تقرير المختبر الجنائي الرقمي: تحليل سجلات أحداث ويندوز (Windows Event Logs)

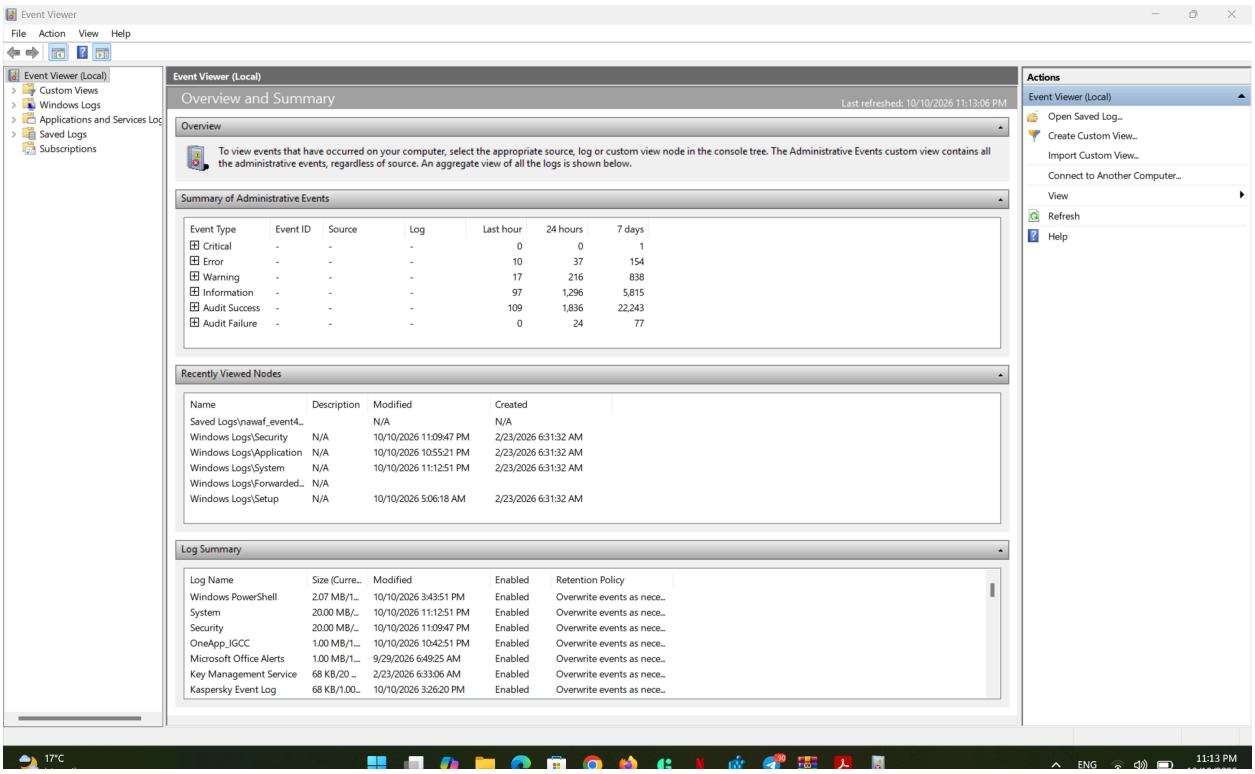
اسم الطالب: محمد حيدر مرشد ناصر المعمري

يوضح هذا التقرير الجنائي الفحص الفني لسجلات أحداث نظام ويندوز (`evtx.`) باستخدام الأدوات القياسية التي تشمل: **Windows Event Viewer**، و **LogViewPlus**، وأداة **Hayabusa**. كما يتضمن التقرير التحليل الفني لسيناريو هجوم واختراق عبر البرمجيات الخبيثة (**Part D**)، لتتبع الأنشطة المشبوهة، وآليات الاستمرارية (Persistence)، واستخراج العلم/الفلاج (Flag) المخفي داخل السجلات.

