

## Project Title: Windows Log Analysis

Objectives: Analyzing windows event logs to monitor security operations and detect potential threats.

Introduction: Windows Event Logs are activity recorded or changes made to the computer, there are five types of event logs which are;

System event log: which contains events logged by windows system components.

Application event log: contains events logged by application or programs.

Setup event log: contains events related to application setup and installations

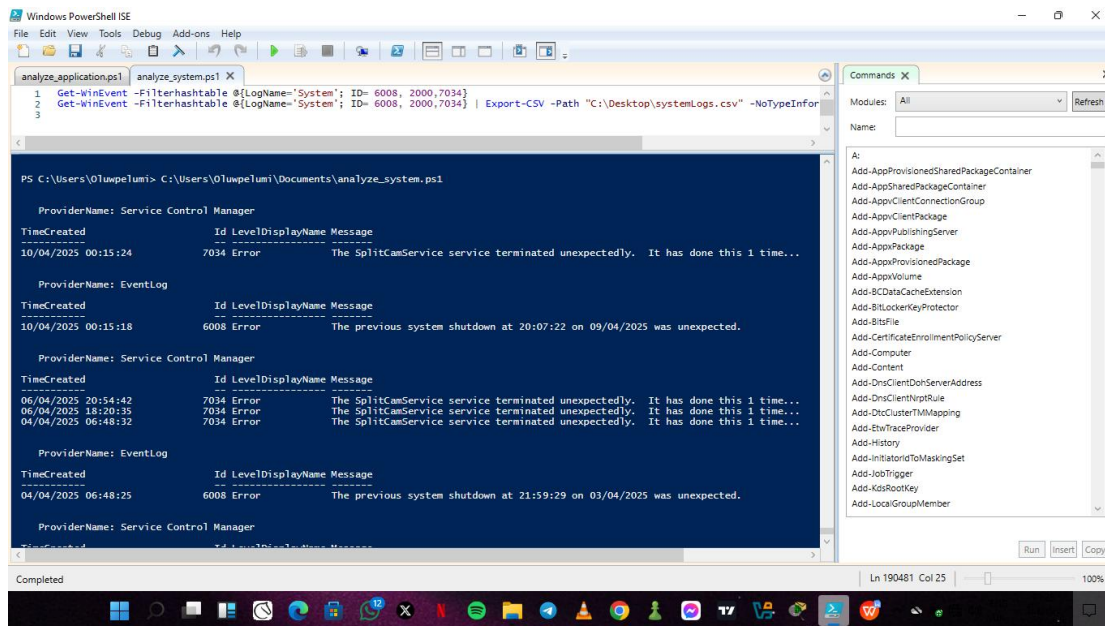
Forwarded Event Log: contains events forwarded from another computer.

Tools and Setup: Windows PowerShell (to write the commands script) Microsoft Excel or WPS(to view the .xlsx file)

## Log Analysis

1. System Event Log: I extracted recent events( e.g service shutdowns, hardware or driver failures) by using event ID which are 7034,6008, 2000 respectively, after formatted in a table view then export my results to Systemlogs.xlsx. Scripts;

```
Get-WinEvent -Filterhashtable @{LogName='System'; ID= 6008, 2000,7034}  
Get-WinEvent -Filterhashtable @{LogName='System'; ID= 6008, 2000,7034} |  
Export-CSV -Path "C:\Desktop\systemLogs.csv" -NoTypeInfo
```



