iNurture
Education Solutions
TOMORROW'S HERE

*Chapter .2.2*

# Data Recovery Methods

# Aim

To equip the students with the basics of forensic data recovery and the methods of recovery, as well as data acquisition

# Instructional Objectives

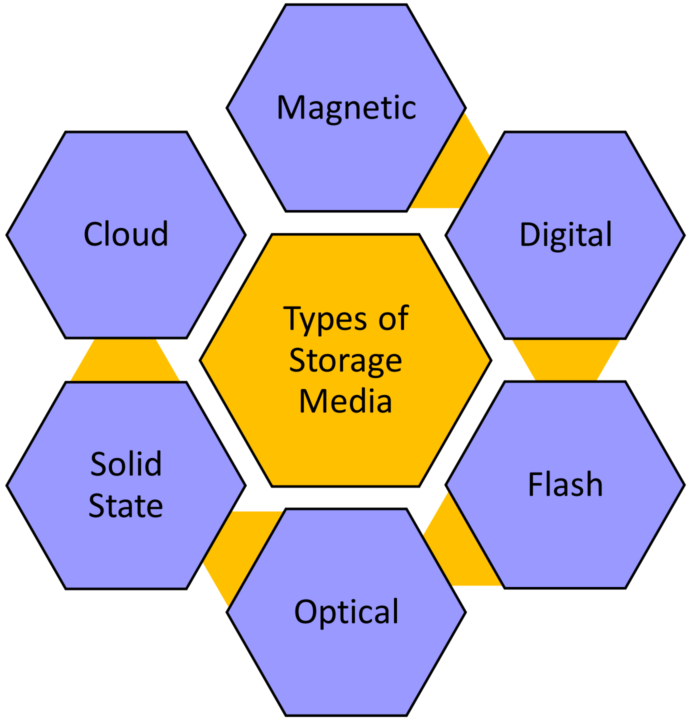
After completing this chapter, you should be able to:

- Explain the concept of forensic data recovery
- Outline the important factors of Data Acquisition
- Explain the steps involved in data deletion
- Illustrate the various data recovery methods and techniques

# Introduction to Data Recovery Methods

# Types of Storage Media

Computer devices are used by us in our daily life. These devices use various methods of data storage media. They are as follows:



# Forensics Data Recovery

# What is Forensic Data Recovery?

Recovering data from a damaged drive which was due to overheating, hardware failure, or accidental damage is known as forensic data recovery.

Forensic Investigator

# Main causes of Data Deletion

The main causes of data deletion is listed below:

- Intentional Action
- Unintentional Action
- Disc Failure
- Natural Disaster
- Criminal Action

# Quiz / Assessment

1) ______________ is the process of retrieving inaccessible or corrupt data, from various digital media storage devices.

a) Data recovery
b) Digital recovery
c) Evidence recovery
d) Acquisition recovery

# Quiz / Assessment

2) Which one of the following is a main cause for data deletion?

a) Evidence action
b) Intentional action
c) Duty action
d) Examine action

# Quiz / Assessment

3) __________ can become corrupt due to overheating, hardware failure, or accidental damage.

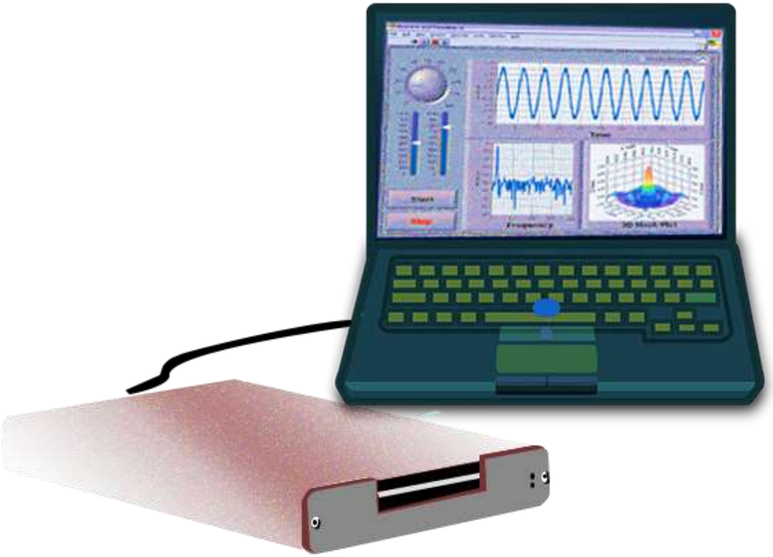
a. Exposure drives
b. Storage drives
c. Data drives
d. Forensic drives

# Data Acquisition

# Data Acquisition

The first step in the forensic process is to identify and acquire possible digital evidence from various sources. This is known as data/evidence acquisition.

