## Introduction

Forensic image analysis is the systematic examination of visual evidence, such as photographs, videos, and digital images, to reveal pertinent information that can aid investigations and legal proceedings. Whether it's identifying individuals, analyzing crime scenes, or enhancing low-quality images, this discipline employs a range of methods and tools to extract valuable details.

## Key Objectives of Forensic Image Analysis

- Identification: Forensic analysts use image analysis to identify suspects, victims, or objects captured in visual evidence. This can involve facial recognition, matching tattoos, or distinguishing characteristics.

- Scene Reconstruction: Analyzing crime scene images helps reconstruct events, timelines, and spatial relationships, providing crucial context for investigators.

- Enhancement: Techniques like image sharpening and contrast adjustment can clarify blurry or poorly lit images, revealing hidden details.

- Authenticity Verification: Forensic experts can determine if an image has been manipulated or tampered with, ensuring the integrity of evidence.

- Comparative Analysis: Side-by-side comparisons are made between questioned and reference images, aiding in the evaluation of similarities or differences.

## Four Steps in Analysis of Forensic Image:

The forensic analysis process includes four steps:

1. Use a write-blocker to prevent damaging the evidentiary value of the drive.
2. Mount up and/or process the image through forensics software.
3. Perform forensic analysis by examining common areas on the disk image for possible malware, evidence, violating company policy, etc.
4. If potential evidence is identified, perform further analysis to determine the cause and establish the timeline of the event(s).

## Using a Write-blocker

What is a write-blocker and how does it relate to computer forensics? A write-blocker is a device that allow acquisition of information on a drive and acts to prevent the possibility of accidentally damaging the evidentiary value of the drive contents. The write-blocker allows *read* commands to pass, but blocks *write* commands — hence the name.

So, what's the big deal even if you accidentally wrote on the image? It calls into question the integrity of the image (the legal term is "spoliation"), and it can make evidence easily dismissible in court. A single byte of change will cause the cryptographic hash, usually MD5 or SHA-1, of the image to change, rendering the entire image as potentially inadmissible in a legal proceeding. For this reason, companies tend to outsource forensic services to trusted professionals to ensure these costly mistakes are avoided.

Write-blockers can range anywhere from $25-$500, depending on the advanced features included. Write-blockers are typically hardware you use to plug the drive into first, then connect to a computer. Nowadays, software programs (for example, SAFE Block by ForensicsSoft) offer write-blocking capabilities without the hassle of dealing with hardware. Note that these types of software licenses can be pricey.

## Mounting/Processing the Image

After making sure the drive is write-protected, an analyst can view the data in the image that was created. The image is typically mounted by or 'loaded into' forensics software, such as FTK Imager from AccessData, for analysis which usually involves searching various areas on the disk for evidence of malicious activity or presence of malware.

If litigation is potentially involved, you may want to stay away from using any open-source software or custom tools that are developed when performing analysis, as the source code can be called into question by a defense attorney. Results identified using an open-source tool on a very complex or high-profile case may damage the integrity of the overall investigation. The debate of using open-source tools versus proprietary tools in digital forensics will always be ongoing. Regardless of how you conduct your investigation, be aware that for every tool you use, you must have a reasonable explanation for why that tool was chosen when questioned.

Once the image is mounted, this will allow the ability to manually browse through the directories on the image and view files, logs, executables, deleted files, etc. Manually browsing the image can be quite risky for various reasons, but mainly you're analyzing data with your naked eye. The only time this is typically done is when someone needs to gain qualitative information quickly.

The other option is to process the image through a professional forensics package such as FTK, X-Way Forensics, EnCase, Oxygen Forensics, etc. These applications will automate the categorization of the different types of files resident on the image. The only downside to doing this is that it time- and

resource-intensive, depending how on the size of the image. But this is the preferred method because it helps the investigator carve through the image carefully and thoroughly. It's much easier to find file paths with the way most forensic tools processes and categorizes the files, and file paths are the key to answering the question, "what happened here?"

## Logical Locations to Analyze

Now that the drive is write-protected and mounted for analysis, we can start viewing the contents of the image, but there are so many places to look. Where do we start?

Typically, common areas such as the desktop, downloads folder, document folder are good places to begin just to confirm there aren't any obvious executables stored there. Other key areas are the Downloads storage location and common libraries (DLLs for Windows systems), Other places that can give a significant amount of info are the browsing history files — that is if the hacker hasn't deleted them. Depending on which browser was being used, each browser stores their cache/history in their unique directories. Two common sources for history files are Chrome and Outlook.

- For Chrome, you can find the cache and history file in C:\Users\(username)\AppData\Local\Google\Chrome\User Data\Default.
- The *Index.dat* file is a common place to review to understand a user's browsing history.
- If emails are involved, check to see if you can still retrieve the PST/OST files. For Outlook 2016, you can find the PST files in Documents\Outlook Files but will need special software to view it. The offline Outlook Data File (.ost) is also saved at C:\Users*(username)*\AppData\Local\Microsoft\Outlook.

If your system has been compromised by an advanced threat, the actor(s) may well have 'camouflaged' themselves, requiring a deeper dive into the entire

system. This usually includes the investigators review of the registry keys and other global and application-specific settings.

The hierarchical database of Registry Keys contains configuration data critical for the operation of Windows and the applications and services that run on Windows. Altering these settings can redirect DNS queries, load injected libraries, change the “pointer” to which binary image is loaded, and more.

## Sandboxing Malware

If malware is found in one of the locations we’ve analyzed, to completely understand it’s purpose and extent, the malware must be closely evaluated. Sandboxing is a great method to use to analyze the behavior of malware and to observe outbound connections, processes running in the background, registry changes, other payloads downloaded, etc. A sandbox is a system that can be used in an effort to mitigate system failures or software vulnerabilities from spreading, while observing the behavior of software, as found in Next Generation firewalls.

For forensic purposes, we use a sandbox to ‘explode’ malware, or run the malware, in an isolated environment where we can document the behavior and hopefully identify the malware. At the very least, we can document the activities taken by the malware. To be sure, malware authors have become much savvier when creating their products and have built new capabilities into the malware to evade sandbox identification and detection.

There are several different types of mainly open-source sandboxes that can be used to test malware. The following are commonly used today:

- Malwr
- Hybrid Analysis
- Joe’s Sandbox
- The Cuckoo Sandbox

Typically, at the end of the sandboxing phase, a report is generated that details everything identified regarding the operation of the malware. It will detail malicious and suspicious indicators, screenshots of the malware running, network traffic analysis, and other details. This can significantly help an investigator analyze the behavior and provide additional guidance toward further routes of investigation.