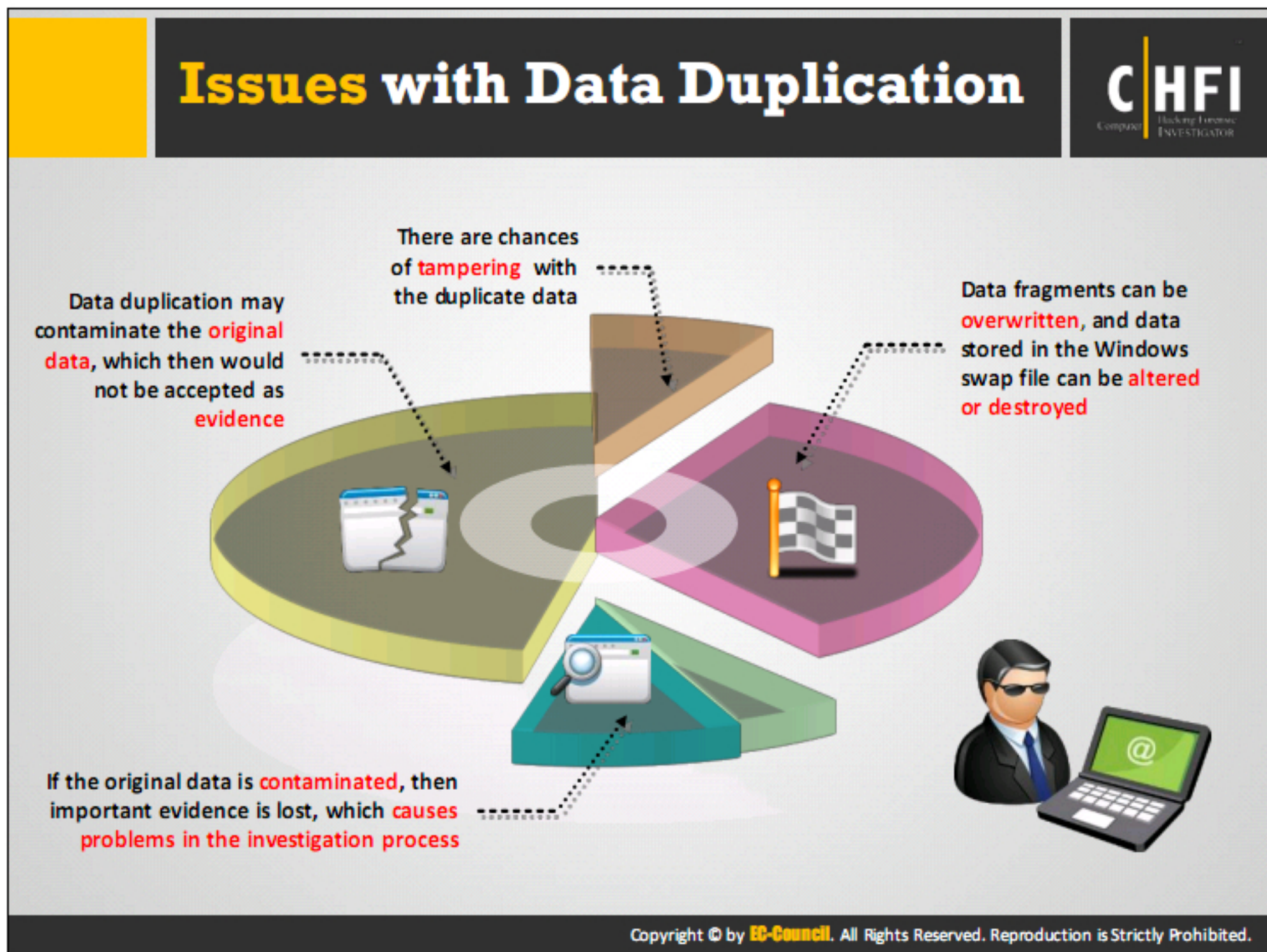
Bit-stream imaging, also known as mirror images and evidence grade backups, is the process of creating a duplicate of a hard disk through bit-by-bit copying of its data onto another storage media. The process copies all the sectors of a target drive, including the hidden and residual data, such as slack space, unused space, residue, swap files, deleted files, etc. Bit-stream programs depend on CRC computations in the validation process.

This type of imaging requires more space and takes more time for completion.

Backups

Backup refers to the process of copying and archiving of system data, which can help to restore the system to its previous state in case of a breakdown, security incident or data loss. Backups do not capture the same or complete disk data; instead, they include OS data such as the live file system structure. This type of data duplication does not contain slack space, deleted files, residue, etc.

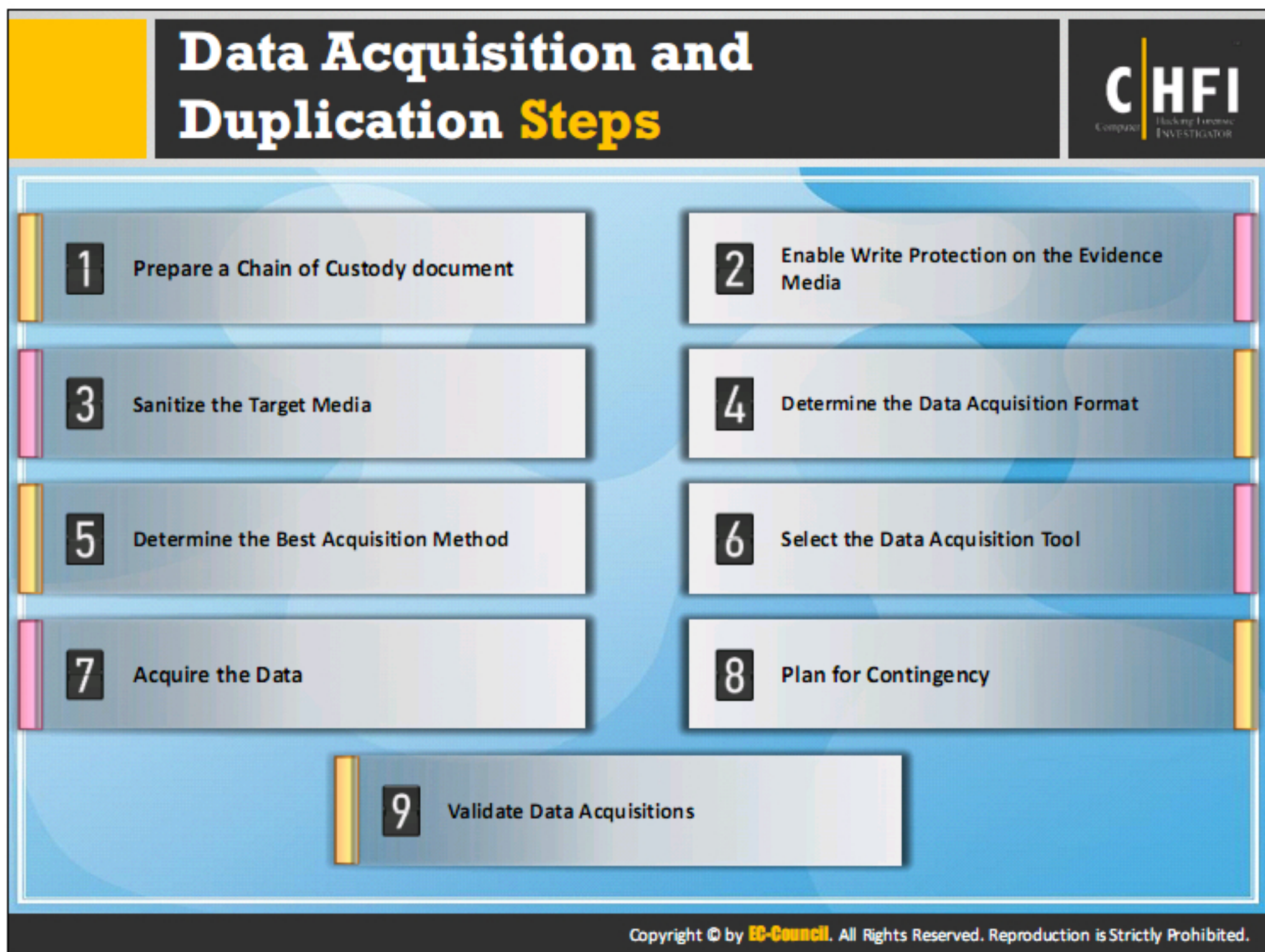
This process often modifies the timestamps and other features, thus contaminating the timeline.



Data Duplication is the process of creating a copy of data that is a replica of the original source. The various issues associated with data duplication are:

- Data duplication process can sometimes overwrite the data fragments and damage its integrity
- The process can alter the data stored in the Windows swap file, which temporarily stores the information a RAM does not use
- During the data duplication, the device used to copy can also write the data to the original evidence source and destroy its authenticity, leaving it unacceptable in the court of law
- In case of contamination of the original data, the critical evidence is lost, which causes problems in the investigation process

There are chances of tampering with the duplicate data as well




Data acquisition is the first pro-active step in the forensic investigation process. The aim of forensic data acquisition is to make a forensic copy of data, which can act as evidence in the court.


Forensic data duplication refers to the creation of a file that has every bit of information from the source in a raw bit-stream format. Steps to follow in the process of data acquisition and data duplication are:

- Prepare a chain of custody document and make a note of all the actions performed over the evidence source and data, along with the names of investigators performing the task, the time and date, and the result
- Enable write protection on the evidence media as most of the devices have two-way communication enabled and can alter the data in source of evidence
- Sanitize the target media, which is going to hold a copy of the evidence data
- Determine the data acquisition format before starting the process and see that the copy remains in the same format as the original data
- Analyze the requirements and select the best acquisition method
- Select the appropriate data acquisition tool, which can serve all the actions required while ensuring safety of the data
- Acquire the complete data along with hidden and encrypted spaces


- Have contingency plans in case of an incident
- After completion of duplication, validate data acquisitions to check the integrity and completeness of the data

Prepare a Chain of Custody Document






- Prepare chain of custody document to **track** and ensure the **integrity** of collected evidence
- The chain of custody document, at the minimum, should have the following information:
 - 🕒 Description of the evidence
 - 🕒 Time of collection
 - 📍 Location from where it was collected
 - 👤 Details of the people who handled it
 - 📝 Reason for the person to handle it



Evidence Collection Form

Description:			
Manufacturer:	Model#:	Serial #:	
Chain of Custody			
Date/Time:	From:	To:	Reason:
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	
Date:	Name/Organization:	Name/Organization:	
Time:	Signature:	Signature:	



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

A chain of custody is a written record consisting of all the processes involved in the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. It also includes the details of people, time, and purpose involved in the investigation and evidence maintenance processes.

Chain of custody documents, track collected information and preserve the integrity of the collected evidence. It should contain details of every action performed during the process and the result. The forensic investigators are always responsible for the protection of the chain of custody document.

Enable Write Protection on the Evidence Media



- According to the National Institute of Justice, write protection should be initiated, if available, to **preserve and protect original evidence**
- The examiner should consider creating a **known value for the subject evidence** prior to acquiring the evidence (for example, performing independent CRC or using hash functions such as MD5, SHA1 and SHA2)
- Write blocker is a hardware device or software application that allows data acquisition from the storage media without altering its contents
- It blocks write commands, thus allowing read-only access to the storage media
 - ⊖ If hardware write blocker is used:
 - ⊕ Install a write blocker device
 - ⊕ Boot the system with the examiner's controlled operating system
 - ⊕ Examples of hardware devices: CRU® WiebeTech® USB WriteBlocker™, Tableau Forensic Bridges, etc.
 - ⊖ If software write blocker is used:
 - ⊕ Boot the system with the examiner's controlled operating system
 - ⊕ Activate write protection
 - ⊕ Examples of software applications: SAFE Block, MacForensicsLab Write Controller, etc.

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

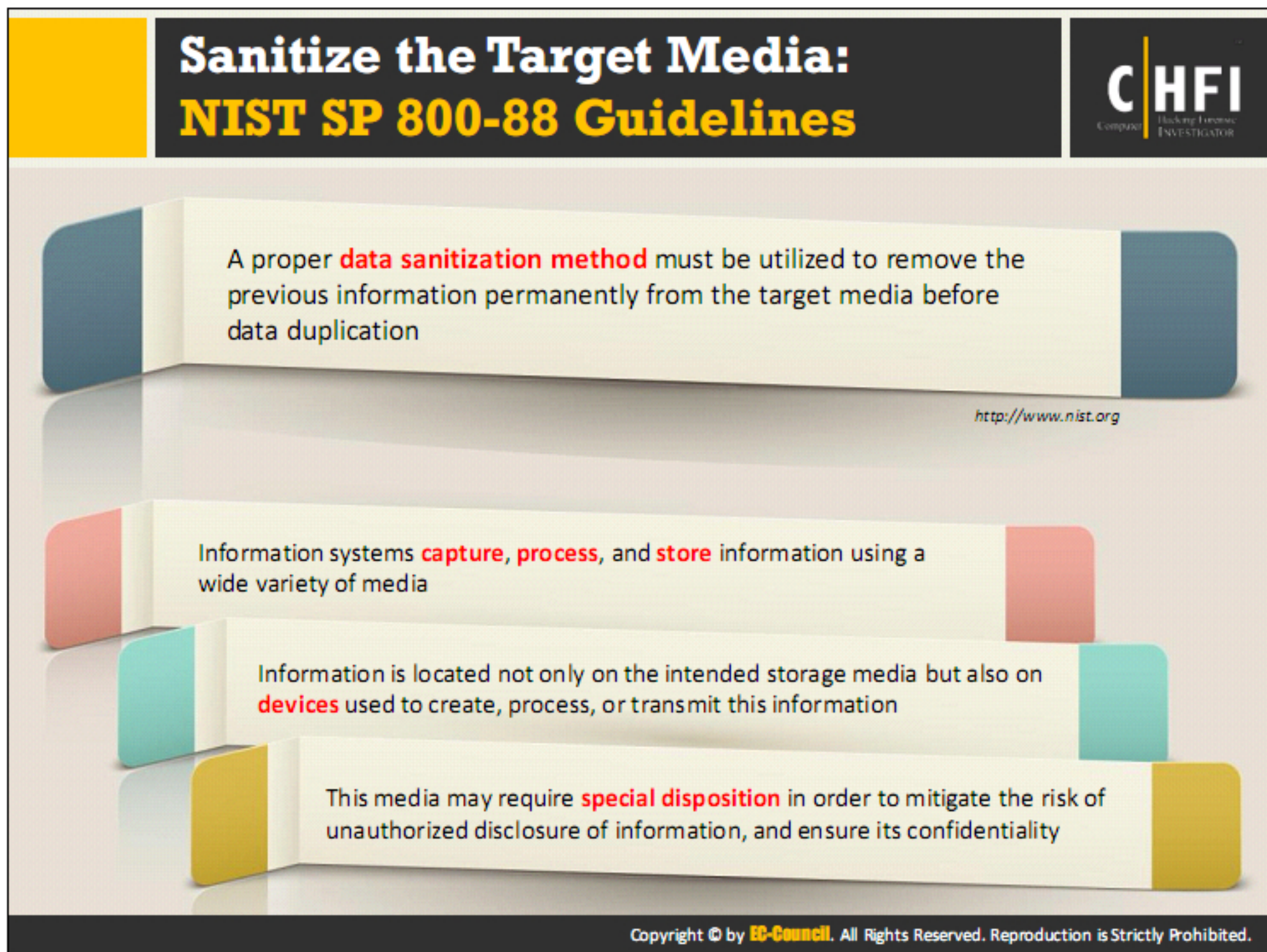
Write protection is the ability of a hardware device or a software program to restrict itself from writing any new data to a computer or modifying the data on it. Enabling write protection allows reading the data, but not writing or modifying.