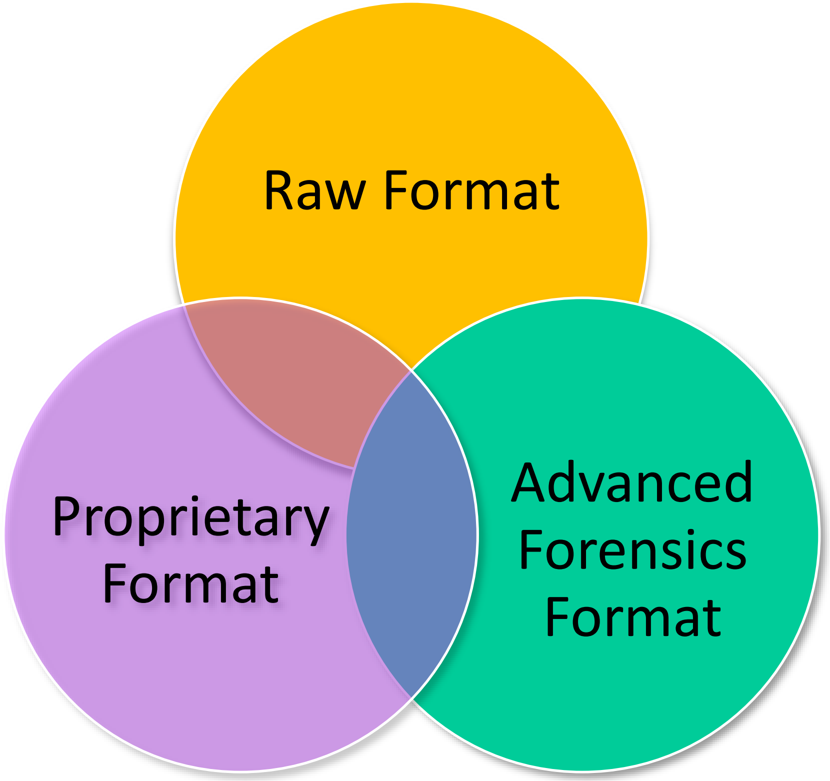
***For Example***, Data acquired from a storage device such as an USB device is stored in a data file. The acquisition tool performs bit by bit copy of the USB drive and writes it to an image file which will the exact replica/duplicate of the source device.



*Data Acquisition*

# Digital Evidence Storage Formats

There are various formats in which digital evidence can be acquired and stored for further assessment. The three most popular methods are:



# Acquisition Tools

Acquisition tools are used to analyze digital data and often find evidence that someone did or did not commit a crime. As the tool output may be evidence introduced in a court trial, it must meet certain legal requirements. Various acquisition tools are as follows:

