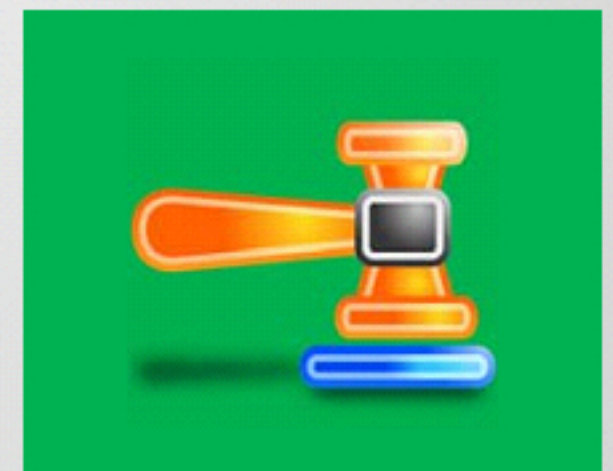


Data Acquisition and Duplication

Module 04

Designed by **Cyber Crime Investigators**. Presented by Professionals.



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

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



Live Data Acquisition

One chance to collect

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

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 DLL s 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

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

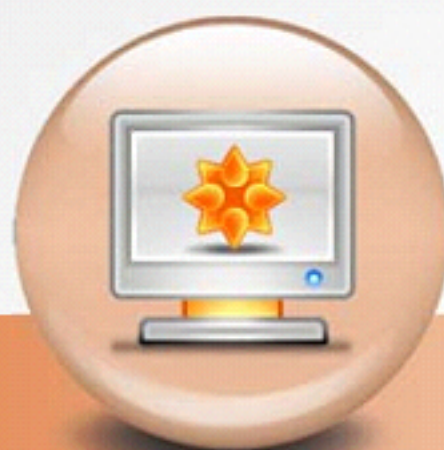
7

Archival media

Common Mistakes in Volatile Data Collection



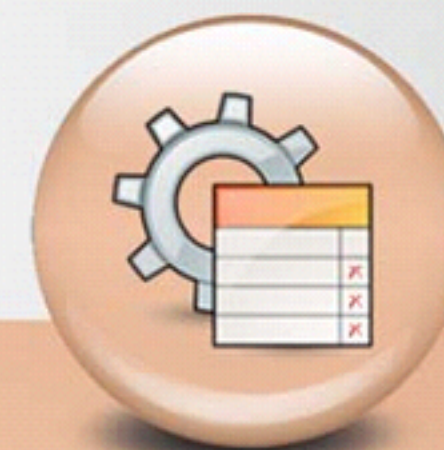
Assuming that some parts of the **suspicious machine** may be reliable and usable (Using native commands on the suspicious computer may trigger time bombs, malware, and Trojans to delete key volatile data)



Shutting down or rebooting the suspicious computer (connections and running processes are closed, and MAC times are changed)



Not having access to **baseline documentation** about the suspicious computer



Not documenting the **data collection process**

Volatile Data Collection Methodology

Step 1

Incident Response Preparation

The following items should be in place before an incident occurs:

- A **first responder toolkit** (response disk)
- An **incident response team (IRT)** or a designated first responder
- Forensics-related policies that allow for forensic collection



Step 2

Incident Documentation

- Ensure the generated logs, and profiles are **organized** and **readable**
- Document all the information about the security incident and use a logbook to record all the actions performed during **data collection**
- Use the first responder toolkit logbook to determine the **tools** appropriate for the situation

Step 3

Policy Verification

- Ensure the actions you plan to take do not violate **existing network** and **computer usage policies**
- Do not **violate** any rights of the registered owner or user of the suspicious system



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

Volatile Data Collection Methodology (Cont'd)

