Disk Image Forensics

Dr. Darryl J D'Souza
Mob No: 9986382162

Disk Image Forensics

Digital storage devices, such as hard drives, solid-state drives, and USB drives, hold vast amounts of data that can be crucial to digital forensics investigations. Disk image forensics is the process of analyzing these devices and their contents to look for useful information during an investigation.

A disk image is a snapshot of a storage device's structure and data typically stored in one or more computer files on another storage device. Traditionally, disk images were bit-by-bit copies of every sector on a hard disk often created for digital forensic purposes, but it is now common to only copy allocated data to reduce storage space. Compression and deduplication are commonly used to reduce the size of the image file set.

Forensic imaging is the process of creating a bit-by-bit copy of the data on the drive, including files, metadata, volume information, filesystems and their structure. Often, these images are also hashed to verify their integrity and that they have not been altered since being created. Unlike disk imaging for other purposes, digital forensic applications take a bit-by-bit copy to ensure forensic soundness. The purposes of imaging the disk is to not only discover evidence preserved in digital information but also to examine the drive to gather clues of how the crime was committed.

Dr. Darryl J D'Souza

Write blocker

Digital evidence is our major issue of concern in Forensic investigation. Forensic investigators need to absolutely assure of the fact that the data they obtain as digital evidence is not altered during the capture, analysis, and control.

In the courtroom everyone including attorneys, judges, jurors need to feel confident that digital evidence has not been tampered and is legitimate.

How can you be assured that digital evidence has not tampered? According to the NIST-National Institute of Standards and Technology, the investigator follows a certain set of rules and procedures to prevent the execution of any program that might modify the contents of the disk. Some of these procedures are:

- Use an operating system and other software that is trusted to not to write anything to the disk without any explicit instruction.
- Use hard disk write block tools to prevent any hard disk writes.
- Wherever possible, set a hardware jumper to make the disk read-only.

What are Write Blockers?

Write Blocker is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data. A write blocking if used correctly can guarantee the protection of the chain of custody. NIST has issued a set of general guidelines for write blocking requirements:

- The write-blocker tool shall not allow a protected drive to be changed.
- The write-blocker tool shall not prevent any operations to a drive that is not protected.
- The write-blocker tool shall not prevent obtaining any information from or about any drive.

What are the different types of Write Blockers?

- Hardware Write Blocker
- Software Write Blocker

Hardware Write Blocker

Hardware write blockers are used to intercept and block any modifying command from ever reaching the storage device. Some of its features include:

- They offer monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.
- They provide built-in interfaces to a number of storage devices.
- Hardware write blockers can connect to other types of storage with adapters.
- Hardware devices that write block also provide a visual indication of function through LEDs and switches. This makes them easy to use and makes functionality clear to users.

Challenges of using Hardware Write Blockers:

- Hardware write blocking devices are very expensive.
- They are awkward to use since they require a physical connection and a different connector for each type of interface for IDE, SCSI, USB, etc.
- Hardware write blockers are comparatively slower as they need to perform protocol conversions.

Hardware Write Blocker

Dr. Darryl J D'Souza

Software Write Blocker

Software write blockers are installed on a forensic workstation. According to NIST's specification on software Write Blocker, a software write blocker tool operates by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface. They provide the ability to simultaneously write block as many disk devices as are connected to a computer without the need for multiple expensive hardware write blocking devices. Some of the features that are provided by different write blocking tools are:

- The user can control automatic write blocking policies for fixed and/or removable disks.
- The user can have write blocking tool remember each fixed device's blocked or un-blocked status for ease of use on media repeatedly used on a workstation/laptop.
- Some of the write blocking tools provide a GUI interface that allows the user the ability to block and unblock any disk or flash storage device.

Benefits of using Software Write Blockers: There are some benefits in using Software Write Blockers instead of Hardware Write Blockers.

- They offer faster imaging than using hardware-based write blockers.
- Software write blockers are more affordable than the hardware ones as they don't need a separate physical connector to be attached to the device for write blocking.