Forensic investigators should be confident about the integrity of the evidence they obtain during the acquisition, analysis, and management. The evidence should be legitimate to convince the authorities of the court.

The investigator needs to implement a set of procedures to prevent the execution of any program that can alter the disk contents. The procedures that would offer a defense mechanism against any alterations include:

- Set a hardware jumper to make the disk read only
- Use operating system and software which cannot write to the disk unless instructed
- Employ a hard disk write block tool to protect against disk writes

Hardware and software write blocker tools provide read-only access to the hard disks and other storage devices without compromising their security. The main differences arise during installation and usage process.



Media sanitization is the process of permanently deleting or destroying data from storage media. The proposed NIST SP 800-88 guidance explains three sanitization methods:

- **Clear:** Logical techniques applied to sanitize data in all storage areas using the standard read and write commands.
- **Purge:** Involves physical or logical techniques to make the target data recovery infeasible by using state-of-the-art laboratory techniques.
- **Destroy:** Enables target data recovery to be infeasible with the use of state-of-the-art laboratory techniques, which result in an inability to use the media for data storage.


The National Institute of Standards and Technology has issued a set of guidelines to help organizations sanitize data to preserve the confidentiality of the information. They are:

- The application of complex access controls and encryption can reduce the chances for an attacker to gain direct access to sensitive information
- An organization can dispose of the not so useful media data by internal or external transfer or by recycling to fulfill data sanitization
- Effective sanitization techniques and tracking of storage media are crucial to ensure protection of sensitive data by organizations against attackers
- All organizations and intermediaries are responsible for effective information management and data sanitization

Physical destruction of media involves techniques, such as cross-cut shredding. Departments can destroy media on-site or through a third party that meets confidentiality standards.

Investigators must consider the type of target media they are using for copying or duplicating the data and select an appropriate sanitization method to ensure that no part of previous data remains on the target media that will store the evidence files. The previous media may alter the properties or changes the data and its structure.

Determine the Data Acquisition Format



There are three data acquisition formats

Raw Format

Proprietary Format

Advanced Forensics Format (AFF)

To preserve digital evidence, vendors and some OS utilities are allowed to write bit-stream data to files. This copy technique creates simple sequential flat files of a data set or suspect drive. The output of these flat files is referred to as raw format.

Advantages	Disadvantages
<ul style="list-style-type: none">Fast data transfersCan ignore minor data read errors on source driveMost computer forensics tools can read raw format	<ul style="list-style-type: none">Requires as much storage as original disk or data setTools (mostly freeware versions) might not collect marginal (bad) sectors on the source drive

Freeware tools have a low threshold of retry reads on weak media spots on a drive, whereas commercial acquisition tools have a higher threshold to make sure all data is collected.

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

The data collected by forensic tools is stored in image files. There are three formats available for these data storage image files. They are:

Raw Format

Previously, a bit-by-bit copy of data from one disk to another was the only option to copy data to preserve and examine the evidence. Therefore, to achieve evidence preservation vendors and some OS utilities allowed writing bit-stream data to files. This copy technique allowed the creation of simple, sequential, flat files of a data set or suspect drive. Raw format is the output of these flat files.

Advantages:

- Data transferring is fast
- Can ignore minor data read errors on the source drive
- A Universal acquisition format that most of the forensic tools can read

Disadvantages:

- Takes same storage space as that of original disk or data set
- Some tools like freeware versions may not collect bad sectors on the source drive

In freeware tools, there is a low threshold of retry reads on weak media spots on a drive than commercial acquisition tools, which have a higher threshold to ensure the collection of entire data.


Determine the Data Acquisition Format (Cont'd)

Raw Format

Proprietary Format

Advanced Forensics Format (AFF)

Commercial forensics tools have their own formats to collect digital evidence. Proprietary formats usually offer features that counterpart vendors' analysis tools such as:

<ul style="list-style-type: none">Option to compress or not compress image files of a source drive to save space on the target driveAbility to split an image into smaller segmented files to archive, such as to CDs or DVDs with data integrity checks integrated into each segmentAbility to integrate metadata into the image file such as date and time of acquisition, hash value of the suspect drive, investigator name, comments, case details, etc.	<p>Disadvantages include:</p> <ul style="list-style-type: none">Inability to share images between different computer forensics analysis toolsFile size limitation for each segmented volume <div></div>
---	---

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

Proprietary Format

Raw format and advanced forensics format are open source formats, and these are the only proprietary format. These formats can change from one vendor to another according to the features they offer. This means that there are a number of proprietary formats available.

Features:

- Saves space on the target drive and allows to compress or not compress image files of a suspect drive
- Allows splitting an image into smaller segmented files and store them on CDs or DVDs
- Ensures data integrity by applying data integrity checks on each segment while splitting
- It can integrate metadata into image file by adding metadata such as date and time of the acquisition, examiner or investigator name, the hash value of the original medium or disk and case details or comments

Disadvantages:

- Sharing of an image between different computer forensics tools is not possible (example, ILook Investigator and IXimager produce three proprietary formats—IDIF, IRBF, and IEIF—that can be read only by ILook)
- Each segmented volume has file size limitation

Determine the Data Acquisition Format (Cont'd)

Raw Format

Proprietary Format

Advanced Forensics Format (AFF)

Advanced Forensics Format is an open source acquisition format with the following design goals

<ul style="list-style-type: none">No size restriction for disk-to-image filesGenerates compressed or uncompressed image filesProvides space for metadata in image files or segmented files	<ul style="list-style-type: none">Simple design with extensibilityOpen source for multiple computing platforms and OSsDeals internal consistency checks for self-authentication
--	---

File extensions include **.afm** for AFF metadata and **.afd** for segmented image files


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

Advanced Forensics Format (AFF)

AFF is an open source data acquisition format that stores disk images and related metadata. The aim was to make a disk imaging format that could not lock users into a proprietary format. The AFF File extensions are .afm for AFF metadata and .afd for segmented image files. There are no AFF implementation restrictions on forensic investigators, as it is an open source format, but it can limit its analysis.


AFF supports two compression algorithms: 1) zlib, faster but less efficient and 2) LZMA, slower but more efficient. The actual AFF is a single file which has segments with drive data and metadata. AFF file contents can be compressed and uncompressed. AFFv3 supports AFF, AFD, and AFM file extensions.

Determine the Data Acquisition Format (Cont'd)



Advanced Forensic Framework 4 (AFF4):

- Redesign and revision of AFF to manage and **use large amounts of disk images**, reducing both acquisition time and storage requirements
- Named as **object-oriented framework** by its creators (Michael Cohen, Simson Garfinkel, and Bradley Schatz)
- Basic types of AFF4 objects: **volumes**, **streams**, and **graphs**. They are universally referenced through a unique URL
- Abstract information model that **allows storage of disk-image data** in one or more places while the information about the data is stored elsewhere
- Stores more kinds of organized information in the **evidence file**
- Offers **Unified data model** and naming scheme



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

Advanced Forensic Framework 4 (AFF4)

Michael Cohen, Simson Garfinkel, and Bradley Schatz created the Advanced Forensic Framework 4 (AFF4) as a redesigned and revamped version of AFF format. The creators named it object oriented as it contained some generic objects with externally accessible behavior. Designed to support storage media with huge capacities AFF4 universe allows addressing of the objects by their name.

The format can support a vast number of images; offer a selection of binary container formats like Zip, Zip64, and simple directories through this format. It also supports storage from network and use of WebDAV used for imaging directly to a central HTTP server. This format supports maps that are zero copy transformations of data, e.g., without storing a new copy of a carved file we only store a map of the blocks allocated to this file. AFF4 supports image signing and cryptography. This format also offers image transparency to clients.

The AFF4 design adopts a scheme of globally unique identifiers for identifying and referring to all evidence. Basic AFF4 object types include:

- **Volumes:** They store segments, which are indivisible blocks of data
- **Streams:** These data objects can help in reading or writing. For, e.g., segments, images, maps.
- **Graphs:** Collections of RDF statements

Determine the Data Acquisition Format (Cont'd)

CHFI
Computer Hacking Forensic Investigator

Generic Forensic Zip (gfzip):
gfzip file format is usable for the **compressed yet randomly accessible storage** of disk image data for computer forensics purposes

Features

- User supplied metadata is embedded in a metadata partition within the file
- Data and metadata partitions are signed using x509 certificates
- Bound signatures (file segment signatures are bound together, thus making metadata falsification impossible)
- Multi level SHA256 digest based integrity guards
- Compressed or uncompressed storage of disk-image data
- Support for packed storage
- Support to set flags for sections of disk-image data
- Support for encryption
- Support for storage of packed data in several archive files
- Support for the experimental data-reduction on acquire (ROA) packed storage

<http://gfzip.nongnu.org>

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

Generic Forensic Zip (gfzip)


Gfzip provides an open file format for compressed, forensically complete, and signed disk image data files. It is a set of tools and libraries that can help in creating and accessing randomly accessible zip files. It uses multi-level SHA256 digests to safeguard the files. It also embeds the user's metadata within the file metadata. This file format focuses on signed data and metadata sections using x509 certificates.

The Gfzip file format is suitable for compressed and non-sequential accessible storage of disk image data for computer forensic purposes.

Features:


- Uncompressed disk images are similar to the dd images.
- Non-sequential seek/read methods are used for read access to compressed disk image data.
- Flags can be set for disk image data sections. For e.g., to mark bad sections.

Data Acquisition Methods




Bit-stream disk-to-image file

- It is the most common method used by **forensic investigators**
- With this method, one or many copies of the suspect **drive** can be generated
- The copies are bit-for-bit replications of the **original drive**
- Tools such as ProDiscover, EnCase, FTK, The Sleuth Kit, X-Ways Forensics, etc. can be used to read the most common types of **disk-to-image files** generated



Bit-stream disk-to-disk

- Because of **software or hardware errors or incompatibilities**, it is sometimes not possible to create a bit-stream disk-to-image file
- To solve the problem, create a **disk-to-disk bit stream** copy of the suspect drive using tools such as EnCase and Symantec Ghost Solution Suite
- These programs can alter the **target disk's geometry** (its head, cylinder, and track configuration) such that the copied data matches the original suspect drive



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

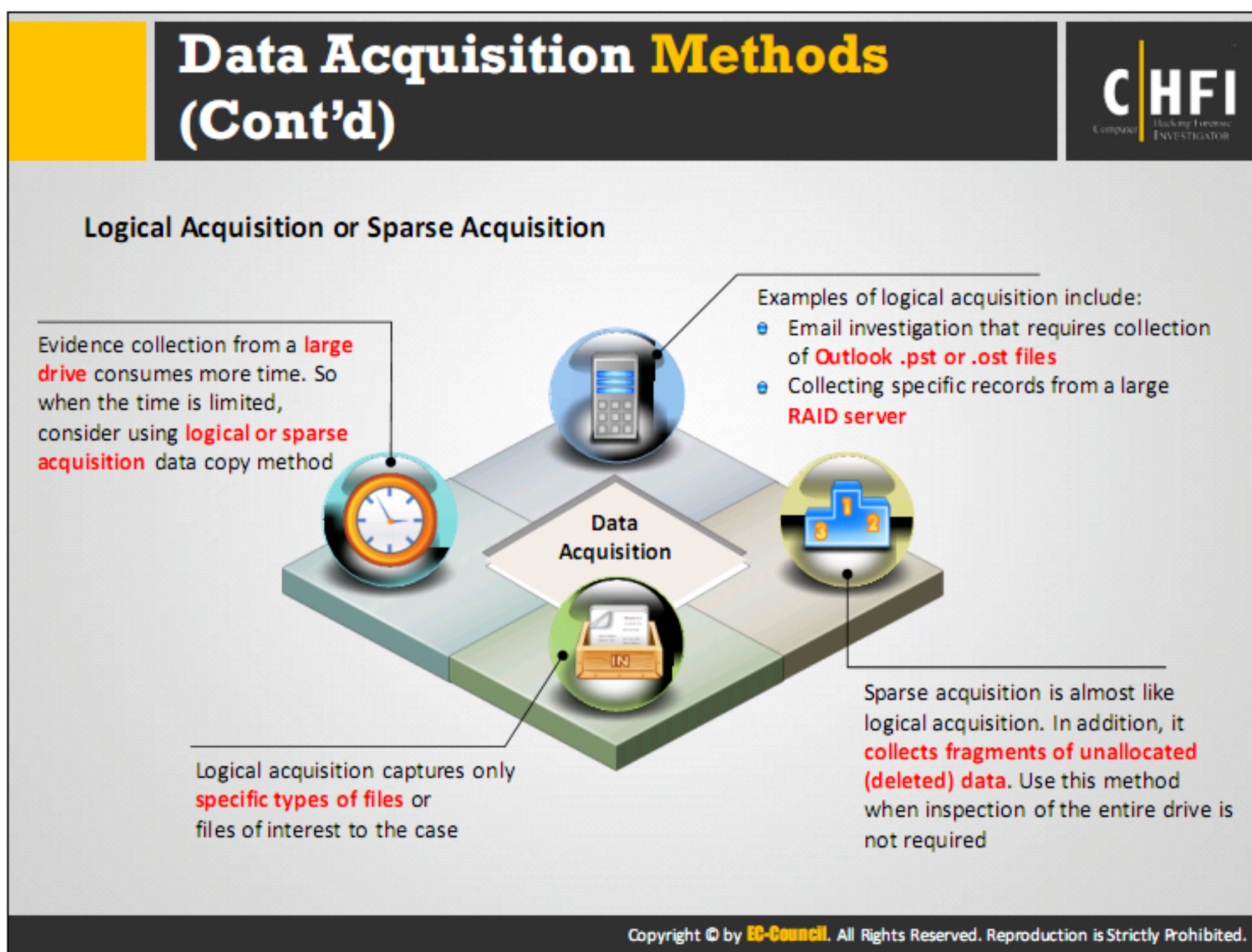
There are following four methods available for data acquisition:

Bit-stream disk-to-image file

Forensic investigators commonly use this data acquisition method. It is a flexible method, which allows creation of one or more copies, or bit-for-bit replications of the suspect drive. ProDiscover, EnCase, FTK, The Sleuth Kit, X-Ways Forensics, ILook Investigator, etc. are the popular tools used to read the disk-to-image files.

Bit-stream disk-to-disk

Sometimes it is not possible to create a bit-stream disk-to-image file due to software or hardware errors or incompatibilities. Investigators face such issues while trying to acquire data from older drives and create a bit-stream disk-to-disk copy of the original disk or drive. Tools like EnCase, SafeBack, and Norton Ghost can help create disk-to-disk bit-stream copy of the suspect drive. These tools can modify the target disk's geometry (its head, cylinder, and track configuration) to match the data copied from original suspect drive.



The other two methods of data acquisition are logical and sparse acquisition. Gathering evidence from large drives is time consuming, therefore investigators use logical or sparse acquisition data copy methods when there is a time limit.