Step 6



Volatile Data Collection Process

- 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

Static Data Acquisition

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

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

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



Original Hard Disk

Duplicating



Duplicate Hard Disk

Only One Chance to Do it Right



Bit Stream Image Vs. Backups

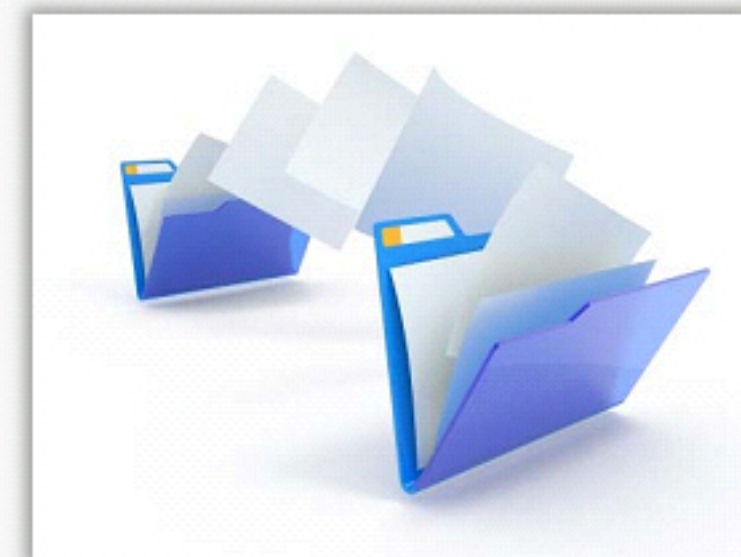
Bit Stream Image

- 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

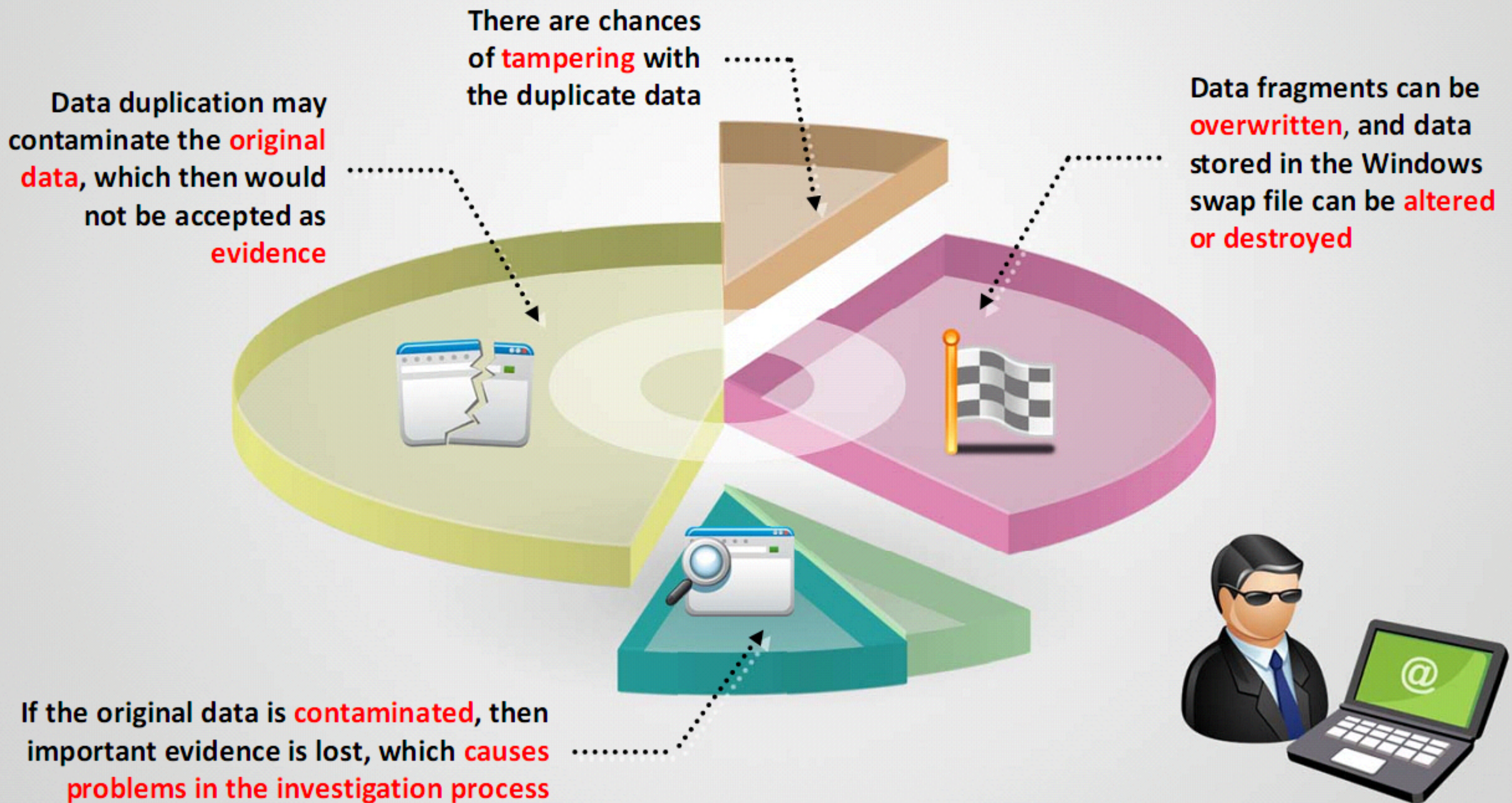


Backups

- 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



Issues with Data Duplication



Data Acquisition and Duplication **Steps**

1 Prepare a Chain of Custody document

2 Enable Write Protection on the Evidence Media

3 Sanitize the Target Media

4 Determine the Data Acquisition Format

5 Determine the Best Acquisition Method

6 Select the Data Acquisition Tool

7 Acquire the Data

8 Plan for Contingency

9 Validate Data Acquisitions

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:	



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.

Sanitize the Target Media: NIST SP 800-88 Guidelines

A proper **data sanitization method** must be utilized to remove the previous information permanently from the target media before data duplication

<http://www.nist.org>

Information systems **capture, process, and store** information using a wide variety of media

Information is located not only on the intended storage media but also on **devices** used to create, process, or transmit this information

This media may require **special disposition** in order to mitigate the risk of unauthorized disclosure of information, and ensure its confidentiality

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

- Fast **data** transfers
- Can ignore minor data read errors on **source drive**
- Most computer forensics tools can **read raw format**

Disadvantages

- Requires as much **storage** as original disk or data set
- Tools (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.

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:

- Option to compress or not compress image files of a source drive to **save space on the target drive**
- Ability to **split an image** into smaller **segmented files** to archive, such as to CDs or DVDs with data integrity checks integrated into each segment
- Ability 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.

Disadvantages include:

- Inability to share images** between different computer forensics analysis tools
- File size limitation** for each segmented volume



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

- **No size restriction** for disk-to-image files
- Generates **compressed or uncompressed** image files
- Provides **space for metadata** in image files or segmented files

- **Simple design** with extensibility
- Open source for **multiple computing** platforms and OSs
- Deals internal consistency checks for **self-authentication**



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

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 Bradly 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



Determine the **Data Acquisition Format** (Cont'd)

Generic Forensic Zip (gzfile):

gzfile 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://gzfile.nongnu.org>

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



Data Acquisition Methods (Cont'd)

Logical Acquisition or Sparse Acquisition

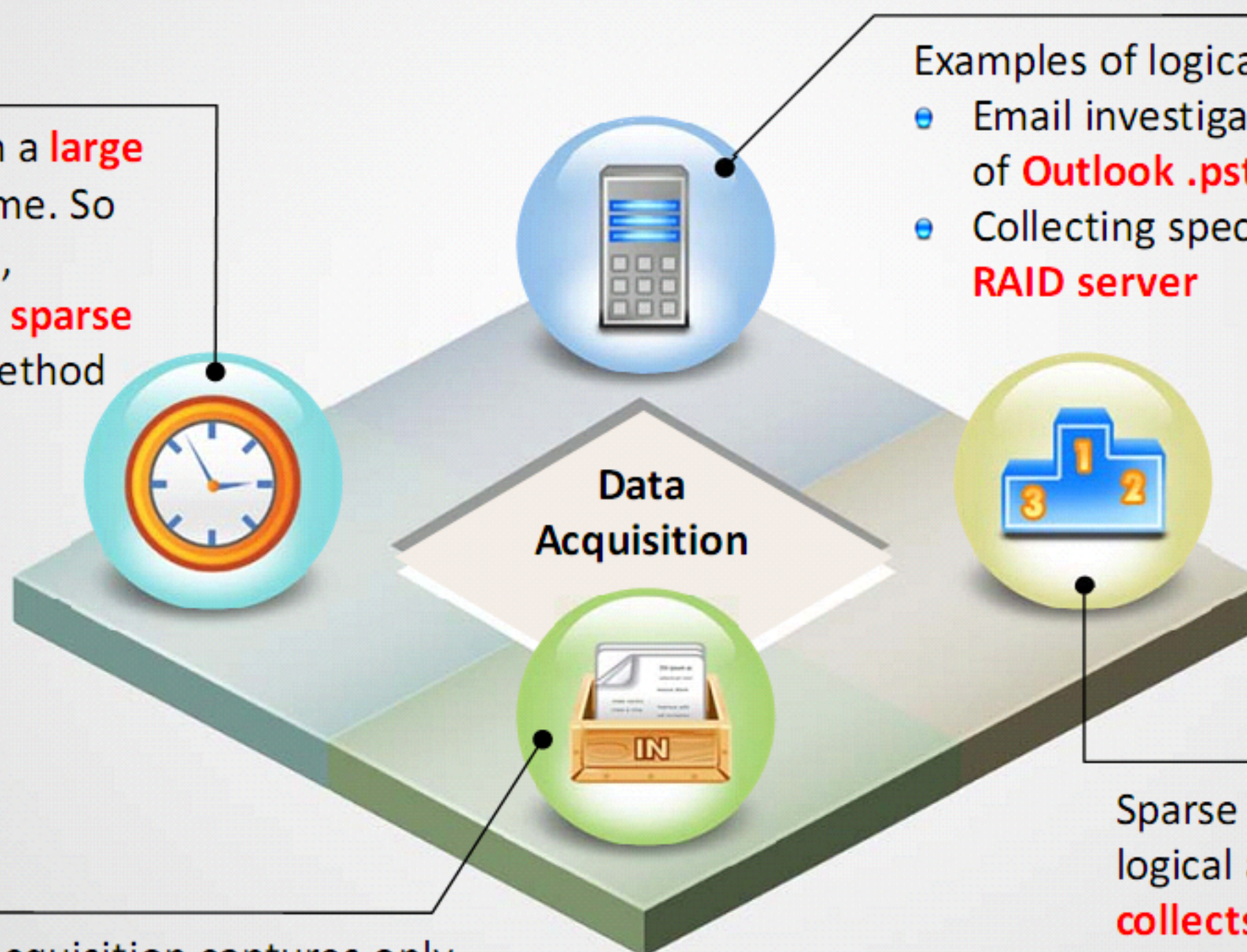
Evidence collection from a **large drive** consumes more time. So when the time is limited, consider using **logical or sparse acquisition** data copy method

Examples of logical acquisition include:

- Email investigation that requires collection of **Outlook .pst or .ost files**
- Collecting specific records from a large **RAID server**

Logical acquisition captures only **specific types of files** or files of interest to the case

Sparse acquisition is almost like logical acquisition. In addition, it **collects fragments of unallocated (deleted) data**. Use this method when inspection of the entire drive is not required



