DFI Exam – 2223S1

General Info (Please double check!) :-

- Date : 23rd Aug 2022 (Tue)
- Time : 1600 - 1810
- Duration : 2 hours
- Answer all questions
- Please read instructions/questions carefully!

Format

General Exam Info :-

Section A (20%)

10 MCQ (Multiple choice questions)

- MCQ can fall into one of the following categories:-
  - **Direct questions**
    - i.e Who is your DFI module coordinator? 1) Boris Choo 2) Boris Tan 3) Boris Lim 4) Boris Ng
  - **Logical questions**
    - i.e Records that investigator will not maintain is? 1) chain of evidence 2) chain of custody 3) logs of investigation 4) Price for a write-blocker
  - **General knowledge**
    - i.e Temporary location to store information not being used by the computer 1) USB 2) Hard Disk 3) Registry 4) Swap file?

Section B (20% * 4)

4 Structured Questions

- Each question has sub-questions

Scope

- Please study **everything**!!! – Good news – *Can skip module overview!*

  - **Theory** – **All lectures notes** for:-
    - **Week1-Week6** – Before term break
    - **Week11-Week16** – After term break
    - **Check out all quizzes** – In chapter's video

  - **Practical** – Good news again!!! **Will not** be tested.

DFI – Areas of Focus

Intro to Forensics - Topic 1

- Definition of Digital Forensics
- Need to know what is "**Chain of Custody**". i.e fill up when evidence changes hand
- Understand the difference between **Private** and **Public** investigator
- Understand what is "**Case Law**". Why "**Case Law**" is required? i.e Allows legal counsel to apply previous similar cases to current one in an effort to address ambiguity in laws when statutes does not exist
- Potential challenge a digital investigator may face today? i.e password protected hard disk?

Understanding Investigation - Topic 2

- **Rule of Computer Forensics** – Preserve the original evidence!!
- **Chain of evidence form** : To record who collected, handled, analysed or controlled evidence during investigation.
- **Understand common investigation cases** i.e email abuse, selling company secret to competitor
- The difference between **Private-sector** investigations and **Public-sector** investigation. i.e. Public investigation usually required search warrants, Public sector usually deal with criminal and private usually deal with abuse of resource

DFI – Areas of Focus

Data Acquisition - Topic 3

- Need to know Evidence Storage Formats. - 3 formats
  - **Row**, **Proprietary** and **Advanced** formats. i.e Encase is Proprietary format!
- Why **Acquisition** is necessary?
- **Acquisition Methods.** i.e disk to image, disk to disk and etc.
- **Purpose of a write-blocking device. Types** of write blocking device i.e **Hardware write-blocker and Software write-blocker**. Software means configuring OS to prevent writing to external disk!
- Types of **Validation** Techniques. Why validation is necessary? i.e CRC-32, MD5, SHA512, etc
- **Remote Acquisition**. Possible issues with remote acquisition. i.e slow speed, firewall, network problems and others

DFI – Areas of Focus

Digital Forensic Tools - Topic 4

- Consult your **business plan** to get the best hardware and software for your DF investigation

- **Computer forensics tools' functions**
  - **Acquisition**
  - **Validation and verification**
    - Data preservation/Data analysis - Hashing, filtering, analyzing file header
  - **Extraction**
    - Key searching, carving, book marking, etc…
  - **Reconstruction**
    - Re-create a suspect drive to show what happened during a crime or an incident
  - **Reporting**

- Maintain a software library on your lab. Keeps useful software drivers
- Computer Forensics tools types 1) S/W 2) H/W
  - Forensics Software 1) Command-line or 2) GUI (i.e Encase/Paraben/Magnet)
  - Forensics Hardware 1) Customized equipment 2) Commercial options: Can buy off the shelf and that include workstations and write blockers
- Always run a validation test when upgrading your forensics tools (both software/hardware)