Console Output

Message	Id	Version	Qualifiers	Level	Task	Opcode	Keywords	RecordId	ProviderName	ProviderId	LogName	ProcessId	ThreadId	MachineName	User	TimeCreated	ActivityId	RelativeTime
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	49878	Service Cor	555908d1-a	System	812	7052	DESKTOP-43EOGA7		30/03/2025 19:28:12		
The previo	6008	0	32768	2	0	0	3602879701	49825	EventLog		System	0	0	DESKTOP-43EOGA7		30/03/2025 19:28:08		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	49743	Service Cor	555908d1-a	System	800	6628	DESKTOP-43EOGA7		23/03/2025 12:52:25		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	49545	Service Cor	555908d1-a	System	856	6164	DESKTOP-43EOGA7		21/11/2024 16:18:47		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	49275	Service Cor	555908d1-a	System	852	1532	DESKTOP-43EOGA7		25/08/2024 08:26:46		
The previo	6008	0	32768	2	0	0	3602879701	49212	EventLog		System	0	0	DESKTOP-43EOGA7		15/08/2024 20:10:23		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	48926	Service Cor	555908d1-a	System	844	980	DESKTOP-43EOGA7		30/03/2025 19:28:12		
The previo	6008	0	32768	2	0	0	3602879701	48859	EventLog		System	0	0	DESKTOP-43EOGA7		30/03/2025 19:28:08		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	48348	Service Cor	555908d1-a	System	824	1624	DESKTOP-43EOGA7		23/03/2025 12:52:25		
The WireG	7034	0	49152	2	0	0	-9.19E+18	45535	Service Cor	555908d1-a	System	832	10760	DESKTOP-43EOGA7		17/12/2024 12:05:45		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	42728	Service Cor	555908d1-a	System	832	2688	DESKTOP-43EOGA7		28/11/2024 16:18:47		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	42214	Service Cor	555908d1-a	System	856	1484	DESKTOP-43EOGA7		21/11/2024 16:18:47		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	40373	Service Cor	555908d1-a	System	844	976	DESKTOP-43EOGA7		21/11/2024 16:18:47		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	39490	Service Cor	555908d1-a	System	848	932	DESKTOP-43EOGA7		21/11/2024 16:18:47		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	36849	Service Cor	555908d1-a	System	836	1364	DESKTOP-43EOGA7		25/08/2024 08:26:46		
The SplitCa	7034	0	49152	2	0	0	-9.19E+18	33489	Service Cor	555908d1-a	System	836	1436	DESKTOP-43EOGA7		25/08/2024 08:26:46		
The previo	6008	0	32768	2	0	0	3602879701	32420	EventLog		System	0	0	DESKTOP-43EOGA7		15/08/2024 20:10:23		

System Result in .xlsx file

2. Application Event: I queried the last 100 events from the past hour and identified application crash event like Event ID 1000, then exported my results to applicationlogs.xlsx. Scripts;

```

Get-EventLog -LogName Application -Newest 100 | where TimeGenerated -gt
(Get-Date).AddHours(-1)
Get-WinEvent -FilterHashtable @{'LogName': 'Application' ; ID=1000, 1001, 1026,
11707}
Get-WinEvent -FilterHashtable @{'LogName': 'Application' ; ID= 1000, 1001,
1026, 11707 ; StartTime= (Get-Date).AddHours(-1)} -MaxEvents 100 | Export-
CSV -Path "C:\Desktop\applicationlogs.csv" -NoTypeInformation

```

```

1 Get-EventLog -LogName Application -Newest 100 | where TimeGenerated -gt (Get-Date).AddHours(-1)
2 Get-WinEvent -FilterHashtable @{{LogName='Application' ; ID=1000, 1001, 1026, 11707}}
3 Get-WinEvent -FilterHashtable @{{LogName='Application' ; ID= 1000, 1001, 1026, 11707 ; StartTime= (Get-Date).AddHours(-1)} -MaxEvents 100 | Export-CSV -Path "C:\Desktop\applicati

```

P2: 80073cf9  
P3: 21996  
P4: 1  
P5: Windows.Desktop  
P6: R  
P7:  
P8:  
P9:  
P10:

Attached Files:  
\\C:\Windows\Temp\FailureReport\Metadata\_22538.txt  
\\C:\ProgramData\Microsoft\Windows\WER\Temp\WER\_2d499136-038b-4d27-a07e-70773b711e67.tmp.WERInternalMetadata.xml  
\\C:\ProgramData\Microsoft\Windows\WER\Temp\WER\_398c2823-87b9-44de-a6ff-e64bee4eca98.tmp.xml  
\\C:\ProgramData\Microsoft\Windows\WER\Temp\WER\_e828f8ca-8965-4a11-90a6-122a56c12674.tmp.csv  
\\C:\ProgramData\Microsoft\Windows\WER\Temp\WER\_a584bc25-0e56-42b6-91ce-c01d6d024c8d.tmp.txt

These files may be available here:  
\\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical\_Update;ScanForUp\_ecfb96dd6e1c077234cee7aee8bcd1ad25b6871\_00000000\_cab\_ce4427e3-19bf-4b44-bbae-5a38346e7740