Logical Acquisition


Logical acquisition gathers only the files required for the case investigation. E.g.:

- Collection of Outlook .pst or .ost files in email investigations
- Specific record collection from a large RAID server

Sparse Acquisition

Sparse acquisition is similar to logical acquisition. Through this method, investigators can collect fragments of unallocated (deleted) data. This method is very useful when it is not necessary to inspect the entire drive.

Determine the Best Acquisition Method



To determine the best acquisition method to use for investigation, consider the following when making a copy of a suspect drive:

1

Size of the source disk



- Whether you can **retain** the source disk as evidence or must return it to the owner, how much time does it take to perform **acquisition**, and location of the evidence?
- Ensure that the target disk can store a **disk-to-image file** if the source disk is very large
- If the **target disk** is not of comparable size, choose an alternative method to reduce data size
- Methods to reduce data size include:
 - Using disk compression tools which exclude **slack disk space** between files
 - Using compression methods that use an **algorithm** to reduce file size
 - Using **archiving tools** such as PKZip, WinZip, and WinRAR to compress
 - Using an algorithm referred to as **lossless compression**
 - Test lossless compression by performing **MD5 or SHA-2 or SHA-3 hash** on a file before and after compression
 - If the **hash value** matches, it means lossless compression is successful, or else it was corrupt

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

While creating a copy of the suspect drive, consider the following to determine the best acquisition method for the investigation process:

1. Size of the source disk:

- Know if you can retain the source disk as evidence or return it to the owner
- Calculate the time taken to perform acquisition and the evidence location
- Make sure that the target disk stores a disk-to-image file if the source disk is very large
- Choose an alternative method to reduce the data size if the target disk is not of comparable size

Methods to reduce data size are:

- Use Microsoft disk compression tools like DriveSpace and DoubleSpace which exclude slack disk space between the files
- Use the algorithms to reduce the file size
- Archiving tools like PKZip, WinZip, and WinRAR can help to compress
- Lossless compression algorithm can also be useful:
 - Perform an MD5 or SHA-1 hash on a file before and after compressing it, in order to test the lossless compression

The compression is successful only if the hash value matches.

Determine the Best Acquisition Method (Cont'd)



2 Whether you can retain the disk

- If the **original evidence drive** cannot be retained because it must be returned to the owner, as in the case of a discovery demand for a civil litigation case, check with the requester, meaning the lawyer or supervisor, to determine whether logical acquisition is acceptable
- If not, ensure that you make a good copy when performing acquisition, as most **discovery demands** provide only one chance to capture the data
- In addition, use a **reliable forensics tool** that you are familiar with



Investigator

3 When the drive is very large

- If the **suspect drive** is very large, use tape backup systems such as Super Digital Linear Tape (SDLT) or Digital Audio Tape/ Digital Data Storage (DAT/DDS)
- SnapBack possesses special **software drivers** to write data from a suspect drive to a tape backup system through standard PCI SCSI cards
- Advantage of this type of **acquisition** is there is no limit to the data size that can be acquired
- Disadvantage is it can be a slow and **time-consuming process**



System

Investigator acquiring data from disk/drive

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

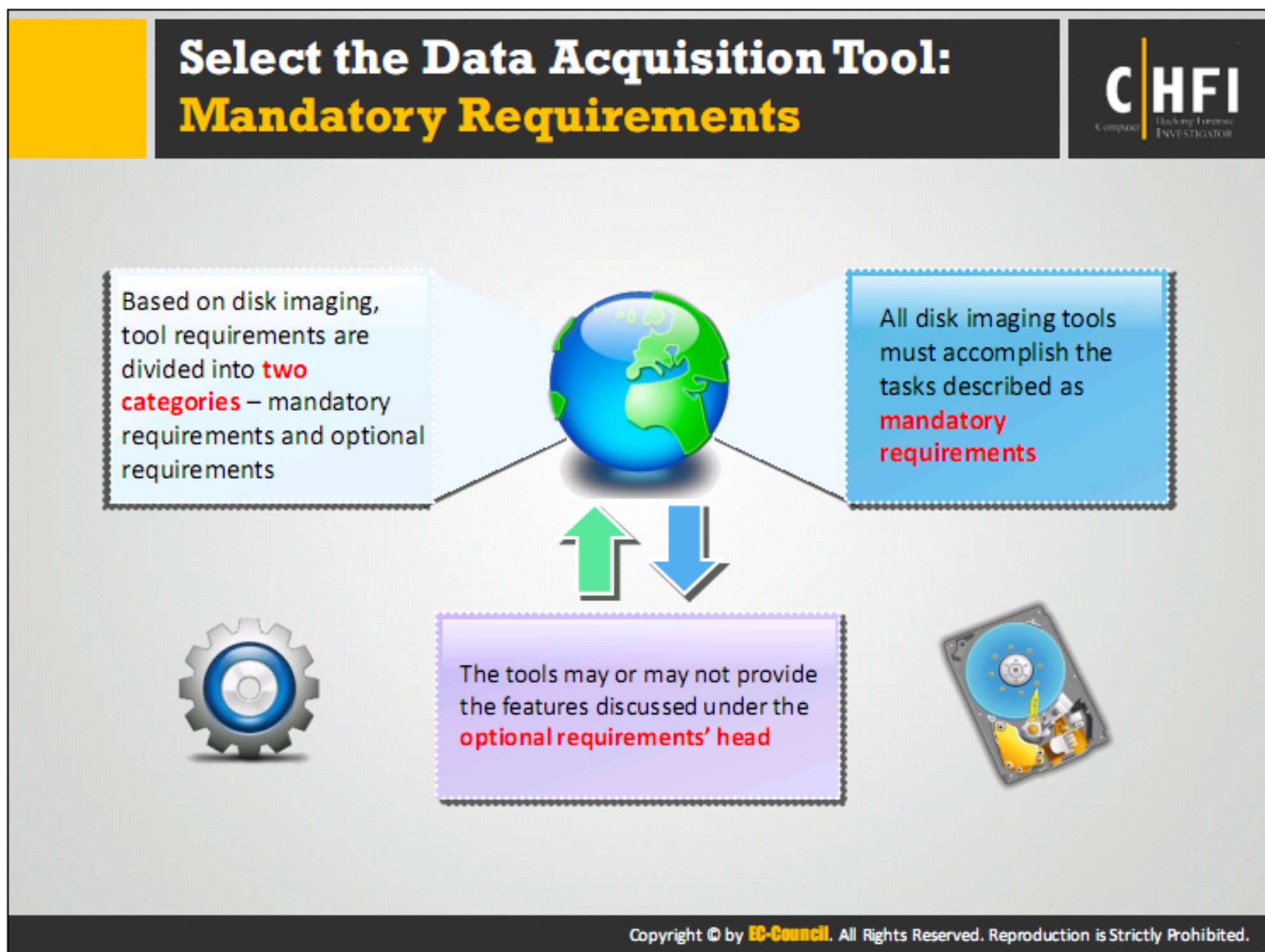
While creating a copy of the suspect drive, consider the following to determine the best acquisition method for the investigation process:

2. Whether you can retain the disk

- If the investigator cannot retrieve the original drive, as in a discovery demand for a civil litigation case, check with the requester, like a lawyer or supervisor if the court accepts logical acquisition
- If investigators can retain the drive, ensure to take a proper copy of it during acquisition, as most discovery demands give only one chance to capture the data
- Additionally, the investigators should maintain a familiar, reliable forensics tool

3. When the drive is very large

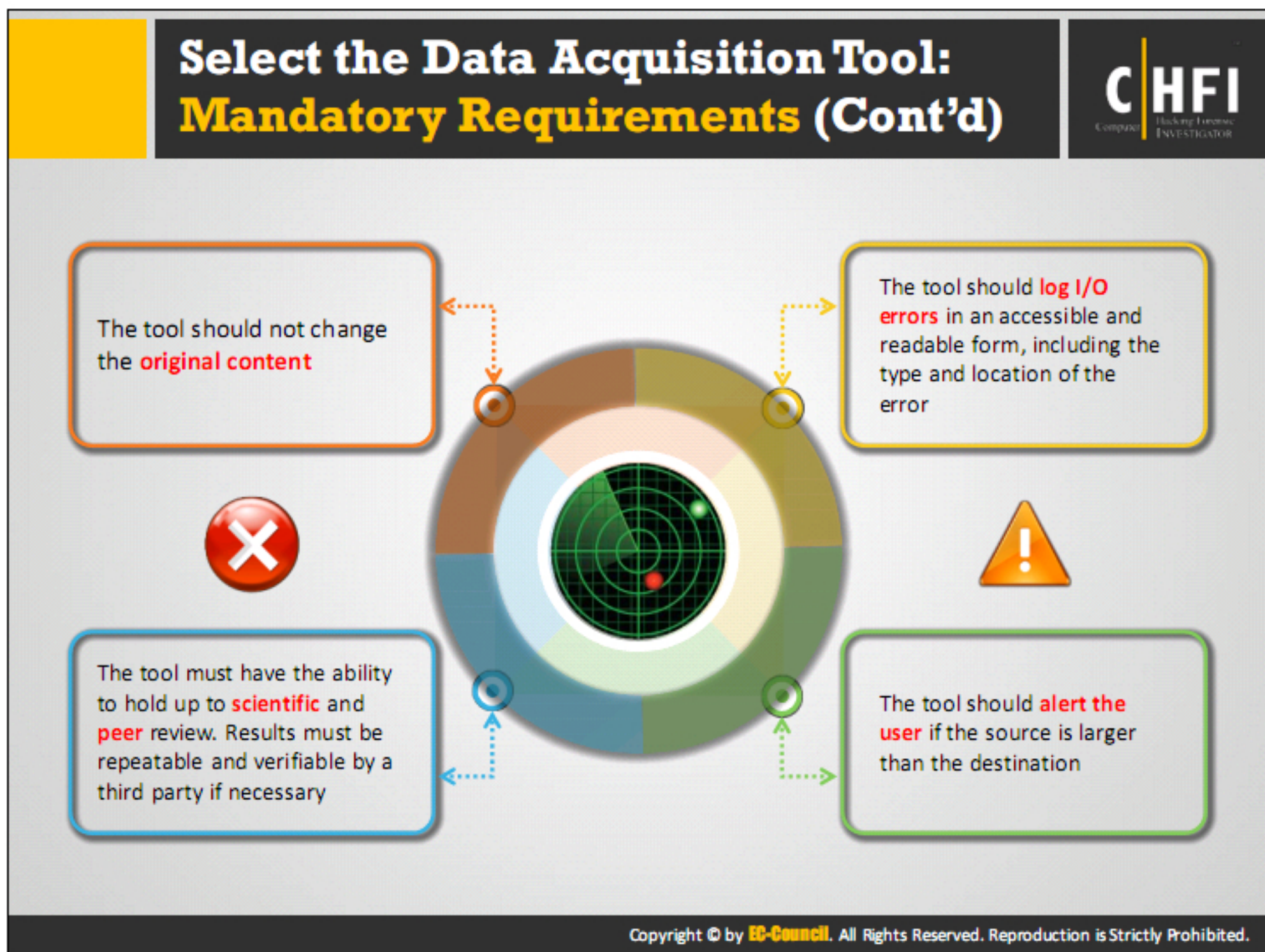
- Use tape backup systems like Super Digital Linear Tape (SDLT) or Digital Audio Tape/ Digital Data Storage (DAT/DDS) if the suspect drive is vast
- SnapBack and SafeBack have software drivers to write data to a tape backup system from a suspect drive through standard PCI SCSI cards
- This method has an advantage of no limit to the required data size
- The biggest disadvantage is that it is a slow and time-consuming process



Digital evidence is critical for the security incident investigation. The investigators usually perform the investigation process on the copy of the original digital evidence. Therefore, while creating a copy of the original evidence with the help of disk imaging tools, the investigator should ensure the reliability and integrity of the digital evidence.