DFI – Areas of Focus

Evidence Processing - OS & File systems - Topic 5

- **Disk Partition** – Before a drive (a,b,c,d) can be used by any OS, a **Partition table** needs to be created on the drive. **Partition table** is stored in **Master Boot Record (MBR)** sector 0.
- The **MBR** is the information in the **first sector** of any hard disk that identifies how and where an operating system is located so that it can be **boot** (loaded) into the computer's main storage or random access memory. As such, the **MBR** holds the information on how the logical partitions, containing file systems, are organized on that medium.
- **RAM Slack & File Slack**
  - What is **RAM Slack** & **File Slack**?
  - Given required information such as **drive size**, **data/file size** and etc, how do we determine **cluster size**, calculate **RAM** and **File slack**. See **week5** lecture notes for more info

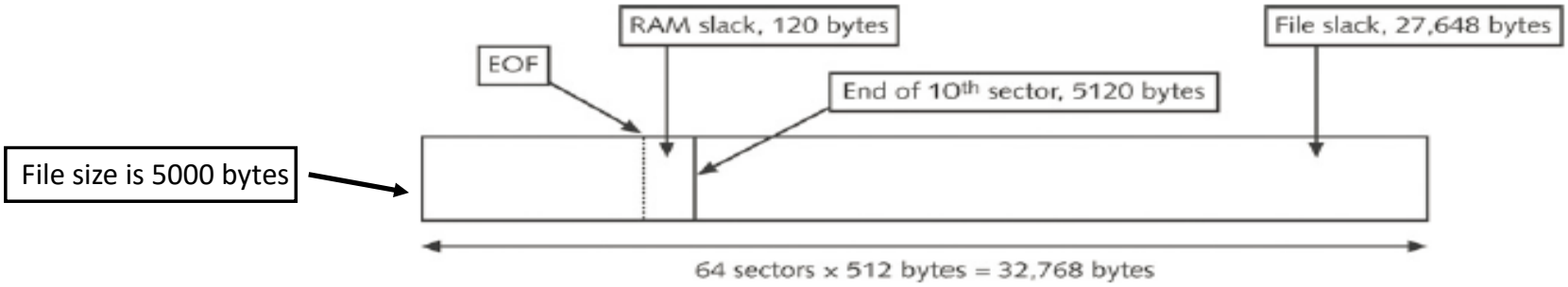


Figure 5-8 File slack space
© 2015 Cengage Learning®

Topic 5 Example : Calculations of Cluster, RAM Slack and File Slack

- **Cluster, space required for a file is made up of number of sectors**

- **Number of Cluster Required to Store a File**
  - (FileSize) / (ClusterSize)
    = Round Up (ClusterRequired)
  - While ClusterSize is determined by no. of sectors

Table 5-2 Sectors and bytes per cluster

Drive size	Sectors per cluster	FAT16
8–32 MB	1	512 bytes
32–64 MB	2	1 KB (1024)
64–128 MB	4	2 KB
128–256 MB	8	4 KB
256–512 MB	16	8 KB
512–1024 MB	32	16 KB
1024–2048 MB	64	32 KB
2048–4096 MB	128	64 KB

