www.codelivly.com

DIGITAL FORENSICS HANDBOOK

CODELIVLY
LEARN CYBERSECURITY

TABLE OF CONTENTS

1.Introduction

In today's digital age, the proliferation of cyber threats and the increasing reliance on digital systems necessitate a robust approach to investigating and mitigating digital crimes. Digital forensics is the practice of collecting, analyzing, and preserving electronic evidence to support the detection and prosecution of cybercriminal activities. This handbook serves as a comprehensive guide for both novice and experienced digital forensics practitioners, providing detailed methodologies and tools required for effective digital forensic investigations.

2. Digital Forensics Investigation Methodology

Understanding the core principles and systematic approaches to digital forensic investigations is crucial. This section covers the structured process that ensures the integrity and admissibility of digital evidence, guiding practitioners through the essential steps of a successful investigation. The digital forensics process may change from one scenario to another, but according to NIST SP800-86, it typically consists of four core steps: collection, examination, analysis, and reporting.

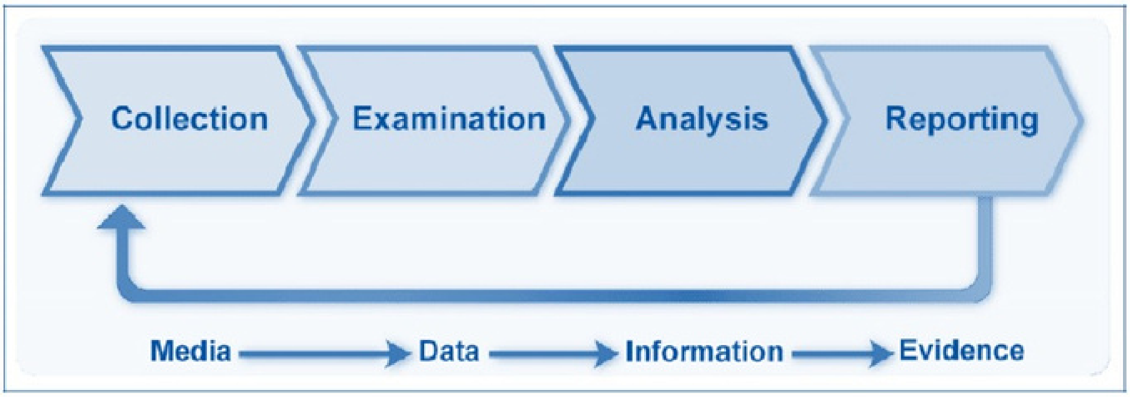


Figure 1. Digital Forensics Process Model - NIST SP800-86

Collection

The collection phase involves acquiring digital evidence, usually by seizing physical assets like computers, hard drives, or phones. It is critical to ensure that data is not lost or damaged during collection (Preservation). You can prevent data loss by copying storage media or creating images of the original. The collection phase starts by identifying the evidence of interest.

Examination

The examination phase involves identifying and extracting data. It can be divided into several steps: prepare, extract, and identify.

When preparing to extract data, you can decide whether to work on a live or dead system. For example, you can power up a laptop to work on it live or connect a hard drive to a lab computer. During the identification step, you need to determine which pieces of data are relevant to the investigation. For example, warrants may restrict an investigation to specific pieces of data.

Analysis

The analysis phase involves using collected data to prove or disprove a case built by the examiners. Here are key questions examiners need to answer for all relevant data items:

- Who created the data
- Who edited the data
- How the data was created
- When these activities occur

In addition to supplying the above information, examiners also determine how the information relates to the case.

Reporting

The reporting phase involves synthesizing the data and analysis into a format that is understandable to laypeople. These reports are essential because they help convey the information so that all stakeholders can understand it.

Note: Chain of custody must be maintained during all phases of the forensics investigation.

3. Building Your Forensics Toolkit

A well-prepared toolkit is fundamental to any forensic investigation. This chapter provides instructions on:

- Building a Bootable USB Drive: Creating a portable and reliable tool for initiating forensic analysis on compromised systems.
- Preparing Your Forensics Workstation: Setting up a dedicated environment optimized for forensic tasks.
- Preparing The Evidence Drive: Ensuring secure and organized storage for collected evidence.

Building a Bootable USB Drive

The main reason for having a bootable USB drive with you is to collect Volatile data from live suspect machines.

1. Wipe the USB drive and overwrite it with Zeros you can use the following command:

- **Windows:** `Format d: /fs.exfat /p:1`
- **Linux:** `dd if=/dev/zero of=/dev/sda bs=1M`

You can replace "d:" and "/dev/sda" with your target drive

2. Download and install/copy your favorite tools to the USB drive

   I recommend at least the following tools:

cmd.exe
nbtStat.exe
Now
Route
Cryptcat.exe
Diskmap.exe
MD5Deep.exe
sha1Deep
sha256deep
NLSinfo.exe
PSList.exe
PSLoggedon.exe
PortQry.exe
PSFile.exe
Autoruns
Wee
procmon
Procdumb
FLOSS
Netstat
Netcat
Dumpit.exe
FTK Imager

Preparing Your Forensics Workstation

You can choose whatever OS you prefer. However, some very nice Linux distributions are tailored for Digital Forensics and are free to use.

For example, you can use the SIFT workstation by SANS which is highly recommended and comes with many of the tools you need preinstalled already.

You can download it from the following link:
https://www.sans.org/tools/sift-workstation/

Hint: If you are preparing your own forensics workstation, make sure you verify the hashes of every tool you download before using it.

Preparing The Evidence Drive

Similar to what we have done when preparing the USB drive, the evidence drive (or drives) must be wiped as well, to make sure we have a clean new drive to be used in our evidence collection process.

To Wipe the evidence drive and overwrite it with Zeros you can use the following command:

- **`Windows:`** `Format d: /fs.exfat /p:1`
- **`Linux:`** `dd if=/dev/zero of=/dev/sda bs=1M`

You can replace "d:" and "/dev/sda" with your target drive

You can also use the Eraser tool by Heidi, which can be downloaded from:

https://eraser.heidi.ie/

4. Evidence Acquisition

Acquiring digital evidence is a delicate process that requires precision and adherence to legal standards. This section delves into various techniques for gathering evidence from different sources:

- **Acquiring Volatile Memory:** Techniques for capturing data stored in volatile memory before it is lost.
- **Acquiring Disk Image:** Methods for creating exact replicas of storage media.