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

Determine the **Best Acquisition Method** (Cont'd)

Whether you can retain the disk

2

- 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

Investigator acquiring data from disk/drive



System

When the drive is very large

3

- 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**

Select the Data Acquisition Tool: Mandatory Requirements

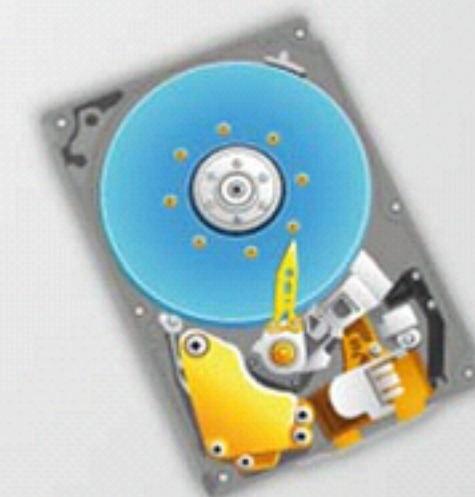
Based on disk imaging, tool requirements are divided into **two categories** – mandatory requirements and optional requirements



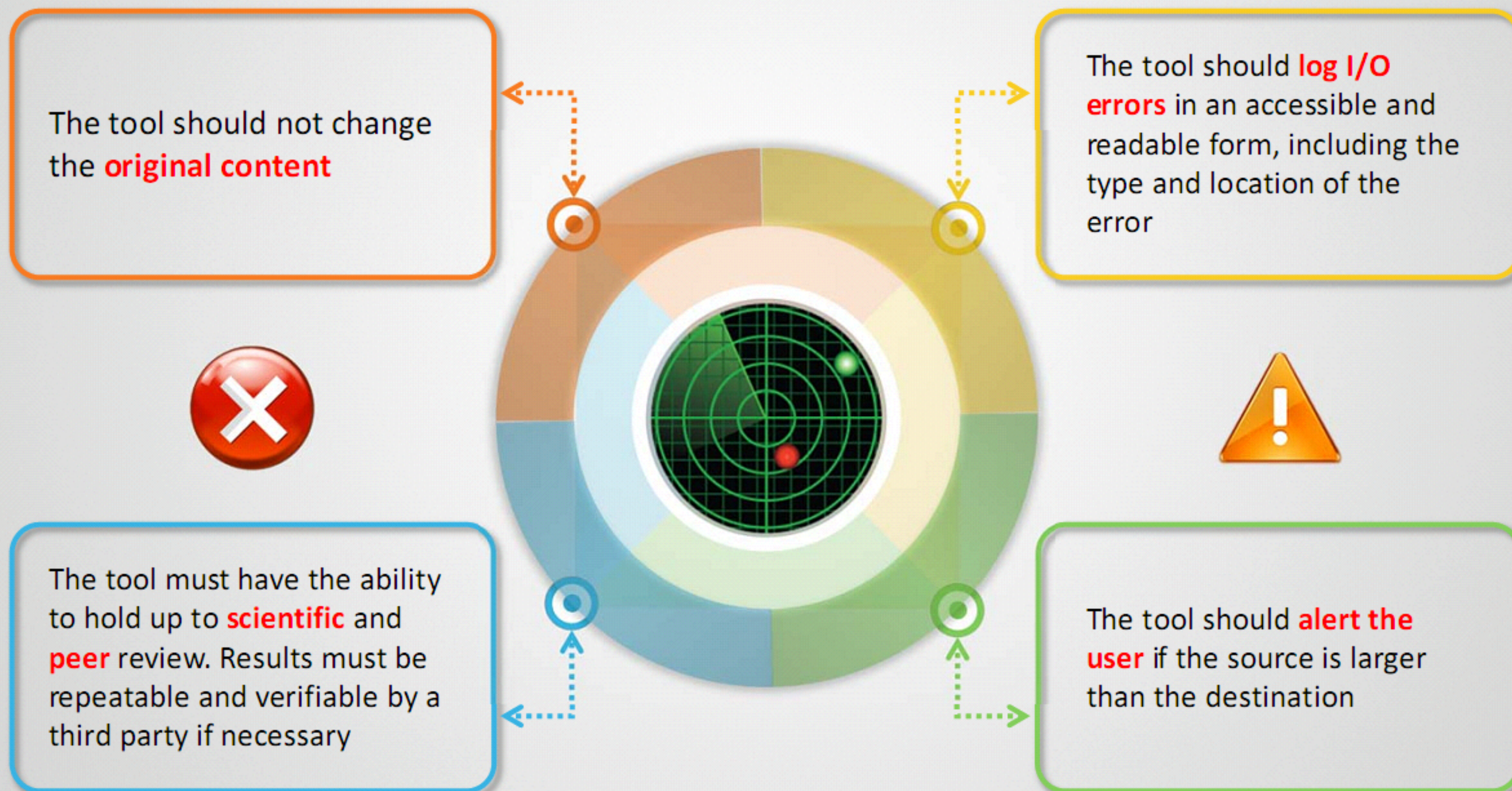
All disk imaging tools must accomplish the tasks described as **mandatory requirements**



The tools may or may not provide the features discussed under the **optional requirements' head**



Select the Data Acquisition Tool: Mandatory Requirements (Cont'd)



Select the Data Acquisition Tool: Mandatory Requirements (Cont'd)

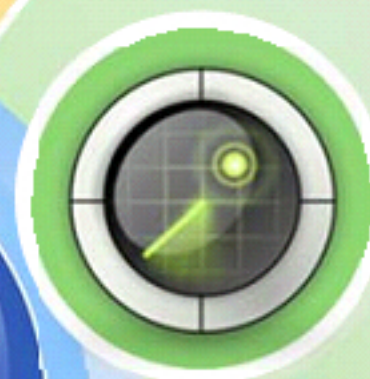
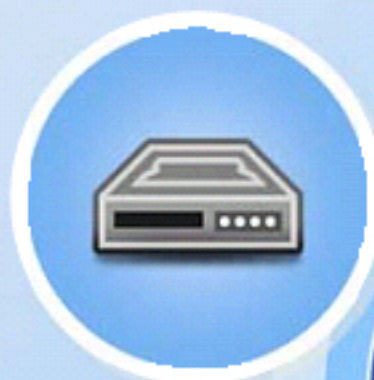


The tool must be able **to access disk drives** through one or more **interfaces** (Interfaces include direct access to the disk controller, Interrupt 13 BIOS interface, Interrupt 13 BIOS extended interface, ASPI SCSI interface, or LINUX interface)

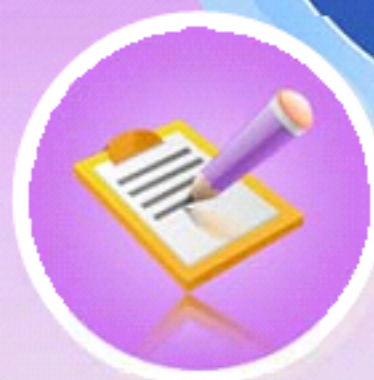
The tool should create a **bit stream copy** of the original content when there are no errors in accessing the source media



The tool should create a **qualified bit stream copy** (A qualified bit-stream copy is defined as a duplicate except in identified areas of the bit-stream) when I/O errors exist in accessing the source media



The tool should copy a file only when the destination is larger or equal to the size of the source, and should **document** the contents on the destination that are not a part of the copy



Tool documentation should be **correct**, i.e., the user should get expected results by implementing it in accordance with the tool's documented procedures

Select the Data Acquisition Tool:

Optional Requirements



The tool shall **compute a hash value** for the complete bit stream copy generated from an image file of the source, compare the computed hash with that of the original source hash value computed at the time of image creation, and display the result of comparison on a disk file



