Essential Technical Concepts

Contents

- In this chapter, we will cover the following topics:
  - Different number system
  - Encoding schema
  - File carving and structure
  - File metadata
  - Hash analysis
  - System memory
  - Storage
  - Filesystem
  - Cloud computing
  - Windows OS
  - Networking

Decimal (Base-10)

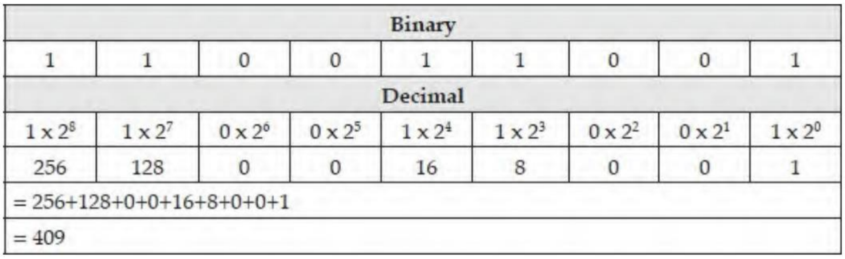
- The base-10 system, which employs 10 digits or symbols (0, 1, 2, 3, 4, 5, 6,7, 8, and 9) to represent its values, is the most extensively used numbering system that we use every day while conducting arithmetic calculations (for example, 17 + 71 = 88).
- The value a number represents is determined by its position in decimal, where each digit is multiplied by the power of 10 corresponding with that digit's location.
- Take, for example, the decimal number 7,564. This number can be interpreted as: 7,654 = 7,000 + 600 + 50 + 4
- An understanding of the decimal numbering system is essential, as the other numbering systems follow similar rules.

Binary

- Data is stored in binary format on computers, which is the base-2 numeric system represented by 1s and 0s.
- The computer language, binary, follows the same laws as a decimal. Binary, on the other hand, contains two symbols (0 and 1) and multiplies by the power of two, unlike decimal, which has 10 symbols and multiplies by the power of 10.
- Each 1 OR 0 in a computer is referred to as a bit (or binary digit), and the total of eight bits is referred to as a byte.

Binary

- For example, the binary number 110011001 can be converted into decimal as 409.



Binary								
1	1	0	0	1	1	0	0	1
Decimal								
1×2^8	1×2^7	0×2^6	0×2^5	1×2^4	1×2^3	0×2^2	0×2^1	1×2^0
256	128	0	0	16	8	0	0	1
= 256+128+0+0+16+8+0+0+1								
= 409								

- Data is stored in computer systems in binary format, including Microsoft Word documents, Digital photographs, videos, Excel sheets, social media tweets and posts, e-mails, and anything and everything created and stored on computer systems.

Hexadecimal (Base-16)

- The values of the hex numbering system are represented by 16 digits or symbols.
- It has the following numbers and letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, and W (capital letters are used to represent numbers from 10 to 15).
- When dealing with computers and other digital systems, hex numerals are frequently encountered, particularly when looking at the memory address location.
- The key objective of this numbering scheme is to express lengthy binary data in a compact format that people can understand.
- Hex does this by combining all of the bits (binary digits) into a single group.

File carving

- In digital forensics, understanding how computers store and portray data is critical; for example, an analyst may need to recover and open a file from unallocated disc space on the target hard disk drive or from a raw dataset without using the software that produced the file (for example, MS Word).
- This method is known as file carving, and it may be used to recover lost files and file fragments from erased or damaged hard drives.
- To carry out file carving, we must first understand how to separate a file from its signature

File carving

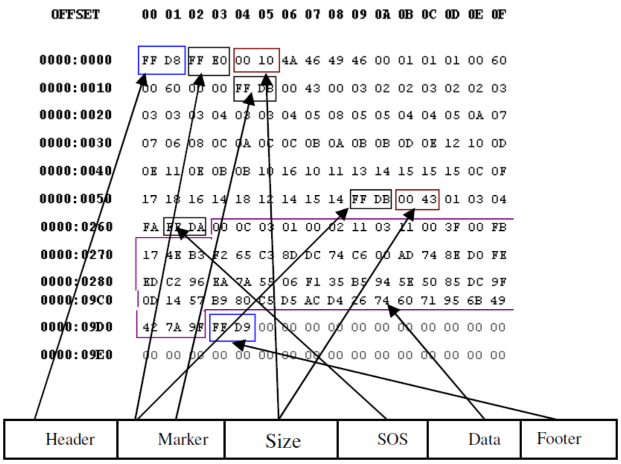
- File carving is most frequently used to recover files from the unallocated space in a drive since it is a forensics approach that recovers files based solely on file structure and content and without any matching file system meta-data.
- Unallocated space is the portion of the disc that, according to the file system architecture, like the file table, no longer contains any file information.
- The entire disc may be affected if the file system structures are broken or absent.
- In plain English, a lot of filesystems do not completely zero away the data when they erase it. Instead, they only take away the location’s information.
- By scanning the disk’s raw bytes and putting them back together, a process known as “file carving” reconstructs files.
- This is often accomplished by looking at a file’s header and footer, which are the first few bytes and last few bytes, respectively

