

Cybersecurity Professional Program

Log Analysis & Timeline

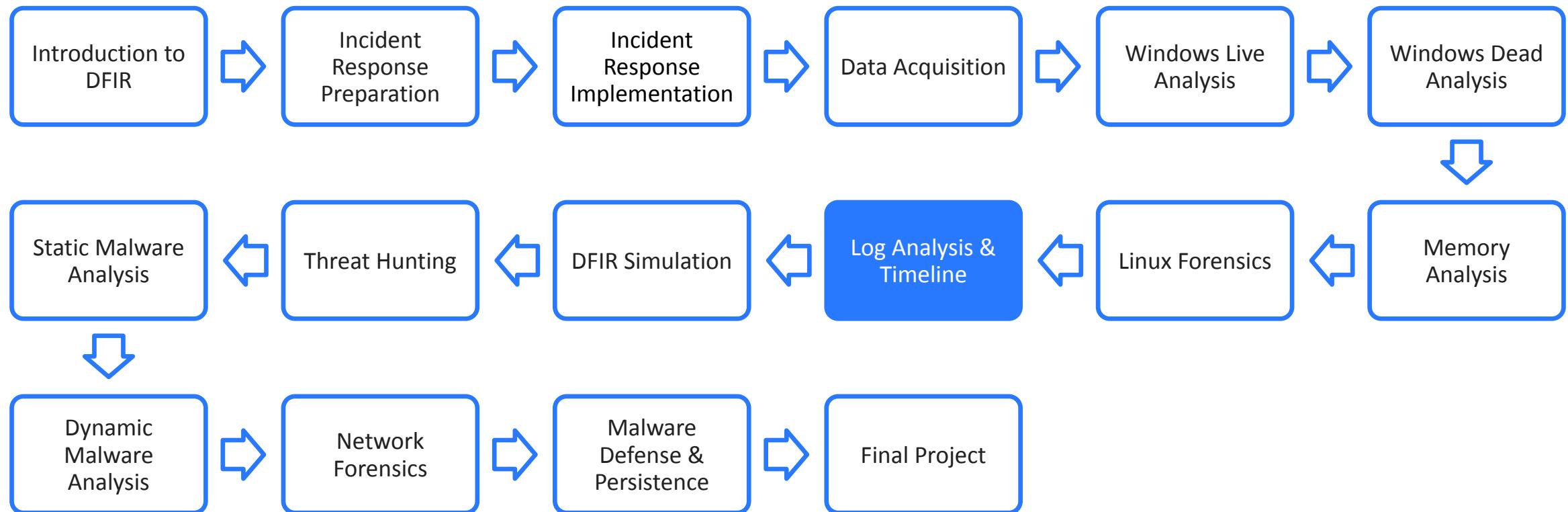
Digital Forensics & Incident Response





Digital Forensics & Incident Response

Course Path





Log Analysis & Timeline

Objectives

The objective of this lesson is to understand the power of logs to detect active incidents and how they work with queries to acquire a comprehensive picture of the event.

- Log Overview
- Windows Logs
- Log Analysis
- Linux Logs
- Statistical Analysis
- Log Attacks



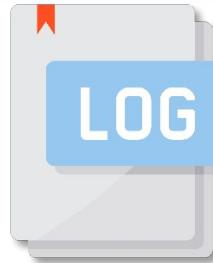


Log Analysis & Timeline

Log Overview



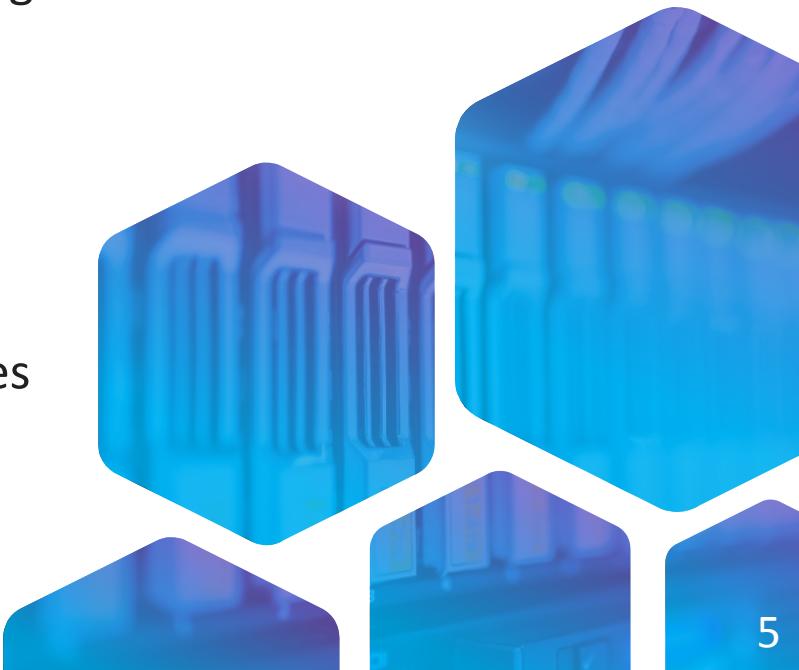
What Are Logs?



- Logs can be created automatically by systems, but some require manual setup.
- Almost all apps and operating systems are generating logs or can be configured to generate logs.



- Some applications and devices differentiate between various types of logs.
- Logs can be found according to their file names or using GUI-based options.