Analysis symbol:  
Rechecking for solution: 0  
Report Id: ce4427e3-19bf-4b44-bbae-5a38346e7740  
Report Status: 4  
Hashed bucket:  
Cab Guid: 0

PS C:\Users\Olumelum>

## Console Output

Windows Log Analysis.d...

systemLogs.xlsx

securitylogs.xlsx

applicationlogs.xlsx

Sign in

Upgrade now

Menu

File Edit View Insert Page Layout Formulas Data Review View Tools Smart Toolbox

Share

Format Painter Paste

Calibri 11 A+ A-

B I U A Grid Color Fill Background Color

Alignment

Number Format

Cells

Formatting

Date Processing

Smart Toolbox

Settings

A1

fx Message

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Message	Id	Version	Qualifiers	Level	Task	Opcode	Keywords	RecordId	ProviderNa	ProviderId	LogName	ProcessId	ThreadId	MachineNa	UserId	Time
	Fault bucket, type 0																
	Event Name:																
	CbsPackageServicingFailure2																
	Response: Not available																
	Cab Id: 0																
	Problem signature:																
	P1: 10.0.21996.1																
	P2: Microsoft-Windows-																
	LanguageFeatures-Basic-en-gb-																
	Package																
	P3: 10.0.21996.1																
	P4: amd64																
2	P5: unknown	1001	0	0	4	0	0	3602879701	58025	Windows Error Report	Application	12136			0	DESKTOP-43EOGA7	23/04
	P6: 8024402c																
	P7: CBS Other																
	P8: Absent																
	P9: Absent																
	P10:																
	FodHelper(LanguageFeaturesO																
	nDemand)																

applicationlogs

100%

21:18 Wednesday 7/20/2025 ENG UK

## Application Result in .xlsx

3. Security: I detected event IDs for login attempts; 4624(success) & 4625(failure) also handle administrative access within the script, exported result to security.xlsx then simulated a login attempts to test scripts accuracy (used ctrl + L to lock my pc then login again and check for the event log) scripts;

```

Get-WinEvent -FilterHashtable @{{LogName='Security' ; ID= 4624 , 4625}}
if (-not ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(
[Security.Principal.WindowsBuiltInRole] "Administrator"))
{
    write-warning "This script needs to be run as Administrator!"
    exit
}
Get-EventLog -LogName Security -Newest 10
Get-EventLog -LogName Security -Newest 10 | Export-CSV -Path
"C:\Desktop\securitylogs.csv" -NoTypeInformation

```

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1 | analyze_security.ps1 X
8 #to check recent event
9 Get-EventLog -LogName Security -Newest 10
10 Get-EventLog -LogName Security -Newest 10 | Export-CSV -Path "C:\Desktop\securitylogs.csv" -NoTypeInformation

InstanceID      : 5379
TimeGenerated   : 23/04/2025 21:51:11
TimeWritten     : 23/04/2025 21:51:11
UserName       :
Site           :
Container      :

MachineName     : DESKTOP-43EOGA7
Data           : {}
Index          : 1687474
Category        : (13824)
CategoryNumber  : 13824
EventID        : 5379
EntryType       : SuccessAudit
Message         : Credential Manager credentials were read.

Subject:
  Security ID: 5-1-5-21-3690534919-1591512601-1815549316-1001
  Account Name: Oluwpeleumi
  Account Domain: DESKTOP-43EOGA7
  Logon ID: 0x76869bd
  Read Operation: %8100

