

COMP3731 Computer Forensics

Mid-term Study Guide

NO NEED TO MEMORIZE THE OFFSETS OF ANY STRUCTURE

Basic Concepts:

- What is **computer forensics**?
- **Steps** to solving a computer crime
- Methods to acquiring digital evidence: bit-stream copy, bit-stream image, static/live acquisition, **logical and sparse acquisition**, **remote acquisition**
- Digital hash functions: their use in forensics, **desired properties**, collisions
- Write protection: why is it important in forensics, **Windows write protection**, Linux LiveCDs (usage of the **dcfldd** command)
- **Forensics tools**: what features should one have, have a general idea of what they mean

Disk Structures:

- What are tracks, sectors, cylinders, heads?
- **CHS and LBA addressing**
- What are **surplus sectors**?
- **MBR, VBR** and typical boot processes
- Reading **partition tables** from MBR/VBR

Windows System Structure:

- Microsoft file structures:
 - Sectors and clusters: why do we use clusters?
 - Disk slack and its importance in forensics
 - FAT file system: idea of how **cluster addresses** are stored, file fragmentation, deletion
 - NTFS: what is the MFT, **resident/non-resident files**, interpreting data **runs**, idea of how **attributes** are encoded within a record, **data streams**
- Windows Registry **terminology**; you should know the **typical** HKEYS, what information they hold and where is the data corresponding to those HKEYS are typically stored
 - What are some of the **interesting places** in a registry?

- What is a timeline analysis?
 - Time formats
 - What are the various Windows artifacts that encode time related data?
 - Idea of how Windows manipulates some of the time stamps
- Windows files and their relevance in forensics: log files, prefetch files, jump lists, and others; you should know where these files are typically present and what data can you hope to extract from these files.

Unix System Structure:

- Linux file structures:
 - Be familiar with the terminology: blocks, block groups, BGD, inodes, super block, block bitmap, inode bitmap, inode table, directories
 - Idea of the organization of a Linux formatted drive: the big picture
 - Inode structure: how are the 15 pointers used?
- Linux memory analysis: general idea of what process descriptors are and how Linux organizes them in memory, how can these descriptors be extracted
- Permissions in Linux
- What are some of the files in a Linux system that can aid a forensic investigation: home directory, shell history, remote logins, temporary directories, log files, scheduled tasks.