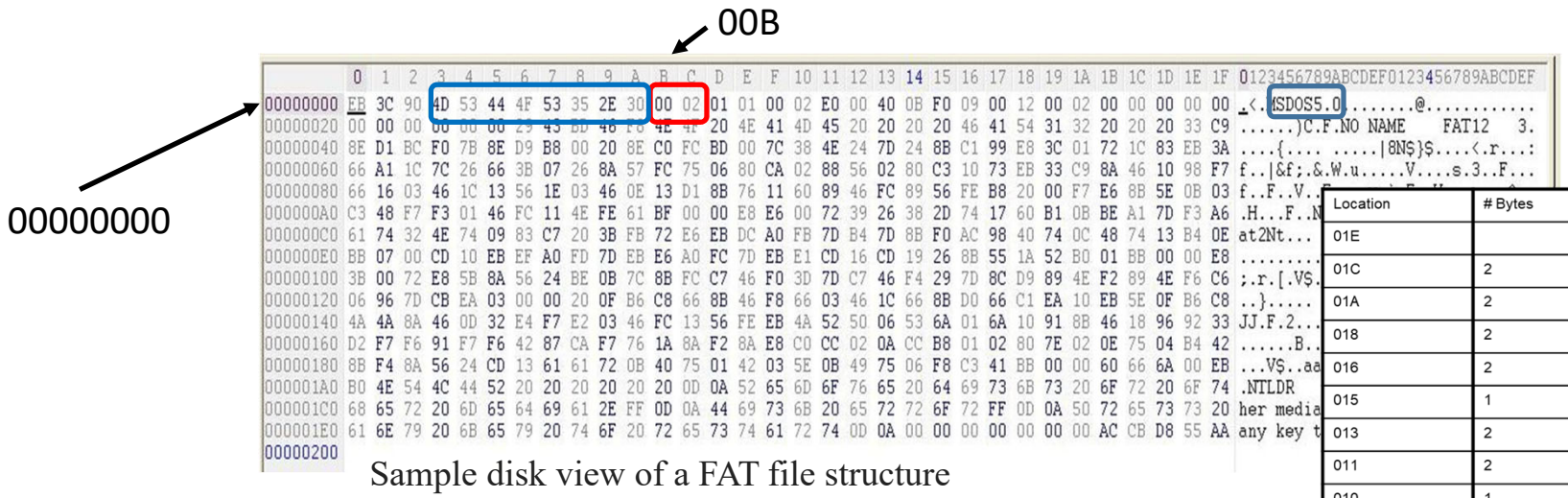
- **RAM Slack**
  - Per Sector Size = **512** Bytes (in general)
  - (SectorsRequired) = (FileSize) / (SectorSize) = Round up (SectorsRequired)
  - Round Up (SectorRequired) * Sector Size = Total Sector Size Required
  - Total Sector Size – File Size = **RAM Slack**

- **File Slack**
  - File Slack = (SizeOfClusterRequired) – (FileSize) – (RAMSlack)

DFI – Areas of Focus

Evidence Processing - OS & File systems - Topic 5 (Cont)

- **File Allocation Table (FAT) –** File structure database that Microsoft originally designed for floppy disks
  - Understand what is **FAT**. i.e what is cluster size



Sample disk view of a FAT file structure

Location	# Bytes	Meaning	Value
01E		OS Boot Loader	
01C	2	# Hidden Sectors	0
01A	2	# Heads	2
018	2	# Sectors / Track	18 (12x)
016	2	# sectors/ FAT	9
015	1	Media Bytes	F0: (floppy)
013	2	# logical sectors	2880(0B40x)
011	2	# Root Dir entries	224 (00E0x)
010	1	# FATS	2
00E	2	# Boot Sectors	1
00D	1	# Sectors/Cluster	1
00B	2	# Bytes/Sector	512 (0200x)
003	8	OEM Name ID	MSDOS5.0
000	3	Jmp to loader	EB 3C 90

Specifications of FAT

  - Must understand concept of FAT. i.e Cluster is make up of sectors and one sector is **512** Bytes. Cluster number is the logical address in OS
  - Need to be able to **interpret specifications** of FAT

DFI – Areas of Focus

Evidence Processing - OS & File systems - **Topic 5** (Cont)

- **NT File System – NTFS :** To improve on FAT file system. In **NTFS**, everything written to disk is a file.
  - **Master File Table (MFT)**
  - Understand how NTFS files are stored in NTFS system
    - Namely "**Resident**" and "**Non-Resident**". 2 types
- On an First data set **NTFS** disk
  1. Is the **Partition Boot Sector**
  2. Next is **Master File Table (MFT)**
     - **Each file** on an NTFS volume is represented by **a record** in master file table (**MFT**)
- MFT contains information about **all files** on the disk
- In the MFT, the **first 15 records are reserved for system files**
- **Need to understand** MFT Structures as well as **Attributes in the MFT**