الجزء الأول: تحليل سجلات الأحداث عبر Event Viewer (Part A)

1. الاستكشاف وتصدير السجلات

تم استخدام أداة **Event Viewer** لاستكشاف سجلات نظام التشغيل الأساسية. تم تصدير مسارات السجلات الرئيسية الثلاثة: **Security**، **Application**، و **System** وحفظها داخل المجلد المخصص للتسليم باسم:

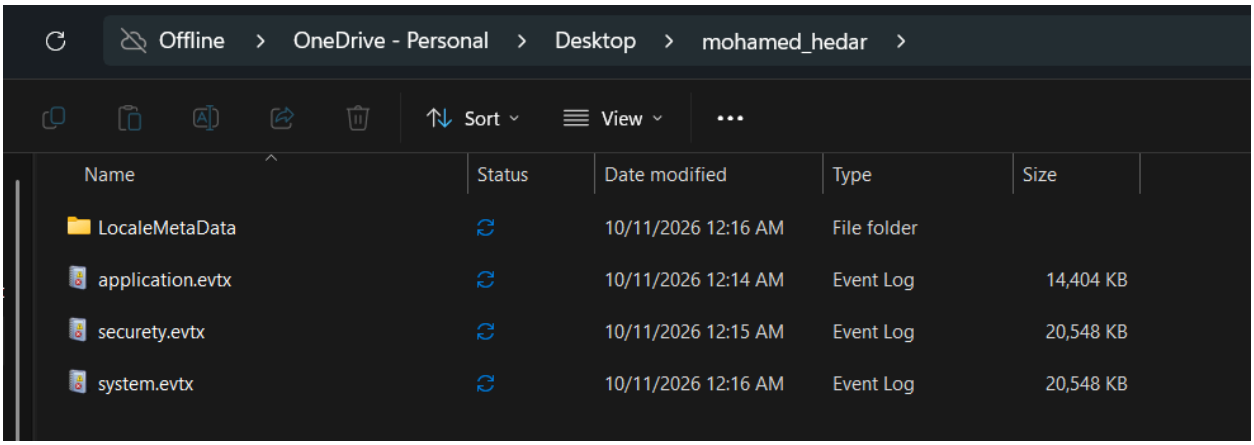


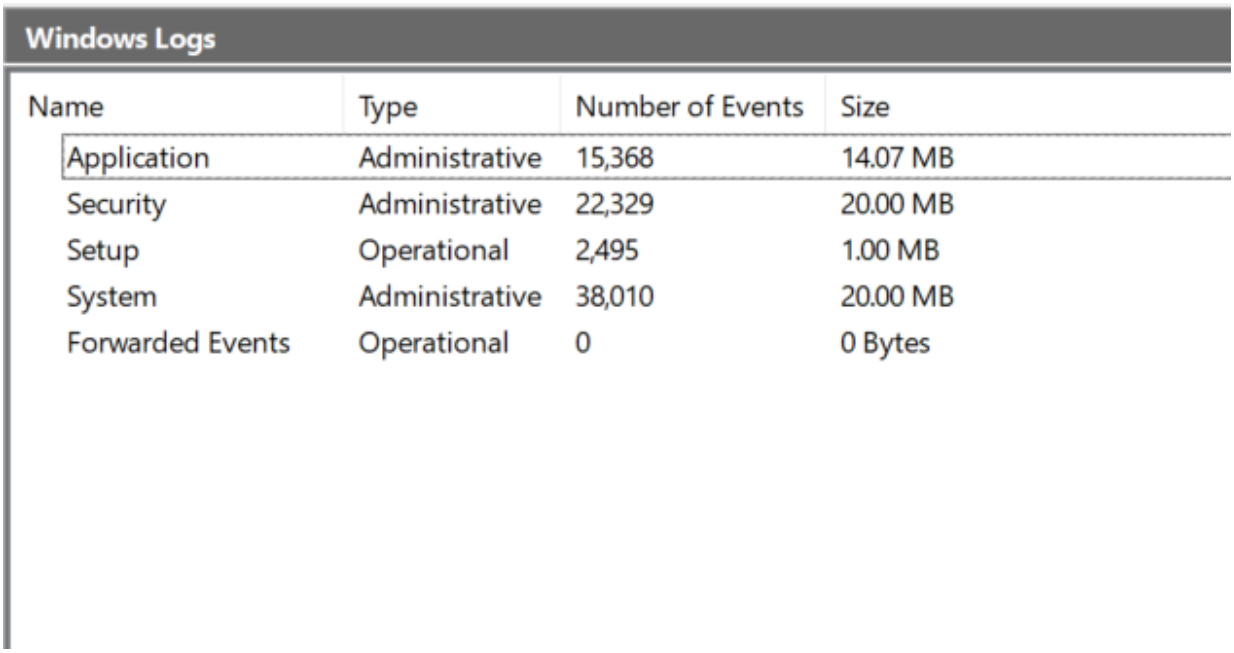
2. الفلترة الجنائية للـ Event IDs (أهم 10 معرفات أحداث)

لتحديد الأحداث المتعلقة بالأمن السيبراني، تم تطبيق الفلترة على أهم المعرفات الجنائية:

معرف الحدث (Event ID)	مصدر السجل (Source)	الوصف والأهمية الجنائية (Forensic Significance)
4624	Security	**تسجيل دخول ناجح:** للتحقق من الجلسات الشرعية وأنواع المصادقة.
4625	Security	**فشل تسجيل الدخول:** أساسي لتتبع هجمات التخمين (Brute-Force).
4688	Security	**إنشاء عملية جديدة (Process):** لتتبع تنفيذ الأوامر والبرمجيات الخبيثة.
7045	System	**تثبيت خدمة جديدة:** لكشف التثبيت غير المصرح به (شائعة Persistence آلية) للخدمات.
1102	Security	**مسح سجل الأمان:** مؤشر عالي الخطورة على محاولة المجرم مسح آثاره الرقمية (Anti-Forensics).
4672	Security	**منح صلاحيات خاصة:** لكشف عمليات تصعيد الصلاحيات إلى مستوى مسؤول (Admin).

4634	Security	**تسجيل الخروج:** لحساب المدة الزمنية لنشاط المستخدم أثناء الاختراق.
4720	Security	**إنشاء حساب مستخدم:** لكشف إنشاء حسابات خلفية (Backdoor Accounts).
4726	Security	**حذف حساب مستخدم:** لتتبع عمليات التنظيف والتغطية بعد الاختراق.
1074	System	**إيقاف/إعادة تشغيل النظام:** لتسجيل عمليات إيقاف التشغيل والأسباب والعمليات المسببة لها.



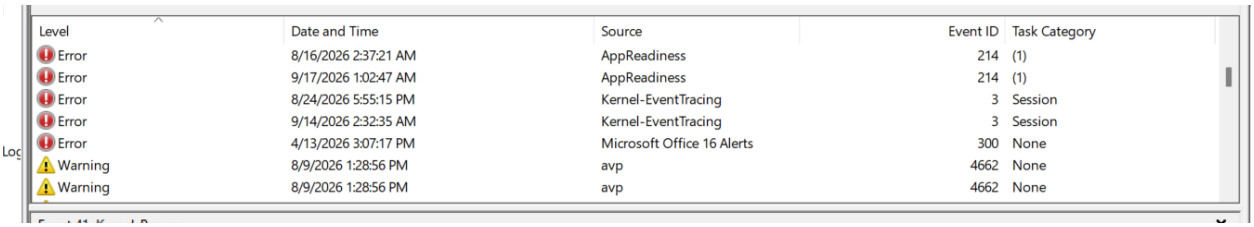


الجزء الثاني: تحليل السجلات باستخدام LogViewPlus (Part B)

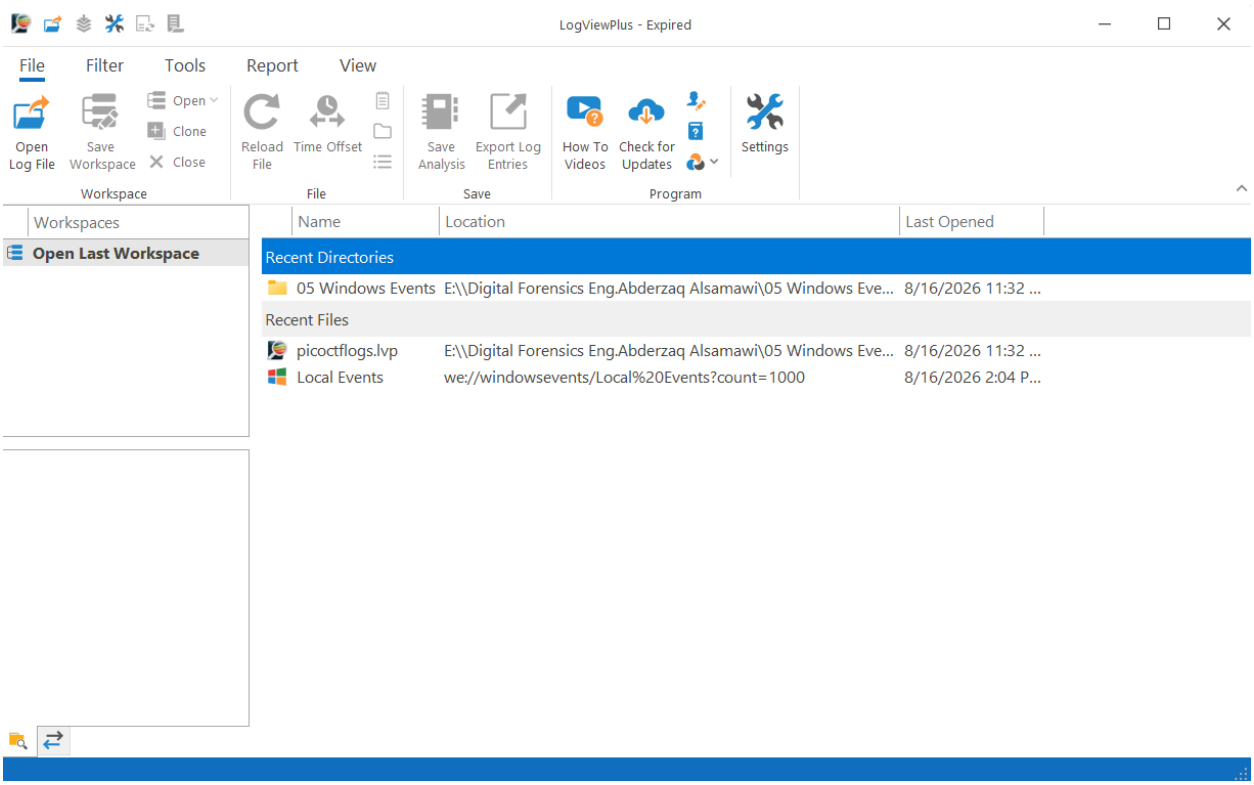
1. التحليل حسب مستوى الخطورة (Severity Levels)

