

# Concepts to note for week4...

3

## FUNCTIONS OF DIGITAL FORENSICS TOOLS

### - MAINLY INCLUDE

- **Acquisition** – Making a copy of original drive
- **Validation & Verification.** Which include the following and others:-
  - **hashing** – Ensure data hasn't been changed
  - **Filtering** – To separate good files and files need to be investigated. Remember you are dealing with million of items
  - **Analysing File Header** – To check on change file type. Sometime file header is changed to hide information
- **Extraction** – Recovering data, keyword searching, file caving, decryption and others
- **Reconstruction** – Recreate a suspect drive to show what happen during a crime
- **Reporting**

# Chapter Quiz:-

1. In software acquisition, there are three type of data copy method.

☐ True

☐ False

• **False**

2 types : physical & logical

2. Which of the following is not a sub-functions of "Extraction"

a. Data Viewing

b. Keyword Searching

c. Bookmarking

d. Reporting

**d. Reporting**

Reporting is required after finding is finalised.

# Chapter Quiz (Cont):-

5

3. In general, forensics workstations can be divided into \_\_\_\_ categories.

a. 2

b. 3

c. 4

d. 5

**b. 3**

- Stationary
- Portable
- Lightweight

4. Many vendors have developed write-blocking devices that connect to a computer through FireWire,\_\_\_\_ 2.0 and 3.0, SATA, PATA, and SCSI controllers.

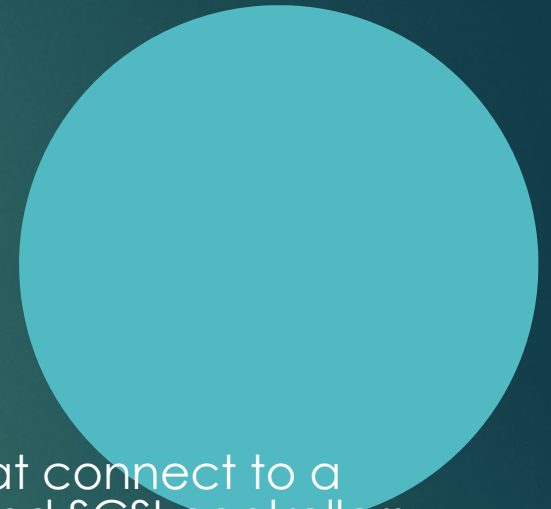
a. USB

b. IDE

c. LCD

d. PCMCIA

**a. USB**





# Revision : File System Metadata and Application Metadata...

6

► For exercise 3A:




## 1) File System Metadata

- Indicates the date the file was first saved on the hard drive on which it is currently residing

## 2) Application Metadata

- Indicates that the document was created (came into existence) by author.

ARTIFACT INFORMATION	
Filename	Thoughts-on-Ambassador-Owls.docx
File System Last Modified Date/Time	3/26/2019 3:49:20 PM
File System Last Accessed Date/Time	3/26/2019 3:49:18 PM
File System Created Date/Time	3/26/2019 3:49:18 PM
Size (Bytes)	151474
Saved Size (Bytes)	151474
Authors	Steve Martin
Last Author	Steve Martin
Last Modified Date/Time	9/23/2017 8:34:00 AM
Created Date/Time	9/23/2017 8:34:00 AM
MD5 Hash	00a43bf9594b8eb33ec95e06b05e0384
SHA1 Hash	c8d1398c9e1b6482f85b4ed072cc8d3bb99a13cc
Artifact type	Word Documents
Item ID	23772

	<b>Thoughts-on-Ambassador-Owls.docx</b>	File System Last Modified...
	WORD DOCUMENTS — Documents File System Last Accessed Date/Time : 3/26/2019	3/26/2019 3:49:20 PM
	<b>http://naturalencounters.com/site/...</b>	Start Time Date/Time
	CHROME DOWNLOADS — Web Relat... File Name : Thoughts-on-Ambassador-Owls.doc	3/26/2019 3:49:18 PM
	<b>Thoughts-on-Ambassador-Owls.docx</b>	
	File extension : .docx Logical size : 151,474 bytes	

# Week 4 Lab – File Caving

7

- ▶ Work on Week 4 Lab – **File Caving**
  - ▶ [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html)
- ▶ Tool **WinHex** will be used to perform **file analysis, file signature analysis, file caving** and others
- ▶ Once finish your winhex exercise, do work on Practical 3 **challenge question** and submit your answer to BS individually. To install prodiscover for your challenge, can go to **BS/Other Resources/Software**
- ▶ Continue to work on **assignment 1** if got time...