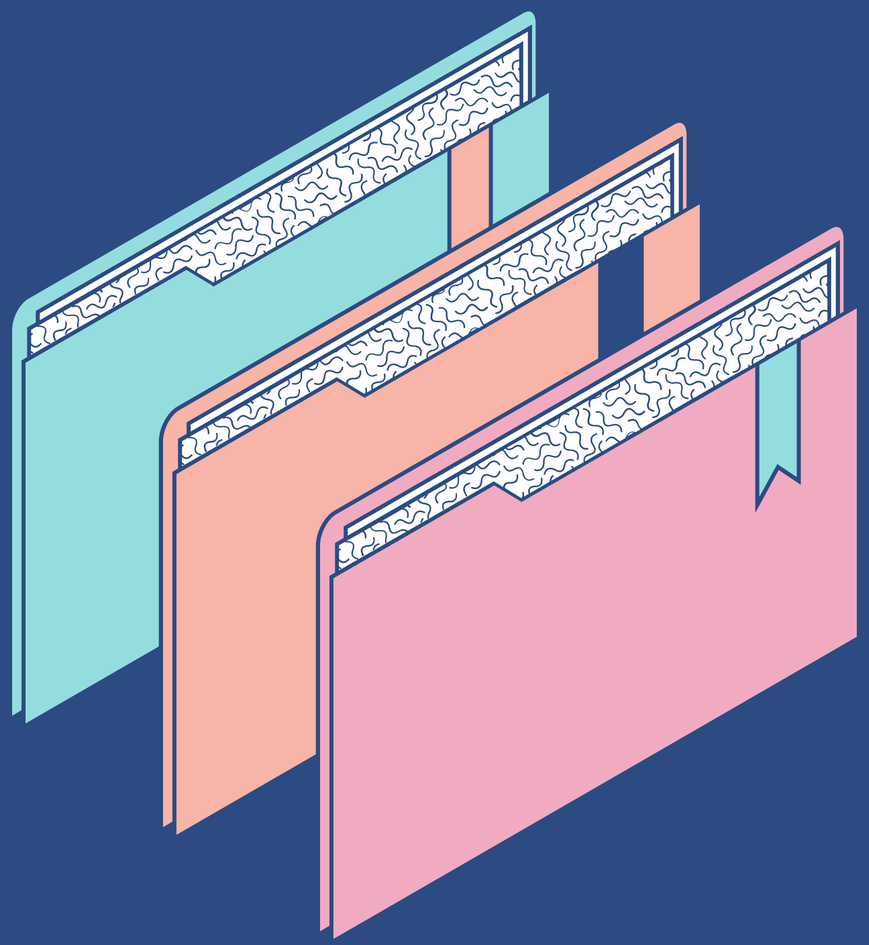
CYBER FORENSICS MTE PROJECT

Windows Event Log Viewer

Akaash Nidhiss 2K19/IT/008
Anasuya Mithra 2K19/IT/018

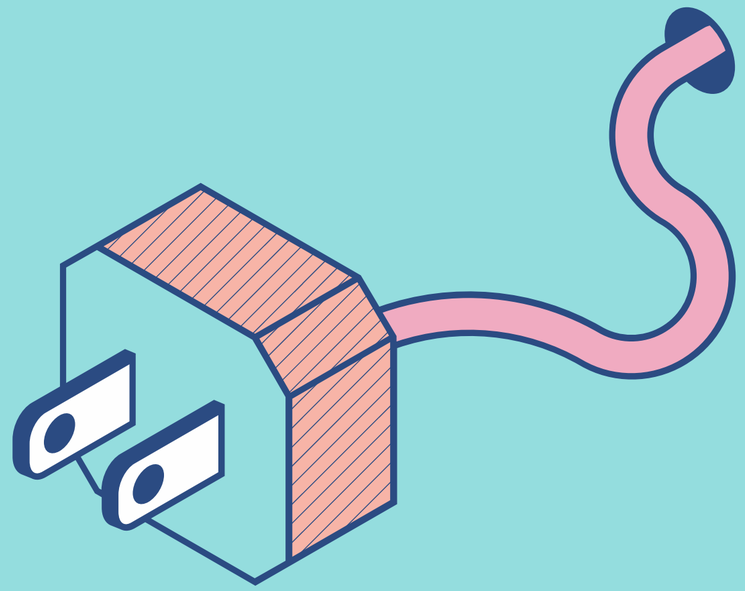


Index

Introduction

The rapid speed by which technology has grown has also increased the spate of cybercrimes. Windows operating system is the most widely used OS, resulting in its users being on the receiving end of these cybercrimes. Such crimes brought about the need for cyber forensics.

Evidence collection is a major part of the field of cyber forensics. Because the log files link certain occurrences to a specific point in time, the Windows event log is the most essential source of evidence during a digital forensic investigation of a Windows system.



Windows Event Log Files

The Windows event log is a complete record of system, security, and application notifications kept by the Windows operating system and utilised by administrators to diagnose system issues and anomalies, and predict future problems.