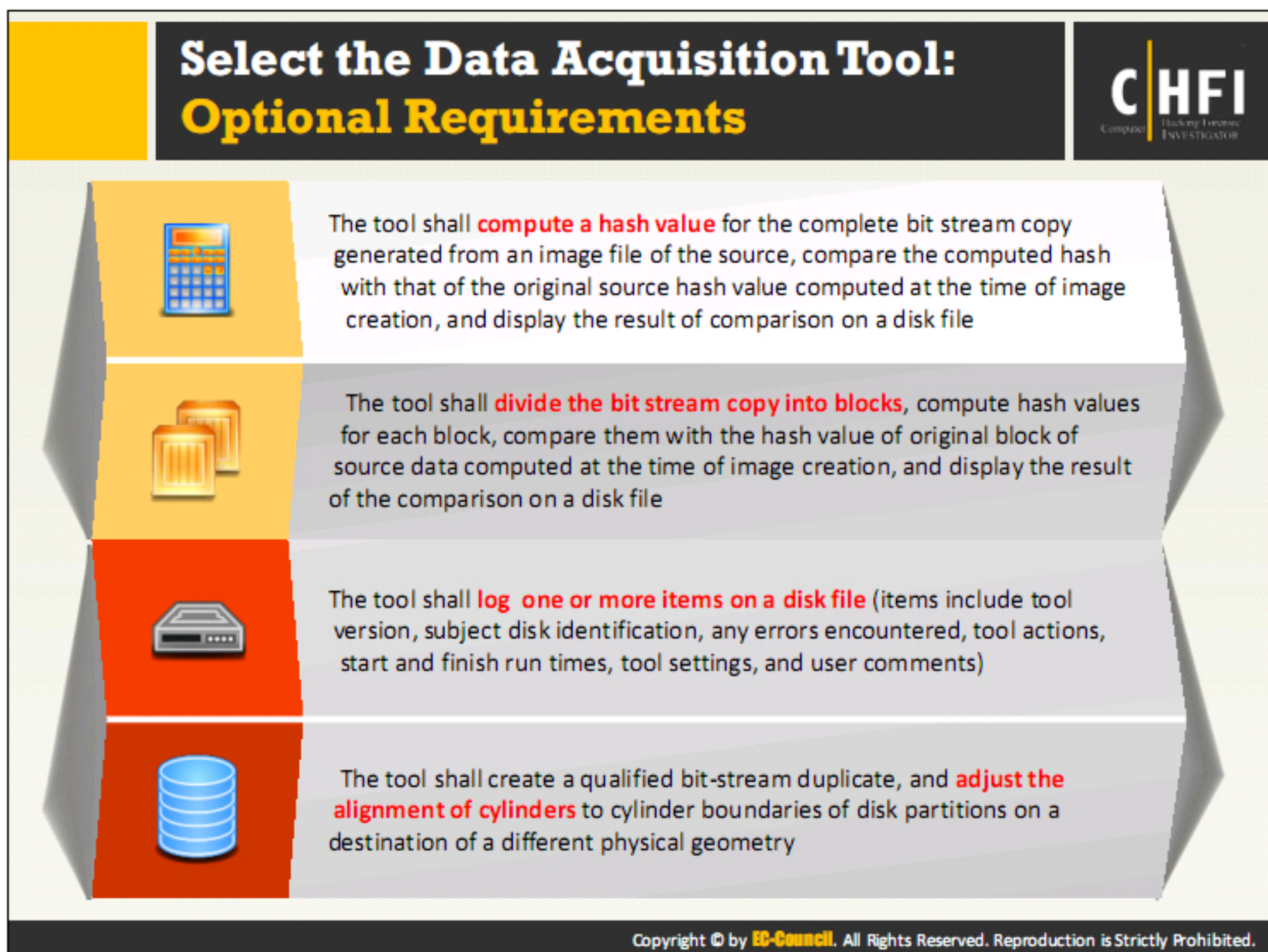
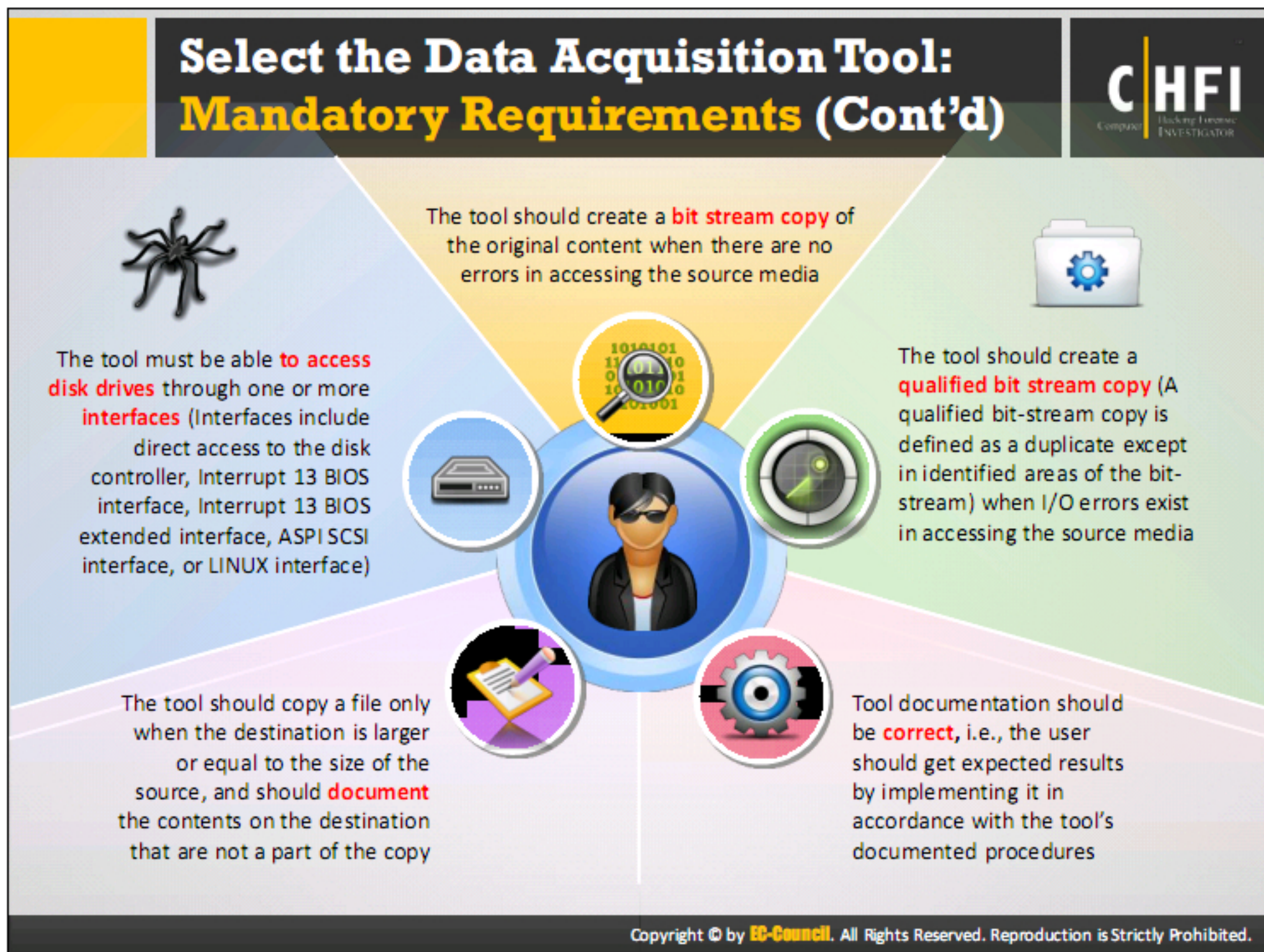
Disk imaging tools have two types of requirements - mandatory and optional:

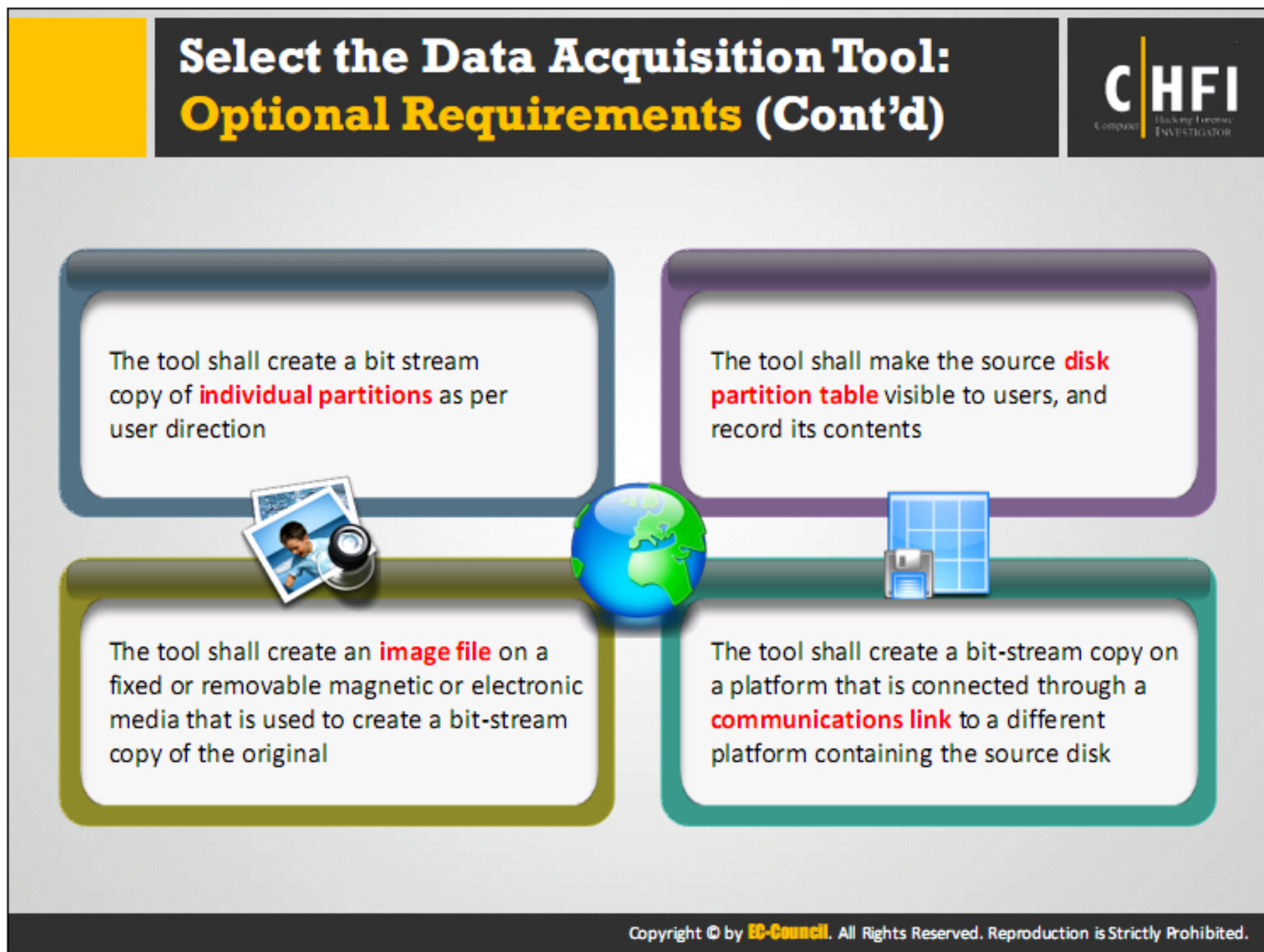
- All the disk imaging tools must accomplish the tasks described as mandatory requirements
- The tools may or might not provide the features discussed under the optional requirements




Following are the mandatory requirements for every tool used for the disk imaging process:

- The tool must not alter or make any changes to the original content
- The tool must log I/O errors in an accessible and readable form, including the type and location of the error
- The tool must be able to compare the source and destination and alert the user if the destination is smaller than the source
- The tool must have the ability to pass scientific and peer review. Results must be repeatable and verifiable by a third party, if necessary
- The tool shall completely acquire all visible and hidden data sectors from the digital source






Data Acquisition and Duplication Tools: Hardware



01 UltraKit

It is a portable kit which contains a complete family of **UltraBlock hardware** write blockers along with **adapters** and **connectors** for acquiring a forensically sound image of virtually any hard drive or storage device




<https://www.digitalintelligence.com>

02 Forensic Falcon

It is a forensic imaging solution with the following features:

- Image and verify
- Preview suspect drive contents
- Image to/from a network location
- Remote operation with a web-based browser interface
- Image a source drive to multiple destination drives using different imaging formats



<http://www.logicube.com>

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

Discussed below are the featured data acquisition and duplication hardware tools can be used to acquire and create duplicate copies of the suspect system data:

UltraKit

Source: <http://www.digitalintelligence.com>

The UltraKit is a portable kit, which provides a complete set of UltraBlock hardware write blockers including adapters and connectors to acquire a forensically sound image of virtually any hard drive or storage device. Just select the relevant Write Protected UltraBlock and attach it to the source drive and use the desktop or laptop to create a forensically protected disk image to an internal drive or externally connected drive enclosure.

Forensic Falcon

Source: <http://www.logicube.com>


Forensic Falcon is a power-rich performance, feature-packed forensic tool which provides expandability to support future digital forensics technological advances. It achieves 23GB/min imaging speed.

Features:

- Image & verify from 4 source drives to 5 destinations
- Preview suspect drive contents directly on the Falcon
- Image to/from a network location


- Remote operation with a web-based browser interface
- Parallel Imaging, Image a source drive to multiple destination drives using different imaging formats

**Data Acquisition and Duplication
Tools: Hardware (Cont'd)**



T3iu Forensic SATA Imaging Bay


It is built for write-blocked acquisitions of 3.5" and 2.5" SATA hard drives



<https://www2.guidancesoftware.com>

Triage-Responder


It allows investigators to investigate and extract evidence from digital devices for access to time-sensitive information, and assist forensics labs by qualifying devices for seizure



<http://www.adfsolutions.com>

Atola Insight Forensic


It is a forensics data recovery and acquisition system that offers complex data retrieval functions along with utilities for manually accessing hard drives at the lowest level, wrapped in a simple and efficient user interface



<http://www.atola.com>

XRY Office

It allows investigators to recover data from a mobile device



<https://www.msab.com>

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

Discussed below are few more featured data acquisition and duplication hardware tools can be used to acquire and create duplicate copies of the suspect system data:

T3iu Forensic SATA Imaging Bay

Source: <https://www2.guidancesoftware.com>

The Tableau T3iu Forensic SATA Imaging Bay is designed for fast write-blocked acquisitions of 3.5" and 2.5" SATA hard drives and for easy integration into workstations using a single SuperSpeed USB 3.0 host connection.

The data transfer bandwidth of USB 3.0 allows system integrators to scale SATA imaging capability of workstations by including multiple T3iu units. The T3iu is a cost effective way to eliminate SATA imaging backlog. The T3iu is a package consisting of three forensic products, a high-performance SATA write blocker, a suspect drive cooler and a suspect drive tray.

Triage-Responder

Source: <http://www.adfsolutions.com>

Triage-Responder is designed particularly for nontechnical first responders. It uses an easy two-step process to scan, analyze and extract evidence from a digital device. It searches the whole target drive in four categories and integrates different technologies, like, ActivitySensor™, which enables the investigators to find and collect valuable files quickly.

The Triage-Responder Kit consists of:

- One portable mini travel case

- One 32GB high-speed USB key
- One boot CD
- One plastic teasing needle

XRY Office

Source: <https://www.msab.com>

XRY Office provides both logical and physical support for mobile forensic examiners. It provides full access to thousands of mobile devices with all the required tools supplied. XRY is a software based solution and is built for a purpose with all the required hardware to recover data from mobile devices in a secure way.

It can implement the following functions:

- SIM Card Reading
- GPS Device Physical Examinations
- Mobile Device Physical and Logical Examinations
- Memory Card Physical Examinations
- HEX Viewer
- Triage Mode
- Find Functions & Watch List
- Hash Algorithms

Atola Insight Forensic

Source: <http://atola.com>

Atola Insight Forensic provides complex data retrieval functionalities with utilities for accessing hard drives at the lowest level, wrapped in an efficient user interface. The tool is designed by recovery engineers, law enforcement agencies, and forensic experts.

Atola Insight Forensic system consists of:











- Atola Insight Forensic software (runs on any Windows PC or laptop)
- DiskSense hardware unit
- Hardware extensions

Features:

- High-performance multi-pass imaging for damaged drives
- Supports various hash calculation: MD5, SHA1, SHA224, SHA256, SHA384, SHA512
- Enables file recovery for NTFS (all versions), Ext 2/3/4, HFS, HFS+, HFSX, ExFAT, FAT16, FAT32
- Includes built-in write blocker

**Data Acquisition and Duplication
Tools: Hardware (Cont'd)**

CHFI
Computer Hacking Forensic Investigator

 US-LATT PRO https://www.wetstonetech.com	 Disk Jockey PRO http://www.diskology.com
 IM Solo-4 G3 Forensic Enterprise Super Kit http://ics-iq.com	 RAPID IMAGE 7020 X2 IT http://ics-iq.com
 ROADMASSTER-3 X2 http://ics-iq.com	 ZClone®Xi http://www.logicube.com
 TD2u Forensic Duplicator https://www2.guidancesoftware.com	 HardCopy 3P http://www.digitalintelligence.com
 Disk Imager Forensic Edition http://www.deepspare.com	 Forensic Tower IV Dual Xeon http://www.forensiccomputers.com

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

Discussed below are some more data acquisition and duplication hardware tools using which one can acquire and create duplicate copies of the suspect system data:

US-LATT PRO

Source: <https://wetstonetech.com>

US-LATT PRO implements live acquisition and triage of Microsoft® Windows systems (XP – Windows 8). It offers the ability to the investigators to triage live evidence with fast and efficient on scene investigations.

IM Solo-4 G3 Forensic Enterprise Super Kit

Source: <http://ics-iq.com>

The Image MASter Solo-4 G3 PLUS Forensic Enterprise Super Kit is a drive data acquisition unit with i7 Processor and ExpansionBox hardware configuration. It provides the ability to the investigators to simultaneously extract data from suspect to evidence hard drives at SATA-3 speed. It can also acquire data from two separate suspect hard drives to two individual evidence hard drives.

ROADMASSTER-3 X2

Source: <http://ics-iq.com>

The RoadMASter-3 X2 provides the forensic examiner with a powerful and flexible platform for forensic data capture and analysis. It is a portable lab built as a rapid forensic data acquisition

and analysis workstation. It is ruggedized and has all the required tools to collect the data from drives.

TD2u Forensic Duplicator

Source: <https://www2.guidancesoftware.com>

TD2u Forensic Duplicator is designed for both field and lab forensic environments. It offers easy operability, reliability, and fast forensic imaging performance. It images at a speed of 15GB/min while simultaneously calculating MD5 and SHA-1 hashes.