The tool shall **divide the bit stream copy into blocks**, compute hash values for each block, compare them with the hash value of original block of source data computed at the time of image creation, and display the result of the comparison on a disk file



The tool shall **log one or more items on a disk file** (items include tool version, subject disk identification, any errors encountered, tool actions, start and finish run times, tool settings, and user comments)



The tool shall create a qualified bit-stream duplicate, and **adjust the alignment of cylinders** to cylinder boundaries of disk partitions on a destination of a different physical geometry

Select the Data Acquisition Tool: Optional Requirements (Cont'd)

The tool shall create a bit stream copy of **individual partitions** as per user direction



The tool shall make the source **disk partition table** visible to users, and record its contents



The tool shall create an **image file** on a fixed or removable magnetic or electronic media that is used to create a bit-stream copy of the original



The tool shall create a bit-stream copy on a platform that is connected through a **communications link** to a different platform containing the source disk

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>

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

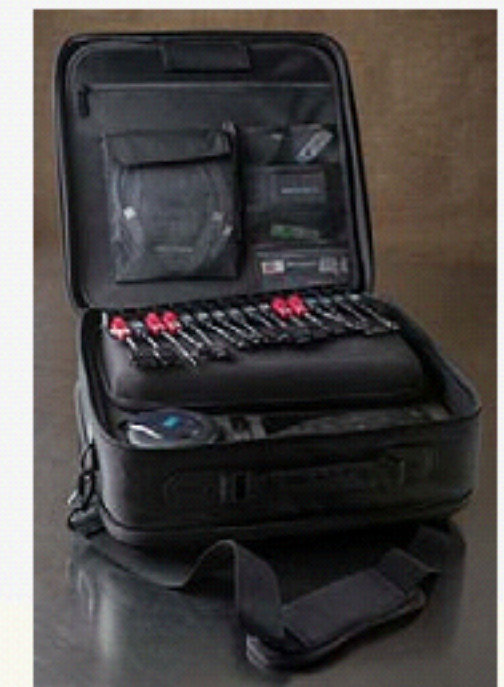


<http://www.atola.com>

XRY Office

It allows investigators to recover data from a mobile device

<https://www.msab.com>



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



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.deepspar.com>



Forensic Tower IV Dual Xeon

<http://www.forensiccomputers.com>

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



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>

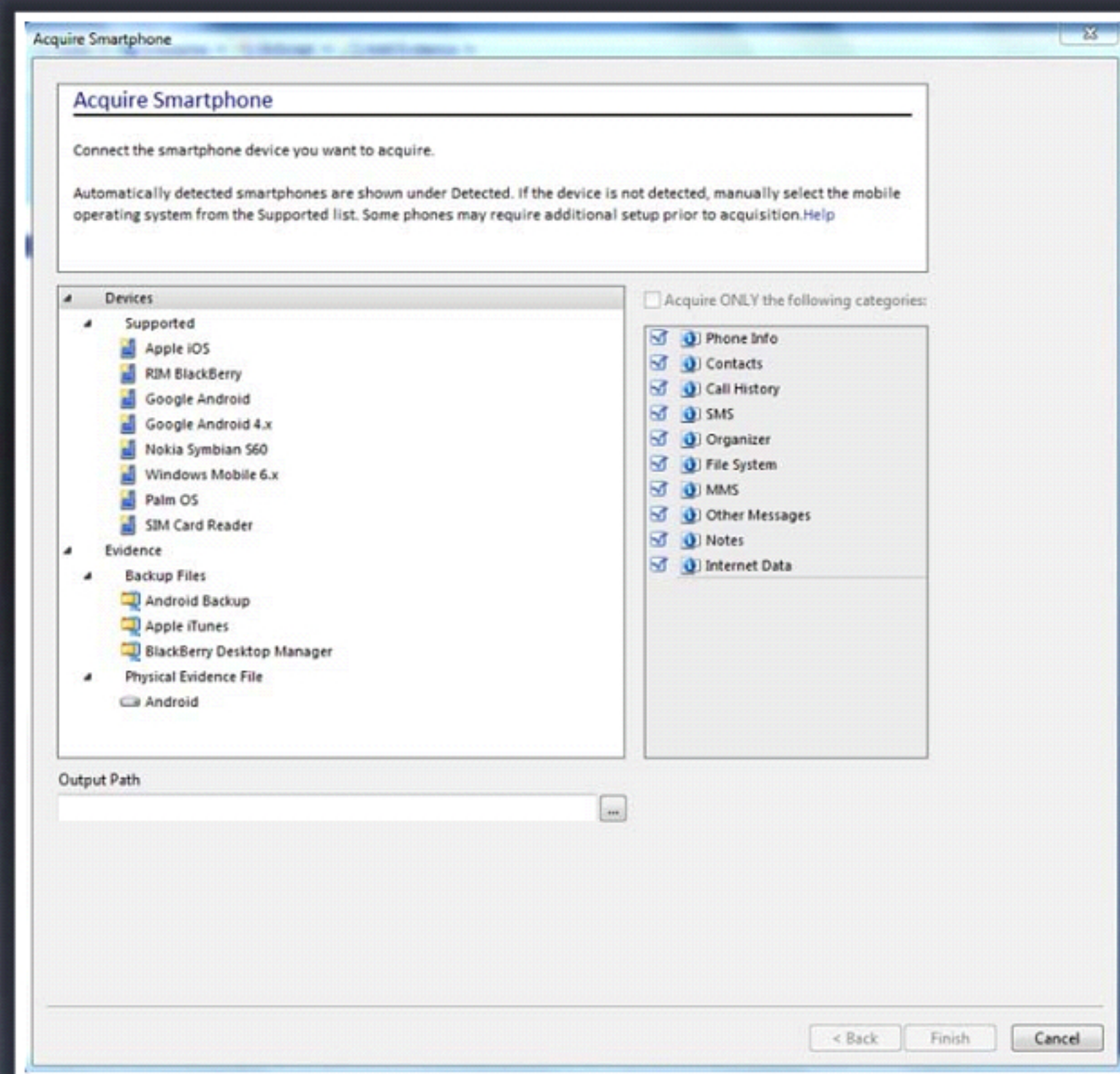
Data Acquisition and Duplication

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>

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>



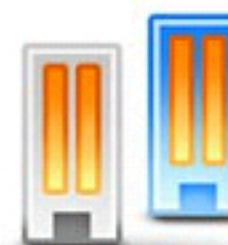
Flash Retriever Forensic Edition

<http://www.infinadyne.com>



R-Tools R-Studio

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



Forensic Replicator

<https://www.paraben.com>

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



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>

Linux Standard Tools

1

Forensic investigators use the built-in Linux commands **dd** and **dcfldd** to copy data from a disk drive

2

These utilities can make a **bit-stream** disk-to-disk copy, disk-to-image file, block-to-block copy/ block-to-file copy

3

The **dd** command can **copy data from any disk** that Linux can mount and access

4

Other forensics tools such as **AccessData FTK** and **EnCase** can read **dd** image files

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
```

Copy one hard disk partition to another hard disk:

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

2

3

Make an ISO image of a CD:

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

Restore a disk partition from an image file:

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

4

5

Copy RAM memory to a file:

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


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
```