- Encase
- Forensic Toolkit
- Hard Drive Image

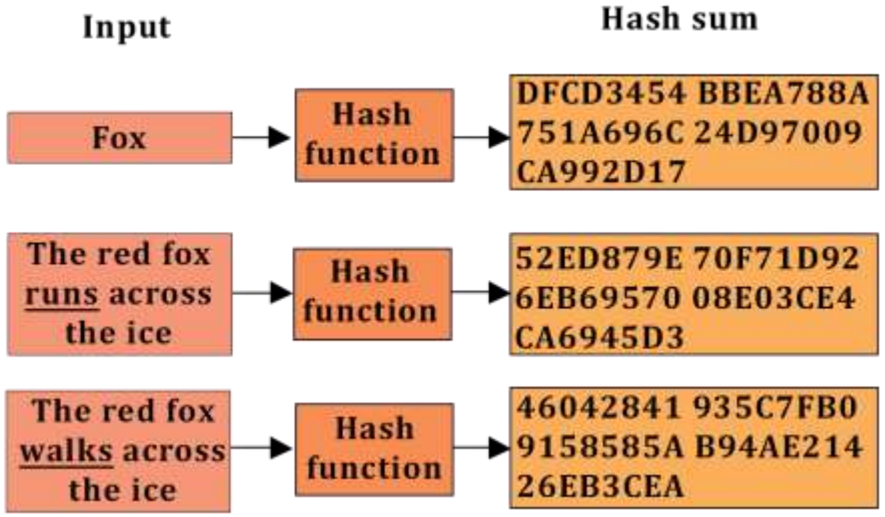
# Validating Data Acquisitions

Acquired data can be verified with the help of a cryptographic checksum of the old and the new data set or images. Various cryptographic checksums are being utilized in the industry, but the three most popular ones are:

- md5
- sha1
- Sha2

The tools for checksum verification are:

- ❑ md5sum
- ❑ Hashdeep

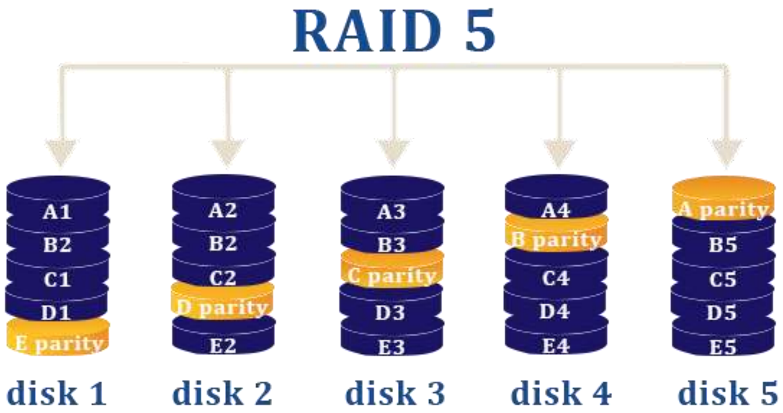

Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA

*Example of Hashdeep*

# RAID Data Acquisitions

RAID stands for Redundant Array of Inexpensive Disks, or Redundant Array of Independent Disks.

It is a virtual storage technique that combines various physical drives into a single logical unit in order to provide data redundancy and performance.

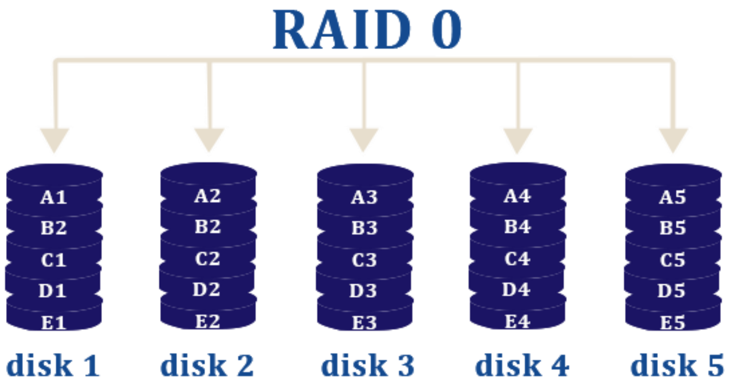


*Example of RAID 5*

# RAID Data Acquisitions

Different types of RAID data acquisition are as follows:

- RAID 0
- RAID 1
- RAID 2
- RAID 3
- RAID 4
- RAID 5
- RAID 6



*Example of RAID 0*

# Quiz / Assessment

1) The first step in the ________________is to identify and acquire possible digital evidence from various sources

a. Forensic process
b. Storage process
c. Data process
d. Drive process

# Quiz / Assessment

2) The data collected by a forensics _____________is stored as an image file, usually in an open source or proprietary format

a. Digital tool
b. Evidence tool
c. Acquisition tool
d. Source tool

# Quiz / Assessment

3) Redundant Array of Inexpensive Disks stands for ___________.

a. RAID
b. RADI
c. RIDI
d. RIDA

# Data Deletion

# Data Deletion

When a file is deleted, only the entry in the file system metadata is removed, while the actual data is still on the disk. After a format and even a repartitioning it might be that most of   raw data is untouched and can be recovered using file carving.

