Digital Forensics

Digital forensics is the process of collecting, analyzing, and preserving digital evidence, sometimes so that it can be submitted as evidence in court during legal proceedings.
When digital forensics (DF) and incident response (IR) come together, when investigating and responding to a security incident to gather and preserve evidence, the term ‘DFIR’ is often used.

Digital Forensics Process

1. **Identification** – The first stage identifies potential sources of relevant evidence or information (devices), as well as key custodians and location of data.
2. **Preservation** – The process of preserving relevant electronically stored information (ESI). This is done by protecting the crime or incident scene, capturing visual images of the scene, and documenting all relevant information about the evidence and how it was acquired.
3. **Collection** – Collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
4. **Analysis** – An in-depth systematic search of evidence relating to the incident being investigated. The outputs of the examination are data objects found in the collected information. These outputs may include system and user-generated files. The analysis aims to draw conclusions based on the evidence found.
5. **Reporting** – Reports are based on proven techniques and methodology and other competent forensic examiners should be able to duplicate and reproduce the same results.

Fundamentals

Data Representation

- Binary
- Base64
- Hexadecimal
- Octal
- ASCII

Binary

- It is a simple and elegant design.
- Binary’s 0 and 1 method is quick to detect an electrical signal off or on state.
- The positive and negative poles of magnetic media are quickly translated into binary.
- Binary is the most efficient way to control logic circuits.

Base64

- Base64 is a reversible encoding algorithm

Hexadecimal

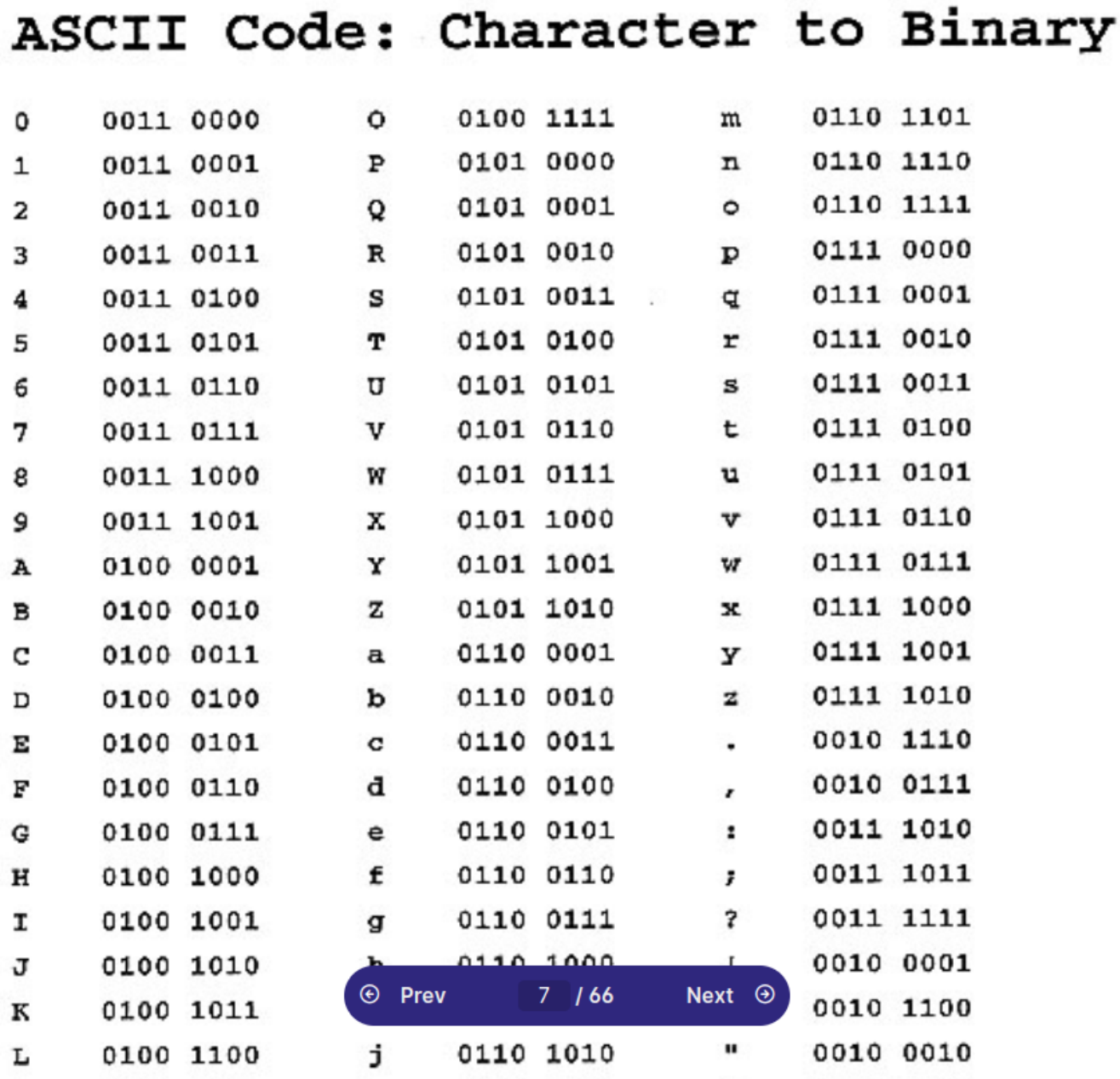
- Hexadecimal is a system we can use to write and share numerical values
- it’s no different than the most famous numeral systems (the one we use every day): decimal
- Combines a set of digits to create large numbers.
- Hex uses a set of 16 unique digits.
- Hex uses the standard 0-9, A, B, C, D, E, and F.