Each event log entry has the following elements -

- Date: Date of occurrence of the event
- Time: Time of occurrence of the event
- User: Username of the user logged onto the machine when the event occurred.
- Computer: Name of the computer.
- Event ID: A Windows identification number that specifies the event type.
- Source: The program or component that caused the event.
- Type: The type of event, including information, warning, error, security success audit or security failure audit.

There are 3 types of windows event log files, classified by the type of information it contains - Application Log, System Log and Security Log.

Application Log File

TYPES OF WINDOWS EVENT LOG FILES

The Application log contains events logged by applications or programs.

When any application crashes, the Windows event log records the problem, the application name, and the reason for the crash.

Application logs are frequently used by app support teams.

Some applications, such as Internet Explorer, Power Shell create own event log instead of using Windows application event log. Such logs look exactly like standard Windows event logs and Event Viewer (as well as Event Log Explorer) can read these event logs.

Commercial software, such as SQL Server or Exchange, or homegrown applications are both visible on the application log file.

Security Log File

TYPES OF WINDOWS EVENT LOG FILES

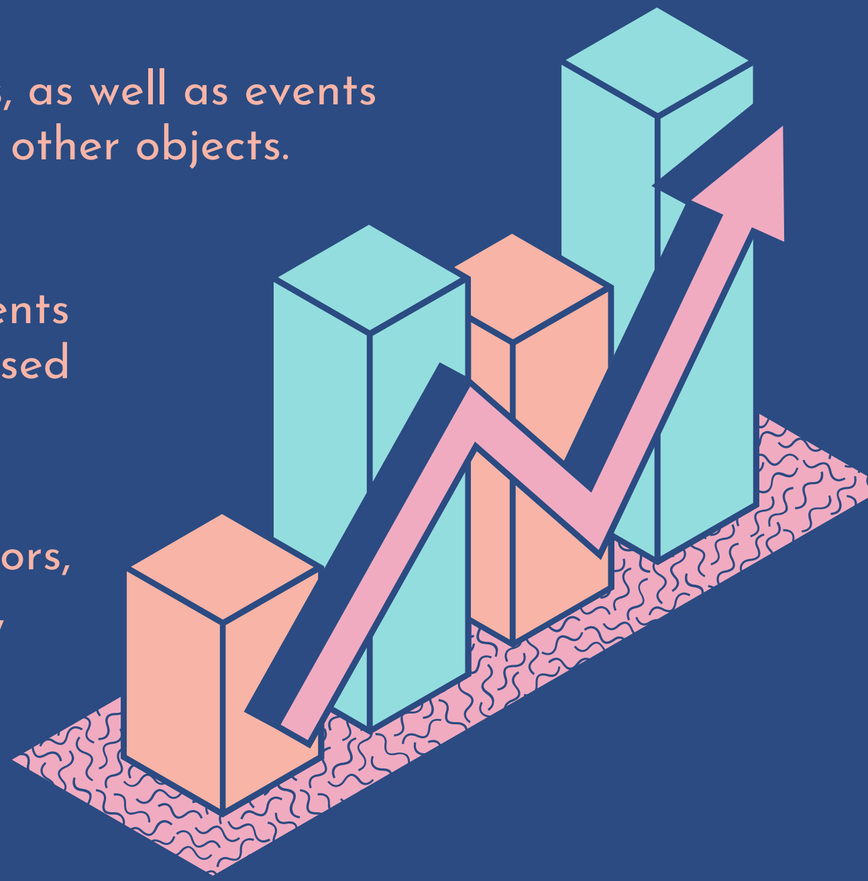
The Security log contains events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files or other objects.

If you enable logon auditing, for example, all attempts to log on to the system are recorded in the security log.

The typical events stored include login attempts and resource access.

Administrators choose which events to report in their security log based on their audit policy.

System and security administrators, as well as forensic examiners, require security logs.



System Log File

TYPES OF WINDOWS EVENT LOG FILES

The System log contains events logged by Windows system components.

The system log, for example, records the failure of a driver or other system component to load during startup.

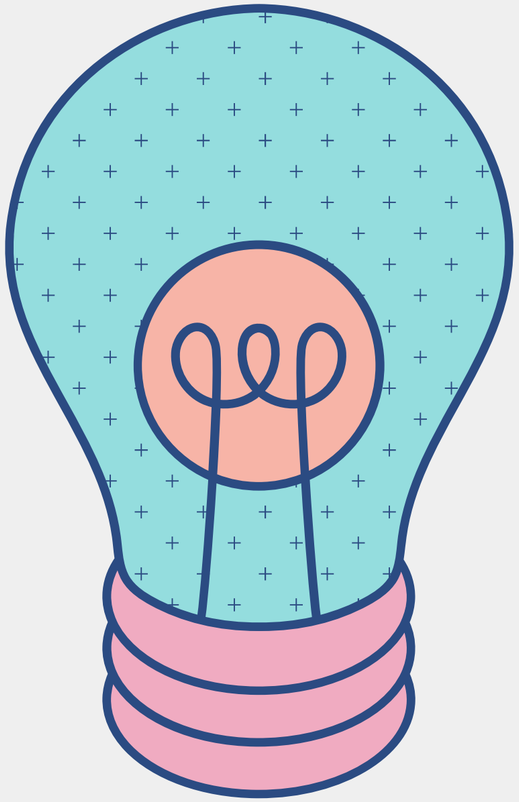
System administrators and technicians require system logs.

win32evtlog

win32evtlog is a python module that encapsulates the Windows Win32 Event Log API.