Disk Imager Forensic Edition

Source: <http://www.deepspare.com>

DeepSpar Disk Imager Forensic Edition is a portable forensic imaging tool. It allows the examiners to view the imaging process to see the read status of each retrieved sector and what data and what type of files are being imaged. Failing hard drives are imaged using very few passes to get maximum information. It reduces the time taken to image bad sectors disks.

Disk Jockey PRO

Source: <http://www.diskology.com>

The Disk Jockey PRO is a disk copy and write blocking tool developed for computer forensics. It is capable of copying the Drive Configuration Overlay (DCO) areas and Host Protected Area (HPA) of a hard disk drive. It can work on Windows or Macintosh systems connected via high-speed USB 2.0 ports, or it can be used as a standalone unit. It can also be used to mount drives to the desktop, copy data between hard disks quickly, verify, test and erase hard disks.

RAPID IMAGE 7020 X2 IT

Source: <http://ics-ig.com>

The Rapid Image™ Hard Drive Duplicators are built to copy a single master hard drive to up to 19 target hard drives at SATA-III Speeds. It can also be configured to copy multiple master drives simultaneously. It can also copy and sanitize drives simultaneously with minimum speed degradation.

ZClone®Xi

Source: <http://www.logicube.com>

The ZXi is a duplicator, it provides advanced features like fast cloning, task macros networking and user profiles along with an easy to use interface. It supports mirror cloning, a 100% bit for bit copy, as well as a CleverCopy mode that copies only data areas. It can also sanitize hard drives safely.

HardCopy 3P

Source: <http://www.digitalintelligence.com>

It is a portable Forensic Hard Drive Duplicator with MD5, SHA256, and an integrated IDE port. It offers up to 7.5 GB Per Minute Data Transfer Rate. It offers two duplication Modes.

- Clone mode: block by block copy of the whole drive; block locations are identical to source
- Image mode: block by block copy (dd image) of the whole drive into a single file or chunked files.











Forensic Tower IV Dual Xeon

Source: <http://www.forensiccomputers.com>

The Forensic Tower IV Dual Xeon sets a standard for forensic laboratory systems. It consists of a case of ten 5.25-inch bays to provide flexibility in configuring a lab system to fulfill client requirements. It is compatible with all commercial forensic acquisition and analysis software such as EnCase®, ProDiscover®, Forensic Tool Kit®, and P2 Commander®.

**Data Acquisition and Duplication
Tools: Hardware (Cont'd)**

CHFI
Computer Hacking Forensic Investigator

 FREDDIE http://www.digitalintelligence.com	 UFED Touch http://www.cellebrite.com
 Data Extractor http://www.deepspar.com	 UFED Pro Series http://www.cellebrite.com
 Project-A-Phone http://www.project-a-phone.com	 FRED https://www.digitalintelligence.com
 Mobile Field Kit https://www.paraben.com	 Ditto Forensic FieldStation https://www.cru-inc.com
 iRecovery Stick https://www.paraben.com	 Forensic UltraDock https://www.cru-inc.com

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

Discussed below are some more data acquisition and duplication hardware tools can be used to acquire and create duplicate copies of the suspect system data:

FREDDIE

Source: <http://www.digitalintelligence.com>

FREDDIE is a portable mobile forensic tool with flexible, integrated, and modular forensic platform built for computer evidence acquisition and analysis. First, remove the hard drive(s) from the subject computer and attach into FREDDIE to extract evidence. This tool can directly gather data from IDE, EIDE, ATA, SATA, ATAPI, SAS, USB or Firewire hard drives and other storage devices.

PRO Data Extractor

Source: <http://www.deepspar.com>

PC-3000 Data Extractor detects and fixes file system issues. It collaborates with PC-3000 hardware to recover data from any media, such as, IDE HDD, SCSI HDD, and flash memory readers. Using algorithms this tool performs logical file recovery to rectify file system structure problems or retrieves data by implementing a sector-by-sector search for header files independent of the OS.

Project-A-Phone

Source: <http://www.project-a-phone.com>

This tool helps to take high-quality screenshots of any device. It has 8-megapixel camera to take clear pictures of the display of the device. This camera connects to the computer to capture a clear screenshot. HD quality videos can also be recorded using this tool. A license of P2CC is issued for this tool for advanced reporting, including hash value validation.

Mobile Field Kit

Source: <http://forensicstore.com>

Paraben's Mobile Field Kit is a portable handheld forensic product. The kit contains all the equipment required to perform a digital forensic analysis of more than 4,000 cell phones, GPS devices, and PDAs.

iRecovery Stick

Source: <https://www.paraben.com>

The iRecovery Stick has special investigation software on a USB drive, which enables to investigate data on iPhones and other Apple mobile devices. It can also restore deleted data like iMessages, text messages (SMS), call history, contacts, calendar entries, and internet history.

UFED Touch

Source: <http://www.cellebrite.com>

It is a standalone mobile forensic extraction device. It has an easy to use the touchscreen and an instinctive GUI. This tool allows file system, physical and logical extractions of all data from a wide range of mobile devices.

UFED Pro Series

Source: <http://www.cellebrite.com>

Cellebrite develops UFED Pro Series for forensic investigators. They require mobile data extraction and decoding tools, which helps to extract valuable data, combine different data to visualize necessary connections, speed up investigations, and identify evidence.

FRED

Source: <http://www.digitalintelligence.com>

FRED systems built for stationary forensic laboratory acquisition and analysis. First, remove the hard drive(s) from the subject system and attach into FRED to extract digital evidence. This tool will get the data directly from IDE, EIDE, ATA, SATA, ATAPI, SAS, Firewire or USB hard drives and save forensic images to CD, Blu-Ray, DVD, or hard drives. This tool can also gather data from CD-ROM, DVD-ROM, Blu-Ray, Micro Drives, Compact Flash, Memory Stick, Smart Media, xD Cards, Memory Stick Pro, Multimedia Cards, and Secure Digital Media.

Ditto Forensic FieldStation

Source: <https://www.cru-inc.com>


The Ditto Forensic FieldStation is a portable forensic tool used to create local, remote or networked disk clones and images. It also helps to log user activity and preserve the chain of custody while using forensic write-blocked methods.

Forensic UltraDock

Source: <https://www.cru-inc.com>

Forensic UltraDock is used to view, evaluate, and image a disk drive safely. It is a professional drive dock that allows multiple hosts and drives connection types. It automatically detects and notifies hidden areas of the drive and also supports common types of drives like SATA and IDE/PATA.

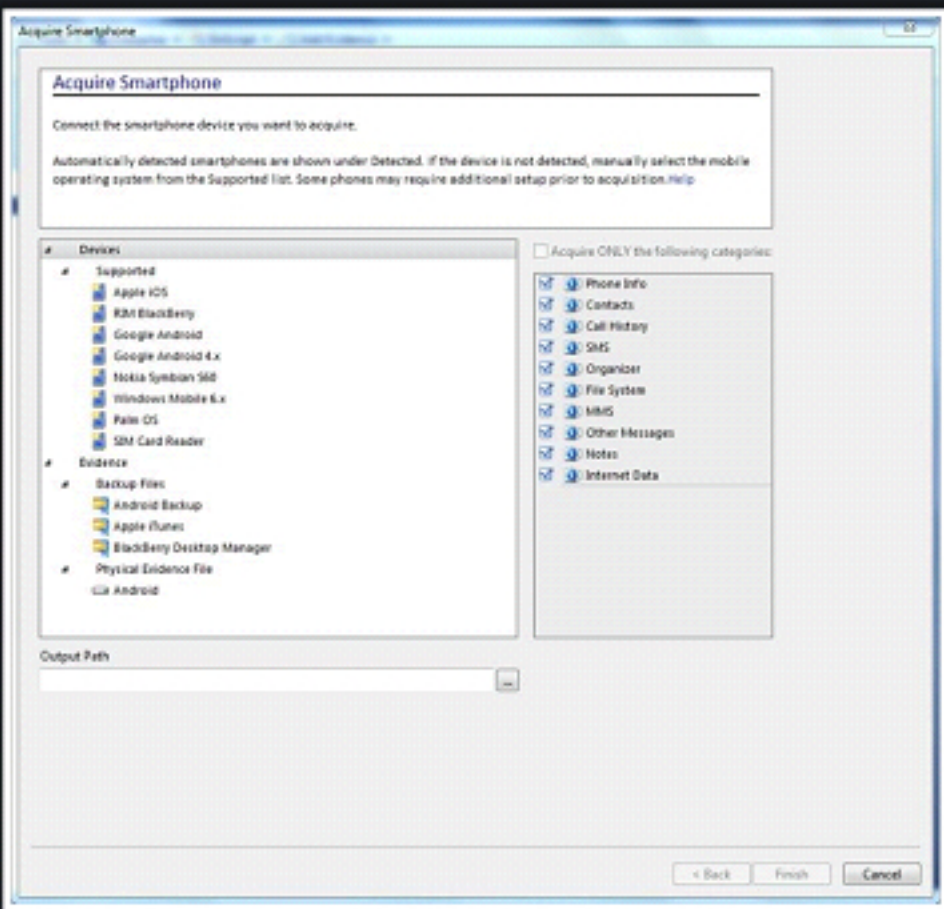
Data Acquisition and Duplication Tools: Software



EnCase Forensic

EnCase Forensic solutions allow forensic practitioners to:

- **Acquire** data from a wide variety of devices
- **Unearth** potential evidence with disk-level forensics analysis
- **Produce** comprehensive reports on findings
- **Maintain** the integrity of the evidence in a format the courts have come to trust



<https://www2.guidancesoftware.com>

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

EnCase Forensic

Source: <https://www.guidancesoftware.com>

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


EnCase Forensic can help investigators to acquire large amounts of evidence, as fast as possible from laptops and desktop computers to mobile devices. The data is acquired directly into EnCase Forensic and integrates the results into the cases.











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

- GREP
- Conditional
- Boolean
- Word searches

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

**Data Acquisition and Duplication
Tools: Software (Cont'd)**



 DriveSpy https://www.digitalintelligence.com	 X-Ways Forensics https://www.x-ways.net
 ProDiscover Forensics http://www.arcgroupny.com	 F-Response Imager https://www.f-response.com
 Data Acquisition Toolbox https://www.mathworks.com	 R-Drive Image http://www.drive-image.com
 RAID Recovery for Windows https://www.runtime.org	 Flash Retriever Forensic Edition http://www.infinadyne.com
 R-Tools R-Studio http://www.r-studio.com	 Forensic Replicator https://www.paraben.com

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

Discussed below are a few data acquisition and duplication software tools using which one can acquire and create duplicate copies of the suspect system data:

DriveSpy

Source: <https://www.digitalintelligence.com>

DriveSpy allows forensic examiners to direct information from one sector range to another. It creates direct disk-to-disk forensic duplicates, processes duplicate drives of both physical drive geometry and sector translation, processes large hard drives, hard drives without partitions, slack space, unallocated space etc.

ProDiscover Forensics

Source: <http://www.arcgroupny.com>

ProDiscover Forensic is a computer security tool, which allows investigators to locate the data on a computer disk and protect the evidence. It also creates useful evidentiary reports for the case. This tool enables entire disk search for keywords, regular expressions, and phrases with Boolean search ability to find the relevant data. Using ProDiscover Forensic the examiners are allowed to analyze files without changing the useful metadata like last-time accessed. ProDiscover Forensic allows one to recover deleted files, review slack space, access Windows Alternate Data Streams, and provide a preview, search, and image-capture of the Hardware Protected Area (HPA) of the disk.

Data Acquisition Toolbox

Source: <http://in.mathworks.com>

Data Acquisition Toolbox™ allows connecting MATLAB® to data acquisition hardware. It supports various DAQ hardware provided by National Instruments and vendors, such as, USB, PCI, PCI Express®, PXI and PXI-Express devices.

This toolbox configures data acquisition hardware and reads data into MATLAB for quick analysis. Using this toolbox data can also be sent over analog and digital output channels provided by data acquisition hardware. The data acquisition software of the toolbox provides different functionalities to control analog input/output, counter/timer and digital I/O subsystems of a DAQ device.

RAID Recovery for Windows

Source: <https://www.runtime.org>

RAID Recovery for Windows is used to recover full content of a broken RAID. It is capable to copy the files and folders over to another disk. It works for NTFS-formatted RAID-0 as well as RAID-5 configurations and supports both, hardware RAIDs controlled by mother board or controller card and software RAIDs controlled by Windows (dynamic disk arrays).

R-Tools R-Studio

Source: <http://www.r-studio.com>

R-Tools R-Studio provides latest data recovery technologies to recover files from NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ (Macintosh) etc. R-Studio consists of advanced RAID reconstruction module and advanced disk copying/imaging module in a single piece of software, which makes data recovery easier. It works on both local as well as network disks and provides flexible parameter settings to control data recovery.

X-Ways Forensics

Source: <http://resources.infosecinstitute.com>

X-Ways Forensics is an advanced digital forensics platform, which works on all available versions of Windows.

Features:

- Disk imaging and cloning
- Various data recovery techniques and file carving
- Extracts metadata from various file types

F-Response Imager

Source: <https://www.f-response.com>

The F-Response Imager is a product built to provide simple and fast imaging. It uses all available system resources to provide optimal performance and scaling, and allows efficient multi-thread scheduling for compressing, reading, hashing, and writing data. It supports all other F-Response

logical and physical devices, such as, F-Response Connector Volumes, DiscoveryShares and MemoryShares.

R-Drive Image Flash

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

R-Drive Image is used to create disk image files for backup or duplication purposes. R-Drive Image recovers the images on the original disks, partitions and also on hard drive's free space on the fly. A full disk can be copied to another one.

Retriever Forensic Edition











Source: <http://www.infinadyne.com>

Flash Retriever Forensic Edition is a professional forensic tool used for analyzing, recovering, and documenting flash-based media. It allows complete flash device imaging in raw format. It supports multiple-media.

Forensic Replicator

Source: <https://www.paraben.com>

Forensic Replicator is a Windows based bit-stream forensic image creation tool. It allows to create bit-by-bit raw DD images of hard drives, check image integrity with hash calculation, document write blocker usage in the report, view image contents etc. This tool consists of a built in software based write protection to help preserve evidence. Hash verification and reporting are also used to maintain data integrity.

Data Acquisition and Duplication Tools: Software (Cont'd)		CHFI Computer Hacking Forensic Investigator
 MacQuisition https://www.blackbagtech.com	 SMART for Linux http://www.asrdata.com	
 Belkasoft Live RAM Capturer http://belkasoft.com	 Paragon Hard Disk Manager 15 Suite https://www.paragon-software.com	
 Magnet RAM Capture https://www.magnetforensics.com	 Macrium Reflect Free http://www.macrium.com	
 OSFClone http://www.osforensics.com	 DAEMON Tools Pro 7 https://www.daemon-tools.cc	
 IQCOPY FOR FORENSIC http://ics-iq.com	 Active@ Disk Image http://www.lsoft.net	

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

Discussed below are few more data acquisition and duplication software tools using which one can acquire and create duplicate copies of the suspect system data:

MacQuisition

Source: <https://www.blackbagtech.com>

MacQuisition™ is a three in one live data acquisition and forensic imaging product. MacQuisition™ can collect data from more than 185 different Macintosh system models. It avoids complicated and time-consuming data collection process. It runs on the Mac OS X operating system and collects data from Mac, Xserve, Mac mini, iMac, MacBook, and MacBook Air systems in their own Mac OS X environment.