*Data Deletion*

# Quiz / Assessment

1) __________ is an area which saves all the deleted files on the drives.

a. Disc
b. Delete
c. Trash
d. Trojan

# Quiz / Assessment

2) __________ or tape media is reused to store data.

a. Drive
b. Disk
c. Linux
d. Digits

# Quiz / Assessment

3) __________ and disk degaussing are few ways to dispose data.

a. Media destruction
b. Media method
c. Media process
d. Media deletion

# Data Recovery Methods and Techniques

# Data Recovery

It is the process of retrieving or collecting pieces of data from a disk drive or any other type of storage media, when data cannot be accessible using normal methods.

Data Recovery Process

# Various Recovery Techniques based on the error or the corruption type

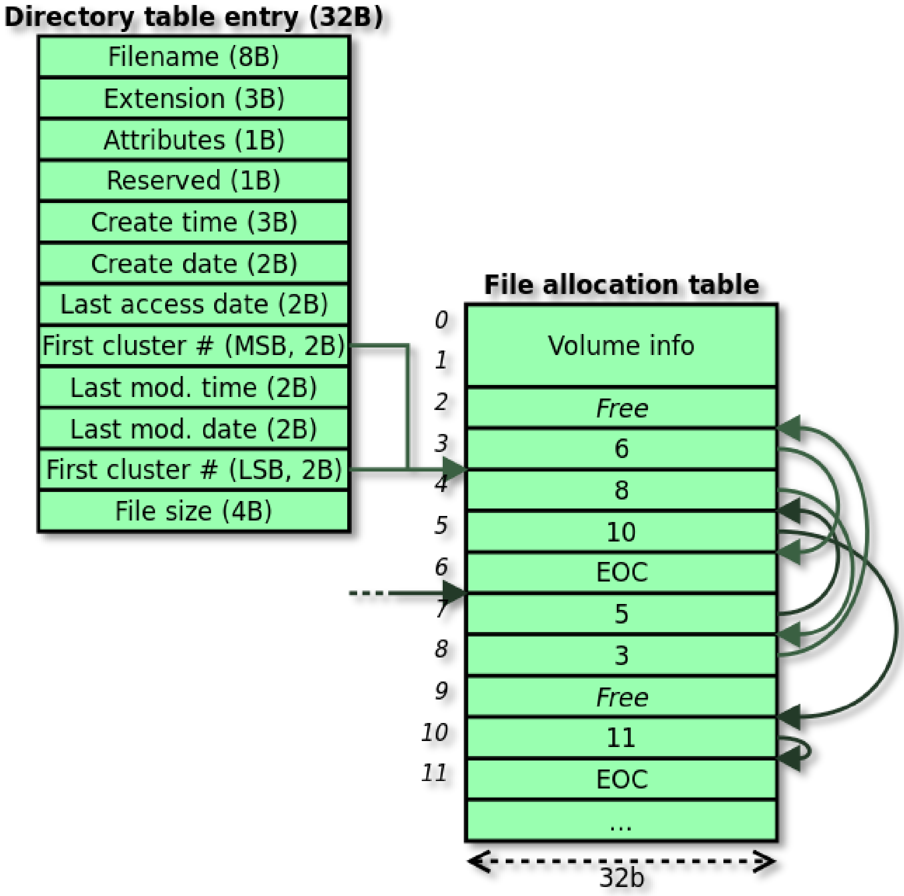
- Physical Damage
- Logical Damage
- Overwritten

# File Carving

- File carving is a specialized process to recover files without having its metadata. This can be done using raw disc access and reading each sector for identifying its contents.

- Most file systems are divided into sectors and clusters (of equal size). An example is the FAT32 file system that might be divided into various fixed size clusters of 4 KiB each.

- Any file smaller than 4 KiB fits into a single cluster, the remaining space in the cluster is called slack space.