- **Acquiring Network Evidence:** Collecting data from network traffic to identify malicious activities.
- **Remote Evidence Collection:** Strategies for gathering evidence from remote locations.
- **Cloud Evidence Collection:** Navigating the complexities of collecting evidence from cloud-based environments.

Acquiring Volatile Memory

To capture the memory dump of the target machine, follow these straightforward steps:
Open **FTKImager.exe”**

- Choose File - Memory capture
- Choose the target USB drive
- Check (Include pagefile) option
- Check the (Create .AD1 file) option to include deleted files, slack space, and unallocated space drive
- Click Capture memory

You can download FTK Imager from the following link:
https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1

Alternatively, you can use other available tools such as:

- **Dumpit.exe**
- **WinPmem**
- **Ram Capturer**
- **Belkasoft Live RAM tool**

Acquiring Disk Image

Live Imaging:

Live imaging involves capturing an image of a system that has been powered up. There are many tools available to acquire a full disk image from the target suspect machine. Two of the most common tools are FTK Imager and Kroll Artifact Parser and Extractor (KAPE).

They both have straightforward GUI interfaces which can be easily navigated. They are both compatible with most Windows OSs.

You can download FTK Imager from the following link:

https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1

You can download KAPE from the following link:

https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

If you want to use Linux for imaging you may use the dd command as shown below:

1. Show connected disks:

```
fdisk -l
```

2. Image the selected drive where "/dev/sdb" is the source dive:

```
dd bs=64k if=/dev/sdb of=target.dd
```

3. Verifying the hash of the file:

```
Md5sum usb2gb.dd
```

Dead-box acquisition:

also known as static imaging, involves capturing an image of a system that has been powered down. This method ensures that the data remains unchanged during the imaging process, as the system is in a static state.

When performing Dead-box acquisition, you might want to use a physical write blocker such as (Tableau Forensic Bridge Kit). It is a physical hardware that sits between the evidence drive and the system performing the acquisition which only allows data to be passed in a one-way direction from the evidence disk to the analysis workstation.

To create a disk image using FTK Imager click on File – Create Disk Image – Select Physical Drive – Choose E01 or dd as the Destination type – and specify the destination Folder and File name.

Virtual Systems Acquisition:

To acquire the running memory from a VMware instance you need to collect the following files:

1. Virtual Memory (VMEM) file.
2. VMware Suspended State (VMSS) file.

You can combine both files into a single file by the following steps:

1. Pause the VMware instance.
2. Create a “.dmp “file by running the following command:

```
C:\Program Files (x86)\VMware\VMware Workstation>vmss2core.exe
suspect.vmss suspect.vmem
```

To acquire a full disk image from a VWware instance, follow the steps below:

1. Pause the VMware instance.
2. Copy the “.vmdk” file and mount it to a new drive.

Acquiring Network Evidence

You may want to inspect the logs from some of the following devices for network-related evidence:

- Firewalls
- Web Proxy Servers
- Web Application Firewalls
- NetFlow traffic from network devices such as Routers and switches.

You can also inspect the network traffic of the suspect machine by establishing a packet capture using tools like Wireshark, WinPcap, or tcpdump.

To download Wireshark:

https://www.wireshark.org/download.html

To download tcpdump:

http://www.tcpdump.org/

To download WinPcap:

https://www.winpcap.org

Remote Evidence Collection

This method includes data which is collected from systems that are suspected of being compromised. Our goal is to collect high-value data in a central location where it can be indexed and further analyzed.

These are some of the ways that can utilized for remote evidence collection:

- Endpoint Detection and Response (EDR) if available.
- Velociraptor (https://docs.velociraptor.app)
- WinPmem (https://github.com/Velocidex/WinPmem)

Cloud Evidence Collection

Amazon Web Services (AWS)

1. Create EC2 volume snapshot.
2. AWS will always assign the root drive (C:\) to /dev/sda1, that is of you only want to collect the root drive.
3. Under the Actions tab click Create Snapshot.
4. Then you may Create a new volume using the snapshot you have taken. This can be done by clicking on the Action tab, then “Create volume from snapshot” option.

To acquire a memory dump of an instance in AWS, simply switch the EC2 instance to Hibernation mode and copy the “hyberfil.sys” file. Alternatively, you can also use any of the traditional OS memory acquisition methods explained earlier in this document.

Microsoft Azure

The acquisition process of Microsoft Azure VMs is pretty similar to AWS, with some minor differences. It includes the following steps:

1. Create an Azure VM snapshot of the target machine (Snapshot page – Create Snapshot
2. Select Full snapshot
3. Select the Source disk

To export the VM snapshot directly:

1. Go to Settings
2. Select Export Snapshot
3. A URL with the virtual hard disk “.VHD’ file will be generated

4. Download the “.VHD” file for further investigation

To capture the memory dump of an Azure VM, you may connect to it via SSH or RDP. Alternatively, you can utilize a built-in service called “Bastion” which is straightforward to use.

Google Cloud Platform (GCP)

GCP is also similar to AWS and Azure. Follow the steps below to collect the evidence from the Compute Engine instance:

1. Create a snapshot by navigating to Storage – Snapshots – Select Complete snapshot
2. Create a new instance and select the created snapshot as a Disk Source
3. Use the dd command to extract the disk image.

To acquire a memory dump from a GCP instance:

1. Create a service account via the GCP IAM component
2. Specify: Compute Admin – Storage Object Admin privileges
3. Connect to the target instance using GCP Cloud Shell using the service account you created or via RDP, then Create a memory dump using winpmem.exe or dumpit.exe