Denary	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

ASCII

ASCII (American Standard Code for Information Interchange) is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is

represented with a 8-bit binary number (a string of eight 0s or 1s).



ASCII Code: Character to Binary

0	0011 0000	O	0100 1111	m	0110 1101
1	0011 0001	P	0101 0000	n	0110 1110
2	0011 0010	Q	0101 0001	o	0110 1111
3	0011 0011	R	0101 0010	p	0111 0000
4	0011 0100	S	0101 0011	q	0111 0001
5	0011 0101	T	0101 0100	r	0111 0010
6	0011 0110	U	0101 0101	s	0111 0011
7	0011 0111	V	0101 0110	t	0111 0100
8	0011 1000	W	0101 0111	u	0111 0101
9	0011 1001	X	0101 1000	v	0111 0110
A	0100 0001	Y	0101 1001	w	0111 0111
B	0100 0010	Z	0101 1010	x	0111 1000
C	0100 0011	a	0110 0001	y	0111 1001
D	0100 0100	b	0110 0010	z	0111 1010
E	0100 0101	c	0110 0011	.	0010 1110
F	0100 0110	d	0110 0100	,	0010 0111
G	0100 0111	e	0110 0101	:	0011 1010
H	0100 1000	f	0110 0110	;	0011 1011
I	0100 1001	g	0110 0111	?	0011 1111
J	0100 1010	h	0110 1000	(	0010 0001
K	0100 1011				0010 1100
L	0100 1100	j	0110 1010	"	0010 0010

Hard Disk Drive Basics

A hard disk drive (HDD) is a non-volatile memory hardware device that controls the positioning, reading and writing of the hard disk, which furnishes data storage. Hard disk drives are commonly used as the main storage device in a desktop computer or laptop. HDDs will typically store an operating system, software programs and user-created files such as documents. Hard disk drives are commonly found in drive bays and are connected to the motherboard via an ATA, SATA, or SCSI cable, and also connected directly to a power supply unit (PSU).

Platters

A hard disk drive platter (or disk) is the circular disk on which magnetic data is stored in a hard disk drive. Hard drives typically have several platters which are mounted on the same spindle. A platter can store information on both sides, requiring two heads per platter.

Sectors

In computer disk storage, a sector is a subdivision of a track on a magnetic disk or optical disc. Each sector stores a fixed amount of user-accessible data, traditionally 512 bytes for hard disk drives, while

newer HDDs use 4096-byte (4 KiB) sectors.

Clusters

A cluster, in the context of a hard disk, is a group of sectors (described above) within a disk and is the grouping by which disk files are organized. A cluster is larger than a sector, and most files fill many clusters of disk space. The hard drive is able to find all the clusters on a disk because each cluster possesses its own unique ID value.