Belkasoft Live RAM Capturer

Source: <https://belkasoft.com>

Belkasoft Live RAM Capturer is a forensic tool that reliably extracts all the contents of a system volatile memory. The tool footprint is minimized as much as possible by using separate 32-bit and 64-bit builds. It is compatible with all versions of Windows including XP, Vista, Windows 7 and 8, 2003 and 2008 Server.

Magnet RAM Capture

Source: <https://www.magnetforensics.com>

Magnet RAM Capture can work on both 32 and 64 bit Windows systems such as XP, Vista, 7, 8, 10, 2003, 2008 and 2012 and can extract a full physical memory rapidly.

OSFClone

Source: <http://www.osforensics.com>

OSFClone is a self-booting tool that can create exact raw disk images. It also supports the open Advance Forensics Format (AFF) for the imaging drives. It creates a forensic image of a disk and preserves unused sectors, file fragmentation, slack space, and undeleted file records of the original hard disk. It also supports dc3dd format for disk images. To verify that a disk clone is identical to the source drive OSFClone is used by comparing MD5 or SHA1 hash of the clone and the source drive.

FDAS - Fast Disk Acquisition System

Source: <http://www.cyanline.com>

FDAS can be abbreviated as Fast Disk Acquisition System. It is a product built by CyanLine. FDAS can copy disk-to-disk directly. The time to copy is equal to the time allowed by the source disk.

SMART for Linux

Source: <http://www.asrdata.com>

SMART is a software designed to support forensic examiners and Information Security personnel to fulfill their forensic investigation duties and goals. The features of SMART allow it to be used for:

- Target system on-site or remote preview
- A dead system post mortem analysis
- testing and verification of forensic programs
- conversion of proprietary evidence file formats

Paragon Hard Disk Manager 15 Suite

Source: <https://www.paragon-software.com>

The Paragon Hard Disk Manager 15 Suite is a system and data management tool. It offers dependable backup and flexible recovery functions, optimization tools, options for partitioning etc. It enables full hard disk or a separate partition copy and allows partition resizing while copying.

Macrium Reflect Free

Source: <http://www.macrium.com>

Macrium Reflect Free is a disk cloning and imaging tool. It protects all personal documents, photos, music, mails etc. and also upgrades hard disk. It supports backup to local, network and USB drives and also burning to all DVD formats.

DAEMON Tools Pro 7

Source: <https://www.daemon-tools.cc>

DAEMON Tools Pro is a professional emulation software that works with disc images and virtual drives.

Features:


- It can mount popular types of images from application or Explorer
- It can fetch images from physical discs with advanced parameters
- It creates both Dynamic and Fixed virtual hard disks
- It can create new as well as edit existing Audio CD and Data images
- It can convert, compress and protect image files with password

Active@ Disk Image

Source: <http://www.disk-image.com>

Active@ Disk Image is a disk image software, which can create an exact copy of any PC disks, such as, HDD, SSD, USB, CD, DVD, Blu-ray etc. and stores it to a folder. These copies or images can be used for PC upgrades, backups, and disk duplication purposes.

Linux Standard Tools




- Forensic investigators use the built-in Linux commands **dd** and **dcfldd** to copy data from a disk drive
- These utilities can make a **bit-stream** disk-to-disk copy, disk-to-image file, block-to-block copy/ block-to-file copy
- The **dd** command can **copy data from any disk** that Linux can mount and access
- Other forensics tools such as **AccessData FTK** and **EnCase** can read **dd** image files

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

The forensic investigators use built-in Linux command **dd** to copy data from a disk drive. This command can create a bit-stream disk-to-disk copy and a disk-to-image file. It can copy any disk data that Linux can mount and access. Forensic tools like AccessData FTK and Ilook, can read dd image files.

In Linux, the advantage of **dd** command is its independence on any additional computer resources. The **dd** command can create images with ext2, ext3, FAT12, FAT16, FAT32, UNIX, NTFS, HPFS and HFS filesystem disks and can also help investigators to retrieve digital evidence and copy it to any media that the Linux OS can access.

Acquiring Data on Linux: dd Command



dd Command Syntax `dd if=<source> of=<target> bs=<byte size> ("USUALLY" some power of 2, not less than 512 bytes (ie, 512, 1024, 2048, 4096, 8192, 16384, but can be ANY reasonable number.) skip= seek= conv =<conversion>`

source: where the data is to be read from, *target:* where the data is to be written, *skip:* number of blocks to skip at start of input, *seek:* number of blocks to skip at start of output, *conv:* conversion options

1

Suppose a 2GB hard disk is seized as evidence. Use DD to make a complete physical backup of the hard disk:

```
dd if=/dev/hda of=/dev/case5img1
```

2

Copy one hard disk partition to another hard disk:

```
dd if=/dev/sda2 of=/dev/sdb2 bs=4096 conv=notrunc,noerror
```

3

Make an ISO image of a CD:

```
dd if=/dev/hdc of=/home/sam/mycd.iso bs=2048 conv=notrunc
```

4

Restore a disk partition from an image file:

```
dd if=/home/sam/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror
```

5

Copy RAM memory to a file:

```
dd if=/dev/mem of=/home/sam/mem.bin bs=1024
```

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

The syntax for the dd command is as follows:

```
dd if <source> of<target> bs<byte size>(usually some power of 2, not less than 512 bytes [i.e., 512, 1024, 2048, 4096, 8192]) skip seekconv<conversion>
```


- source: from where to read the data
- target: where to write the data
- skip: number of blocks to skip at the start of the input
- seek: number of blocks to skip at the start of the output
- conv: conversion options

An investigator may use the following commands for the respective tasks:

- To make a full physical backup of a hard disk, use
`dd if=/dev/ hda of=/dev/case5i mg1` command
- To copy one hard disk partition to another hard disk, use
`dd if=/dev/sda 2 of=/dev/sdb2 bs4096 convnotrunc,noerror` command
- To make an image of a CD, use
`dd if=/dev/ hdc of=/home/sam/mycd.iso bs2048 convnotrunc` command
- To copy a floppy disk, use
`dd if=/dev/fd0 of=/home/sam/floppy.image convnotrunc` command

- To restore a disk partition from an image file, use the
`dd if/home/sam/partition.image of/dev/sdb2 bs4096 convnotrunc,noerror`
command
- To copy RAM memory to a file, use the
`dd if/dev/mem of/home/sam/mem.bin bs1024` command

Acquiring Data on Linux: dcfldd Command



dcfldd works similar to the **dd** command but **possesses many features designed for computer forensics acquisitions**. Following are the important functions **dcfldd** offers that are not possible with **dd**:

01	Hashing on-the-fly - dcfldd can hash the input data as it is being transferred, helping to ensure data integrity
02	Status output - dcfldd can update the user of its progress in terms of the amount of data transferred, and how much longer the operation will take
03	Flexible disk wipes - dcfldd can be used to wipe disks quickly, and with a known pattern if desired
04	Image/wipe Verify - dcfldd can verify that a target drive is a bit-for-bit match of the specified input file or pattern
05	Multiple outputs - dcfldd can output to multiple files or disks at the same time
06	Split output - dcfldd can split output to multiple files with more configurability than the split command
07	Piped output and logs - dcfldd can send all its log data and output to commands as well as files natively

To acquire data from a 64MB USB drive:

- Run the commands from a privileged root shell session
- Type the following command at the shell prompt to acquire an entire media device in one image file:

```
dcfldd if=/dev/sda  
of=usbimg.dat
```

If the disk or suspect media is to be segmented, use the dcfldd command with the split command, placing split before the output file field as shown below:

```
dcfldd if=/dev/sda split=2M  
of=usbimg hash=md5
```

This command generates segmented volumes of 2MB each

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

The **dd** command is a data management tool and not specifically designed for forensics, therefore, it has few drawbacks. Nicholas Harbour of the Defense Computer Forensics Laboratory (DCFL) designed a tool called **dcfldd**, which works similar to **dd** but includes several features to support forensics data acquisition.

Features:

- Records all the errors to an output file for ease in examination
- Supports hashing algorithms such as MD5, SHA-1, SHA-256, etc.
- Informs about the acquisition progress
- Splits image file into segmented volumes
- Verifies acquired data with the original source

An example of the **dcfldd** command:

```
dcfldd if=/dev/sdb of=sdb_image.img
```

Parameter explanation:

- if =>** input file
- /dev/sdb =>** source /suspect drive (whole disk)
- of =>** output file

- `sdb_image.img` => name of the image file

If it is required to split the image file into smaller chunks and hash the image at the end. The following command is used:

```
dcflddd if=/dev/sdb split=2M of=sdb_image.img hash=md5
```

An advanced `dcflddd` command look like:

```
dcflddd      if=/dev/sdb      hash=md5,sha256      hashwindow=2G      md5log=md5.txt  
sha256log=sha256.txt \ hashconv=after bs=4k conv=noerror, sync split=2G  
splitformat=aa of=sdb_image.img
```


Parameter explanation:

- `if` => input file
- `/dev/sdb` => source /suspect drive (whole disk)
- `hash` => Definition of hash algorithms
- `hashwindows` => Will hash data chunks of 2 GB
- `md5log` => Saves all md5 hashes in a file called md5.txt
- `sha256log` => Saves all sha hashes in a file called sha256.txt
- `hashconv` => Hashing AFTER or BEFORE the conversion
- `bs` => block size (default is 512)
- `4k` => block size of 4 kilobyte
- `conv` => conversion
- `noerror` => will continue even with read errors
- `sync` => if there is an error, NULL fill the rest of the block
- `split` => Split image file in chunks of 2 GB
- `splitformat` => the file extension format for split operation
- `of` => output file
- `sdb_image.img` => name of the image file

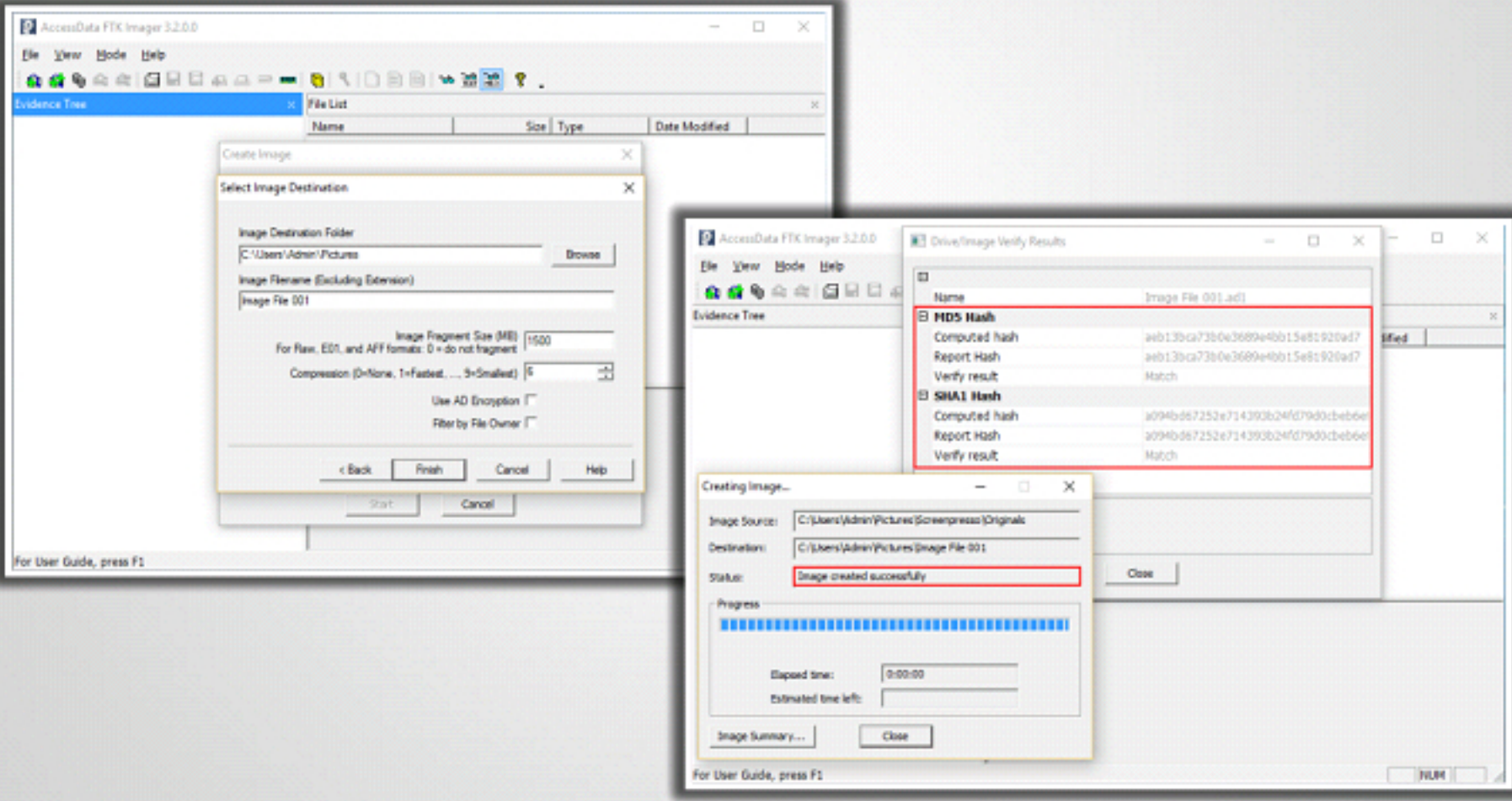
To validate the image file with the source, use the “`vf`” switch command:

```
dcflddd if=/dev/sdb vf=sdb_image.img
```

Acquiring Data on Windows: AccessData FTK Imager



AccessData FTK Imager is a **disk imaging program** which can preview recoverable data from a disk of any kind and also **creates copies**, called forensics images, of that data



The screenshot displays three overlapping windows from the AccessData FTK Imager 3.2.0.0 application. The background window shows the 'Evidence Tree' and 'File List'. Overlaid on top is the 'Create Image' dialog, which includes fields for 'Image Destination Folder' (C:\Users\Admin\Pictures), 'Image Filename (Excluding Extension)' (Image File 001), 'Image Fragment Size (MB)' (1500), and 'Compression' (None). Another window, 'Verify Image', shows the 'MD5 Hash' and 'SHA1 Hash' results for 'Image File 001.adf', with both hashes matching. A third window, 'Creating Image...', shows the progress of the image creation process, with a status of 'Image created successfully' and a progress bar.

<http://accessdata.com>


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

AccessData FTK Imager






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


Its architecture is database-driven and enterprise-class, which allows managing large data, sets. It also provides stability and faster processing speeds. Its built-in data visualization and explicit image detection technology help to detect and report the relevant content for the investigation rapidly. FTK can function simultaneously with all AccessData's solutions and allows correlating data sets from various sources, like computer hard drives, network data, mobile devices, internet storage, etc.

Acquiring RAID Disks



There is no simple method to get **an image of a RAID server's disks**. Therefore, one needs to address the following concerns:

-  How much **data storage** is needed to obtain complete data for a forensics image?
-  What type of **RAID** is used?
-  Do you have the right acquisition tool to **copy the data** accurately?
-  Can the tool read a forensically copied RAID image?
-  Can the tool read split data saves of each RAID disk and combine all images of each disk into one RAID virtual drive for analysis?