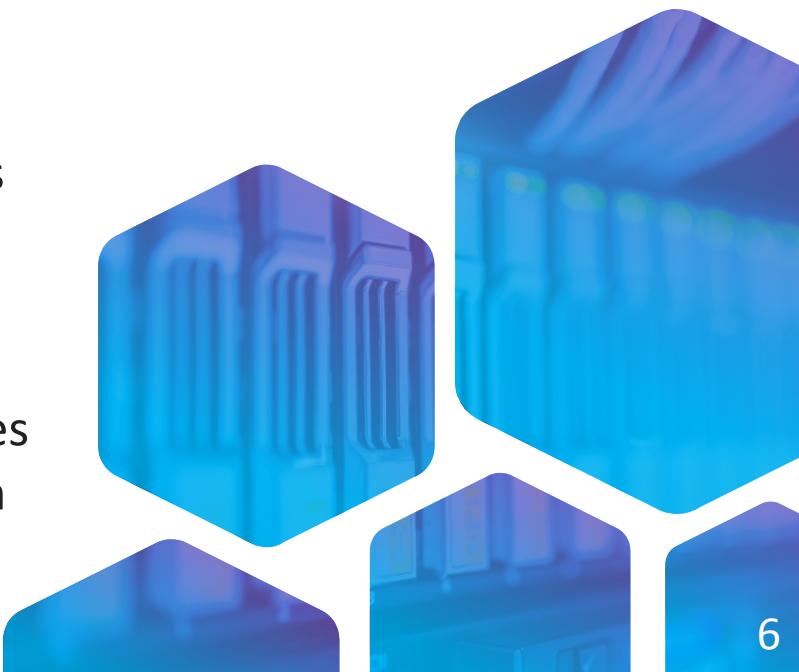
Why Use Logs?



- Store information that is not found elsewhere.
- Record useful information about certain events in the system.



- Logs can assist in the troubleshooting process when errors occur.
- Regarded as evidence in a court of law
- Required for many governance, risk management, and compliance (GRC) strategies
- Included in an incident response investigation



Log Overview

Log Classification



Informational



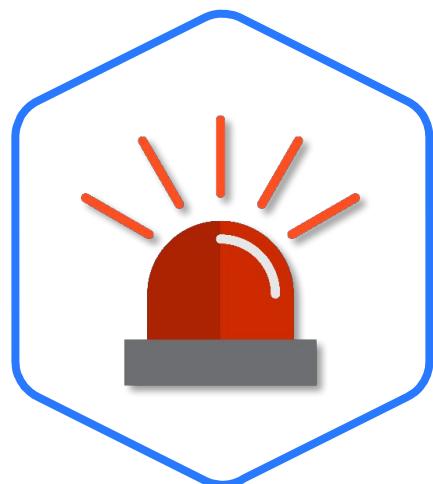
Debug



Warning



Error



Alert

Common Log Generators

Syslog

Used by Linux OS with TCP/UDP protocol on port 514

SNMP

Network device management

LEA

Proprietary checkpoint protocol

Event Viewer

Used by Microsoft Windows

Database

Many applications work with database event logs.

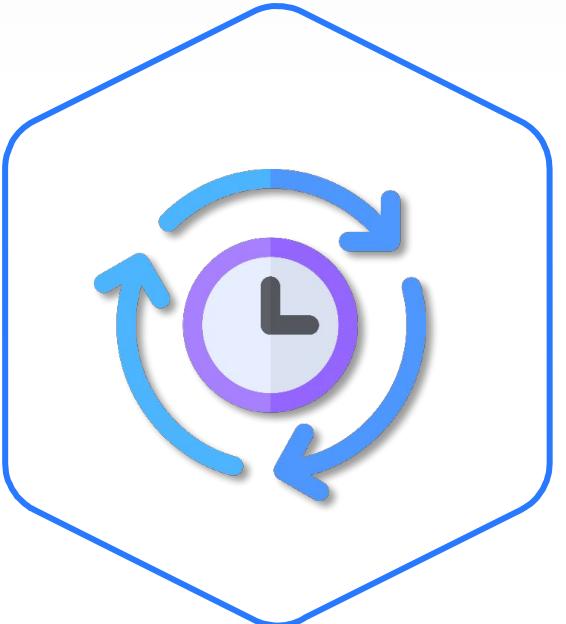
SDEE

Backward compatible with RDEP



Log Overview

Network Time Protocol (NTP)

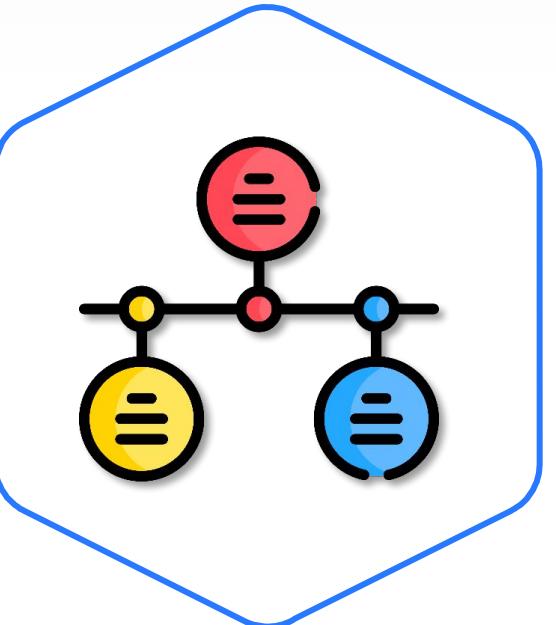


- Syncs clocks across the network
- Ensures a more accurate event timeline
- Can operate locally or over the internet



Log Overview

Timeline



- Constructs a picture of all key logged events
- Reveals the sequence of events
- Mandatory in many forensic reports





Log Analysis & Timeline

Windows Logs

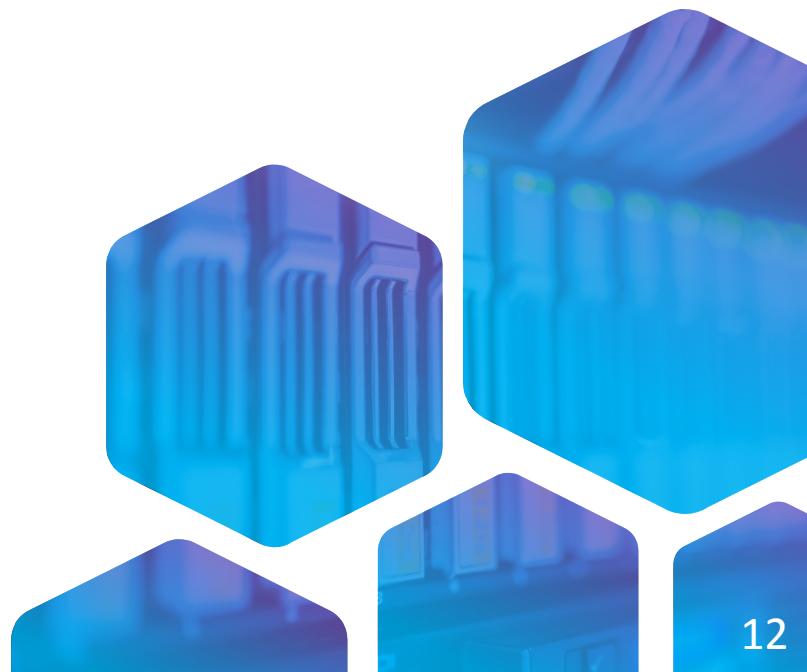
Windows Logs



- Types: Application, service, security, and system
- Application and service logs include many useful logs, such as PowerShell and Terminal Services.