FAT 32 structure

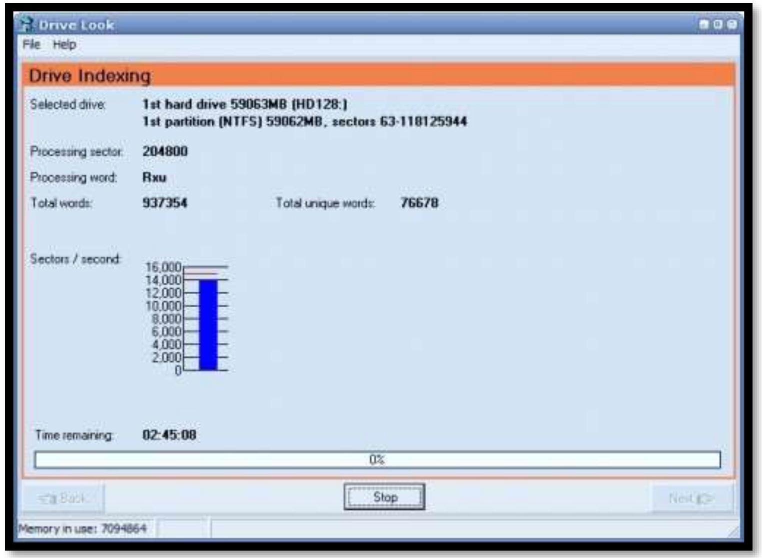
# Data Recovery Software

Various data recovery software is available as freeware, as well as commercially.

**Bad Sectors:** A bad sector is permanent damage on the hard disk partition, where data is stored.

**Causes of bad sectors**

- Bad sectors are a physical error on disc drives. Many hard drives, could have many bad sectors as part of a manufacturing defect.
- Physical error and heat are the main causes of bad sectors.



Drive Indexing

Selected drive: 1st hard drive 59063MB (HD128:)
1st partition (NTFS) 59062MB, sectors 63-118125944

Processing sector: 204800

Processing word: Rxu

Total words: 937354 Total unique words: 76678

Time remaining: 02:45:08

Memory in use: 7094864

Drive Look software, an example for data recovery software

# Quiz / Assessment

1) A __________is permanent damage on the hard disk partition, where data is stored

a. Good sector
b. Bad sector
c. High sector
d. Moderate sector

# Quiz / Assessment

2) _________ is a specialized process to recover files without having its metadata.

a. File craving
b. File data
c. File recovery
d. File access

# Quiz / Assessment

3) Each drive contains system specific partitions, called __________, that contain firmware to maintain all defective sectors from the drive.

a. System process
b. System area
c. System sector
d. System hold

# Activity

Online

**Online/Offline Activity**
(30 min)

- Explain the steps to recover data from a crashed hard drive as a forensic expert.

# Summary

- ✓ The process of retrieving inaccessible or corrupt data, from various digital media storage devices is known as Data Recovery.

- ✓ Data from devices such as hard disks, USB and flash devices, tape and optical drives, mobile and PDA devices, etc. can be recovered by using Data Recovery process.

- ✓ Running an easily available software on the storage medium being investigated is a common method used to recover data from corrupt media storage devices.

- ✓ Data/digital evidence acquisition is the foremost step in the forensic process used to identify and acquire possible digital evidence from various sources.

# Summary

- ✓ The three most popular methods in which digital evidence can be acquired and stored for further assessment are: Raw Format, Proprietary Format, Advanced Forensic Format.

- ✓ Some of the tools are utilized during forensics data acquisition process, depending on the OS, the applications, and the current state of the system in question include – Encase, FTK Images, DD, DD Rescued.

- ✓ Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks (RAID) is a virtual storage technique that combines various physical drives into a single logical unit in order to provide data redundancy and performance.

# e-References

- *Data Recovery - a Brief Introduction.* Retrieved from http://www.streetdirectory.com/travel_guide/114076/data_recovery/data_recovery___a_brief_introduction.html

- *Data Recovery Services.* Retrieved from http://www.datarecovery.net/data-recovery-services.aspx

- *Techniques in Computer Forensics: A Recovery Perspective.* Retrieved 2013, from http://www.cscjournals.org/manuscript/Journals/IJS/Volume3/Issue2/IJS-13.pdf

- *Data Acquisition & Imaging.* Retrieved from http://einvestigations.com/computer-forensics/data-acquisition-and-imaging/

- *Data Recovery Techniques.* Retrieved from http://www.recovermyfiles.com/data-recovery-techniques.php

# External Resources

1. Hayes, D. D. (2015). *A Practical Guide to Computer Forensics Investigations.* US: Pearson Education, Inc.
2. Nelson, B., Phillips, A., &Steuart, C. (2010). *Guide to Computer Forensics and Investigations, Fourth Edition*. USA: Cengage Learning.
3. Philipp, A., Cowen, D., & Davis, C. (2010). *Hacking Exposed Computer*