File carving

- When directory entries are damaged or missing, file carving is a fantastic technique for recovering files and pieces of files.
- Forensics professionals use this method, in particular, to recover evidence in criminal situations.

File carving

- The JPEG extraction algorithm need not search for footer from start of the header. Instead, it has to jump from the marker to marker until Start of Scan (SOS) marker.



```
OFFSET     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0000:0000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60
0000:0010  00 60 00 00 FF DB 00 43 00 03 02 02 03 02 02 03
0000:0020  03 03 03 04 03 03 04 05 08 05 05 04 04 05 0A 07
0000:0030  07 06 08 0C 0A 0C 0C 0B 0A 0B 0B 0D 0E 12 10 0D
0000:0040  0E 11 0E 0B 0B 10 16 10 11 13 14 15 15 15 0C 0F
0000:0050  17 18 16 14 18 12 14 15 14 FF DB 00 43 01 03 04
0000:0260  FA FF DA 00 0C 03 01 00 02 11 03 11 00 3F 00 FB
0000:0270  17 4E B3 F2 65 C3 8D DC 74 C6 00 AD 74 8E D0 FE
0000:0280  ED C2 96 EA 7A 55 06 F1 35 B5 94 5E 50 85 DC 9F
0000:09C0  0D 14 57 B9 80 C5 D5 AC D4 26 74 60 71 95 6B 49
0000:09D0  42 7A 9F FF D9 00 00 00 00 00 00 00 00 00 00 00
0000:09E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

File carving

- Carving tools
  - **Autopsy**
    - The most common tool used in forensics to extract files from images is **Autopsy**. Download it, install it and make it ingest the file to find "hidden" files. Note that Autopsy is built to support disk images and other kind of images, but not simple files.
  - **Binwalk**
    - **Binwalk** is a tool for searching binary files like images and audio files for embedded files and data.
  - **Foremost**
    - Another common tool to find hidden files is **foremost**.
  - **Scalpel**
    - **Scalpel** is another tool that can be use to find and extract **files embedded in a file**.
  - **Bulk Extractor**
    - This tool comes inside kali but you can find it here: https://github.com/simsong/bulk_extractor
    - This tool can scan an image and will **extract pcaps** inside it, **network information(URLs, domains, IPs, MACs, mails)** and more **files**
  - **PhotoRec**
    - You can find it in https://www.cgsecurity.org/wiki/TestDisk_Download
    - It comes with GUI and CLI version. You can select the **file-types** you want PhotoRec to search for.
  - **FindAES**
    - Searches for AES keys by searching for their key schedules. Able to find 128. 192, and 256 bit keys, such as those used by TrueCrypt and BitLocker.

File structure

- Each file type has its encoding scheme that specifies how information is kept, and a digital file is made up of a series of bits. This schema’s name is “file format”.
- The file format can be either open source (such as PNG, an ISO/IEC raster image format) or proprietary (such as Adobe Photoshop) (like the Windows Media Audio [WMA] file format).
- Many common multimedia file formats may hold multiple content kinds, which is the case with some file formats.
- For example, the OGG format may hold video, music, text, and metadata in a single container. AVI, WAV, and 3GP files are also included in this category.
- Users are identified as file types by their extensions, according to the researchers. The DOCX or DOC extension is used for MS Word files, whereas the XLSX or XLS end is used for MS Excel files.
- As digital forensic investigators, however, we cannot only depend on the file extension to determine the file type because it may be altered to anything (for example, an MS Word file can be changed to a DLL or PNG file to conceal its true identity).

File structure

- File signature (header) can be checked to establish the type of strategy to detect it.
- The first 20 bytes of most digital files contain a signature; you may check this signature by opening the subject file in Windows Notepad or another text editor like Notepad++.
- To analyze a text file or document file, change the extension to, say, JPG and then analyze the JPG file first 20 bytes in a Hex editor.
- HexEditor would reveal the original file signature as being editable in Notepad.exe.

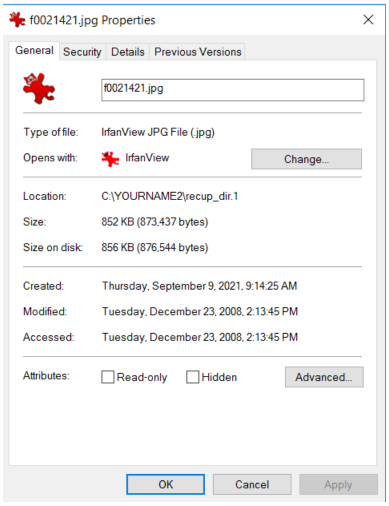
File structure

- There are many free Hex editors; some common ones used extensively are as follows:
  - wxHexEditor (www.wxhexeditor.org/home.php)
  - Free Hex Editor Neo (www.hhdsoftware.com/free-hex-editor)
  - PSPad (www.pspad.com/en)

Digital file metadata

- Metadata is information about information.
- Metadata is connected with almost all digital file formats.
- Although it is frequently included in the same file, certain file formats save their information in a distinct file.
- Metadata contains information about the file with which it is related.