- Can be used to troubleshoot blue screen of death (BSOD) errors
- Can be used to investigate successful and failed logons





Windows Event Viewer

- Presents details of events (at the bottom of the window)
- Each event category has a unique ID.
- The details section displays events in XML format.

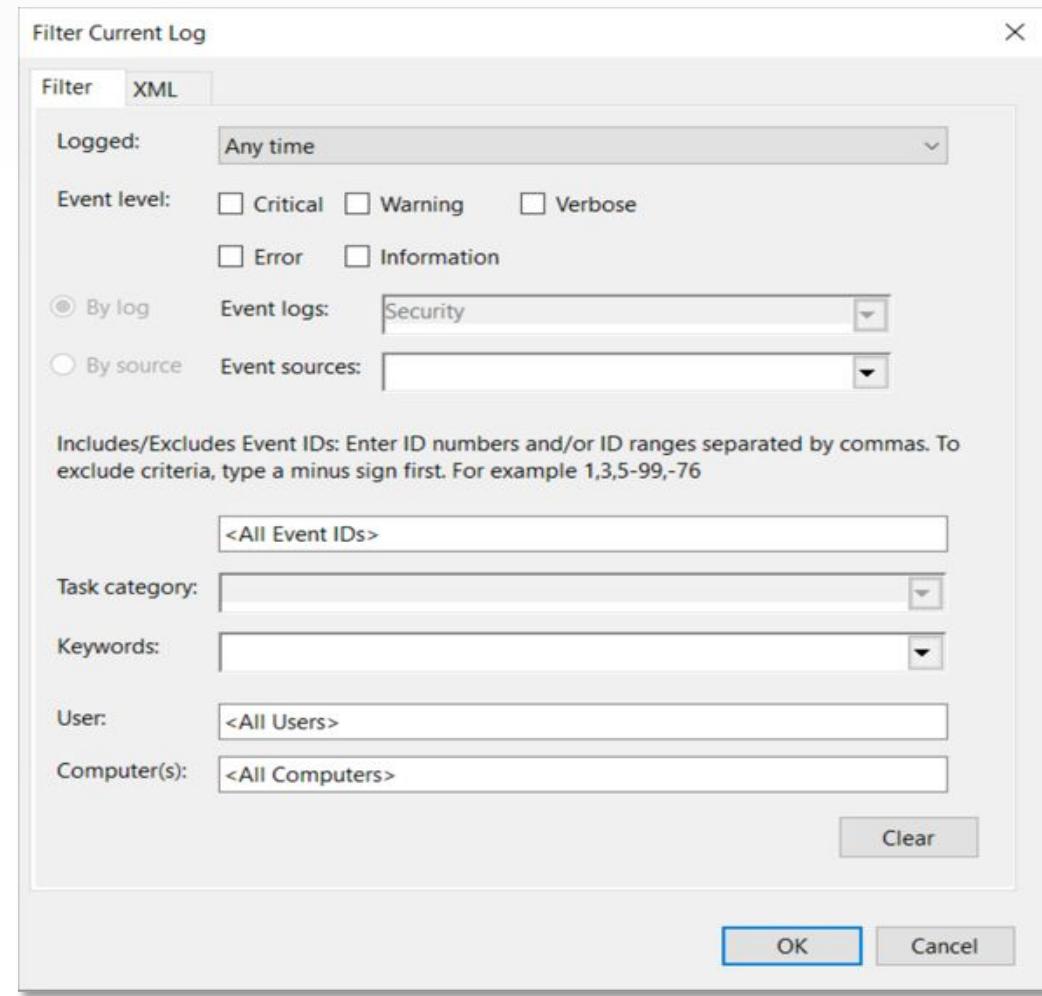
The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with 'Event Viewer (Local)', 'Custom Views', and 'Windows Logs' expanded. Under 'Windows Logs', 'Application' is selected, and the 'Event Log' tab is active. The main pane shows a table of events with columns: Level, Date and Time, Source, Event ID, and Task Category. An error event (Event ID 1000) is highlighted. The right pane, titled 'Actions', contains a list of options like 'Open Saved Log...', 'Create Custom View...', and 'Import Custom View...'. A detailed view of the selected event (Event 1000, Application Error) is shown in a modal dialog. The 'General' tab is selected, displaying event properties such as Log Name: Application, Source: Application Error, Event ID: 1000, Level: Error, and User: N/A. The 'Details' tab shows XML event data.

Application Number of events: 11,243				
Level	Date and Time	Source	Event ID	Task Category
Information	8/04/2016 10:36:31 PM	Security-SPP	900	None
Information	8/04/2016 10:32:47 PM	Windows Error Repo...	1001	None
Error	8/04/2016 10:32:44 PM	Application Error	1000	(100)
Information	8/04/2016 10:22:24 PM	gupdate	0	None
Information	8/04/2016 10:07:01 PM	Security-SPP	903	None
Information	8/04/2016 10:07:01 PM	Security-SPP	16384	None
Information	8/04/2016 10:06:31 PM	Security-SPP	902	None
Information	8/04/2016 10:06:31 PM	Security-SPP	1037	None
Information	8/04/2016 10:06:31 PM	Security-SPP	1003	None
Information	8/04/2016 10:06:31 PM	Security-SPP	1066	None
Information	8/04/2016 10:06:31 PM	Security-SPP	900	None
Information	8/04/2016 9:37:00 PM	Security-SPP	903	None
Information	8/04/2016 9:37:00 PM	Security-SPP	16384	None
Information	8/04/2016 9:36:30 PM	Security-SPP	902	None
Information	8/04/2016 9:36:30 PM	Security-SPP	1037	None
Information	8/04/2016 9:36:30 PM	Security-SPP	1003	None

From: ThriveDX

Event Viewer Log Filtering

- Enables faster viewing of essential event information
- Filters include date and time, event level, event ID, and more.
- It is also possible to filter by XML.