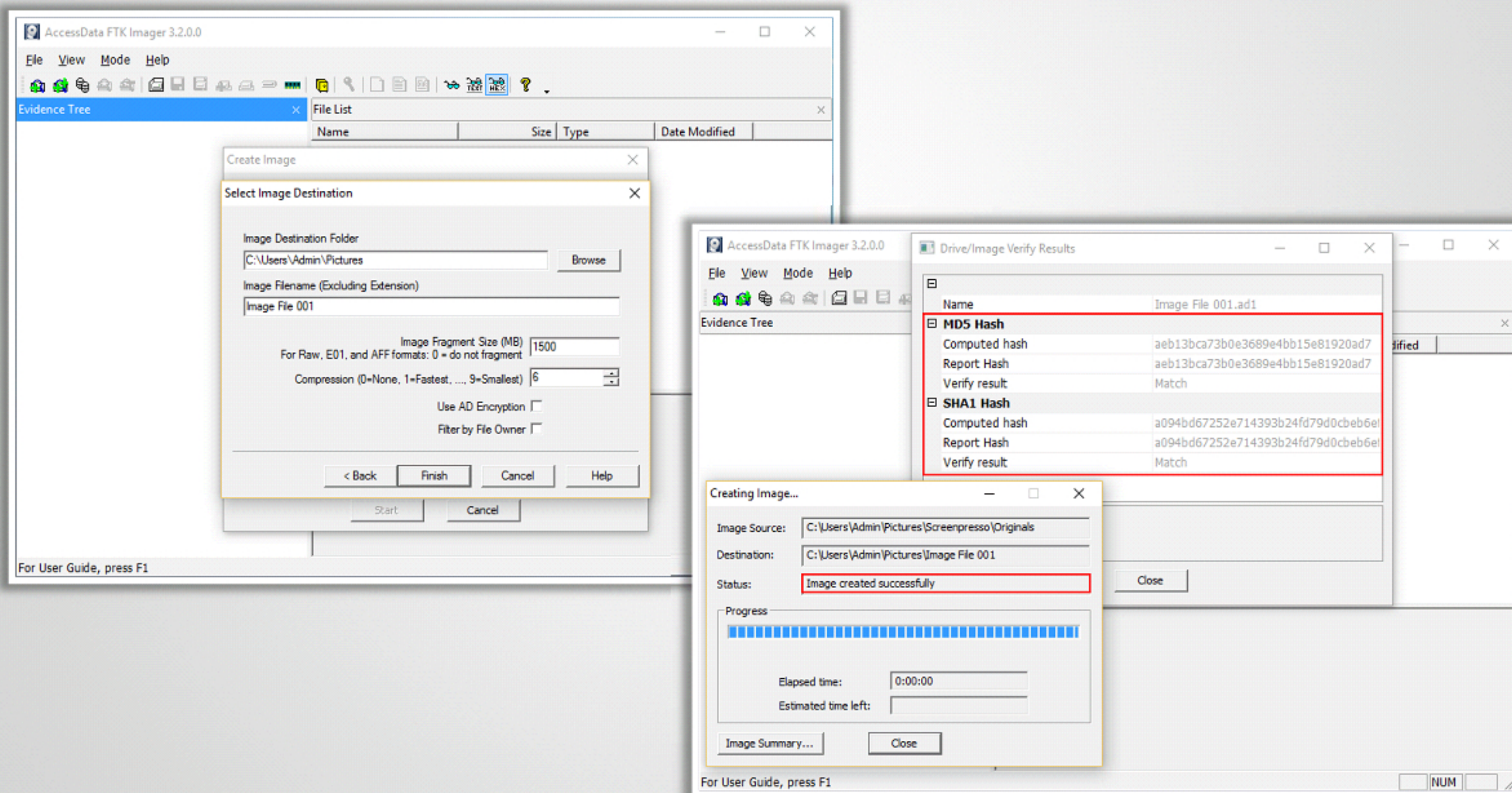
If the disk or suspect media is to be segmented, use the dcfldd command with the split command, placing split before the output file field as shown below:

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

This command generates segmented volumes of 2MB each

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



<http://accessdata.com>

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:



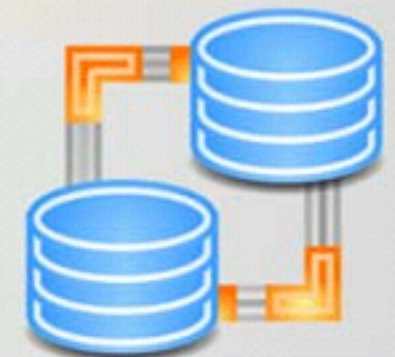
How much **data storage** is needed to obtain complete data for a forensics image?



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?

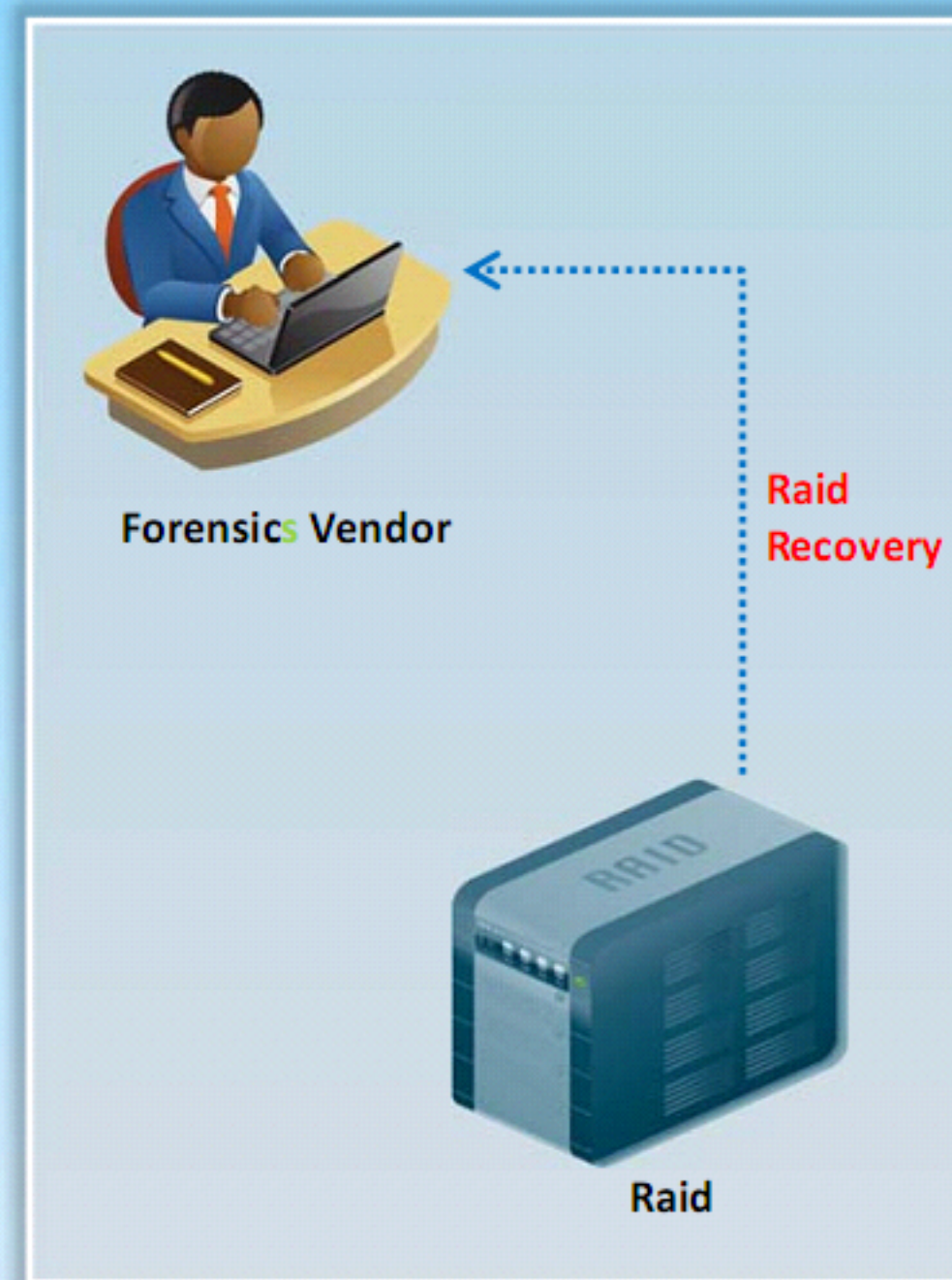


Can the tool read split data saves of each RAID disk and combine all images of each disk into one RAID virtual drive for analysis?