- Author name, organization name, computer name, date/time produced, and comments are examples of information found in MS Word files.
- Metadata may be quite beneficial in many circumstances when it comes to digital forensics.
- We may, for example, trace file authors using the information linked with them.
- We may also look for useful information in the file's metadata (most operating systems currently offer searching inside the file metadata information), and most digital forensic suites support searching within the metadata of acquired forensic picture files

Digital file metadata



f0021421.jpg Properties

f0021421.jpg

Type of file: IrfanView JPG File (.jpg)

Opens with: IrfanView

Location: C:\YOURNAME2\recup_dir.1

Size: 852 KB (873,437 bytes)

Size on disk: 856 KB (876,544 bytes)

Created: Thursday, September 9, 2021, 9:14:25 AM

Modified: Tuesday, December 23, 2008, 2:13:45 PM

Accessed: Tuesday, December 23, 2008, 2:13:45 PM

Attributes: □ Read-only □ Hidden

Digital file metadata

- Several free tools can also view and edit the metadata information of digital files as follows:
  - ExifTool by Phil Harvey (www.sno.phy.queensu.ca/~phil/exiftool). Read, write, and edit Meta-information for a wide variety of digital files (most image formats).
  - Exif Pilot (www.colorpilot.com/exif.html). Image metadata editor/viewer.
  - GIMP (www.gimp.org). Image editor; can manipulate/view image file metadata.
  - Pdf Metadata Editor (http://broken-by.me/pdf-metadataeditor). For PDF files.
  - Mp3tag (www.mp3tag.de/en). For audio files.
  - XnView (www.xnview.com/en/). View/edit image metadata.
  - MediaInfo (https://mediaarea.net/en/MediaInfo). Metadata viewer/editor for video and audio files

Timestamps decoder

- From the standpoint of digital forensics, metadata analysis is critical for any sort of investigation since it may disclose a wealth of information about the case at hand.
- Some users (for example, criminals) may attempt to modify the metadata of the file to erase the evidence and mislead investigators.
- Forensic specialists are responsible for detecting such tampering and attempting to reveal it to the court.
- The majority of computer forensics software allows for mass extraction and search of file metadata.
- Digital files contain a variety of information, the most essential of which is the timestamp metadata, which is used to indicate various date/time events related to the file of interest, such as the last access date/time, the last updated date, and the creation date.
- During the investigations, we may come across a date/time that is encoded in a specific fashion that we must decode (for example, date/time data in the Windows registry that are recorded in binary format and must be converted to ASCII) from www.digital-detective.net/digital-forensic-software/freetools.

Hash analysis

- Hashing is an important concept in digital forensics; in fact, you must compute the hash value of every digital evidence you obtain throughout your investigation (whether it be a hard disc image or a single file) to verify that the acquired data (i.e., the digital evidence) has not been tampered with.
- Hash works by converting a digital file (input) into a fixed string value (output); the resultant hash value is unique and cannot be created using any other file or piece of data.
- A hash generator tool may be used to determine the hashing value of any digital file or piece of data.
- MD5 and SHA-256 are two of the most well-known cryptographic hash algorithms.
- Hashing, referred to as digital fingerprinting, is used in digital forensics investigations the first time to ascertain the acquired forensics image even before analysis begins (to make identical copies of the acquired forensics image) and then the second time after the investigation to verify the integrity of the data and forensics processing.

Calculate file hash

- Hashing capabilities are included in all digital forensics suites; however, you may use a third-party application or the built-in hashing tool in Windows OS:
  - Febooti Hash and CRC:
    - Using a third-party tool (www.febooti.com), install this program on your Windows PC, then right-click on the file you wish to calculate the hash for, select Properties, and then the Hash/CRCtab.
  - HashMyFile:
    - (http://www.nirsoft.net/utils/hashmyfiles.html) is a portable program to display the hash values of chosen directories and files using various hashing techniques (for example, md5, SHA 256).

System memory

- Memory refers to the physical component of a computer that stores data for immediate or later usage.