Windows Logs

Event IDs

4720 A user account was created.

4726 A user account was deleted.

4727 A security-enabled global group was created.

4624 A successful logon

1102 An audit log was cleared.

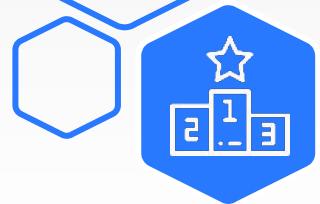
4732 A member was added to a security-enabled local group.

4725 A user account was disabled.

4625 An account failed to log on.

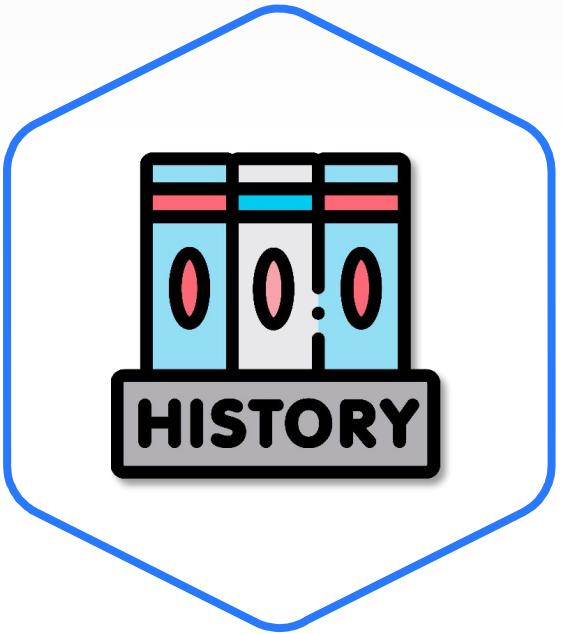
Windows Logs

Logon Type IDs



- | | |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2 Interactive login</p> <p>3 Network</p> <p>4 Batch</p> <p>5 Service</p> | <p>7 Unlock</p> <p>8 Network clear text</p> <p>10 Remote interactive</p> <p>11 Logon with cached credentials</p> |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|

PowerShell Logs



- Store historical PowerShell commands
- Two ways to view historical PowerShell records:
 - Open PowerShell and click the **UP** key.
 - Open the file at the following location:

%AppData%\Microsoft\Windows\PowerShell\PSReadLine

PowerShell history helps detect *fileless* attacks.



Lab DFIR-09-L1

Event Viewer Investigation

10–15 Min.



Mission

Search for events and understand their structure.

Steps

- Answer the questions in the file.

Env. & Tools

- Text editor
- Windows VM
- Event Viewer

Related Files

- Lab document
- *Security.evtx*



Log Analysis & Timeline

Log Analysis

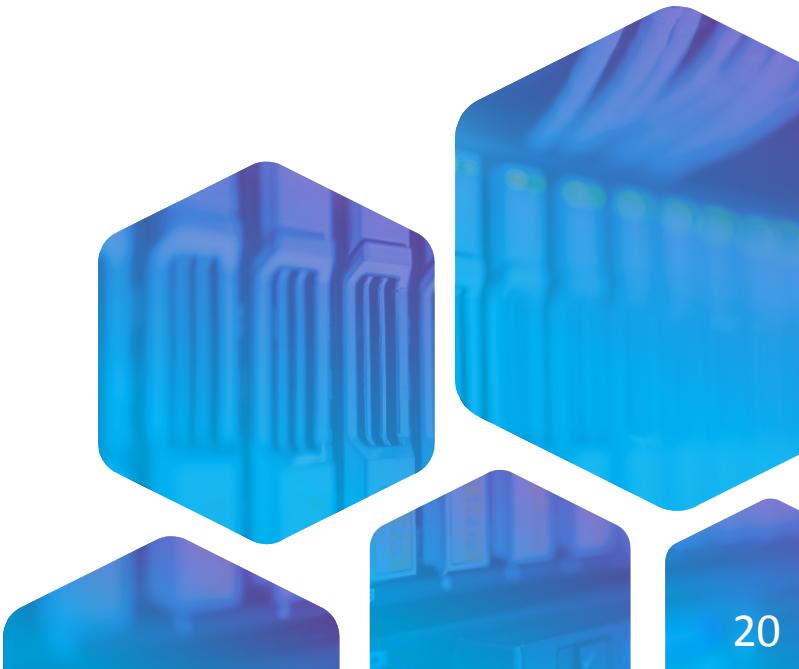
Pre-Analysis Notes



- Define log analysis goals.
- Analyze logs to characterize the element that may be involved in an event.



- Use logs to choose appropriate tools for the investigation.
- Note that it is not recommended to search through a log line by line.



Query Builder



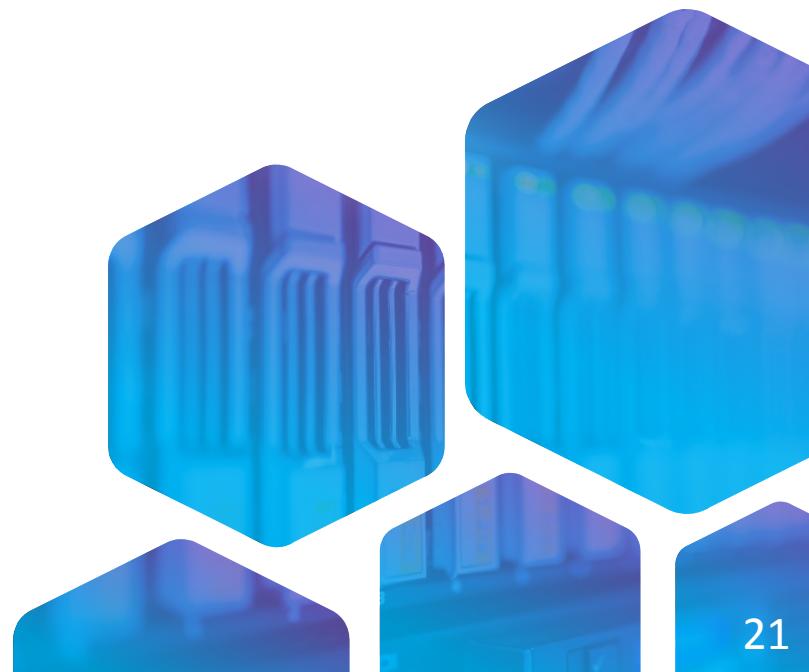
Microsoft Log Parser 2.2

- CLI interface used to parse and investigate logs via SQL
- Can extract data from text-based files, such as LOG, CSV, XML, and EVTX