Slack Space

Slack space is the leftover storage that exists on a computer's hard disk drive when a computer file does not need all the space it has been allocated by the operating system. The examination of slack space is an important aspect of computer forensics as we can find the remaining data from previous files allocated in the same cluster.

Solid State Disk Drive Basics

A solid-state drive (SSD) is a new generation of storage devices. SSDs have evolved beyond traditional mechanical hard disks by using flash-based memory which is significantly faster, allowing SSDs to speed up computers significantly because of their low read-access times and fast throughputs.

Garbage Collection

Garbage collection is a process used by solid-state drives to optimize space and improve efficiency. The goal of garbage collection is to keep as many empty blocks as possible so that when the SSD needs to write data, it can do so without waiting for a block to be erased.

Trim

When files are sent to locations such as the Recycle Bin, they are not immediately deleted. Moving them to this location tells the operating system that it is ok to overwrite these files, as they are no longer wanted by the user. TRIM on an SSD will simply select the data and clear it, removing any chance of forensic investigations recovering the file, or parts of the file.

Wear Leveling

Wear leveling is a technique that some SSDs utilize to increase the lifetime of the memory using a very simple approach: evenly distribute writing on all blocks of an SSD so they wear evenly. Using this method, all physical cells in the SSD receive the same number of writes, to avoid writing too often on the same blocks, causing damage over time.

File System

A filesystem is a set of data types that is employed for:

- Data storage
- Hierarchical categorization
- Data management
- File navigation
- Accessing the data
- Recovery of data

There are many different kinds of file systems:

- FAT16
- FAT32
- NTFS
- EXT3 / EXT4

FAT16
FAT16 is the original file system used in DOS and Windows 3. x, and was originally only designed for use on relatively small partitions. If there is an issue, and the File Allocation Table is lost or damaged, the data on the hard disk can't be used because the operating system is unable to locate the files.

FAT32
FAT32 is a revised version of FAT16 that can be used to create much larger partitions and has native support for long filenames and was introduced with Win98.
Advantages:

- It is compatible with a huge variety of devices: smartphones, tablets, computers, digital cameras, gaming consoles, surveillance cameras, and so on.
- It is also cross-compatible with almost all operating systems that were launched since 1995. FAT32 works with Windows 95 OSR2, Windows 98, XP, Vista, Windows 7, 8, and 10. MacOS and Linux also support it.

Disadvantages

- FAT32 can only work with files that are less than 4 GB in size.
- FAT32 only works with partitions with a maximum capacity of 8 TB.
- If you have a drive that is formatted in FAT32, you do not get any data protection in case of power loss.
- The FAT32 file system does not include any built-in file compression features.
- FAT32 was not designed to be secure and does not include any built-in encryption features

NTFS
NTFS (NT File System) is a proprietary journaling file system developed by Microsoft. Starting with Windows NT 3.1, it is the default file system of the Windows NT family. improved support for metadata and advanced data structures to improve performance, reliability, and disk space use.
NTFS is supported in other desktop and server operating systems as well. Linux and BSD have a free and open-source NTFS driver, called NTFS-3G, with both read and write functionality. macOS comes with read-only support for NTFS, but due to write support for NTFS being unstable, file writing is disabled by default.

EXT3 / EXT4
Linux architecture

- User Space – The applications are located in the user space, which sends system calls to the system call interface. System call is nothing but a request that is sent to the kernel of the operating

system, for a service.

- Kernel Space – Kernel is the core of the operating system that answers the system calls from the user space by providing the requested resources, managing the I/O (input/output) devices, memory devices, file management etc.
- Disk Space – The device driver in the kernel space sends the I/O request to the hard disk of the system which contains critical file data.

Third extended filesystem (Ext3), is a journaled file system that is commonly used by the Linux kernel. It is the default file system for many popular Linux distributions.

The stable version of ext4 was introduced in 2008 by Linux. The maximum volume size of data supported by ext4 is 1exbibyte and file size is up to 16 tebibytes. The maximum length of the filename is 56 bytes. The fragmentation in terms of physical blocks where data is stored, is replaced by extents. This modification, which was not available in ext2 and ext3, increased the performance of the file system. Extent is a data storage area that reduces file fragmentation and file scattering.

Digital Evidence and Handling

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form. There are a wide range of forms that digital evidence can take.