- According to how long information is retained on them, we may distinguish between two primary sorts.
  - Volatile memory: Stores data for a limited period; in fact, it requires electricity to maintain data, but when the power is switched off, it quickly loses its contents. RAM is an example of volatile memory.
  - Non-volatile memory: Even if the power is switched off, the nonvolatile memory may keep data for a long time. This is most commonly used for long-term storage. Computer hard drives, flash memory, and ROM is examples of this type of memory (read-only memory).

Types of computer memory storage

-

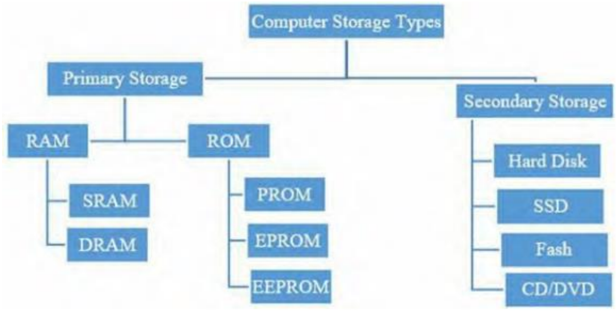


Figure 2.8: *Computer memory types*

Types of computer memory storage

- Primary storage
  - This form of storage, often called main storage or system storage, contains a volatile memory that loses data when the power is switched off.
  - Primary storage is used to temporarily store data and programs, and it has a smaller storage capacity, and faster read/write operations than secondary storage.
  - It is also more expensive.
  - RAM and cache are the two types of primary storage memory found in computers (CPU memory).
- Secondary storage
  - Secondary storage is non-volatile, long-term storage.
  - Without secondary storage, all programs and data would be lost the moment the computer is switched off.
  - There are three main types of secondary storage in a computer system: solid-state storage devices, such as USB memory sticks.

Types of computer memory storage

- Backup storage
  - External memory or auxiliary memory are other terms for secondary storage.
  - This is a type of non-volatile memory that keeps its contents whether the power is on or off.
  - It is used to keep data for a long time.
  - Secondary storage is slower than primary storage, such as RAM, but it is far less expensive.

Cloud computing

- Cloud computing is a modern technological model that allows a service provider to deliver various computing services to users over the internet as a result of the explosive growth of the internet and online communications.
- For example, rather than buying an external hard drive to store your backup data, you can store it for a small fee on a cloud provider.
- The cloud provider will be in charge of user data management in the cloud (for example, making backup copies and protecting this data from malicious software and cyberattacks).
- Cloud computing is not just for storing user data; it is also being used by businesses to cut IT infrastructure costs. Instead of purchasing a software license for each user individually, a company can use a cloud computing service that provides needed applications (such as the MS Office suite) for its work.
- When using expensive software such as SQL Server and Windows Server OS, the cost appears to be higher; however, paying for such software on a usage basis while in the cloud is more cost-effective than installing it on-premises.

Cloud computing

- Software as a service (SaaS)
  - In this model, a user purchases a cloud computing account and then chooses which applications he or she wants to install. Instead of using these applications on a local machine, a user will do his or her work on a cloud (remote) server.
  - Google Apps for Education and Microsoft Office 365 are two examples of such services.
- Platform as a service (SaaS)
  - This model is popular among software/Web development companies, in which a customer—for example, a Web development company—pays for an account with a cloud service provider that provides a customized environment based on the needs of the client (for example, to install needed
  - Web development tools, prepare the development and testing environment, and so on).
  - This enables a customer to begin work quickly and at a low cost

Cloud computing

- Infrastructure as a service (SaaS)
  - In this model, a cloud provider rents out the client’s required hardware (physical server and data center hardware) over the internet.
  - The client purchases and installs required applications and operating systems and then configures them to meet business requirements.
  - Web hosting companies and businesses typically use this service for data storage, backup, and recovery outside of their offices.
  - What we are interested in learning from this discussion is how cloud computing services will make it more difficult for law enforcement to investigate criminal cases.
  - For example, if a UK citizen is a suspect in a criminal case and his data is uploaded to a cloud storage provider in Singapore, can the UK police force the Singaporean provider to hand over a copy of the user data?