Table 5-5 Attributes in the MFT

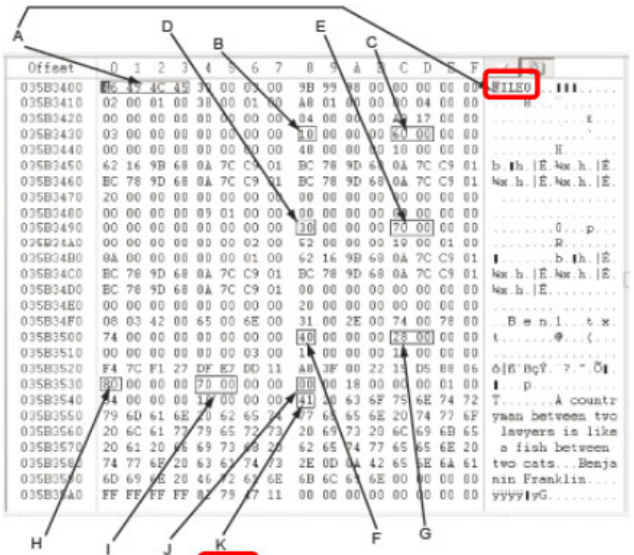
Attribute ID	Purpose
0x10	$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	$File_Name The long and short names for a file are contained here. Up to 255 Unicode bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filenames have only one attribute ID 0x30. Long filenames have two attribute ID 0x30s in the MFT record: one for the short name and one for the long name.
0x40	$Object_ID ($Volume_Version in Windows NT) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	$Security_Descriptor Contains the access control list (ACL) for the file.

Basic information of a file in MFT starts at 0x10

The **Master File Table** allocates space for each file record. The attributes of a file are written to the allocated space in the MFT. Small files and directories (typically 512 bytes or smaller), can entirely be contained within the master file table's (MFT) record.

DFI – Areas of Focus

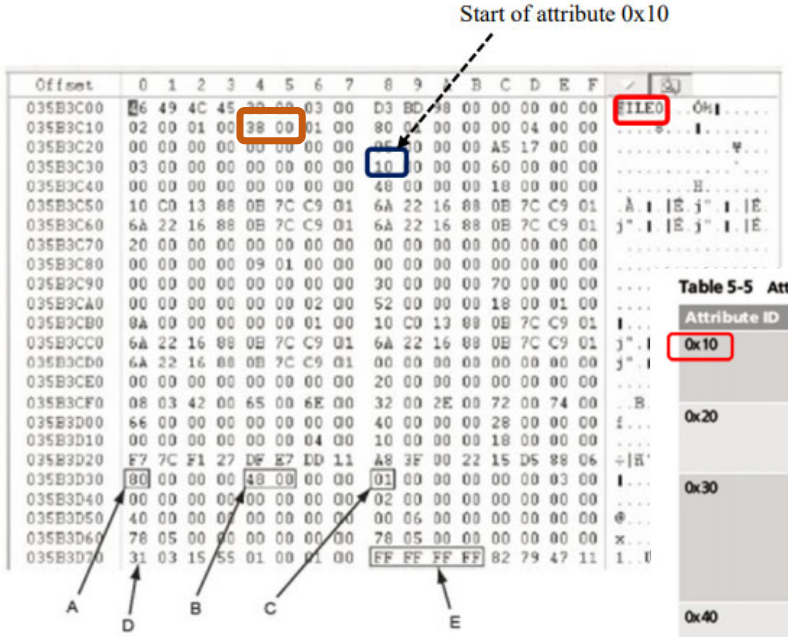
MFT and File Attributes (Cont)



A: All MFT records start with FILE0
B: Start of attribute 0x10
C: Length of attribute 0x10 (value 60) **60 00 → 00 60**
D: Start of attribute 0x30
E: Length of attribute 0x30 (value 70) **70 00 → 00 70**
F: Start of attribute 0x40
G: Length of attribute 0x40 (value 28)
H: Start of attribute 0x80
I : Length of attribute 0x80 (value 70)
J : Attribute 0x80 resident flag
K: Starting position of resident data

Figure 5-10 Resident file in an MFT record
Courtesy of X-Ways AG, *www.x-ways.net*

Resident file attributes



A: Start of nonresident attribute 0x80
B: Length of nonresident attribute 0x80
C: Attribute 0x80 nonresident flag
D: Starting point of data run
E: End-of-record marker (FF FF FF FF) for the MFT record

Figure 5-12 Nonresident file in an MFT record
Courtesy of X-Ways AG, *www.x-ways.net*

Non-resident file attributes

Table 5-5 Attributes in the MFT

Attribute ID	Purpose
0x10	$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	$File_Name The long and short names for a file are contained here. Up to 255 Unicode bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filenames have only one attribute ID 0x30. Long filenames have two attribute ID 0x30s in the MFT record: one for the short name and one for the long name.
0x40	$Object_ID ($Volume_Version in Windows NT) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	$Security_Descriptor Contains the access control list (ACL) for the file.