Log Parser Lizard

- A built-in Microsoft Log Parser 2.2
- User-friendly GUI with options to extract data from various types of logs





Microsoft Log Parser 2.2

- Can investigate Windows event logs from files or from the Event Viewer
- Supports many log types, including IIS, CSV, XML, and EVT

```
logParser.exe -i:EVT -o:csv "SELECT TimeWritten,EventID, ComputerName,Strings FROM Security WHERE EventID = '4624' and Message like '%Logon%' AND ComputerName like '%.local%'"
```



Log Analysis

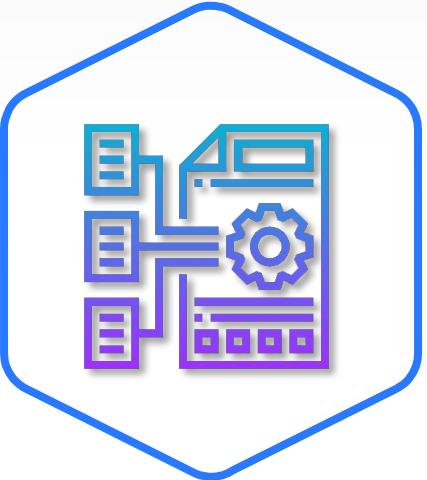
Log Parser Lizard

- The top pane is used for queries, and the bottom pane displays the results.
- Charts can be used to discover trends in the logs.

Time Written	Event ID	Event Type	Event Type Name	Event Category	Event Category Name	Source Name	Strings	Computer Name	SID	Message	Data
03/05/2020 2...	4,624	8	Success Audit event	12,544	The name for category 12544 in Source "Microsoft-Windows-Security-Auditing" cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer	Microsoft-Windows-Security-Auditing	S-1-0-0 - 0x0 S-1-5-7 ANONYMOUS LOGON INT AUTHORITY 0x66345 3 NtLmssp INTLM - {00000000-0000-0000-0000-00000000}- INTLM V1 0 0x0 - - -%1833 - - -%1843 0 x0 -%1843	DESKTOP-H4PVCFE		An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: %&1843 Elevated Token: %&1843 Impersonation Level: %&1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x66345 Linked Logon ID: 0x0 Network Account Name [...] [...TEXT IS TRUNCATED. RIGHT CLICK TO SHOW SELECTED TEXT...]	
03/05/2020 1...	4,624	8	Success Audit event	12,544	The name for category 12544 in Source "Microsoft-Windows-Security-Auditing" cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer	Microsoft-Windows-Security-Auditing	S-1-0-0 - 0x0 S-1-5-7 ANONYMOUS LOGON INT AUTHORITY 0x6668d 3 NtLmssp INTLM - {00000000-0000-0000-0000-00000000}- INTLM V1 0 0x0 - - -%1833 - - -%1843 0 x0 -%1843	DESKTOP-H4PVCFE		An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: %&1843 Elevated Token: %&1843 Impersonation Level: %&1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x6668d Linked Logon ID: 0x0 Network Account Name [...] [...TEXT IS TRUNCATED. RIGHT CLICK TO SHOW SELECTED TEXT...]	

From: ThriveDX

Manual Log Review Limitations



Aggregate vs.
distinct logs



Search through
millions of logs



Hard to see
the big picture

Lab DFIR-09-L2

Event Viewer Tools

30–40 Min.



Mission

Examine the Event Viewer investigation process via SQL queries.

Steps

- Download the applications.
- Investigate logs using Microsoft Log Parser 2.2.
- Investigate logs using Log Parser Lizard.