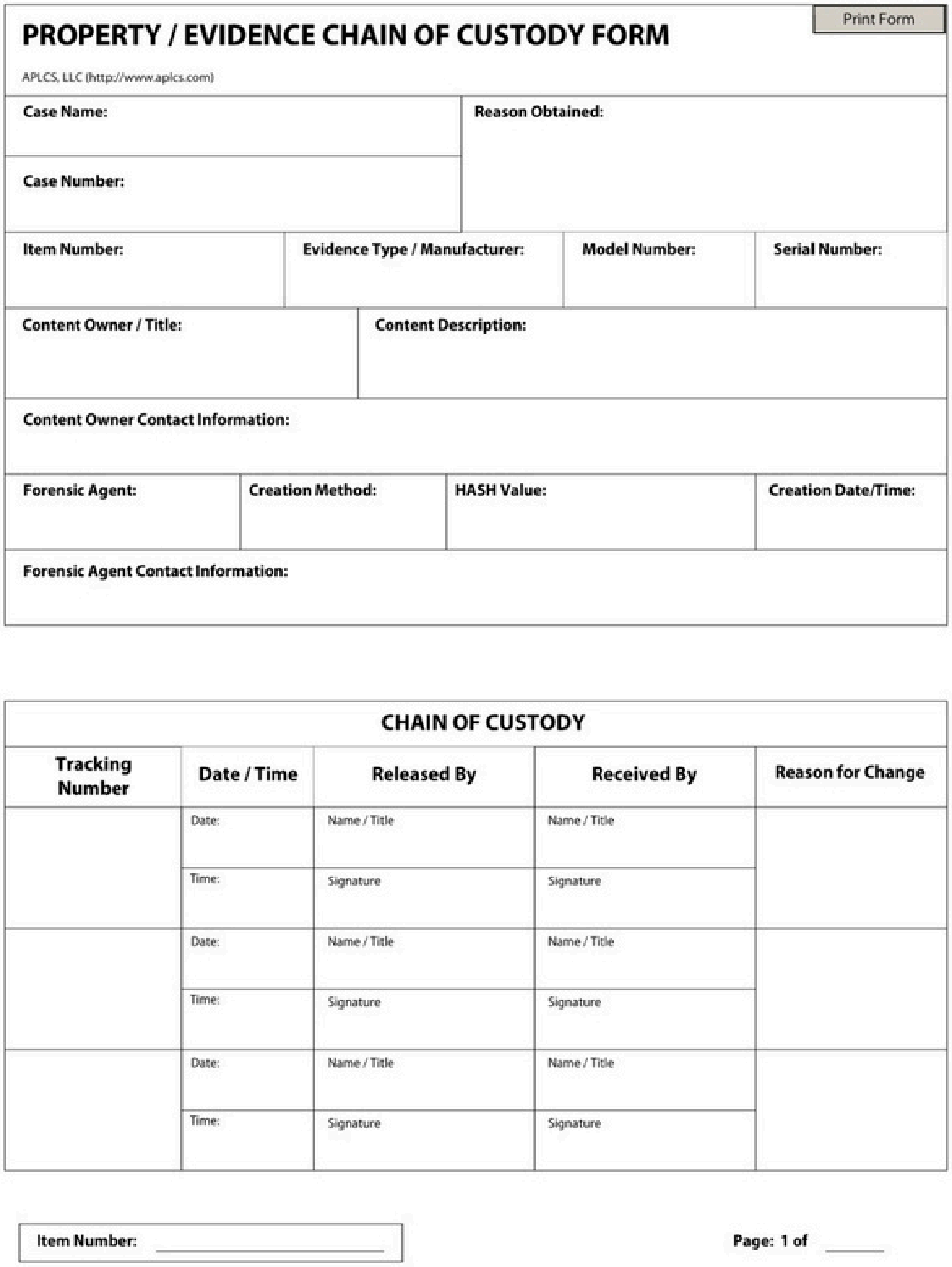
5. Preserving Evidence

Preservation of evidence is critical to maintaining its integrity and admissibility in court. The original evidence must be kept in its original state without any modifications and it should be kept in a safe place throughout the investigation process.

In addition, proper Chain of Custody must be followed and documented whenever someone handles the evidence***. “The chain of custody is the most critical process of evidence documentation. It is a must to assure the court of law that the evidence is authentic, i.e., it is the same evidence seized at the crime scene. It was, at all times, in the custody of a person designated to handle it and for which it was never unaccounted”*** By NIST.

In summary, evidence integrity is the cornerstone of a successful digital forensics investigation. It safeguards the reliability and trustworthiness of digital evidence, protects the rights of individuals involved in a case, and upholds the integrity of the criminal justice

A sample of a Chain of Custody document is shown below:



Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:

Reason Obtained:

Case Number:

Item Number:

Evidence Type / Manufacturer:

Model Number:

Serial Number:

Content Owner / Title:

Content Description:

Content Owner Contact Information:

Forensic Agent:

Creation Method:

HASH Value:

Creation Date/Time:

Forensic Agent Contact Information:

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date: Time:	Name / Title Signature	Name / Title Signature	
	Date: Time:	Name / Title Signature	Name / Title Signature	
	Date: Time:	Name / Title Signature	Name / Title Signature	

Item Number: ______________________

Page: 1 of ______

Sample of a Chain of Custody document
Source: https://rossum.ai/use-cases/miscellaneous/chain-of-custody-form/

6. Evidence Analysis

Analyzing the collected evidence is where the investigative insights are derived. This section covers various types of analysis, including:

- Memory Analysis: Examining data stored in RAM for traces of malicious activity.
- System Storage Analysis: Analyzing data stored on hard drives and SSDs.
- Log Files Analysis: Interpreting system and application logs to reconstruct events.
- Network Evidence Analysis: Investigating network traffic to identify patterns and anomalies.
- Cloud Environment Analysis: Assessing evidence obtained from cloud services.

Memory Analysis

During memory analysis, you might find interesting valuable data and information related to your investigation. This includes but is not limited to:

- Strings
- Running processes
- Loaded DLLs
- Device drivers
- Registry keys
- Network connections
- Command history

SANS lays out a six-step methodology for Memory Analysis, which includes the following steps:

1. Identify Rouge Processes
2. Analyze Process DLLs and handles
3. Review Network Artifacts
4. Look for evidence of code injection
5. Check for signs of a rootkit
6. Dump suspicious processes and drivers

Various free and commercial tools exist for conducting memory analysis. In this document, we will explore three of the most well-known free tools which are **Strings, Volatility, and Autopsy.**

Strings

Strings is a command-line tool that can be used to search for valuable text information in the memory dump file. This could include suspect names, usernames, IPs, files, hostnames, application names, and more.

It can be downloaded and installed from the following link:

https://docs.microsoft.com/en-us/sysinternals/downloads/strings

Below is an example of using Strings to dump all the strings in a memory dump to a text file via the command line:

```
strings “D:\memdump.mem” | t_wtee “D:\strings.txt”
```

The “w_wtee” option is used to display the output and write it to the text file

Apart from manually searching the Strings output, here are some common String searches that might be useful in your investigation:

“To find IP addresses, use the strings command with the following parameters:

```
strings pagefile.sys | grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b"
```

To find URIs and URLs, use http or https:

```
strings pagefile.sys  | grep "^https?://" | sort | uniq | less
```

To find email addresses, use the following command:

```
strings pagefile.sys | grep '([[:alnum:]_.-]{1,64}+@[[:alnum:]_.-
]{2,255}+?\.[[:alpha:].]{2,4})”
```

You can replace “grep” with “Select-String” if you are using Windows OS.