- **E-mails** - These can contain written communication between two or more individuals, and may also contain files as attachments.
- **Digital Photographs** - The photos themselves can be evidence, additionally extra information may be present as photo metadata, which can include the location and device used to take the photograph.
- **Logs** - System logs can contain a wide range of information, depending on the device that has created the log, and the level of logging enabled. Examples can include Windows Event logs that can show login times to show when a user account was accessed.
- **Files** - User files such as notes, code, images, installed software, and more can all provide context about the activity of a user.
- **Messages** - Similar to emails, messages (text, iMessage, Facebook Messenger, WhatsApp, etc) can provide information about a conversation between two or more individuals.
- **Browser History** - This can help us to understand what websites and resources have been accessed from a device, and at what time.
- **Backups** - If files have been deleted, they may be present in backups, allowing us to investigate them even if they have been overwritten on the original storage medium.
- **Video/audio files** - These files, similarly to digital photographs, could be evidence themselves, but could also have metadata to help provide additional information.

Evidence Handling

Proper handling and securing of evidence are critical. Mistakes in how evidence is acquired can lead to

that evidence being tainted and, subsequently, not forensically sound.
There are several key tenets for evidence handling that need to be followed

- **Altering the original evidence**
  Actions taken by digital forensics examiners should not alter the original evidence.
- **Using write-blockers**
  Although most forensic software tools have built-in software write blockers, you also need an assortment of physical write blockers to cover as many situations or devices as possible. A write blocker is used to keep an operating system from making any changes to the original or suspect media to keep from erasing or damaging potential evidence. Software write blockers work at the operating system level and are specific to the operating system.
- **Document**
  One central theme you will often hear in law enforcement is the phrase: “If you didn’t write it down, it didn’t happen.” This is especially true when discussing digital forensics. Every action that is taken should be documented in one way or another. This includes detailed notes and diagrams. Another way to document is through photographs. Proper documentation allows examiners to reconstruct the chain of events if ever the integrity of evidence is called into question.

Order of Volatility

When examining digital evidence, it is important to understand the volatile nature of some of the evidence an examiner will want to look at. Volatile evidence is evidence that can be lost when a system is powered down. For network equipment, this could include active connections or log data that is stored on the device.

1. **Registers & Cache**
   The contents of the CPU cache and registers are extremely volatile since they are constantly changing. An investigator needs to retrieve data from the cache and register immediately before that evidence is lost.
2. **Memory**
   The information located on random access memory (RAM) can be lost if there is a power spike or if the system is disconnected from power. This is a fast, temporary, type of memory in which programs, applications and data are stored.
3. **Disk (HDD and SSD)**
   We know that once data has been overwritten, it is impossible to recover it, and SSDs have the additional risk of Garbage Collection or TRIM deleting files that could be used as evidence. If the system is offline then the disk space can’t be overwritten and the disk is no longer considered volatile.
4. **Remote Logging and Monitoring Data**
   The potential for remote logging and monitoring data to change is much higher than data on a hard drive, but the information is not as vital. So, even though the volatility of the data is higher here, we still want that hard drive data first.

5. **Physical Configuration, Network Topology, Archival Media**
   Here we have items that are either not that vital in terms of the data or are not at all volatile. The physical configuration and network topology is information that could help an investigation but is likely not going to have a tremendous impact.

Metadata and File Carving

Metadata is information that describes the data and can include details such as the author of the document, and in photos, it can contain the camera settings, GPS location, resolution, and much more. **File carving** is a process of searching for files in a data stream and is used to carve deleted files from disk images, so we can investigate files that have been deleted by a user, provided they haven't been overwritten with new data. (Linux command-line tool : Scalpel)

Metadata Linux commands: ls -lisap {file} and stat {file}
A great command-line tool we can use in Kali Linux is exiftool, which works to retrieve metadata from files. **Usage: exiftool {filename}**