Older hardware-firmware RAID systems can be a challenge when making an image

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


RAID disk acquisition may be challenging for forensics examiners due to the RAID system design, configuration, and size. The greatest concern is the size of the RAID system, as many systems are growing into many terabytes of data.

Copying small RAID systems to one large disk is possible with the availability of larger disks. Investigators should use a proprietary format acquisition with compression to store more data in small storage capacities.

Acquiring RAID Disks (Cont'd)



- Several computer forensics vendors have added **RAID recovery features**. These vendors specialize in one or two types of RAID formats.
- The following are some **vendors** offering RAID acquisition functions:
 - Guidance Software EnCase
 - X-Ways Forensics
 - Runtime Software
 - R-Tools Technologies
- Have an idea about which vendor supports which particular **RAID format**, and stay up-to-date on the latest improvements in these products
- A RAID system is too large for a static acquisition. So it is recommended to retrieve only the data relevant to the investigation with the **sparse** or **logical** acquisition method
- When dealing with very large **RAID servers**, consult with the computer forensics vendor to know how best to capture RAID data



The diagram illustrates the process of RAID recovery. A forensic vendor, represented by an icon of a person at a laptop, is shown performing a 'Raid Recovery' operation on a RAID storage unit. A dashed line connects the vendor to the RAID unit, with the label 'Raid Recovery' written vertically along the line.

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


Computer forensics vendors have added many RAID recovery features and these vendors specialize in one or two kinds of RAID formats.

Some of the vendors offer RAID acquisition functions are:

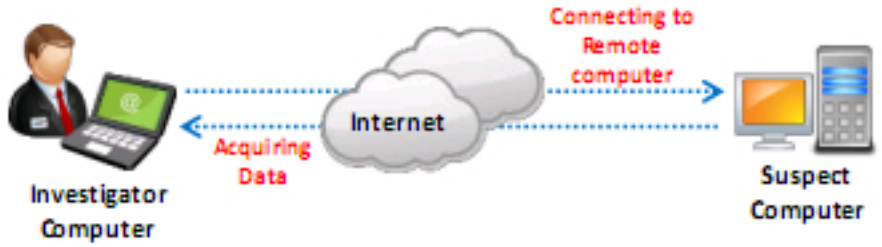
- Technologies Pathways ProDiscover
- Guidance Software EnCase
- X-Ways Forensics
- Runtime Software
- R-Tools Technologies

Having up-to-date knowledge on the latest improvements in these products and which vendor supports which RAID format is necessary. Separation of each physical disk into smaller sets has eliminated the need of one large drive for storing acquired data. Investigators require similar sized drives matching each disk in the RAID array for acquiring RAID disks. For a static acquisition, a RAID system is too large. Collecting a complete image of evidence drives is not always practical. Therefore, it is preferable to recover only the data relevant to the investigation with the logical or sparse acquisition method. When dealing with very large RAID servers, in order to determine how to best capture RAID data, consult the computer forensics vendor.

Remote Data Acquisition



- Data can be copied from a suspect computer by **connecting remotely** to it via a network connection
- Remote acquisition tools vary in **configurations and capabilities**
 - Some require **manual intervention** on remote suspect computers to initiate the data copy
 - Some acquire data covertly through an **encrypted link by pushing a remote access** program to the suspect computer
- Remote acquisitions should be done as **live acquisitions**, not as static acquisitions




Drawbacks

- LAN's data transfer speeds and routing table conflicts could cause problems
- On a WAN, it is difficult to gain permissions needed to access more secure subnets
- Heavy traffic on the network could cause delays and errors during the acquisition
- Remote access program being detected by the antispyware, antivirus, and firewall tools

Remote acquisition can be performed using remote acquisition tools such as:

- ProDiscover Incident Response Edition
- WetStone's LiveWire Investigator
- F-Response
- Runtime Software (DiskExplorer for FAT, and DiskExplorer for NTFS)



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

Computing devices and various forensics tools provide investigators with the ability to collect disk data from a suspect computer remotely via a network connection. Remote acquisition tools vary in capabilities and configuration. Some of them need manual supervision on remote suspect computers to start copying data, while others can directly extract data through an encrypted link by loading a remote access program to the suspect's computer.

Investigators can perform such data acquisitions without the knowledge of the user. Remote acquisitions save time but only support live acquisitions.

Drawbacks of remote acquisitions include:

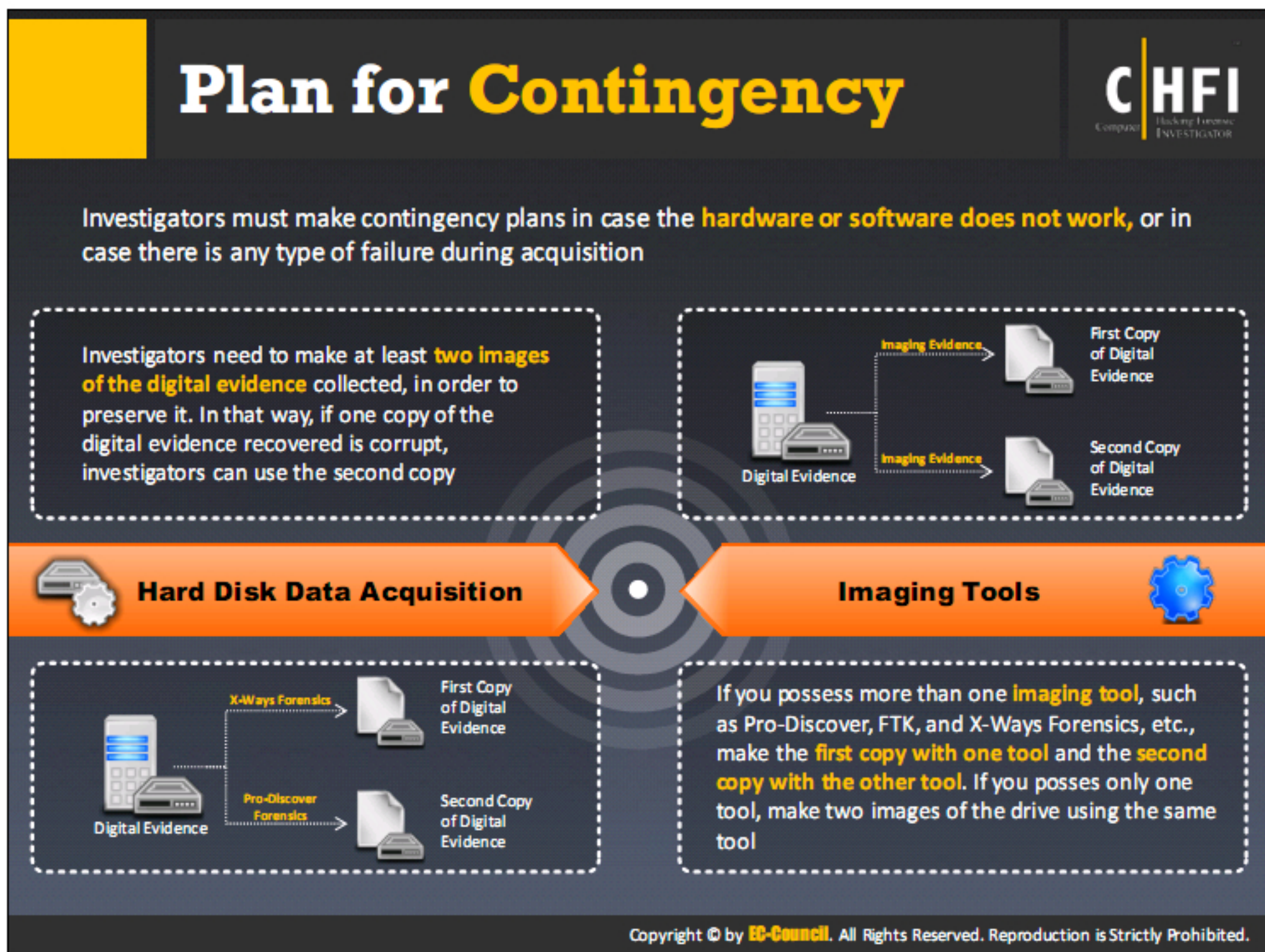
- Problems could arise with the LAN's data transfer speeds and routing table conflicts
- On a WAN, problems arise in gaining the permissions that require access to more secure subnets
- Heavy network traffic on the network can also cause errors and delays in data acquisition regardless of the tool used
- Antivirus, anti-spyware, and firewall tools are capable of detecting this remote access program

Remote acquisition tools include ProDiscover, WetStone LiveWire, F-Response and Runtime Software (DiskExplorer for FAT, DiskExplorer for NTFS, and HDHost).



Investigators can sometimes make few mistakes during data collection that result in the loss of significant evidence. Therefore, the investigators have to be cautious during data acquisition. Some of the mistakes investigators commit are as follows:

- Choosing the wrong resolution for data acquisition: Bit resolution is important when selecting a data-acquisition board.
- Using the wrong cables and cabling techniques: The use of an incorrect type of cable and cabling technique may affect the information integrity and can damage the data.
- Taking insufficient time for system development: The data acquisition system needs careful dealing to develop completely. Forensic investigators can overlook some critical considerations when they do not give enough time to the data acquisition process, leading to data damage.
- Making the wrong connections: Electronic evidence is fragile in nature. Even a minor mistake such as wrong connections of media devices may cause irreversible damage to data.
- Having poor knowledge of the instrument: Investigators should be well aware of the technology they are using in a particular situation. Poor knowledge of tools and technology may jeopardize the integrity of the information.

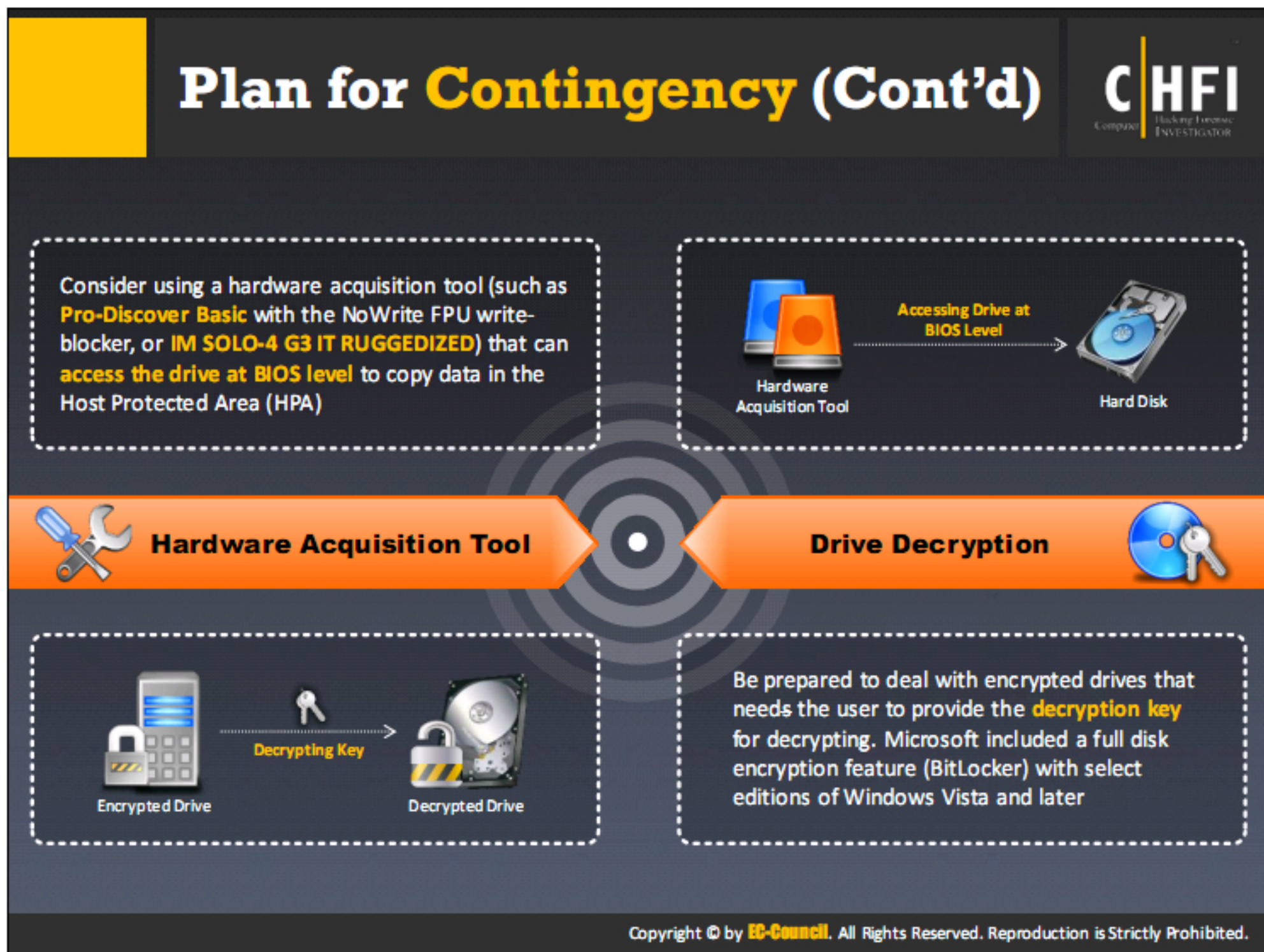


In digital forensics investigation, plan for contingency refers to a backup program an investigator should have in case hardware or software does not work or there is any failure during an acquisition. Contingency planning is necessary for all cyber investigations as it assists investigators to prepare for the unexpected events.


It is a process that helps in completing the investigation process by providing an alternative solution to the failed software or hardware tool.

Plan for Contingency include maintaining:


- Hard Disk Data Acquisition
- Imaging Tools
- Hardware Acquisition Tool
- Drive Decryption



Validate Data Acquisitions



- Digital evidence validation involves using a **hashing algorithm** utility to create a **binary or hexadecimal number** that represents the uniqueness of a data set such as a disk drive or file
- The unique number is referred to as a **"digital fingerprint"**
- Hash values are **unique**. If two files have the same hash value, they are 100% identical even if the files are named differently



Digital Fingerprint


- Utility algorithms that produce hash values include **CRC-32, MD5, SHA-1, and SHA-256**
- **CRC-32:**
It is a 32-bit CRC code used as an error detection method during data transmission. If the computed CRC bits are identical to the original CRC bits, it means that no error occurred
- **MD5:**
It is a cryptographic hash function with a 128-bit hash value. The hash value can be used to demonstrate integrity of data, and can be performed on various data types such as files, physical drives, partitions, etc.
- **SHA-1 and SHA-256:**
They are cryptographic hash functions that produce 160-bit and 256-bit message digests respectively


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

Validating digital evidence is one of the most important aspects of computer forensics. Validation is essential to verify the evidence data integrity. Validating digital evidence requires a hashing algorithm utility developed to create a binary or hexadecimal number, called digital fingerprint, which represents the uniqueness of a file or disk drive. When two files have the same hash values, they are considered identical, even if they have different filenames, as hash values are unique. Even a slight modification in the input will change the hash value completely.