*Basic information of a file in MFT starts at **0x10***

*See **slide 29 on chapter 5** for more information on attribute*

– *At offset 0x14* - length of the header (indicates where the next attribute starts) *38 00 → 00 38 = 56 bytes!!*

DFI – Areas of Focus

- **Analysis & Validation** - Topic 6
  - Understand what is **scope creep**
  - Purpose and features of **Hexadecimal Editors**. i.e **WinHex** can be used to do bit shifting, hashing and etc
  - Addressing **Data-Hiding Techniques** and understand areas on harddisk that can be used to hide data. i.e Slack space.
    - **Hiding entire partitions**
    - **Changing file extensions**
    - **Setting attribute to hidden**
    - **Bit-shifting**
    - **Encryption**
    - **Password protection**
  - Understand what is **Steganography**, when to use Steganography
  - Understand what is **Watermarking**, when to use Watermarking

DFI – Areas of Focus

Digital Forensic Lab - Topic 7

- To stay relevant, we need to upgrade skills through training/certification
- A **digital forensics lab** is where you conduct investigations, store evidence and do most of your work. Must know what to check when auditing a computer forensics laboratory. i.e visitors' log and door lock
- A lab facility must be **physically secured** so that evidence is not lost, corrupted or destroyed
- A **forensic workstation** needs to have adequate memory, storage, and ports to deal with common types of cases that come through the lab
- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab – **Justification** is always required!!

DFI – Areas of Focus

Crime & Incidence Scene Processing - Topic 8

- Define **Digital Evidence** i.e Digital evidence is anything stored or transmitted on electronic or optical media
- **Tasks investigators perform**. i.e Acquisition, Identification, Evaluation, Admission
- **Rule of Evidence** – Consistent practices. Must handle all evidence consistently. Must ensure **evidence is not altered**!
- **Collecting Evidence in Private-Sector Incident Scenes**
  - Corporate policy – Stating right to inspect computing assets at will. i.e displaying a warning banner or publish company's policy
- Identifying the type of OS or digital device at start of investigation
- Ways to store digital evidence. i.e. CDs, DVDs, Magnetic tapes and etc.
- **Tools** required for initial-response field kit. i.e digital camera