This event occurs when a user performs a read operation on stored credentials in Credential Manager.
Source : Microsoft-Windows-Security-Auditing
ReplacementStrings : {5-1-5-21-3690534919-1591512601-1815549316-1001, Oluwpeleumi, DESKTOP-43EOGA7, 0x76869bd...}
InstanceID      : 5379
TimeGenerated   : 23/04/2025 21:51:11
TimeWritten     : 23/04/2025 21:51:11
UserName       :
Site           :
Container      :

```

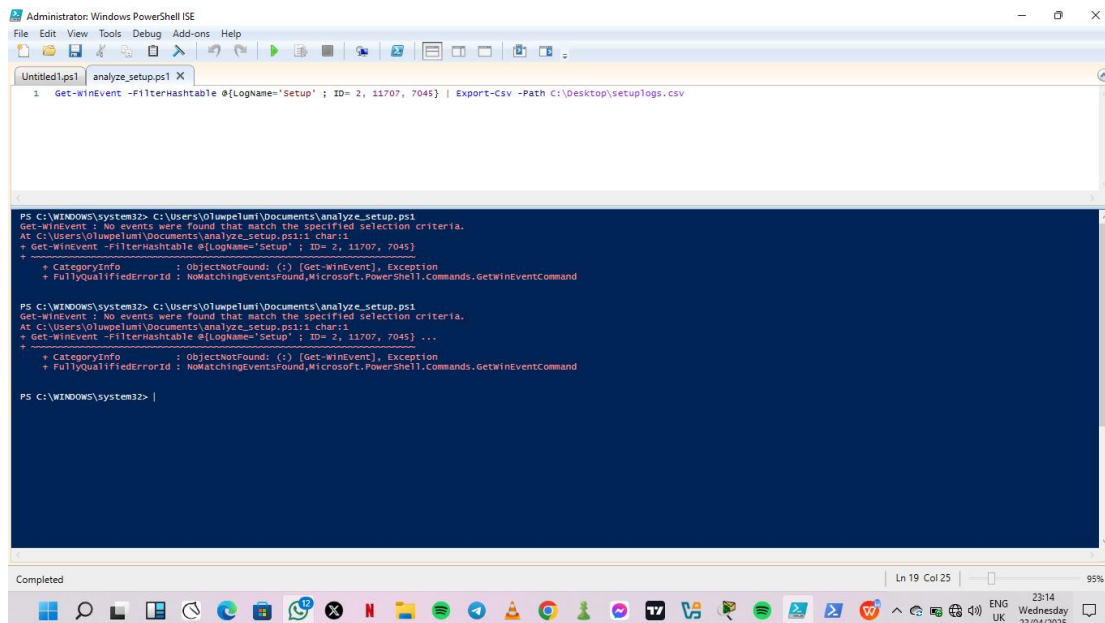
## Console Output

EventID	MachineName	Data	Index	Category	CategoryNumber	EntryType	Message	Source	ReplacementStrings	InstanceID	TimeGenerated	TimeWritten	UserName	Site	Container
5379	DESKTOP-43EOGA7	System.Byte[]	1687483	-13824	13824	SuccessAudit	Credential Manager credentials were read.  Subject: Security ID: 5-1-5-21-3690534919-1591512601-1815549316-1001 Account Name: Oluwpeleumi Account Domain: DESKTOP-43EOGA7 Logon ID: 0x76869bd Read Operation: %8100  This event occurs when a user performs a read operation on stored credentials in Credential Manager.	Microsoft-Windows-Security-Auditing	{5-1-5-21-3690534919-1591512601-1815549316-1001, Oluwpeleumi, DESKTOP-43EOGA7, 0x76869bd...}	5379	23/04/2025 21:51:11	23/04/2025 21:51:11			

## Security Results in .xlsx

4. Setup Event: Detect system updates, installations, and configuration events, Event IDs are 2, 11707, 7045 respectively and export results to setuplogs.xlsx. Scripts;