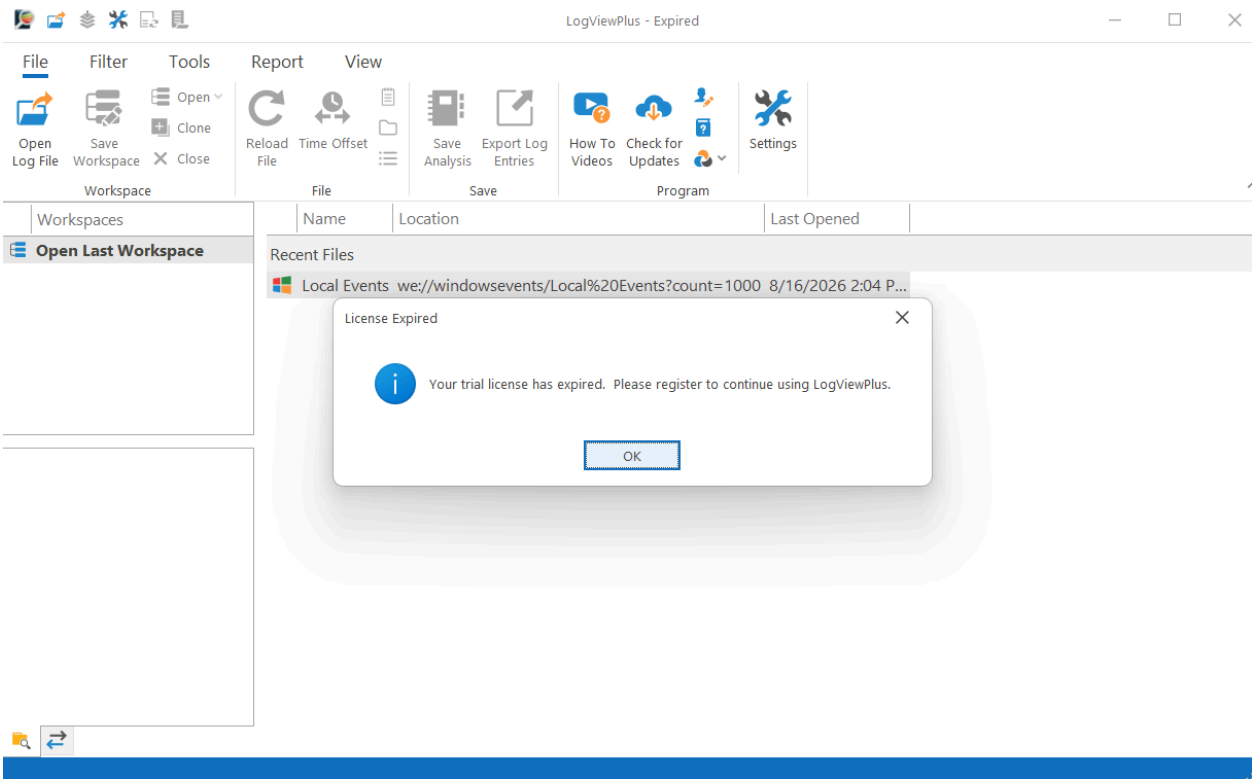
تم استيراد ملفات السجلات المصدّرة إلى أداة **LogViewPlus** وتطبيق التصفية حسب المستويات التالية:

- **Error (خطأ):** لتحديد نقاط الفشل الحرجة في العمليات أو التطبيقات أو برامج التشغيل.
- **Warning (تحذير):** يشير إلى مشكلات غير حرجة أو سلوكيات غير طبيعية تتطلب المتابعة.
- **Information (معلومات):** يتضمن أنشطة النظام الروتينية والعمليات الطبيعية.