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

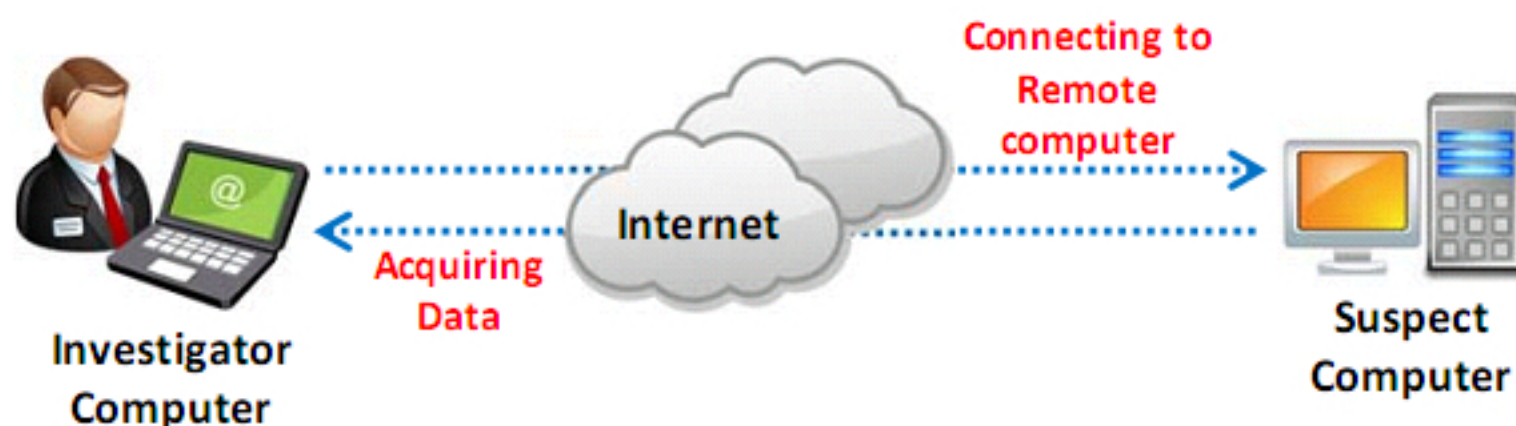
Acquiring RAID Disks (Cont'd)

- 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



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)



Data Acquisition Mistakes



An investigator may commit some common mistakes while **collecting data** from the system that result in the loss of **critical evidence**. Common mistakes investigators commit include:

Choosing
wrong
resolution
for data
acquisition



Use of
wrong
cables and
cabling
techniques



Insufficient
time for
system
development



Making the
wrong
connections



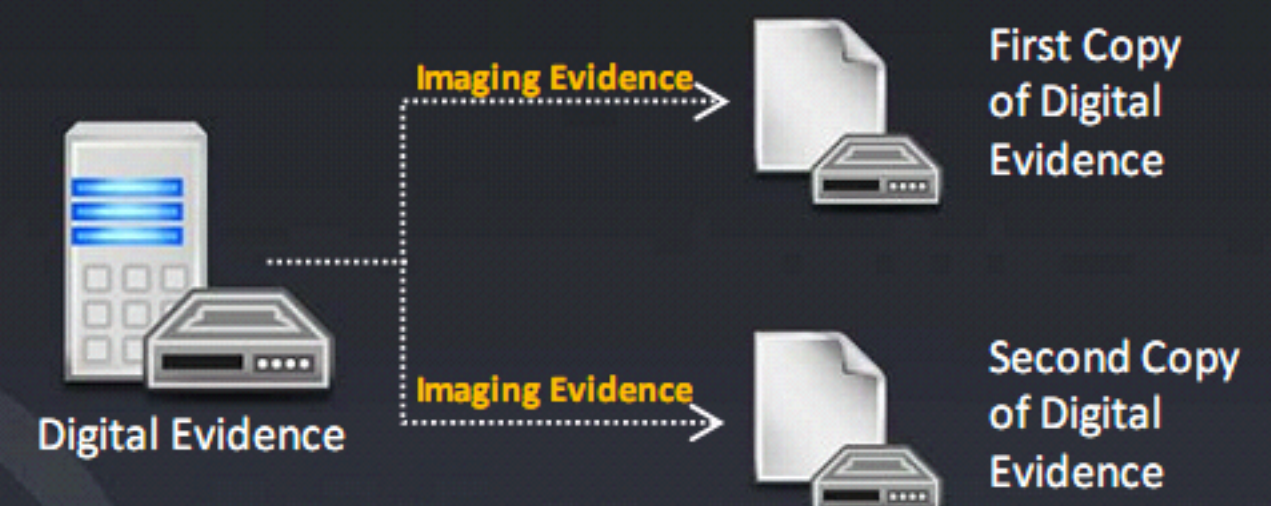
Poor
knowledge
of the
instrument



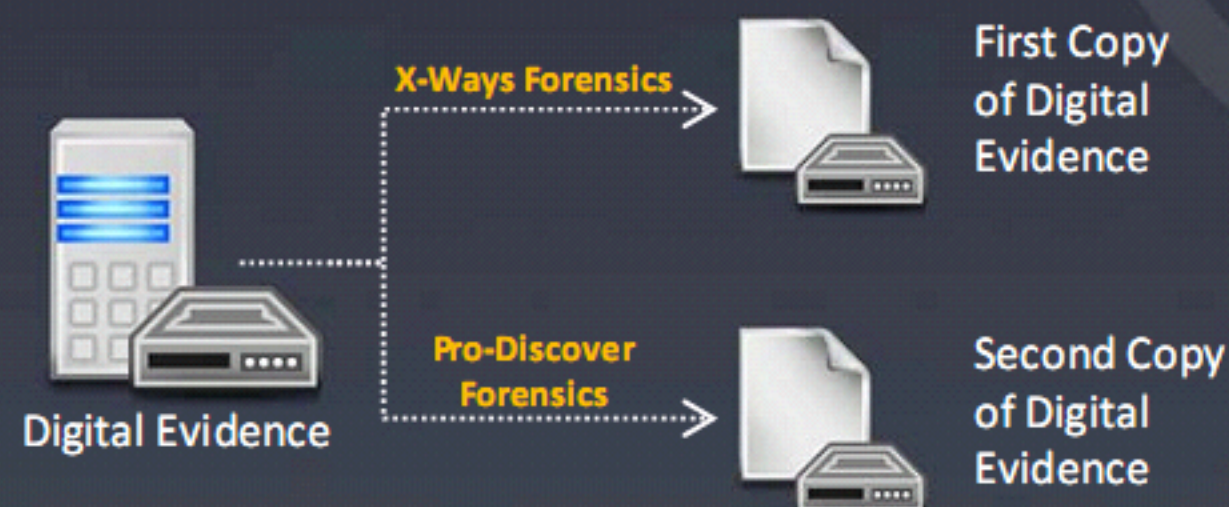
Plan for Contingency

Investigators must make contingency plans in case the **hardware or software does not work**, or in case there is any type of failure during acquisition

Investigators need to make at least **two images of the digital evidence** collected, in order to preserve it. In that way, if one copy of the digital evidence recovered is corrupt, investigators can use the second copy