```
Get-WinEvent -FilterHashtable @{LogName='Setup' ; ID= 2, 11707, 7045}
```



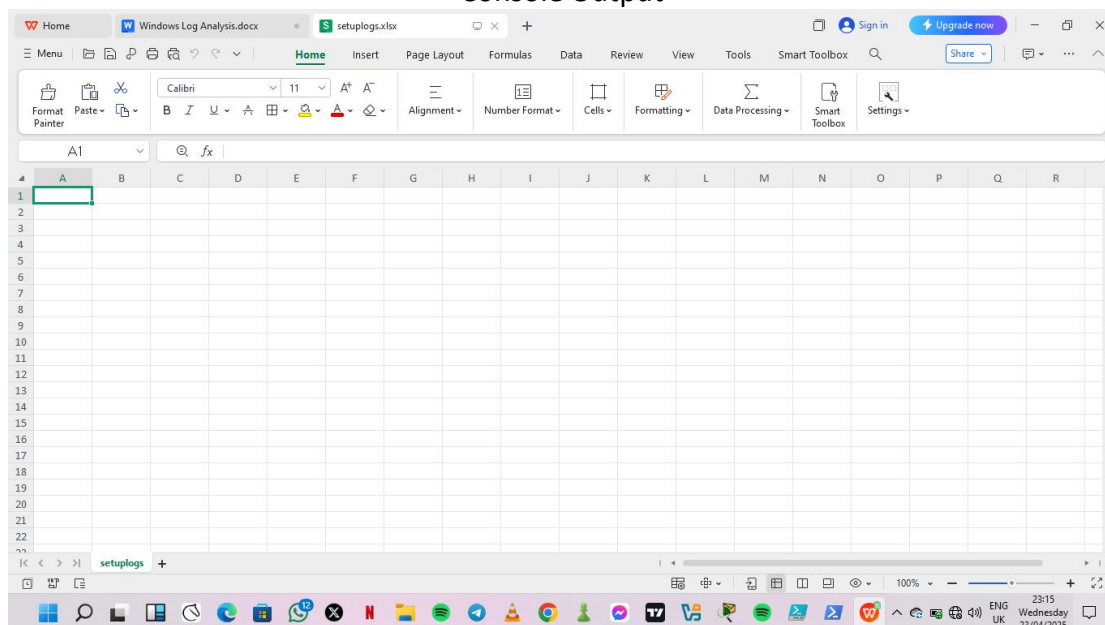
```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1 X
analyze_setup.ps1 X
1 Get-WinEvent -FilterHashtable @(LogName='Setup' ; ID= 2, 11707, 7045) | Export-Csv -Path C:\Desktop\setuplogs.csv

PS C:\WINDOWS\system32> C:\Users\oluwpelemi\Documents\analyze_setup.ps1
Get-WinEvent : No events were found that match the specified selection criteria.
At C:\Users\oluwpelemi\Documents\analyze_setup.ps1:1 char:1
+ Get-WinEvent -FilterHashtable @(LogName='Setup' ; ID= 2, 11707, 7045)
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (:) [Get-WinEvent], Exception
+ FullyQualifiedErrorId : NoMatchingEventsFound,Microsoft.PowerShell.Commands.GetWinEventCommand

PS C:\WINDOWS\system32> C:\Users\oluwpelemi\Documents\analyze_setup.ps1
Get-WinEvent : No events were found that match the specified selection criteria.
At C:\Users\oluwpelemi\Documents\analyze_setup.ps1:1 char:1
+ Get-WinEvent -FilterHashtable @(LogName='Setup' ; ID= 2, 11707, 7045) ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (:) [Get-WinEvent], Exception
+ FullyQualifiedErrorId : NoMatchingEventsFound,Microsoft.PowerShell.Commands.GetWinEventCommand

PS C:\WINDOWS\system32> |
```

## Console Output



Setup Result in .xlsx(It is empty because there is no events ID recorded in the Setup log)

5. Forwarded Event: My forwarded event log is disabled, to activate it. I need an extra computer to forward event logs.

## Summary of Findings

### System Log:

- Detected instances of unexpected shutdowns (Event ID 6008).
- Logged service crashes and restarts (Event ID 7034).
- Some hardware-related warnings and errors detected (e.g., Event ID 2000).

### Application Log:

- Successful and failed software installations were observed (Event ID 11707, 11724).
- A few application crashes detected (Event ID 1000, 1001).

#### Security Log:

- Normal logon activity recorded (Event ID 4624).
- No unusual or excessive failed login attempts (Event ID 4625) found within the checked period.

#### Setup Log:

- No recent system updates or setup-related events detected.
- Possible that updates are managed externally, or the log has been cleared.

#### Forwarded Events:

- Log is operational but not receiving live forwarded events due to standalone environment.

## Recommendations

- Enable Auditing Policies: Ensure all relevant security auditing (logon, privilege use) is enabled via AuditPol.
- Regular Log Reviews: Implement scheduled log reviews or alerts for critical Event IDs (6008, 7034, 4625).
- Retention Policy: Verify log retention settings to avoid overwriting important events.
- Forwarding Setup: For production use, implement Windows Event Forwarding with multiple systems for centralized monitoring.
- Update Confirmation: Check Windows Update settings or group policy to confirm update logs are being written properly.

## Conclusion

The event log analysis confirms that the system is generally stable with normal activity in logs. Some critical and warning events were identified, but no evidence of system compromise or misconfiguration was found. Future enhancements such as centralized log monitoring, alerting, and full audit policy coverage are recommended for proactive system health and security tracking.