Live Analysis

Live Analysis

System live analysis is a good practice to conduct a light investigation and to have first look at potential incident to determine if any serious issue is there which needs detailed traditional forensics analysis.

Just keep in mind that we should be well trained to conduct the live analysis as unlike working on forensics images we may have only one chance to do it right. Therefore:

- Maintain forensic integrity and Minimize system changes.
- Avoid installing any tools on the target system.
- Avoid copying anything on the target system.
- Validate the publisher of third-party tools.
- Use light tools which require minimum user interaction.
- When its possible record the results for further analysis.
- Prepare chain of custody and document everything
- Generate hash value forever collected data and record them.
- Document All the steps!

What to look for?

One of the main factors in a successful investigation is to know what to look for! Otherwise, we get confused as much as Alice was in the wonderland.

Digital Forensics Wonderland: A considerable amount of forensics images [hardsik, RAM, memory cards…], Logs, data, records, etc. that make investigators' life miserable if you don't have a proper strategy [sop, cheatsheet, playbooks, and indeed enough expreince] to formulate initial hypothesises. We should actively sharpen our skills by understanding the different Techniques, Tactics, and Procedures (TTP) used by cybercriminals, and learn how to look for their traces.

Two essential concepts that help us to investigate a potential case:

- Indicators of Compromise
- Indicators of Attack

What to look for?

IoC and IoA: Game of Indicators!

Indicators of compromise (IoC) is a forensics artifact left by intruders in systems or network logs that proves some form of malicious/suspicious activity or infection has occurred.

In contrast, **Indicators of attack (IoA)** is any sign of the beginning of a malicious or suspicious activity that helps us to detect them at early stages or even before they become a successful attack.

IoCs are retrospective by nature as they mainly help to discover the breaches that have happened in the past.

Vs.

IoAs are actively identifying ongoing attacks or any activity that may lead to a potential breach.

What to look for?

The proactive system analysis is a little bit challenging as we are looking for any potential malicious activities rather than following a specific indicators.

We should collect and examine different evidences to look at first and make the decision on further investigation accordingly.

The six categories that are used in proactive system analysis while looking for any potential malicious activities

- System Information and configurations
- Users, Groups and Privileges
- Services and Applications
- Process, Dlls, and Handle
- Network and Internet
- Files and Scripts

Note 1: *The above checklist is for high-level live analysis. We may need more details for in-depth forensics investigation and root cause analysis.*
Note 2: *Windows logs and registry are valuable sources of data for investigators.*

Windows: Technical Checklist

1. System Information and Configurations

One of the first actions we should do as an investigator is to study the current state of the windows machine. It gives us an overall idea of how to plan the rest of the analysis.

Data Types: Current System settings and configurations [e.g. OS installation date, essential folders, hotfixes, drives, Environment Variable, shadow copies, top-level network information, etc.]

Investigation Value: To understand the current state of the machine and to plan accordingly.

For you to try

- *Winver - It's a straightforward yet useful command to quickly check the version and build the number of running Windows.*

- systeminfo

We can filter out specific information by using the findstr command. For instance, if we look for OS name and version, we can use the command below:

systeminfo | findstr /B /C:"OS Name" /C:"OS Version"

- SET Command - Environment variables

Windows: Technical Checklist

2. Users, Groups and Privileges

Abusing valid users' credentials, manipulating existing accounts, or creating new accounts upon initial access are common techniques used by attackers. These techniques are not only for gaining initial access and can be used for persistence, privilege escalation, or even defence evasion.

Data Types: User account information, login timestamps, account activities, account groups, and privileges.

Investigation Value: To look for any questionable activities related to user accounts such as suspicious and unexpected login hours, locations, and privileges.