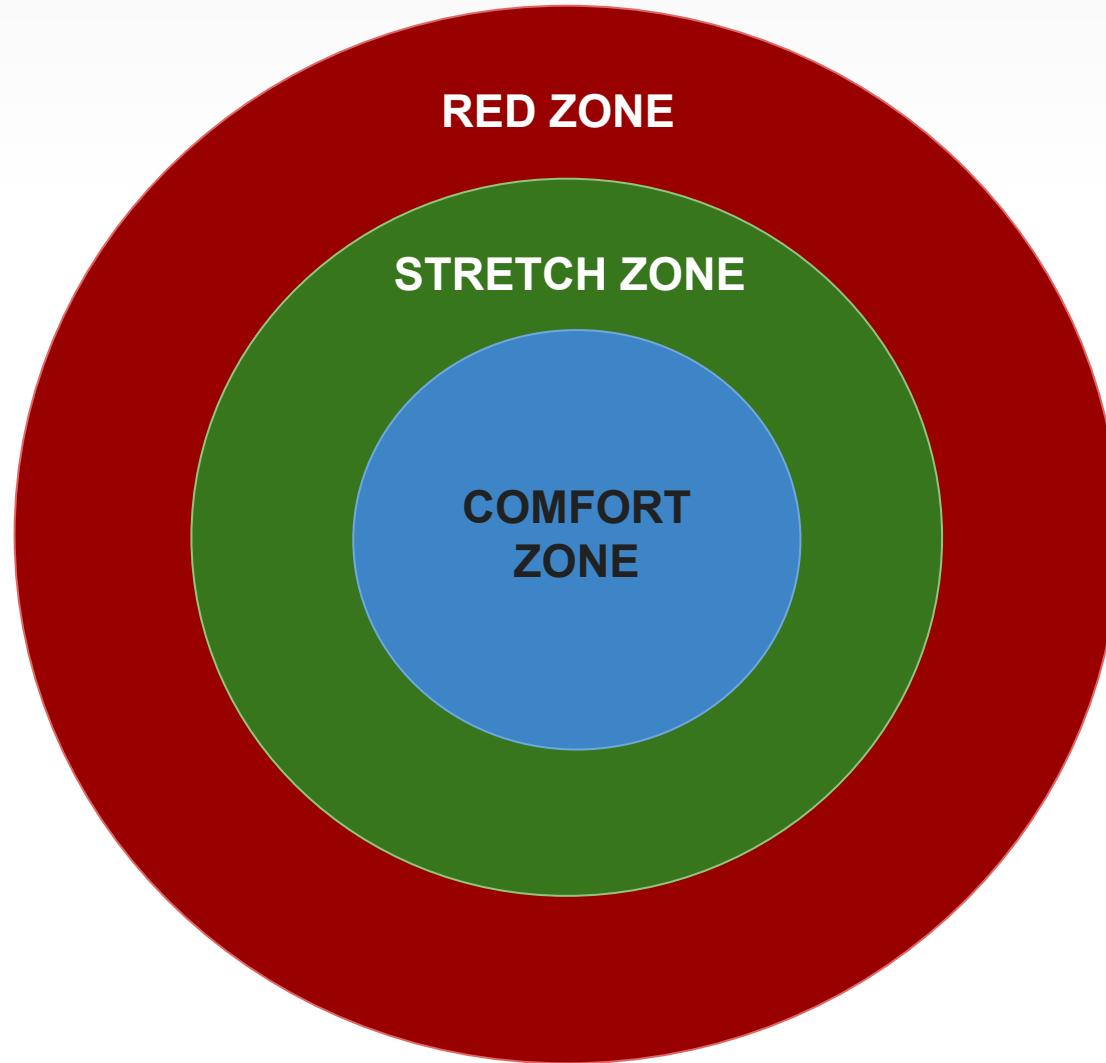
Env. & Tools

- Text editor
- Log Parser Lizard
- Microsoft Log Parser 2.2

Related Files

- Lab document
- ***Security.evtx***

Pulse Check





Log Analysis & Timeline

Linux Logs

Linux Log Basics



- Logs are different in CentOS/RedHat and Ubuntu/Debian.
- Almost all log files are in the ***/var/log*** directory.

To view or access the log files, you must have root permission.



Linux Log File Contents

/var/log/messages Global system messages

/var/log/cron Active cron job data

/var/log/kern.log Data logged by the kernel

/var/log/dpkg.log
/var/log/yum.log Logs data when a package
is installed or removed

/var/log/secure
/var/log/auth.log Authentication and
authorization privileges

/var/log/boot.log Boot message data

Linux Log Commands

head

Reads the first 10 lines of a file

more

Basic terminal paging program that displays contents page by page

grep

Searches for specific strings in files

tail

Reads the last 10 lines of a file

less

Like the **more** command but with search options

awk

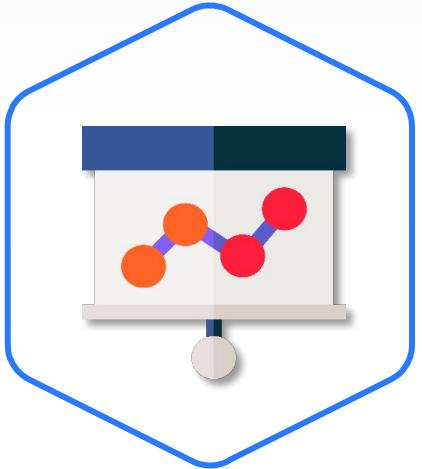
Text processing program for better log viewing



Log Analysis & Timeline

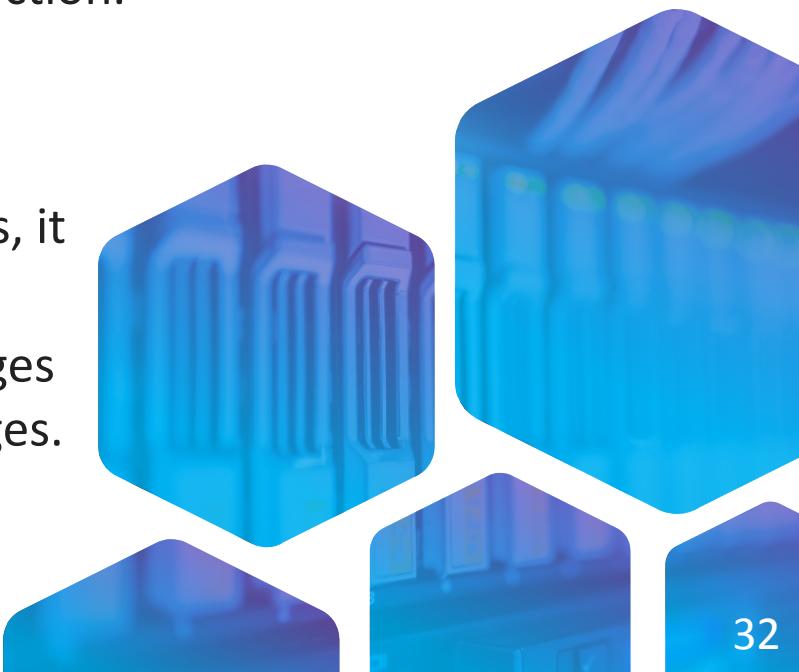
Statistical Analysis

Introduction to Statistical Analysis

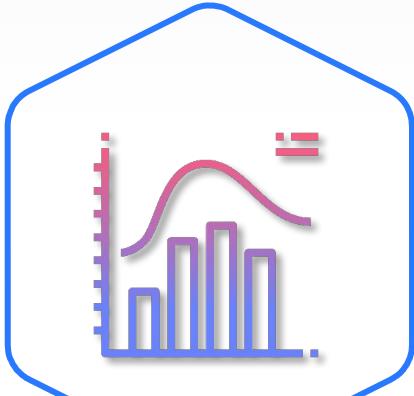


- Some events will not be noticed if they occur only once.
- When a malicious event occurs only once, it may appear to be a legitimate action.