Hard Disk Data Acquisition



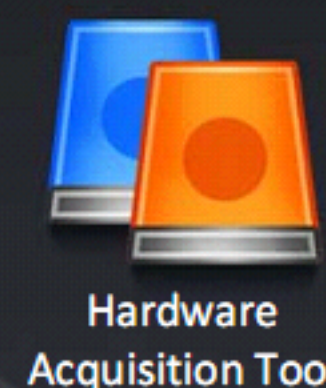
Imaging Tools



If you possess more than one **imaging tool**, such as Pro-Discover, FTK, and X-Ways Forensics, etc., make the **first copy with one tool** and the **second copy with the other tool**. If you possess only one tool, make two images of the drive using the same tool

Plan for Contingency (Cont'd)

Consider using a hardware acquisition tool (such as **Pro-Discover Basic** with the NoWrite FPU write-blocker, or **IM SOLO-4 G3 IT RUGGEDIZED**) that can **access the drive at BIOS level** to copy data in the Host Protected Area (HPA)



Accessing Drive at
BIOS Level



Hard Disk



Hardware Acquisition Tool

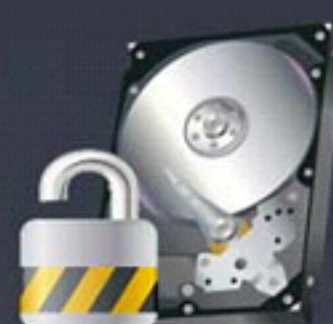
Drive Decryption



Encrypted Drive



Decryption Key



Decrypted Drive

Be prepared to deal with encrypted drives that needs the user to provide the **decryption key** for decrypting. Microsoft included a full disk encryption feature (BitLocker) with select editions of Windows Vista and later

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



- Utility algorithms that produce hash values include **CRC-32, MD5, SHA-1, and SHA-256**

- **CRC-32:**

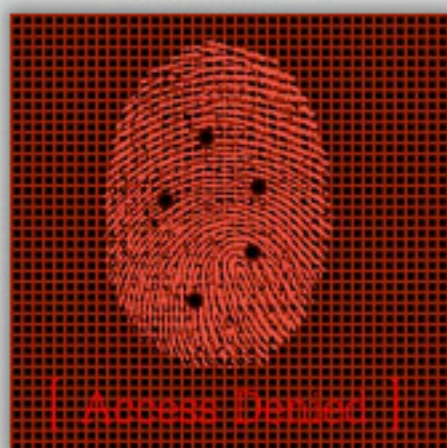
It is a 32-bit CRC code used as an error detection method during data transmission. If the computed CRC bits are identical to the original CRC bits, it means that no error occurred

- **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



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

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

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

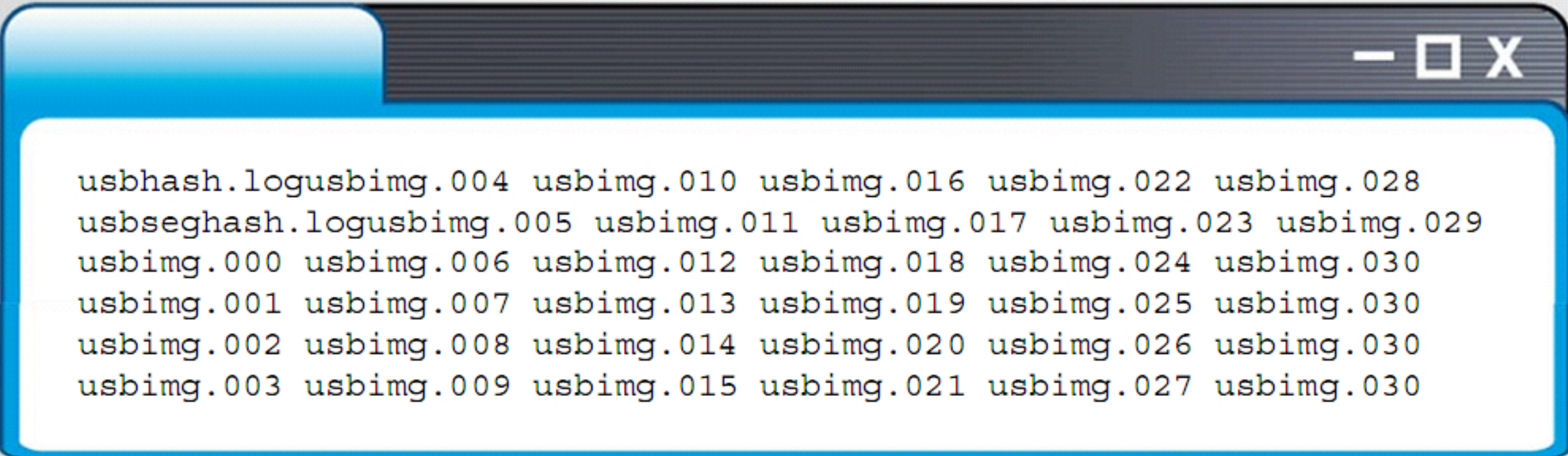
Enter the following command at the shell prompt to create an MD5 hash output file during dcfldd data acquisition:

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



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
```



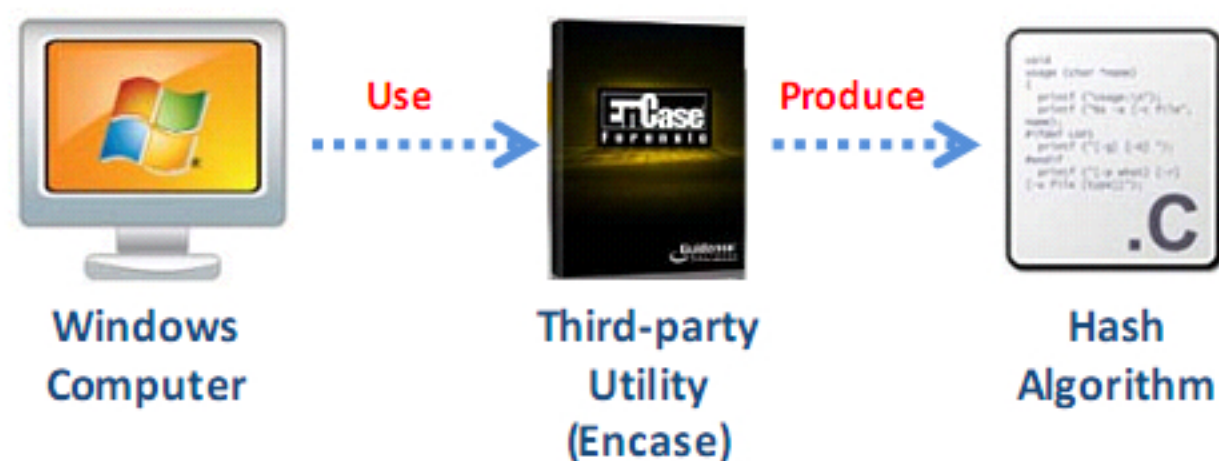
- The **vf** (Verify File) option is another **dcfldd** command that compares the image file to the original medium such as a drive or partition. It is applicable only to the **non-segmented image file**. Enter the following command at the shell prompt to use the **vf** option:

```
dcfldd if=/dev/sd vf=sda_hash.img
```

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

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



- 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.

Acquisition Best Practices



Permit only authorized personnel to **access**



Do not turn the system "**ON**" if it is "**Off**"



Maintain list of individuals involved in the **search**



Place all the magnetic media in **antistatic packages**



Note when the system was last **accessed**



Properly label the containers used to hold **evidence**



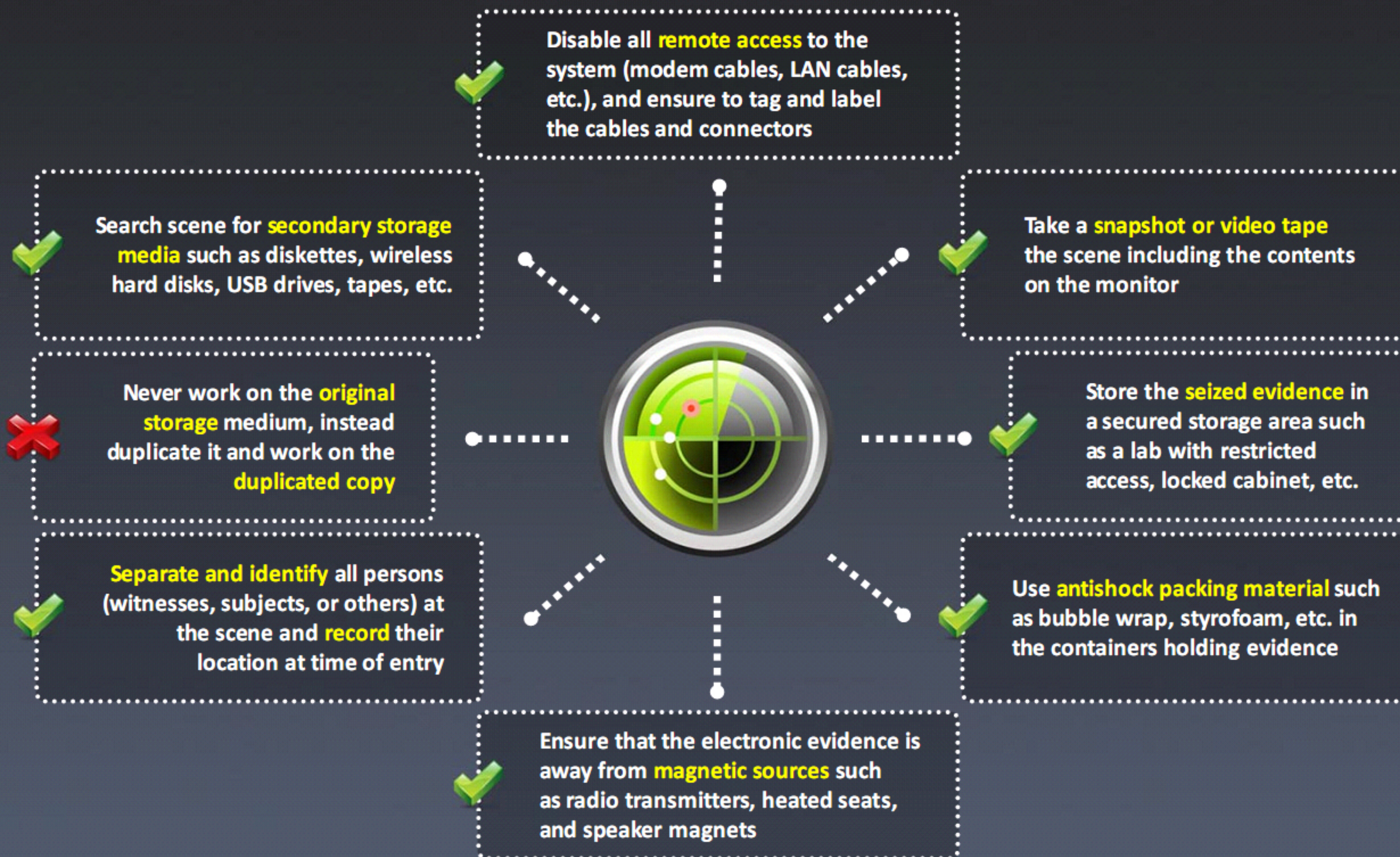
Establish a **chronology** of access to the media



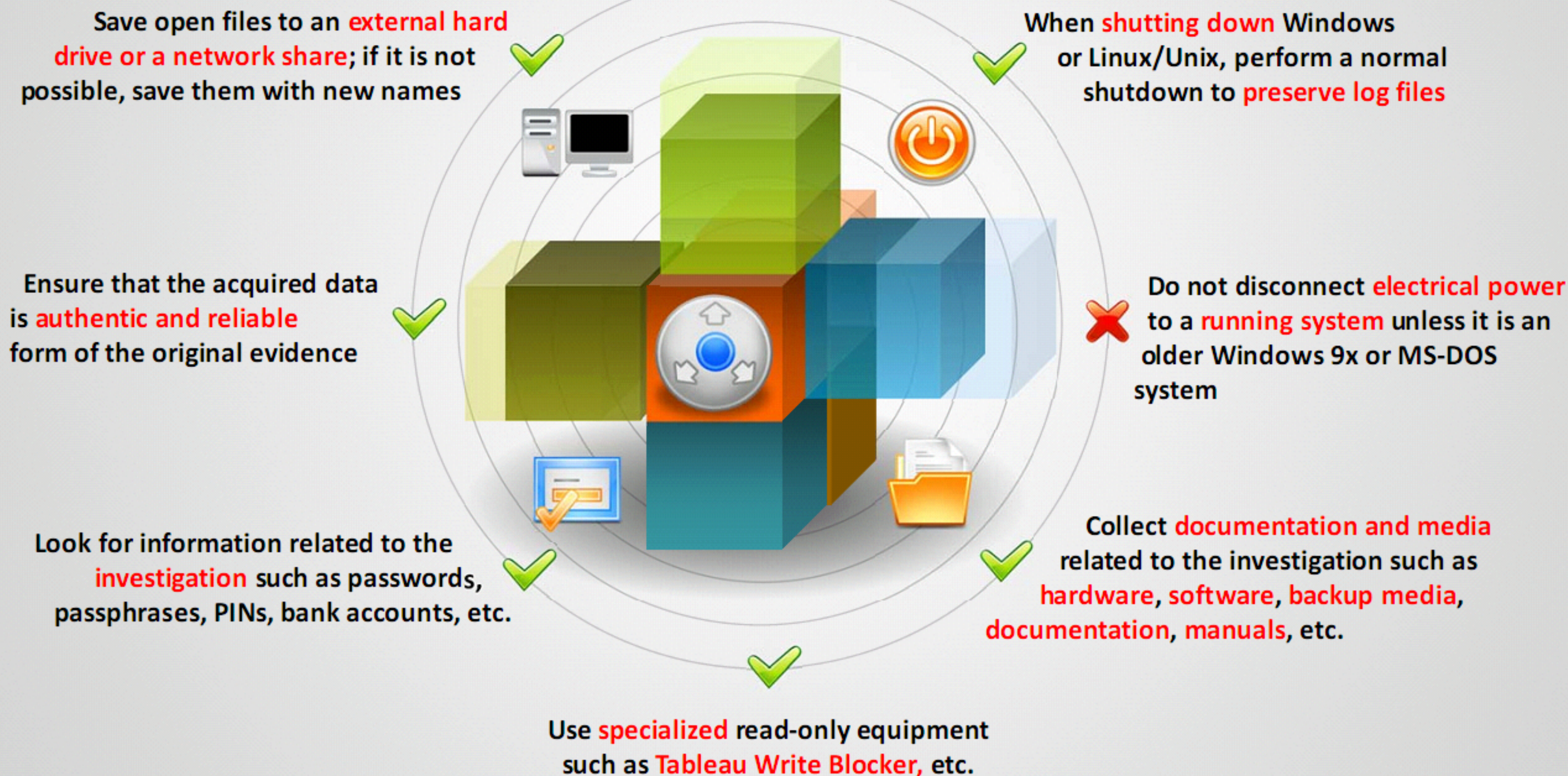
Protect the evidence from **extreme temperatures**










Acquisition Best Practices (Cont'd)



Acquisition Best Practices (Cont'd)



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 

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