The protocol for writing an instrumentation manifest is defined by the Windows Event Log API. Each event provider and the events it logs are identified by an instrumentation manifest. An event consumer, such as the win32evtlog, utilises the API to read and render the events.

Our Program uses this module in python to read and display Application, System and Security Log files.



CODE

Output

APPLICATION LOG FILE

	Event Category:	Time Generated:	Source Name:	Event ID:	Event Type:	Event Data:
0	2	2022-05-06 04:23:10	MSSQLSERVER	1073749952	4	xplog70.dll2019.150.2000xp_msver
1	2	2022-05-06 04:23:10	MSSQLSERVER	1073774914	4	xplog70.dll
2	1	2022-05-06 04:23:09	MSSQLSERVER	1	4	SqlCeip started pid: 7080 instance: CPEFlag: True
3	0	2022-05-06 04:20:08	Software Protection Platform Service	1073742727	0	None
4	0	2022-05-06 04:20:08	Software Protection Platform Service	1073758208	4	2122-04-11T22:50:08ZRulesEngine
5	0	2022-05-06 04:20:03	gupdate	0	4	Service stopped
6	0	2022-05-06 04:20:02	edgeupdate	0	4	Service stopped
7	2	2022-05-06 04:19:15	MSSQLSERVER	1073759714	4	015607231348849
8	0	2022-05-06 04:19:03	Software Protection Platform Service	1073742726	0	10.0.22000.593

Output

SECURITY LOG FILE

Windows Event Log Viewer

	Event Category:	Time Generated:	Source Name:	Event ID:	Event Type:	Event Data:
0	13824	2022-05-06 03:49:48	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f838vscodevscode.github-authentication/github.auth11%%809902022-05-05T22:19:44.4972107Z29664
1	13824	2022-05-06 03:49:48	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f838vscodevscode.microsoft-authentication/microsoft.login.keylist11%%8099322122602120 22-05-05T22:19:44.4972107Z29664
2	13824	2022-05-06 03:49:46	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f838vscode.login/account11%%8099322122602120 22-05-05T22:19:44.4972107Z29664
3	13824	2022-05-06 03:49:46	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f838test-keytar-loads*00%%8100322122602120 22-05-05T22:19:44.4972107Z29664
4	13824	2022-05-06 03:49:32	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f981vscodevscode.microsoft-authentication/microsoft.login.keylist11%%8099322122602120 22-05-05T22:19:26.9627730Z27088
5	13824	2022-05-06 03:49:30	Microsoft-Windows-Security-Auditing	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f981vscode.login/account11%%8099322122602120 22-05-05T22:19:26.9627730Z27088
6	13824	2022-05-06	Microsoft-Windows-	5379	8	S-1-5-21-4291028088-1715395961-2231046786-1001AkaashAKAASH0x3f981test-keytar-loads*00%%8100322122602120 22-05-05T22:19:26.9627730Z27088

Output

SYSTEM LOG FILE

Windows Event Log Viewer

	Event Category:	Time Generated:	Source Name:	Event ID:	Event Type:	
0	1014	2022-05-06 00:27:03	Microsoft-Windows-DNS-Client	1014	2	wpad128020000000A32000500000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
1	0	2022-05-06 00:27:02	Server	-1073739319	1	\Device\NetBT_Tcpip_{9FAC61D3-3EFC-41D5-84F7-99ACD1A31416}
2	1014	2022-05-06 00:27:00	Microsoft-Windows-DNS-Client	1014	2	wpad1280000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
3	0	2022-05-06 00:26:59	BTHUSB	1074069522	4	
4	268	2022-05-06 00:26:59	Microsoft-Windows-Kernel-Power	566	4	2411549140276426970490202697049020510false15
5	0	2022-05-06 00:26:59	Microsoft-Windows-Power-Troubleshooter	1	4	2022-05-05T18:51:39.9553958Z2022-05-05T18:56:59.2588956Z29191756156641100019797279164400000023
6	0	2022-05-06 00:26:59	VBoxNetLwf	-1073479668	1	\Device\VBoxNetLwf
7	268	2022-05-06 00:26:59	Microsoft-Windows-Kernel-Power	566	4	2412048331891171826970490202697049020491false20
8	100	2022-05-06 00:26:58	Microsoft-Windows-Kernel-Power	105	4	false2697049020

Conclusion

Windows Event Logs are critical from a Digital Forensic standpoint because they record every event that occurs in the Operating System. When an unauthenticated user gains access to a system, it takes various steps and procedures to gain access. These steps can be utilised to track down the offender. The incident response team is in charge of gathering important artefacts for future investigation. Event logs are kept in the system root directory as offline physical files. These files can be manually retrieved or obtained using other utility software, such as the Python Program we have implemented.