- When malicious events occur in large volumes, it is much easier to detect them.
- Example: A user who sent 1,000 email messages in one week sends 10,000 more email messages.



Frequency & Baseline



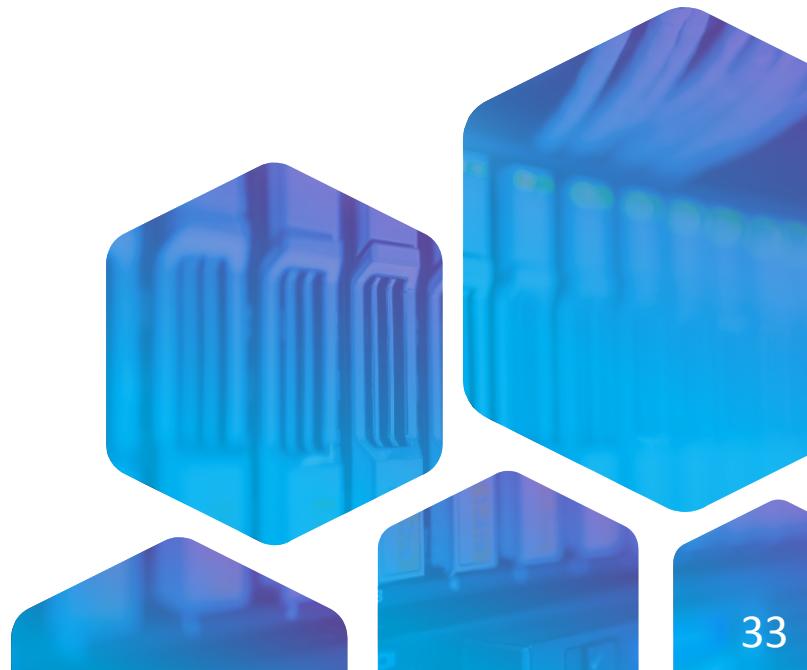
Frequency

- A spike in data over time may be considered abnormal behavior.
- Data can be monitored by hour, week, month, and year.



Baseline

- Sets a standard for normal behavior for the purpose of comparison
- Baseline example: The number of *su* commands used per hour each day



Statistical Analysis

Anomaly Detection



- Detecting events that did not previously occur in the system
- Determining normal operations of users every hour to establish a baseline
- Using proprietary systems that offer user behavior analytics (UBA) to monitor unusual events

Anomaly detection can trigger false positive alerts.





Log Analysis & Timeline

Log Attacks

Log Attacks

?Why Attack Logs

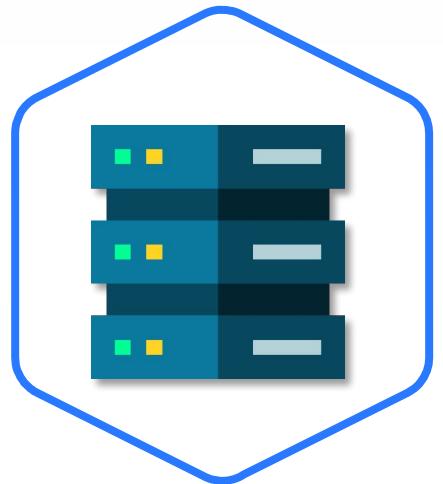
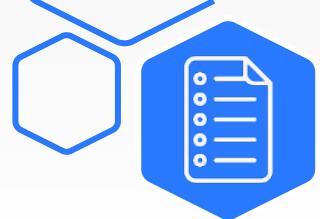


- Attackers do not want to get caught.
- Removing evidence from the target is crucial to remaining anonymous.

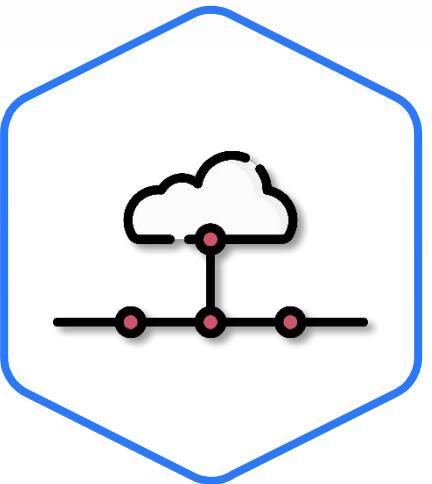
Information in logs about passwords, hosts, and users can be used during an attack.



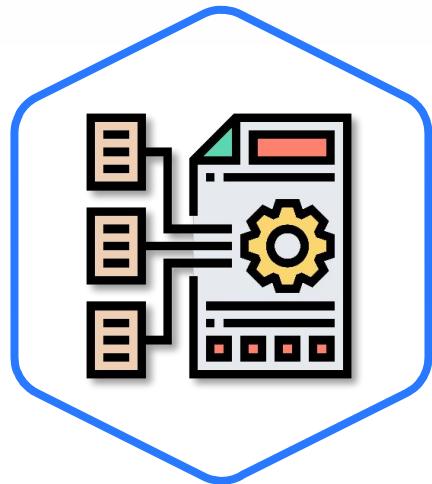
What to Attack



The host in which logs are generated



Transmitted logs



Agents that collect logs



The database in which logs are stored

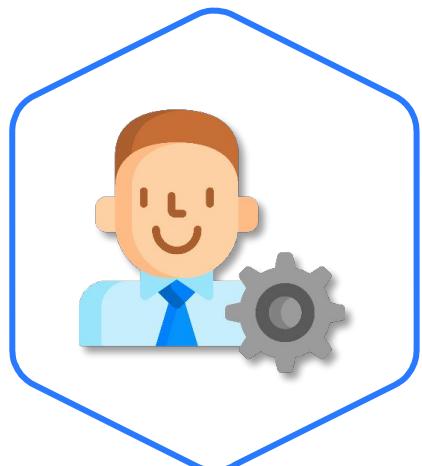
Log attacks are aimed at disrupting a service or changing, deleting, and viewing log data.