Another convenient option in strings is -n which allows you to specify the minimum number of characters for each string to be extracted.

Volatility

Volatility is an advanced open-source memory forensics command-line-based tool, which is available to be downloaded at:

https://github.com/volatilityfoundation/volatility

We will explore some of the common useful commands in Volatility below:

1. To display image information:

```
vol.py -f “/path/to/file” imageinfo
vol.py -f “/path/to/file” kdbgscan
```

2. To display process information:

```
vol.py -f “/path/to/file” --profile <profile> pslist
vol.py -f “/path/to/file” --profile <profile> psscan
vol.py -f “/path/to/file” --profile <profile> pstree
vol.py -f “/path/to/file” --profile <profile> psxview
```

3. To dump a specific process:

```
vol.py -f “/path/to/file” --profile <profile> procdump -p <PID> --dump-
dir=“/path/to/dir”
```

4. To check the DLL files associated with a process:

```
vol.py -f “/path/to/file” --profile <profile> dlllist -p <PID>
```

5. To display command line history:

```
vol.py -f “/path/to/file” --profile <profile> cmdline
vol.py -f “/path/to/file” --profile <profile> cmdscan
vol.py -f “/path/to/file” --profile <profile> consoles
```

6. To display network information:

```
vol.py -f “/path/to/file” --profile <profile> netscan
vol.py -f “/path/to/file” --profile <profile> netstat
```

7. Registry hives list:

```
vol.py -f “/path/to/file” --profile <profile> hivescan
vol.py -f “/path/to/file” --profile <profile> hivelist
```

8. To display ranges within memory that may contain injected code:

```
vol.py -f “/path/to/file” --profile <profile> malfind
```

Note: The examples below apply to Volatility version 2. For Volatility version 3 syntax, you may check out the following cheatsheet:

https://blog.onfvp.com/post/volatility-cheatsheet/

For more details and usage examples of Volatility, here are some useful resources:

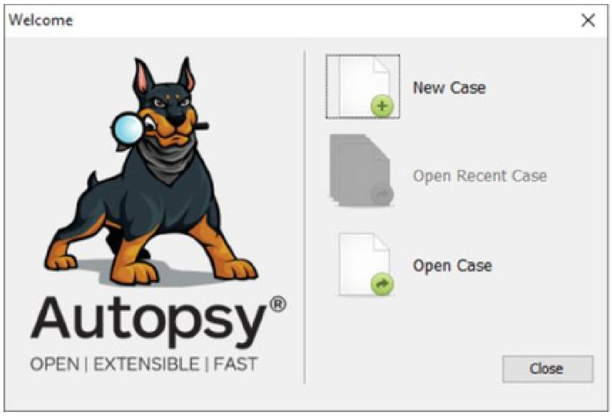
- https://blog.onfvp.com/post/volatility-cheatsheet/
- https://www.andreafortuna.org/2017/06/25/volatility-my-own-cheatsheet-part-1-image-identification/
- https://blog.onfvp.com/post/volatility-cheatsheet/
- https://memoryforensic.com/memory-forensics-cheat-sheets/

Volatility Workbench is a GUI tool for Volatility with the same functionality as the original CLI tool. ***You can download it here:***

https://www.osforensics.com/tools/volatility-workbench.html

Autopsy

Another great GUI tool we must mention here is Autopsy. Autopsy® is the premier end-to-end open-source digital forensics platform. It can be used in memory analysis, disk image analysis, log analysis, registry analysis, and many more use cases.



You Can download it from here:

https://www.autopsy.com/download/

To Start a new Digital Forensics case in Autopsy:

https://www.youtube.com/watch?v=fEqx0MeCCHg

SANS Memory Forensics Cheat Sheet:

https://www.sans.org/posters/dfir-memory-forensics/

System Storage Analysis

Autopsy can be very helpful in examining any of the following:

- Web artifacts (Downloads and history)
- Email artifacts
- Attached devices
- Recovering deleted files
- Timeline analysis
- keyword searches

Master Files Table Analysis ($MFT)

MFT can be found within the root directory of the filesystem. To analyze the MFT table you can use the MFT Explorer tool by Eric Zimmerman.

Eric Zimmerman has created a suite of tools for carving and analyzing data available at: https://ericzimmerman.github.io/#!index.md.

SANS cheat sheet for the tools is also available at:
https://www.sans.org/posters/eric-zimmerman-tools-cheat-sheet/

Prefetch Analysis

Prefetch files are beneficial for us to find out if specific executables have run in the past. You can use another tool by Eric Zimmerman called Prefetch Parser (PECmd.exe)/ Prefetch files are created in “C:\Windows\Prefetch” directory.

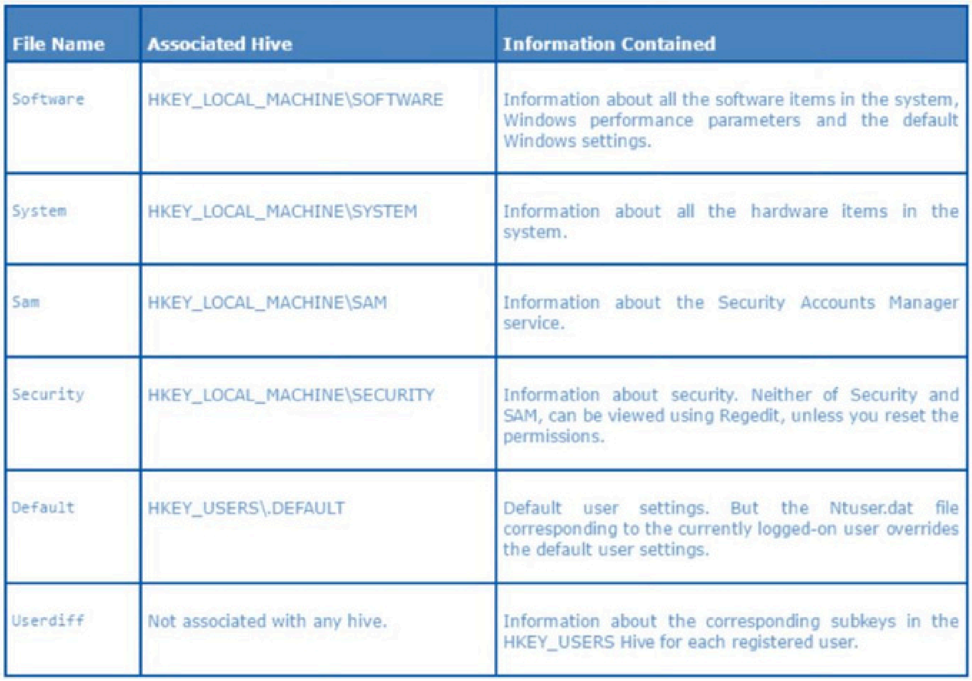
For a deep dive into Prefetch analysis, check out the following YouTube video: https://www.youtube.com/watch?v=f4RAtR_3zcs