Memory, Pagefile, and Hibernation File

Memory
In computing, memory refers to a device that is used to store information for immediate use in a computer or related computer hardware device. Computer memory operates at a high speed, for example, random-access memory (RAM), as a distinction from storage that provides slow-to-access information but offers higher capacities.
Memory Analysis
Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.
Memory Dump
A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant. A memory dump can contain valuable forensics data about the state of the system before an incident such as a crash or security compromise, such as running processes, network connections, and malware that doesn't take the form of files, but instead resides purely in memory.
Pagefile.sys
The Pagefile.sys is used within Windows operating systems to store data from the RAM when it becomes full. The Pagefile.sys is a contiguous file, so it can be read more quickly, that is located on the root of the hard drive and, normally, the more infrequently used memory pages are stored to it. Whilst RAM is used by the system to store active data as, due to the speed of its operation of it, the system functions more quickly than if that data were stored and read from the hard drive. However, through normal use, RAM is filled by the system and then Windows is able to identify which data to move from it to the Pagefile.sys where it can remain until required again.

It can also be used as a backup of data in the event of a system crash. By default, the Windows operating system configures the size of the Pagefile.sys, however, it can also be altered by the user.

Normally the Pagefile.sys can be a significant proportion of data present on the hard drive, however, removing it can greatly reduce the operating speed of the computer.

The Swap file in Linux

Similar to Windows, Linux uses swap space to store RAM when it is full or when the data is not in current use. Within Linux however, traditionally it is a swap partition rather than a swap file and is therefore separate from the other files as it is contained on its own partition.

Hibernation File

Starting with Windows 2000, Microsoft introduced the hibernation feature that allows the operating system to store the current state of operation when you turn off the computer, or the system goes into sleep mode. During hibernation everything from memory is copied to the disk in a file called hiberfil.sys, when the computer is restored, the system moves to the saved state. Hibernation files are a good source of information for digital forensic practitioners, as they store data in RAM file without having to run special tools.

Hashing and Integrity

Hashes

Hash values, which come in the form of text strings, are the unique fingerprint of a file or string.

Gathering Hashes in Windows

get-filehash {file} (default:SHA-256)
get-filehash -algorithm md5 {file}

Gathering Hashes in Linux

sha256sum {file}
md5sum {file}
sha1sum {file}

Evidence Integrity

In most investigations involving a hard drive, a hash will be generated from the hard drive, and then a complete copy of the storage media will be taken at a bit-by-bit level, meaning that everything possible from the disk is copied to a fresh hard drive. This new hard drive then has its hash generated, to ensure that this is the exact same value as the original, proving that an exact copy was successfully generated.

Evidence Collection

Equipment

- Forensic Laptop or Workstation
- Electro-Static Evidence Bags with Tamper-proof Stickers
- Labels
- Photographs
- Grounding Bracelets
- Hardware Write-Blockers
- Blank Hard Drives

Specialist Equipment

- Wireless Stronghold/Faraday Boxes – to block any wireless signals from reaching the evidence, preventing remote access or wiping.
- Specialized Write-Blockers – write-blockers that could also be used on cell phones, GPS devices, IoT devices, and other non-standard hard drives.
- Phone Jammers – acting the same as a faraday box or wireless stronghold.
- Dedicated Flash Drives – containing tools like Encase, FTK, CSILinux, and MacQuisiton

ACPO Principles

The main principles of the ACPO Good Practice Guide for Computer-Based Electronic Evidence are:

ACPO Principle 1
That no action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

ACPO Principle 2
Where a person finds it necessary to access original data held on a digital device, that the person must be competent to do so, and able to explain their actions and the implications of those actions on the digital evidence to a Court.

ACPO Principle 3
That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third-party forensic expert should be able to examine those processes and reach the same conclusion.

ACPO Principle 4
That the individual that is leading the investigation has the overall responsibility to ensure that the ACPO principles are followed throughout the investigation.

Chain of Custody

The Chain of Custody is a crucial process within computer forensics, and its primary purpose is to ensure that all of the evidence collected in a case has not been tampered with by an unauthorized individual and the original evidence remains unchanged. This involves documenting various information regarding the evidence, such as who, when, and how the evidence was copied or transferred to another person. The Chain of Custody should be maintained from the moment the evidence was collected or acquired to when it is presented in court.

Evidence Integrity Hashing
Before you even think about starting to perform analysis on digital evidence or making a forensic copy of it, or even opening the evidence on your workstation, you should always calculate its hash first. Since hashes are small strings that are unique (with the exception of hash collisions) to the input, they are a quick and easy way to ensure evidence integrity.
If the evidence is physical, such as an external hard drive, you should use a hardware write blocker

when you connect your workstation to the device. Write blockers only allow the workstation to have read access on the device and blocks any attempts to write to it.