- **CRC-32:** Cyclic Redundancy Code algorithm-32 (CRC-32) is a hash function based on polynomial division idea. The number 32 indicates the size of the resulting hash value or checksum, which is 32 bits. The checksum identifies errors after data transmission or storage.
- **MD5:** It is an algorithm used to check the data integrity by creating 128-bit message digest from the data input of any length. Every MD5 hash value is unique to that particular data input.
- **SHA-1:** SHA-1 (Secure Hash Algorithm-1) is a cryptographic hash function developed by the United States National Security Agency, and it is a US Federal Information Processing Standard issued by NIST. It creates a 160-bit (20-byte) hash value called a message digest. This hash value is a hexadecimal number, 40 digits long.
- **SHA-256:** It is a cryptographic hash algorithm that creates a unique and fixed-size 256-bit (32-byte) hash. Hash is a one-way function, which means, decryption is impossible. Therefore, it is apt for anti-tamper, password validation, digital signatures, and challenge hash authentication.

Linux Validation Methods






The two Linux shell commands **dd** and **dcfldd** have many options that can be combined with other commands to **validate data**



Other shell commands are required to **validate acquired data** with the **dd** command. Whereas, **dcfldd** command has additional options to validate data collected from an acquisition



md5sum and **sha1-sum** are the two **hashing algorithm** utilities in current distributions of Linux that can **compute hashes** of single or multiple files, single or multiple disk partitions, or an entire disk drive

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

Linux uses various commands and functions to perform operations. Two Linux shell commands, dd and dcfldd in combination with other commands can help the investigators validate the acquired data.

The dd command can help validate the collected data when combined with other commands, whereas the dcfldd command has additional options that validate data. Linux provides two hashing algorithm utilities, sha1sum and md5sum. Both can calculate hashes of a single or multiple files, individual or multiple disk partitions or a whole disk drive.

Linux Validation Methods (Cont'd)



Validating dd Acquired Data:

dd command produces segmented volumes of the **/dev/sdb** drive, with each segmented volume named **image_sdb** and an extension of **.aa,.ab,.ac**, etc.:

```
dd if=/dev/sdb | split -b 650m - image_sdb
```

Use the Linux shell commands as follows to validate all segmented volumes of a suspect drive with the **md5sum** utility:



1. Start Linux, open a shell window and navigate to the directory containing image files. To calculate the hash value of the original drive, type **md5sum /dev/sdb > md5_sdb.txt** and press **Enter**
2. Type **cat image_sdb. | md5sum >> md5_sdb.txt** and press **Enter** to compute the MD5 hash value for the segmented volumes, and append the output to the **md5_sdb.txt** file
3. Type **cat md5_sdb.txt** and press **Enter** to check if both hashes match by examining the **md5_sdb.txt** file. If the two hash values are identical, it indicates that data acquisition is successful. The output would be similar to:

```
34963884a4bc5810b130018b00da9de1 /dev/sdb
34963884a4bc5810b130018b00da9de1
```
4. Type **Exit** and press **Enter** to close the Linux shell window

Note: To use **sha1sum** utility, replace all **md5sum** references in commands with **sha1sum**

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

Linux Validation Methods (Cont'd)



Validating dcfldd Acquired Data



1

Dcfldd is designed for forensics data acquisition and has validation options integrated: **hash** and **hashlog**



2

Hash option designates a hashing algorithm of **md5**, **sha1**, **sha256**, **sha384**, or **sha512**



3

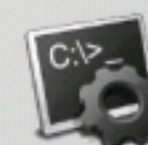
Hashlog **outputs** hash results to a **text file** that can be stored with the image files



4

Enter the following command at the shell prompt to create an MD5 hash output file during **dcfldd** data acquisition:

```
dcfldd if=/dev/sda split=2M of=usbimg hash=md5 hashlog=usbhash.log
```

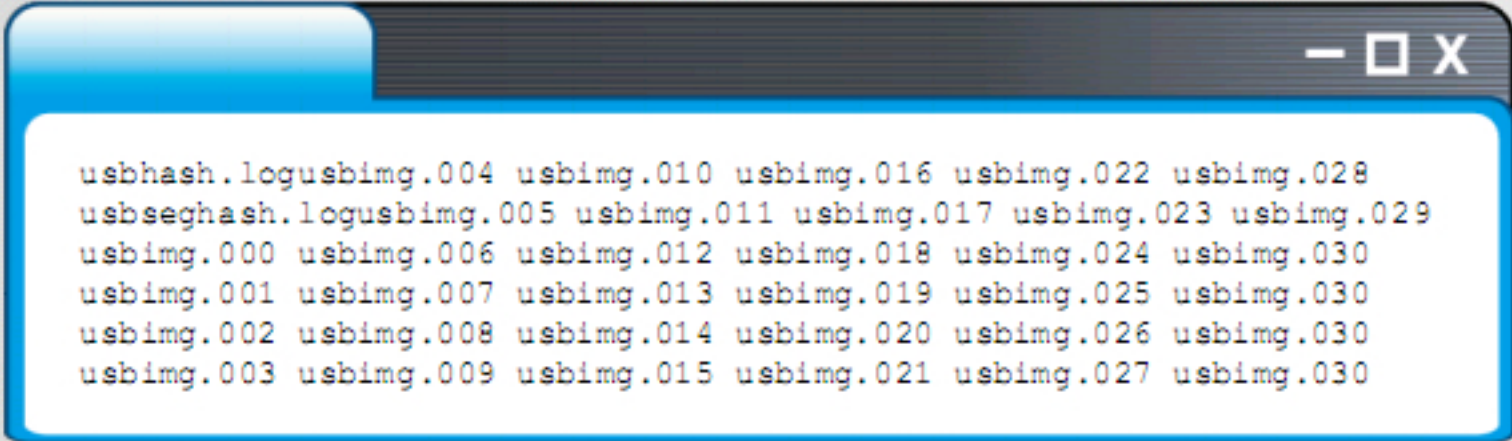


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Linux Validation Methods (Cont'd)



- Enter the **list directory command (ls)** at the **shell prompt** to see the results of files generated with the **split command**. The following should be the output:



```
usbhash.logusbimg.004 usbimg.010 usbimg.016 usbimg.022 usbimg.028
usbseghash.logusbimg.005 usbimg.011 usbimg.017 usbimg.023 usbimg.029
usbimg.000 usbimg.006 usbimg.012 usbimg.018 usbimg.024 usbimg.030
usbimg.001 usbimg.007 usbimg.013 usbimg.019 usbimg.025 usbimg.030
usbimg.002 usbimg.008 usbimg.014 usbimg.020 usbimg.026 usbimg.030
usbimg.003 usbimg.009 usbimg.015 usbimg.021 usbimg.027 usbimg.030
```




- The **vf** (Verify File) option is another **dcfldd** command that compares the image file to the original medium such as a drive or partition. It is applicable only to the **non-segmented image file**. Enter the following command at the shell prompt to use the **vf** option:

```
dcfldd if=/dev/sdavgf=sda_hash.img
```


Note: Use the md5sum command to validate the segmented files from **dcfldd**

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

Windows Validation Methods



- Windows has no built-in **hashing algorithm tools** for computer forensics as in Linux and Unix
- However, Windows third-party programs such as **X-Ways**, **EnCase**, **FTK**, and **ProDiscover** do have a variety of built-in tools for validation



```
graph LR; A[Windows Computer] -- Use --> B[Third-party Utility (Encase)]; B -- Produce --> C[Hash Algorithm];
```

- Commercial computer forensics programs also have **built-in validation features**, and each program has its own validation technique to be used with acquisition data in its proprietary format
- For instance:
 - ProDiscover's .eve files contain **metadata** in segmented files or acquisition files, including the hash value for the suspect partition or drive
 - Image data loaded into ProDiscover is **hashed**, and the value generated is compared with the hash value in the stored metadata
 - If the **hashes do not match**, ProDiscover reports that the acquisition is corrupt and cannot be considered as evidence

Note: In most computer forensics tools, raw format image files do not contain metadata. For raw acquisitions, therefore, a separate manual validation is recommended at the time of analysis.

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

Windows does not have built-in hashing algorithm tools for validating acquired data as part of computer forensics. Instead, Windows based systems use several third-party programs to validate the data. These programs range from hexadecimal editors, like X-Ways WinHex, Breakpoint Software, Hex Workshop, etc. to computer forensics programs, like ProDiscover, EnCase, AccessData FTK, etc.

Commercial forensics programs consist of built-in data validation options, and every program has its own validation technique, which it uses on the acquired data in a proprietary format. For e.g., ProDiscover's .eve files contain the metadata in segmented files or acquisition files including the hash value for the suspect drive or partition. ProDiscover hashes the Image loaded into it as input and compares its hash value to that of the stored metadata. If the hashes do not match, then, ProDiscover alerts that the acquisition is corrupt and not reliable for evidence. This hash function is the Auto Verify Image Checksum. In most of the forensic tools, raw format image files do not contain metadata. Instead, the investigator needs to perform a manual validation for all raw acquisitions during analysis. The raw format acquisitions validation file generated before analysis is essential for the digital evidence integrity. This validation file can later help the investigator to verify whether the acquisition file is in a proper condition or not.

In FTK Imager, when the investigator selects the Expert Witness (.e01) or the SMART (.s01) format, the tool shows extra options for validation. This validation report also contains the MD5 and SHA-1 hash values. The tool applies MD5 hash value to the segmented files or proprietary format image. After loading this image into the forensics tools, the tool reads MD5 hash and compares it with the image to check the integrity of the acquired data.



Acquisition Best Practices (Cont'd)





Save open files to an **external hard drive or a network share**; if it is not possible, save them with new names

When **shutting down** Windows or Linux/Unix, perform a normal shutdown to **preserve log files**

Do not disconnect **electrical power** to a **running system** unless it is an older Windows 9x or MS-DOS system

Collect **documentation and media** related to the investigation such as **hardware, software, backup media, documentation, manuals, etc.**


Use **specialized read-only equipment** such as **Tableau Write Blocker, etc.**

Look for information related to the **investigation** such as passwords, passphrases, PINs, bank accounts, etc.

Ensure that the acquired data is **authentic and reliable** form of the original evidence

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


Acquisition Best Practices (Cont'd)

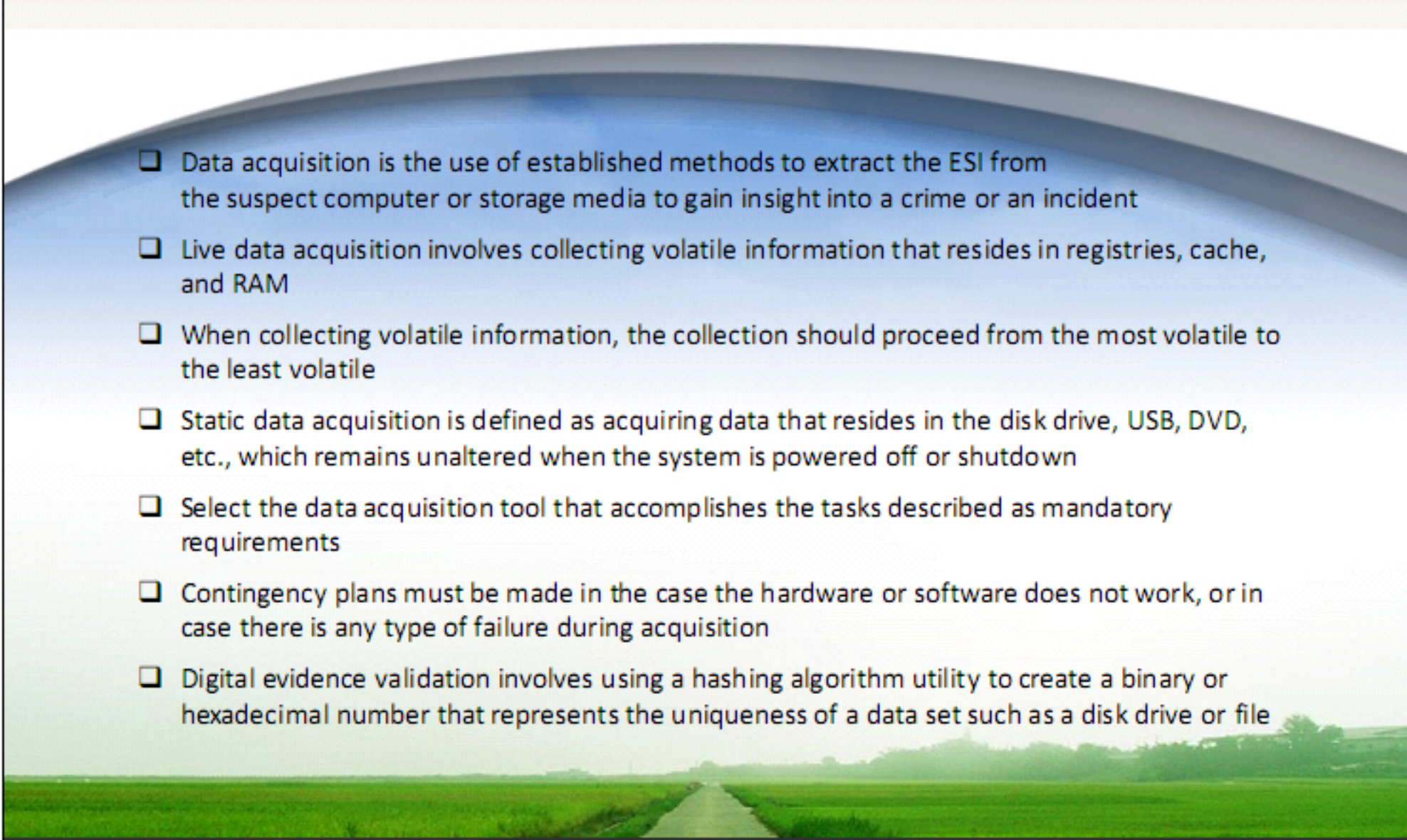


- 01 Make sure that the **chain of custody** is protected all the time
- 02 Never **manipulate** live systems, this might destroy critical evidence
- 03 Examine all the **peripherals** (Printers, WAP's, PDA's, Fax machines, etc.)
- 04 Record the **model and serial numbers** of the system and its components
- 05 Secure the scene by being **professional**, and **courteous** to onlookers
- 06 Save data from **current applications** as safely as possible
- 07 Record all **active windows** or shell sessions

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

Module Summary





- ☐ Data acquisition is the use of established methods to extract the ESI from the suspect computer or storage media to gain insight into a crime or an incident
- ☐ Live data acquisition involves collecting volatile information that resides in registries, cache, and RAM
- ☐ When collecting volatile information, the collection should proceed from the most volatile to the least volatile
- ☐ Static data acquisition is defined as acquiring data that resides in the disk drive, USB, DVD, etc., which remains unaltered when the system is powered off or shutdown
- ☐ Select the data acquisition tool that accomplishes the tasks described as mandatory requirements
- ☐ Contingency plans must be made in the case the hardware or software does not work, or in case there is any type of failure during acquisition
- ☐ Digital evidence validation involves using a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set such as a disk drive or file

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

In this module, we have learned about different types of storage processes, different systems use to store the data, and different methods of data acquisition from digital media. The module also discusses the process of handling volatile and non-volatile information in various parts of a system and ways to extract them without any losses. It defines the different data types present across various devices and the methods to extract them in a legally sound manner.

The module discusses software and hardware tools that aid the investigators in finding, extracting, storing and managing different data types as well as processes to validate the evidence. It contains guidelines for efficient extraction of evidence related data. In the next module, we will learn various anti-forensics methods used by investigators and methods to overcome them.