DFI – Areas of Focus

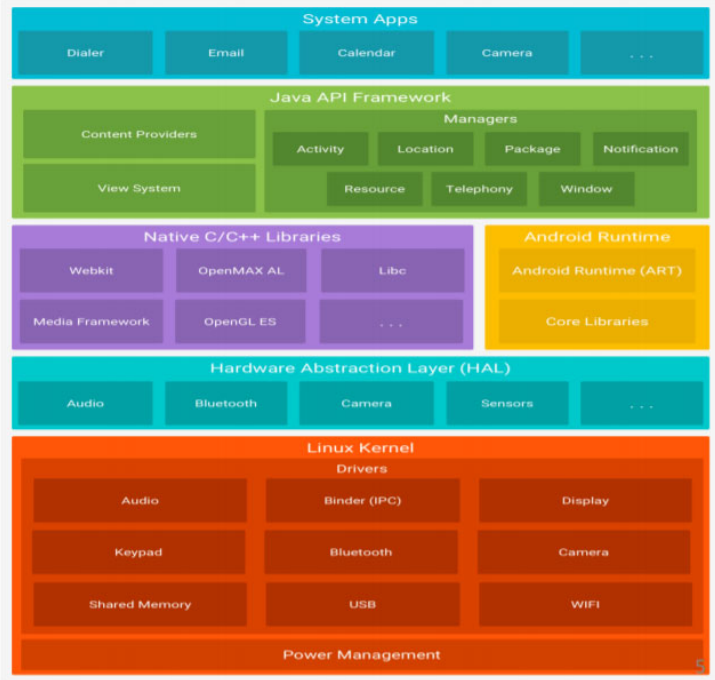
Historic Cellular - Topic 9

- How does a mobile phone contacts based station?
- Purpose of **MTSO** (Mobile Telephone Switching Office) – "**Brain**"
- What is **Handoff**?
- For Mobile Telecommunication Technologies, many were discussed. Focus on **iDEN**, **CDMA** and **GSM**
- **Cellular Phone Identification Number.** Need to understand **format** as well as meaning of :-
  - **MIN** – Mobile Identity Number. Understand what is MIN.
  - **MEID** – Mobile Equipment ID. MEID format. i.e RR : Regional Code, ZZZZZZ : Manufacturer assigned to uniquely ID device
  - **IMEI** – International Mobile Equipment Identity. Understand what is IMEI

DFI – Areas of Focus

Data Type : Android - Topic 10

- Understand what is Android OS
- **Android Architecture** :
  - **System Apps** – Build in and user's App
  - **Java API Framework** – API interface, Activity Manager to manage application life cycle
  - **Native C/C++ Libraries** – includes SQLite, C / C++ libraries, 3D graphics
  - **Android Runtime** – Each application runs in its own process and with its own instance of the Android Runtime (**ART**). Designed to run in environment with limited battery/memory and CPU by executing DEX (Dalvik Executable) files.
  - **Linux Kernel** – Device Drivers, Process Management, Memory Management, Networking
- Need to understand how to do **data acquisition** on Android phone. i.e Steps involved, Types of acquisition

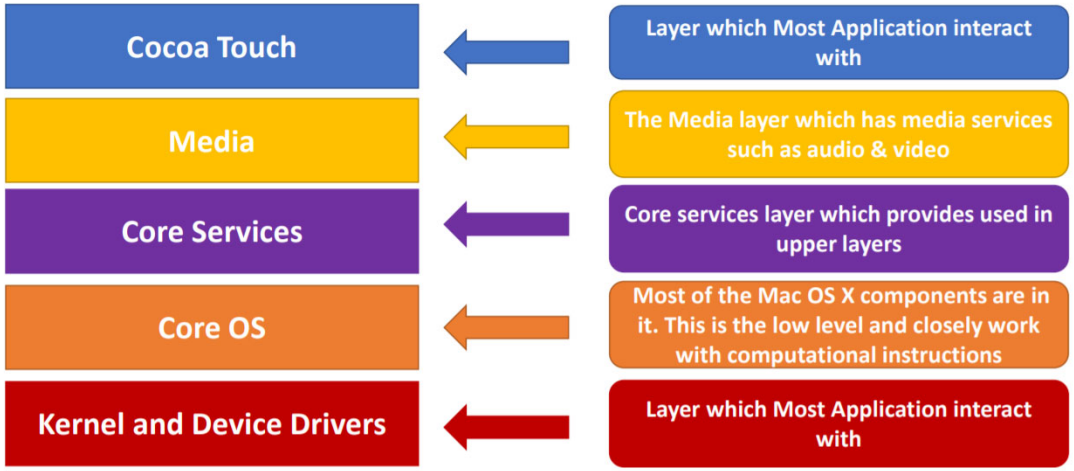


Android Architecture

DFI – Areas of Focus

Data Type iOS - Topic 11

- **iOS Architecture**. Need to understand how each layer function.
- Acquisition Procedures of iOS
- What is **Plist** file? What is **EXIF** file?
- What is **.db** file?
- Different type of iOS device. i.e iPhone, iPad, iPod



DFI – Areas of Focus

Rooting and Jailbreaking - Topic 12

- Rooting and Jailbreaking
  - Meaning of Rooting in Android, Jailbreaking in iOS
  - **Impacts of jailbreaking** i.e void warranty
  - **Motivation behind Rooting & Jailbreaking.** i.e gain root privileges, remove vendor installed software
  - **Tools** used in Rooting & Jailbreaking. i.e JailBreakMe