For you to try - net users

net user "Username"

net user username | findstr /B /C:"Last logon"

wmic useraccount list full

wmic useraccount get /?

wmic useraccount get name, accounttype, sid, status

net localgroup

net localgroup [Group name]

Windows: Technical Checklist

3. Services and Applications

Cybercriminals target different layers of any organization from technology, to people and processes. Vulnerable services and applications can open the door for them, so as an investigator, we should proactively examine any available services and installed application to look for any security issues.

Data Types: List of enabled services and installed applications along with their versions and configurations.

Investigation Value: To look for any possible vulnerability, weakness, and misconfiguration that may be used by attackers as an entry point.

For you to try -

Reg Query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /S

reg query hklm\software\microsoft\windows\currentversion\uninstall /s | find "DisplayName“

For more info : https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg-query

Windows: Technical Checklist

4. Process, Dlls, and Handle

Identifying mysterious running processes is very curial for every investigation as it may help to detect ongoing attacks. It's not all about running malware or suspicious processes, it could be a standard windows process that is misusing by an attacker.

Data Types: All running process [name, location, hash, parent ID], all the loaded DLLs, and open handles [Files, Folders, Registry Keys].

Investigation Value: To look for any malicious [Known Bad] or suspicious [Potential Unknown Bad] processes, and attacks such as DLL injection!

For you to try -

https://learn.microsoft.com/en-us/sysinternals/downloads/

Windows: Technical Checklist

5. Network and Internet

Many factors tag this network information as one the most crucial point of investigation such as remote access attacks, Botnets and C&C, remote trojans, and any type of network-based attacks. Besides, a careless end-user with Internet access has become a preferred attack vector for cybercriminals to walk into our digital environment. Thus, all web browsing and Internet surfing activities must be investigated carefully as well.

Data Types: Active connections, the process to port mapping, enabled protocols, visited URLs, installed extensions, downloaded files, and browsing history.

Investigation Value: To look for any suspicious remote accesses, visited URLs and IPs, malicious network connections, etc.

For you to try -

netstat –a - to find all of the listening *and* established connections on the PC

netstat –an - names in the output have been turned into IP addresses

Netstat –anb -Windows processes that are listening or have these connections open

netstat -ano |find /i "ESTABLISHED"

Windows: Technical Checklist

5. Network and Internet

netstat -ano |find /i "ESTABLISHED“

-a: Shows all connections, including those that are listening and not currently transferring data.

-n: Displays numerical addresses instead of trying to resolve hostnames (faster execution).

-o: Shows the process ID (PID) and the name of the program associated with each connection.

|find /i "ESTABLISHED": This pipes the output of netstat to the find command.

/i makes the search case-insensitive.

"ESTABLISHED" tells find to search for lines containing the word "ESTABLISHED".

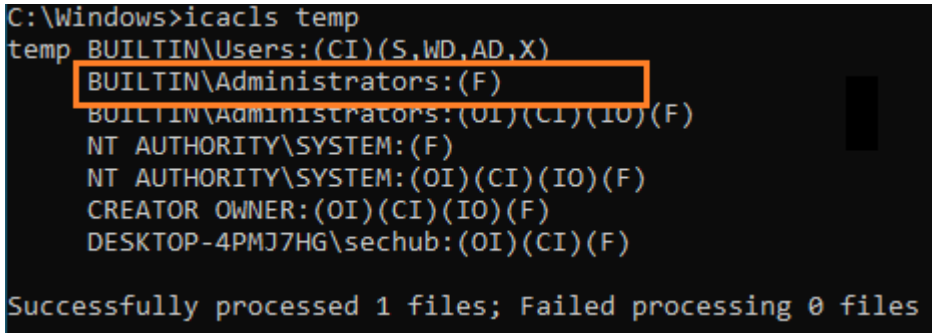
Windows: Technical Checklist

6. Files and Folders

Finally files and writable folders [common ones in particular suchas windos, temp, download].

Data Types: Executable files, Scripts, password protected or hidden files, compressed files, all downloaded files, etc.

Investigation Value: To look for any suspicious file or scripts.



https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/icacls