Taking a Forensic Copy
Once the hash of the evidence has been recorded, it is best to make a forensic copy of the original evidence if possible and perform analysis on the copy, as this will allow the original evidence to remain untouched.

Storing Digital Evidence
Physical evidence should be stored in antistatic bags which prevent damage through electric discharge to the data it holds. Taking a step further, Faraday cages may be used, which prevents wireless communication and cellular signal exchange of the device within it. In any case, the evidence should be kept within a locked container, which only the authorized examiners have access to, and kept within an authorized personnel's watch during transportation.

Chain of Custody Form
Every forensic examiner who works with the evidence should fill out a Chain of Custody form. The form should include the description of the evidence when/where it has been acquired or transferred, and by whom, the contacts of the examiners, how the evidence has been accessed, collected or stored and other details regarding the evidence.

Disk Imager: FTK Imager

Collect forensically-sound copies of hard drives, which can later be analyzed to retrieve evidence.

Live Forensics

Volatile artifacts often only exist while a system is turned on, and shutting the system off would cause these artifacts to be lost. This volatile data could be extremely important to an investigation, so it's crucial to collect it, but not jeopardize other data that could be affected by aspects such as SSDs that use Garbage Collection or TRIM. To acquire volatile data, but not leave the system running for extended periods of time where unnecessary, live forensics techniques can be used to quickly acquire evidence. Data stored in RAM quickly fades once a system is powered off, and while there are ways to preserve it, acquiring this information while the system is online is the most effective.

Live Acquisition: KAPE

KAPE is an efficient and highly configurable triage program that will target essentially any device or storage location, find forensically useful artifacts, and parse them within a few minutes.

Windows Investigations

Windows Artifacts - Programs

LNK Files / Shortcut Analysis

- LNK files are used by the Windows OS to link one file to another, which is how we can have application shortcuts that work as a redirector – so when we click on a shortcut it will go and find the application wherever it resides in the file system and runs the corresponding application. We can collect valuable metadata from LNK files such as the location of the folder it is linked to, the date the LNK file was created, modified, last accessed, the file size, and more.
- LNK files can be found at: C:\Users$USER$\AppData\Roaming\Microsoft\Windows\Recent
- To view these files in a human-readable format, we can use Windows File Analyzer.

Prefetch Files

- Prefetch files can provide us with incredibly useful information about programs including the name of the application, the path to the executable file, when the program was last run, and when the program was created/installed.
- Prefetch files can be found at: C:\Windows\Prefetch
- To view these files in a human-readable format, we can use Prefetch Explorer Command Line also known as PECmd.exe.

Jump List

- Using the Windows Jump List feature we are able to find two different types of files: automaticDestination-ms and customDestination-ms. These files contain information about applications that are pinned to the taskbar, such as the file path, timestamps, and application identifiers (AppIDs).
- The Jump List files can be found at: C:\Users% USERNAME%\AppData\ Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- C:\Users%USERNAME%\AppData\ Roaming\Microsoft\Windows\Recent\CustomDestinations
- To analyze these files we can use tools such as JumpList Explorer.

Windows Artifacts - Browsers

- Cookies
- Favorites
- Downloaded Files
- URLs Visited
- Searches
- Cached Webpage
- Cached Images

Tools:

- KAPE
- Browser History Viewer
- Browser History Capturer

Windows Artifacts - Logon Events

Identifying what user accounts have logged into a system, and at what time, can be useful for both digital forensic investigations and incident response. Doing so can help us attribute activity to a user account by showcasing they were the account signed in before these events occurred.
Windows Event Logs are stored at the following location: C:\Windows\System32\winevt\Logs.
Event IDs:

- Event ID 4624 (Successful Logon)
- ID 4672 (Special Logon)
- ID 4625 (Failed Logon)
- and ID 4634 (Logoff)

Windows Artifacts - Recycle Bin

The Windows Recycle Bin is a system folder designed to temporarily store deleted files and folders before they are permanently removed from the computer's hard drive or storage device. When a user deletes a file or folder in the Windows operating system, it is typically moved to the Recycle Bin, allowing the user to restore the item if it was deleted accidentally. However, once the Recycle Bin is emptied, the items within it are considered permanently deleted.