Registry Analysis

The registry hives are located in “%SystemRoot%\system32\config” folder. They include 5 root keys:

- HKEY_LOCAL_MACHINE
  - SAM
  - Security

    - Software
    - System
- HKEY_CURRENT_USER
    - Ntuser.dat
    - Ntuser.dat.log
- HKEY_USERS
    - Default
    - Default.log
    - Default.sav
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG
    - System
    - System.alt
    - System.log
    - System.sav



File Name	Associated Hive	Information Contained
Software	HKEY_LOCAL_MACHINE\SOFTWARE	Information about all the software items in the system, Windows performance parameters and the default Windows settings.
System	HKEY_LOCAL_MACHINE\SYSTEM	Information about all the hardware items in the system.
Sam	HKEY_LOCAL_MACHINE\SAM	Information about the Security Accounts Manager service.
Security	HKEY_LOCAL_MACHINE\SECURITY	Information about security. Neither of Security and SAM, can be viewed using Regedit, unless you reset the permissions.
Default	HKEY_USERS\.DEFAULT	Default user settings. But the Ntuser.dat file corresponding to the currently logged-on user overrides the default user settings.
Userdiff	Not associated with any hive.	Information about the corresponding subkeys in the HKEY_USERS Hive for each registered user.

To examine the registry hives, we recommend using the “Registry Explorer” tool by Eric Zimmerman:
https://f001.backblazeb2.com/file/EricZimmermanTools/net6/RegistryExplorer.zip

For more information and documentation on Registry Explorer:
https://aboutdfir.com/toolsandartifacts/windows/registry-explorer-recmd/
Eric Zimmerman's tools Cheat Sheet
https://www.sans.org/posters/eric-zimmerman-tools-cheat-sheet/

Windows Registry Analysis 101:
https://www.forensicfocus.com/articles/windows-registry-analysis-101/

SANS Registry Cheat Sheet

https://tinyurl.com/y7ncd2vp

Log Files Analysis

Windows event log analysis is a crucial component of digital forensics that involves examining the event logs generated by the Windows operating system. These logs provide a detailed record of system, application, and security-related events, which can offer valuable insights into user activities, system changes, and potential security incidents.

Types of Windows Event Logs

1. **System Logs** : Record events related to the operating system and its components. This includes hardware changes, driver issues, and system startup and shutdown events.
2. **Application Logs** : Contain events logged by applications running on the system. This can include errors, warnings, and informational messages from software applications.
3. **Security Logs** : Capture security-related events, such as login attempts, logoffs, account management activities, and resource access. These logs are essential for identifying unauthorized access and other security incidents.

Key Elements in Event Log Analysis

1. **Event IDs**: Each event log entry is assigned a unique identifier (Event ID) that describes the type of event. Familiarity with common Event IDs helps investigators quickly identify significant events.
2. **Time Stamps**: Time stamps are crucial for constructing a timeline of events, correlating activities, and understanding the sequence of actions in the system.
3. **User Information**: Logs often include the username associated with an event, providing insights into who performed specific actions.

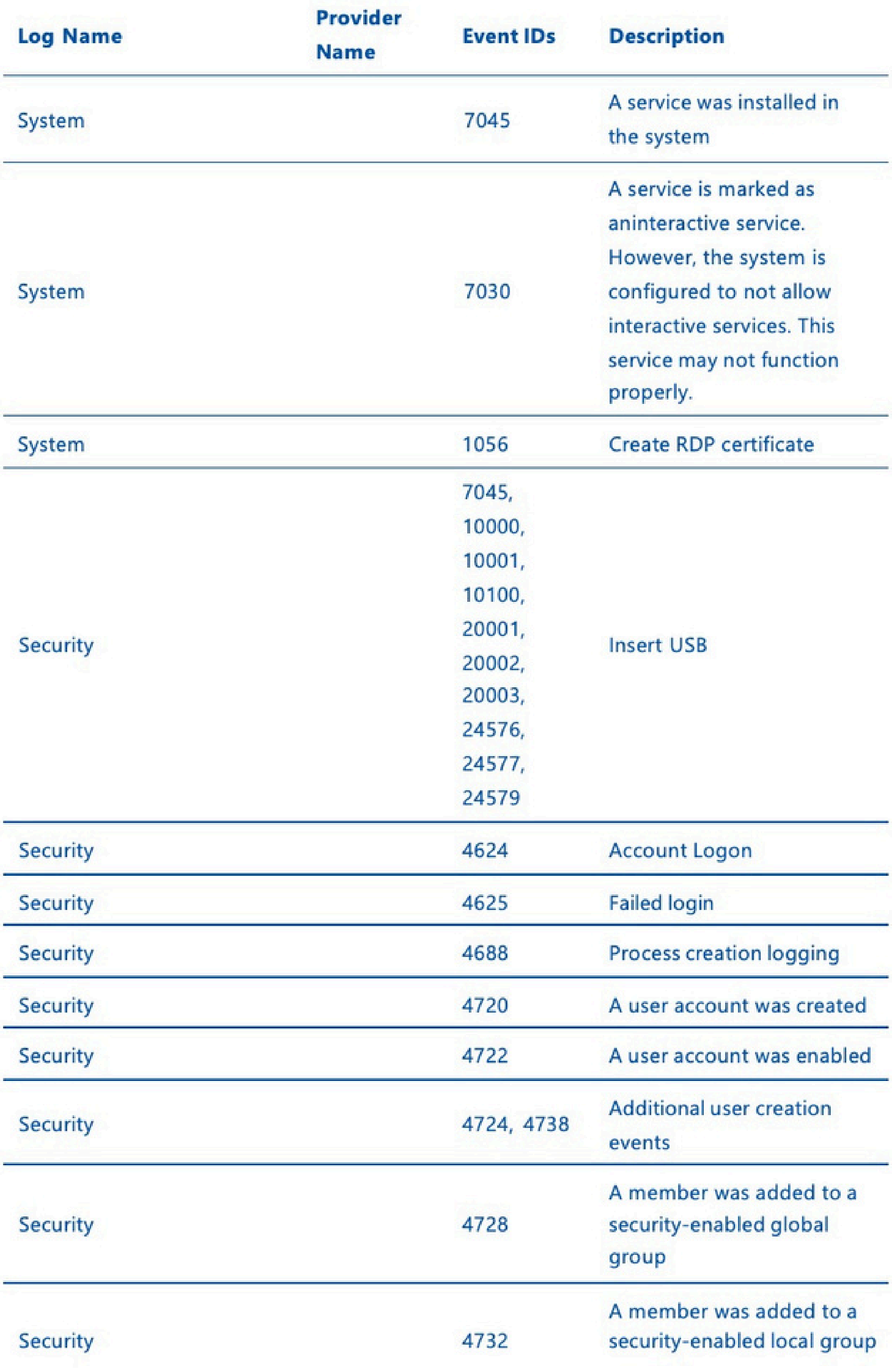
4. **Event Source**: Indicates the application or system component that generated the event, helping to identify the origin of specific activities.