Windows Log Attacks



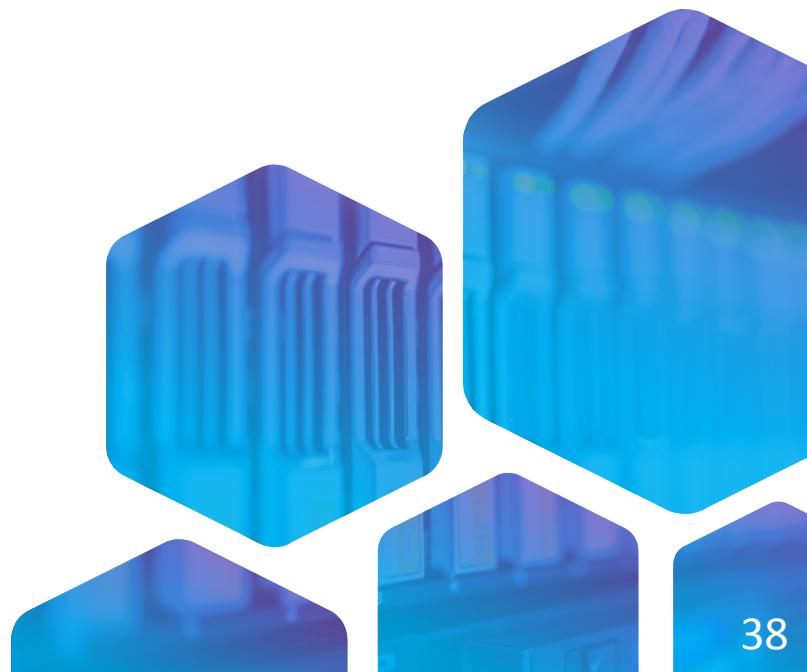
Deleting Logs Using the Event Viewer

- Not useful, since logs are generated when logs are deleted
- SIEM monitors this type of event.



Deleting Files from `%system32%\winevt\logs`

- Requires high-level privileges
- To execute this, the Event Log service must be disabled.
- Doesn't delete all recent logs



Linux Log Attacks



- Unlike Windows, manipulating log files is easy in Linux.
- You must have sudo permission to modify logs.
- The following command modifies a log in a UNIX-like system: ***sudo nano /var/log/messages***





Important for Upcoming Lab



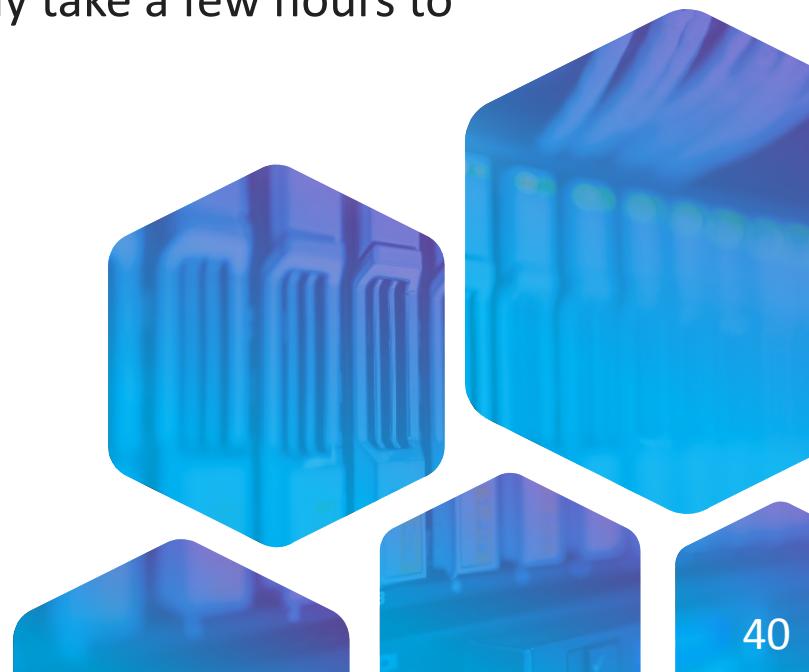
The class files for the DFIR-10 Capture the Flag lab take time to download.

- Downloading all necessary files will ensure you have enough class time to perform the exercise.
- The files are large and will likely take a few hours to download over Wi-Fi.



Files you will need from Canvas prior to class:

- *memdump.mem*
- *hacker'sWindows.ova*
- *pagefile.sys*
- Autopsy installer



Lab DFIR-09-L3

Manipulate Log Files
10–15 Min.



Mission

Delete and modify logs in Linux and Windows machines.

Steps

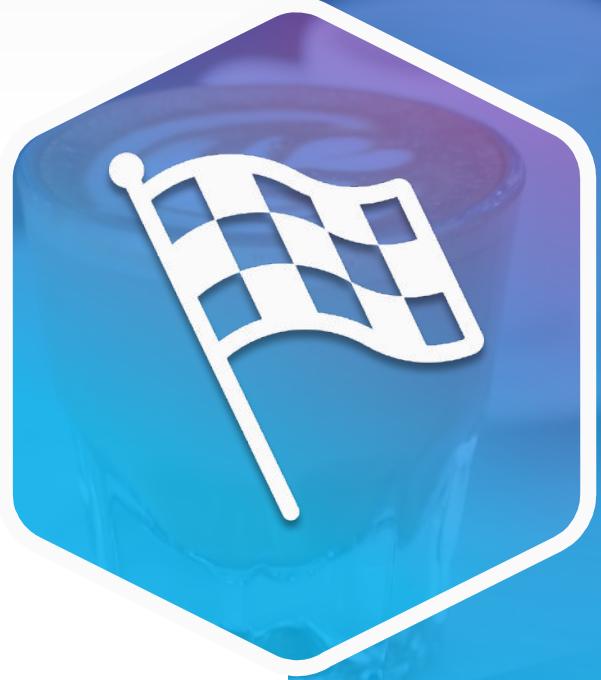
- Modify authentication logs in the SIFT machine.
- Delete Windows logs without leaving a trace.
- Delete Windows logs and leave a trace.

Env. & Tools

- SIFT VM
- Windows VM

Related Files

- Lab document



Thank You

Questions?