- **Recovery of deleted files**: Files that have been recently deleted and are still present in the Recycle Bin can be easily restored by forensic examiners. This can provide valuable evidence or information related to a case, as it may contain relevant documents, images, or other data that were intentionally or unintentionally deleted.
- **Tracing user activity**: The presence of specific files in the Recycle Bin can indicate a user's attempt to delete evidence or conceal their activities. Forensic experts can analyze the metadata of the deleted files, such as timestamps and file paths, to establish a timeline of events and identify potential motives or patterns of behavior.
- **File remnants and data carving:** Even after the Recycle Bin has been emptied, the underlying data of the deleted files may still be present on the storage device. When a file is deleted, the operating system typically marks the occupied space as free, but the actual data remains until it is overwritten by new data. Forensic examiners can use specialized tools and techniques, such as data carving, to recover these remnants and reconstruct the deleted files, providing additional evidence for an investigation.
- **Analysis of Recycle Bin artifacts**: The Recycle Bin maintains several system files that store information about the deleted items, such as their original file paths, deletion timestamps, and other metadata. These artifacts can be valuable for forensic investigations, as they can help investigators understand the user's actions and intentions, as well as provide context for other digital evidence.

On Windows 10, we can find the Recycle Bin directory for all users located at C:$Recycle.Bin
If the user has emptied the Recycle Bin, we lose this artifact and cannot analyze it.

Tools:

- Command Prompt (CMD)
- RBCmd
- CSVQuickViewer

Linux Investigations

Linux Artifacts: Passwd and Shadow

/etc/shadow, contains encrypted passwords as well as other information such as account or password expiration values. The /etc/shadow file is readable only by the root account to prevent standard users from grabbing the contents and then using a tool such as hashcat or John The Ripper to brute force, perform a dictionary attack, or use rainbow tables to crack the hashes and reveal the plaintext passwords.
/etc/passwd file is used to keep track of every registered user that has access to a system. All users will have read access, but only super users will have the ability to write to the file.

Linux Artifacts: /Var/Lib and /Var/Log

On Debian-based systems, we can find a very useful file at the following location: /var/lib/dpkg/status. This file includes a list of all installed software packages, and can be a gold mine if you're looking to see what programs the user has installed to the system.

Operating System Logs:

- **/var/log/auth.log** – Contains system authentication information, including user logins.
- **/var/log/dpkg.log** – Contains information that is logged when a package is installed or removed using the 'dpkg' command. This is similar to the packages command from the var/lib section above.
- **/var/log/btmp** – This file contains information about failed login attempts.
- **/var/log/cron** – Whenever the cron daemon starts a cron job, it logs the information about the cron job in this file. This is useful because cron jobs can be abused for persistence on a system.
- **/var/log/secure** – Contains information related to authentication and authorization privileges.
- **/var/log/faillog** – Contains user failed login attempts.

Web Server Logs

- The client IP address making the request
- The resource they are trying to access
- The HTTP method, which will most often be GET (to get a resource, such as images in a web page)
- The user-agent used by the client IP (this should typically be a browser user-agent, such as Chrome, Firefox, etc)
- and the timestamp of the reques
- var/log/apache2/access.'log

Linux Artifacts: User Files

Hidden files and directories

ls -a = list directory contents and do not ignore entries starting with "."

Clear files and directories (Desktop, Trash, Documents, Downloads)

- A user’s desktop
- A user’s default directories, including; Downloads, Music, Pictures, Public, Templates, Videos
- The Trash Bin

Steganography

- “The practice of concealing messages or information within other non-secret text or data.”
- cat Dog.jpg secretmessage.zip > Dog2.jpg

Tools:

- exiftool
- steghide

Volatility

Volatility is an open-source memory forensics framework for incident response and malware analysis.

Autopsy

- Autopsy is a forensic-grade tool that is used by the military, law enforcement, and corporate examiners to investigate what happened on a smartphone or a computer.
- Autopsy has a plug-in architecture that allows the user to find add-on modules or even develop custom modules written in Java or Python, providing additional functionality and automation.
- This awesome tool comes built-in with Kali Linux, and can also be downloaded and used on systems running the Windows operating system for free.