Several tools can assist in analyzing Windows event logs, including:

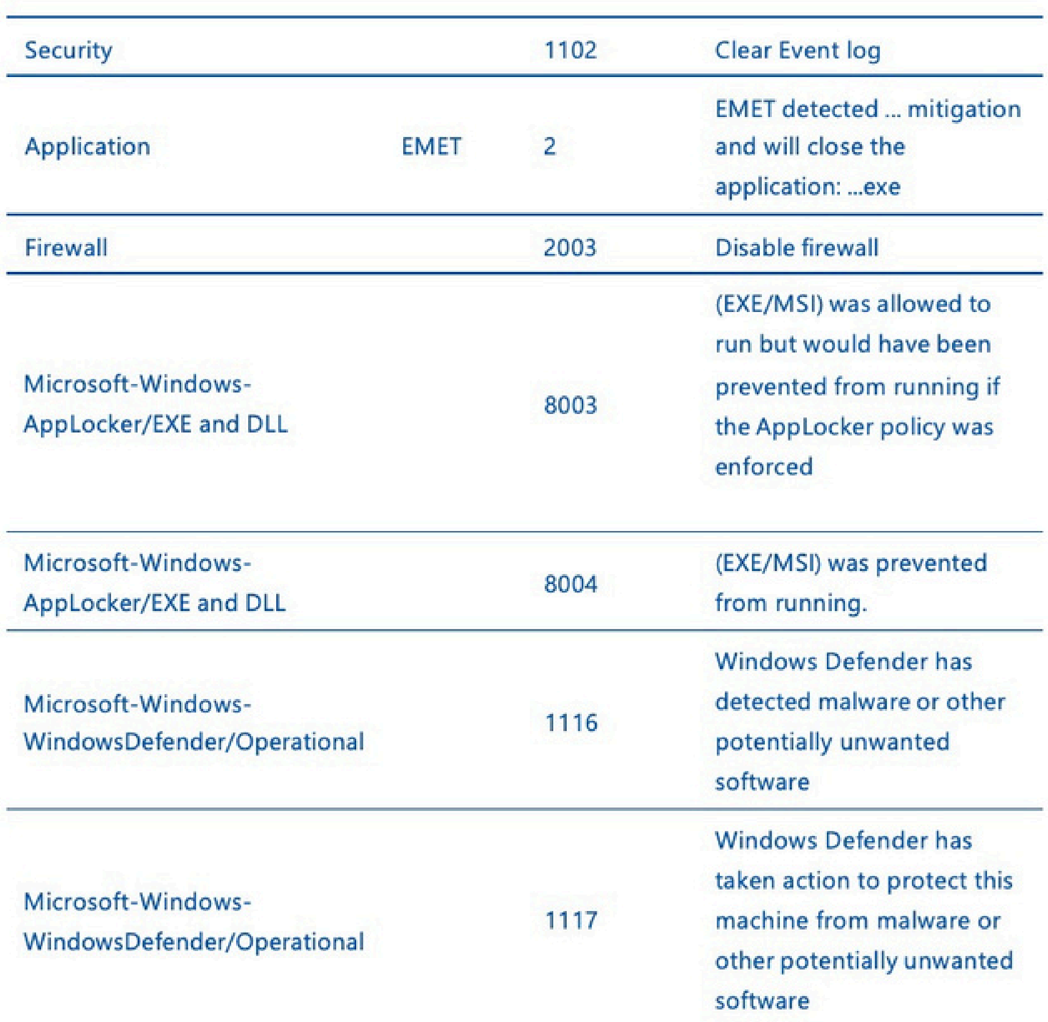
- **Event Viewer**: A built-in Windows utility that allows users to view and analyze event logs.
- **Log Parser**: A powerful tool from Microsoft for querying and analyzing log files, including event logs.

Event logs are located in the logs directory “C:\Windows\System32\winevt\logs”.

Here is a list of some of the common event IDs which could be useful in your investigation:



Log Name	Provider Name	Event IDs	Description
System		7045	A service was installed in the system
System		7030	A service is marked as aninteractive service. However, the system is configured to not allow interactive services. This service may not function properly.
System		1056	Create RDP certificate
Security		7045, 10000, 10001, 10100, 20001, 20002, 20003, 24576, 24577, 24579	Insert USB
Security		4624	Account Logon
Security		4625	Failed login
Security		4688	Process creation logging
Security		4720	A user account was created
Security		4722	A user account was enabled
Security		4724, 4738	Additional user creation events
Security		4728	A member was added to a security-enabled global group
Security		4732	A member was added to a security-enabled local group



Security		1102	Clear Event log
Application	EMET	2	EMET detected … mitigation and will close the application: …exe
Firewall		2003	Disable firewall
Microsoft-Windows-AppLocker/EXE and DLL		8003	(EXE/MSI) was allowed to run but would have been prevented from running if the AppLocker policy was enforced
Microsoft-Windows-AppLocker/EXE and DLL		8004	(EXE/MSI) was prevented from running.
Microsoft-Windows-WindowsDefender/Operational		1116	Windows Defender has detected malware or other potentially unwanted software
Microsoft-Windows-WindowsDefender/Operational		1117	Windows Defender has taken action to protect this machine from malware or other potentially unwanted software

Network Evidence Analysis

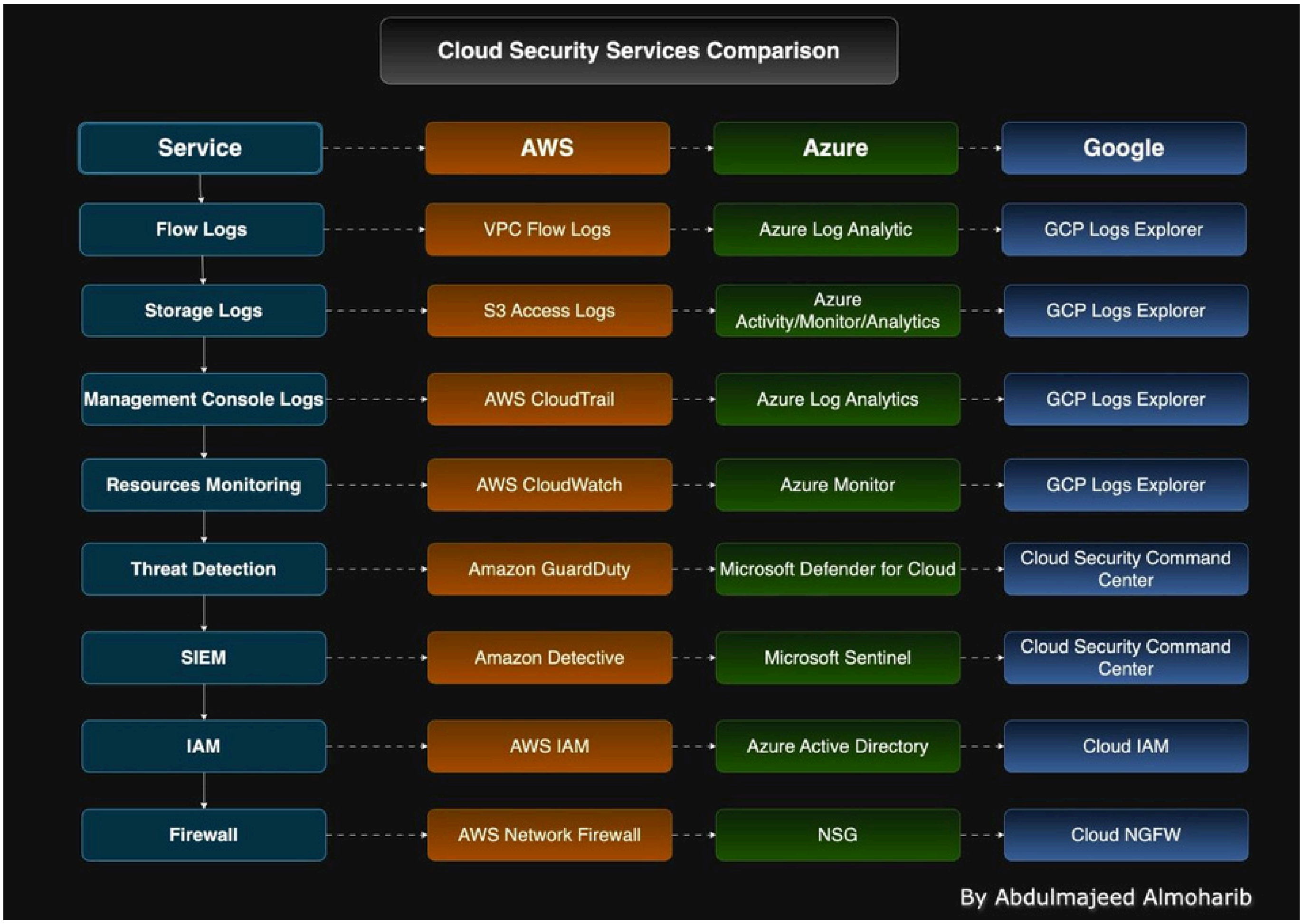
Network evidence analysis focuses on examining data transmitted over a network to uncover details about cyber incidents, unauthorized access, and other malicious activities. This type of analysis helps forensic investigators understand how attacks were carried out, and identify the source of the attacks.

Two of the most well-known tools for network packet analysis are:

1. Wireshark
   https://www.wireshark.org/download.html
2. Tcpdump
   https://www.tcpdump.org

Due to the complexity and length of explaining network packet analysis, we suggest watching this Network Forensics Fundamentals series by Phil Hagen: https://www.youtube.com/playlist?list=PLkb5lfjv-rnDZ-13i13BTRIdhXoGeyT99

Cloud Environment Analysis



Cloud Security Services Comparison

Service	AWS	Azure	Google
Flow Logs	VPC Flow Logs	Azure Log Analytic	GCP Logs Explorer
Storage Logs	S3 Access Logs	Azure Activity/Monitor/Analytics	GCP Logs Explorer
Management Console Logs	AWS CloudTrail	Azure Log Analytics	GCP Logs Explorer
Resources Monitoring	AWS CloudWatch	Azure Monitor	GCP Logs Explorer
Threat Detection	Amazon GuardDuty	Microsoft Defender for Cloud	Cloud Security Command Center
SIEM	Amazon Detective	Microsoft Sentinel	Cloud Security Command Center
IAM	AWS IAM	Azure Active Directory	Cloud IAM
Firewall	AWS Network Firewall	NSG	Cloud NGFW

By Abdulmajeed Almoharib

Different Cloud service providers (CSPs) have different terminologies and log environments. We recommend this excellent poster by SANS for a great overview of different CSPs: https://www.sans.org/posters/enterprise-cloud-forensics-incident-response-poster/

7. Malware Analysis

Malware analysis is a specialized area within digital forensics focused on understanding malicious software. This chapter provides a comprehensive look at:

- **Static Malware Analysis:** Examining malware without executing it to understand its structure and potential impact.
- **Dynamic Malware Analysis:** Running malware in a controlled environment (sandbox) to observe its behavior.
- **Conducting IOCs Research:** Identifying Indicators of Compromise (IOCs) to detect and mitigate future threats.

An excellent malware analysis methodology was created by Lenny Zeltser (https://Zeltser.com).

This methodology comprises the following seven steps that aid analysts in their process:

1. Create a controlled laboratory environment where examinations can be conducted.
2. Examine the behavior of the suspected malware as it interacts with the operating system (OS) environment.
3. Examine the suspicious application's code, to gain a sense of the inner workings.
4. Perform dynamic analysis to determine what actions to take that could not be identified in static analysis.
5. Determine if the malware is packed and unpack it as necessary.
6. Continue the process until the analysis objectives have been completed.
7. Prepare a supplement to the forensics reporting and return the laboratory to its state before the analysis.

Static Malware Analysis

Static analysis includes several different techniques such as:

1. Fingerprinting
2. Strings extraction (Using floss tool available at: https://cloud.google.com/blog/topics/threat-intelligence/floss-version-2/
3. File format analysis

4. Packer analysis
5. Disassembly

PEStudio is one the most famous free tools for static analysis. You can download it from the link below:
https://www.winitor.com/download

Static analysis with process dump:

1. Download process dump ps32/pd64
   https://split-code.com/processdump.html
2. Open cmd as administrator
3. pd64.exe -db gen (Finds all processes and creates hash values)
4. Run malware
   pd64.exe -p malware.exe
5. Open IDAfree (https://hex-rays.com/PRoducts/ida/support/download_freeware)
6. File - open – new created file by process dump
7. Check imports and exports tabs

Static analysis with IDA and OllyDbg:

1. Open IDA (IDA is a free decompiler)
2. New - drag malware.exe to IDA
3. Check exports and imports tabs
4. Open Olydbg (Runs malware step by step - https://www.ollydbg.de/download.htm)
5. Open the malware file
6. Click play
7. if it terminates that means the malware detects our attempt to debug it

Dynamic Malware Analysis

One of the best platforms to conduct dynamic malware analysis is FLARE VM by Mandiant. FLARE utilizes a PowerShell script to download and configure a local sandbox on a variety of Windows platforms. You can download it from here:

https://github.com/mandiant/flare-vm

To get started and install FLARE VM you may follow the instructions from the following links:

https://cloud.google.com/blog/topics/threat-intelligence/flare-vm-the-windows-malware

https://medium.com/@haroon00525/flare-vm-lab-setup-isolated-lab-environment-for-malware-analy
6e7c23af875

Due to the length and complexity of explaining dynamic malware analysis, we recommend watching the following YouTube Bootcamp by HackerSploit:

https://www.youtube.com/watch?v=uHhKkLwT4Mk&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io

SANS Malware Analysis: Tips & Tricks Poster

https://www.sans.org/posters/malware-analysis-tips-tricks-poster/

Malware Analysis and Reverse-Engineering Cheat Sheet
https://www.sans.org/posters/malware-analysis-and-reverse-engineering-cheat-sheet/

Conducting IOCs Research

Several online tools and websites are invaluable for conducting Malware IoC research. These resources help researchers gather, validate, and share IoCs with the broader cybersecurity community:

1. **VirusTotal:** This is a free online service that analyzes files and URLs for malware. Researchers can upload suspicious files or URLs to VirusTotal, which scans them using multiple antivirus engines and provides detailed reports, including detected IoCs like file hashes and IP addresses. https://www.virustotal.com/
2. **Hybrid Analysis:** A malware analysis platform that offers both static and dynamic analysis. It provides detailed behavioral reports and IoCs such as file modifications, network connections, and system changes observed during the analysis. https://www.hybrid-analysis.com/
3. **MalwareBazaar:** A repository of malware samples shared by the cybersecurity community. Researchers can download samples for analysis or search for specific IoCs like file hashes and domain names. https://bazaar.abuse.ch/
4. **AlienVault Open Threat Exchange (OTX):** A collaborative platform where researchers share threat data, including IoCs. OTX provides comprehensive threat intelligence and

5. allows users to search for specific indicators related to malware campaigns. https://otx.alienvault.com/
6. **ThreatMiner:** A search engine for threat intelligence that aggregates data from various sources, including malware reports, domain information, and SSL certificates. It helps researchers identify relationships between different IoCs and malware families. https://www.threatminer.org/
7. **Abuse.ch:** A collection of projects that track and provide data on various types of cyber threats, such as botnets and ransomware. It offers feeds of IoCs like IP addresses, domain names, and file hashes associated with known threats. https://abuse.ch/
8. **Cuckoo Sandbox:** An open-source automated malware analysis system that allows researchers to submit malware samples for dynamic analysis. Cuckoo provides detailed reports on the behavior of the malware, including generated IoCs. https://cuckoosandbox.org/
9. **CIRCL DMA (Dynamic Malware Analysis):** Dynamic Malware Analysis (DMA) is a service offered by CIRCL and operated by Joe Security LLC[1], a renowned Swiss security company specialized in leading sandbox technologies. CIRCL and Joe Security already collaborated regarding Joe's MISP [2] integration. The platform allows the analysis of potential malicious software or suspicious documents in a secure and virtualized environment. https://www.circl.lu/services/dynamic-malware-analysis/

8. Digital Forensics in the Incident Response Cycle

The priority between incident recovery and digital forensics can vary based on several factors:

1. **Severity and Scope of the Incident**: If an incident severely disrupts critical operations, immediate recovery efforts may take precedence to ensure business continuity. Conversely, if the incident's impact on operations is minimal, there may be more room to prioritize forensics.
2. **Evidence Volatility**: In cases where digital evidence is volatile and could be lost or altered quickly, prioritizing forensics is crucial to ensure that vital information is preserved.

3. **Regulatory and Legal Requirements**: Some industries have strict regulations regarding incident reporting and evidence preservation, which might necessitate prioritizing forensics over recovery.
4. **Organizational Objectives**: The organization’s priorities and objectives will influence the balance between recovery and forensics. For instance, a financial institution might prioritize forensics to comply with regulatory investigations, while an e-commerce site might prioritize recovery to restore customer services quickly.
5. **Resource Availability**: The availability of skilled personnel and tools can affect how activities are prioritized. Organizations with dedicated teams for both incident response and digital forensics can handle both simultaneously, whereas those with limited resources might need to prioritize one over the other.

In summary, Incident recovery and digital forensics are both essential components of a comprehensive incident response strategy. While incident recovery aims to restore normal operations and mitigate damage, digital forensics focuses on understanding the incident and preserving evidence. The prioritization of these activities depends on the specific context of the incident, including its severity, impact on operations, regulatory requirements, and the organization’s objectives. Ideally, organizations should strive to balance both activities, ensuring that immediate threats are addressed while preserving critical evidence for future analysis and legal proceedings.

9. Documentation and Reporting

Thorough documentation and clear reporting are essential for communicating findings and supporting legal proceedings. This final section emphasizes the importance of detailed and accurate reporting, providing templates and guidelines for effective documentation.

A proper digital forensics document should include the following elements:

1. Documentation overview
2. Executive summary
3. Incident investigation report
4. Forensic report
5. Preparing the incident and forensic report
6.

It could also include details such as:

- Case ID, Agent Name, and Location

Sample Reports:

https://github.com/arvindpj007/Digital-Forensics-Report/blob/master/Forensic%20Examination%20Report.pdf