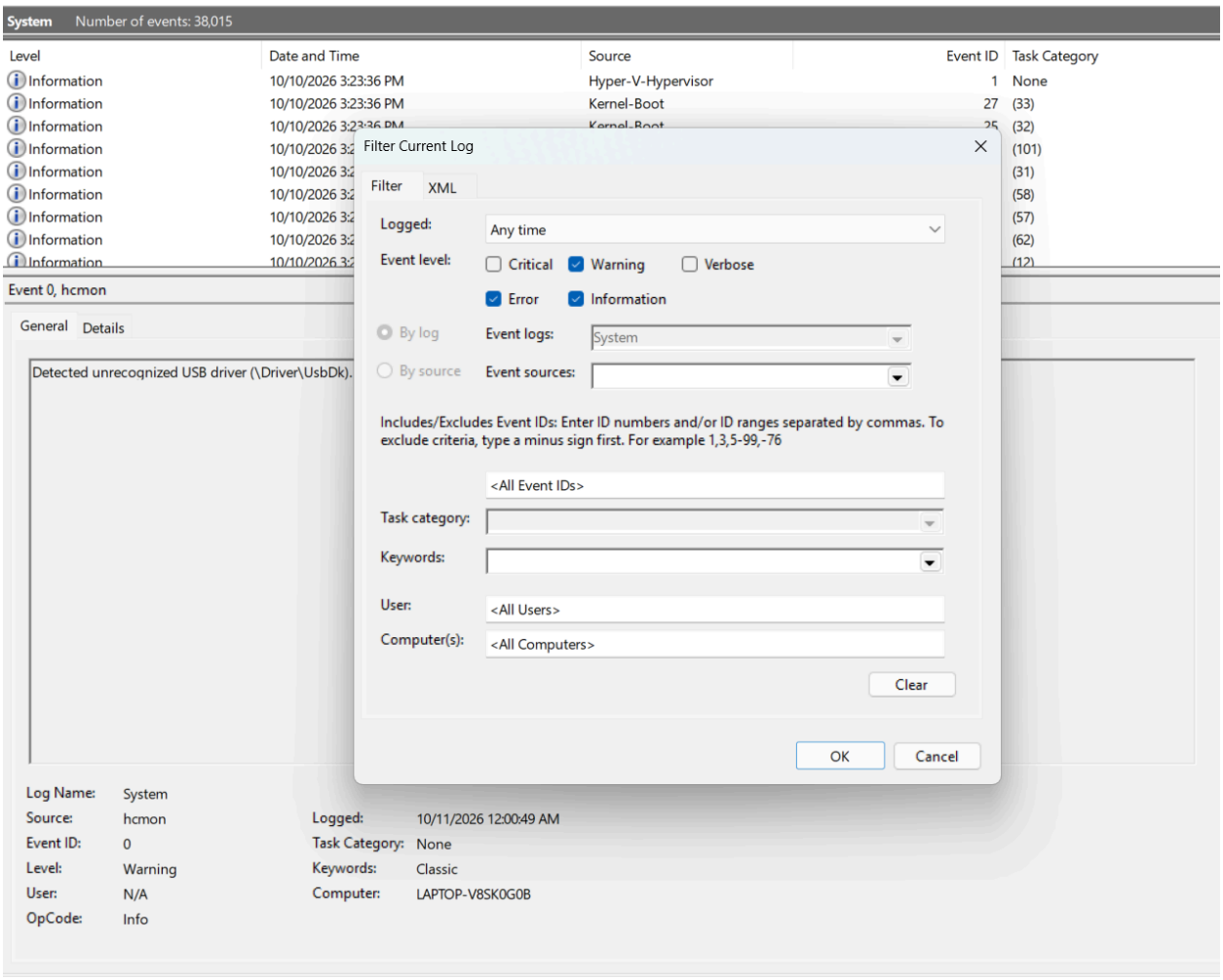


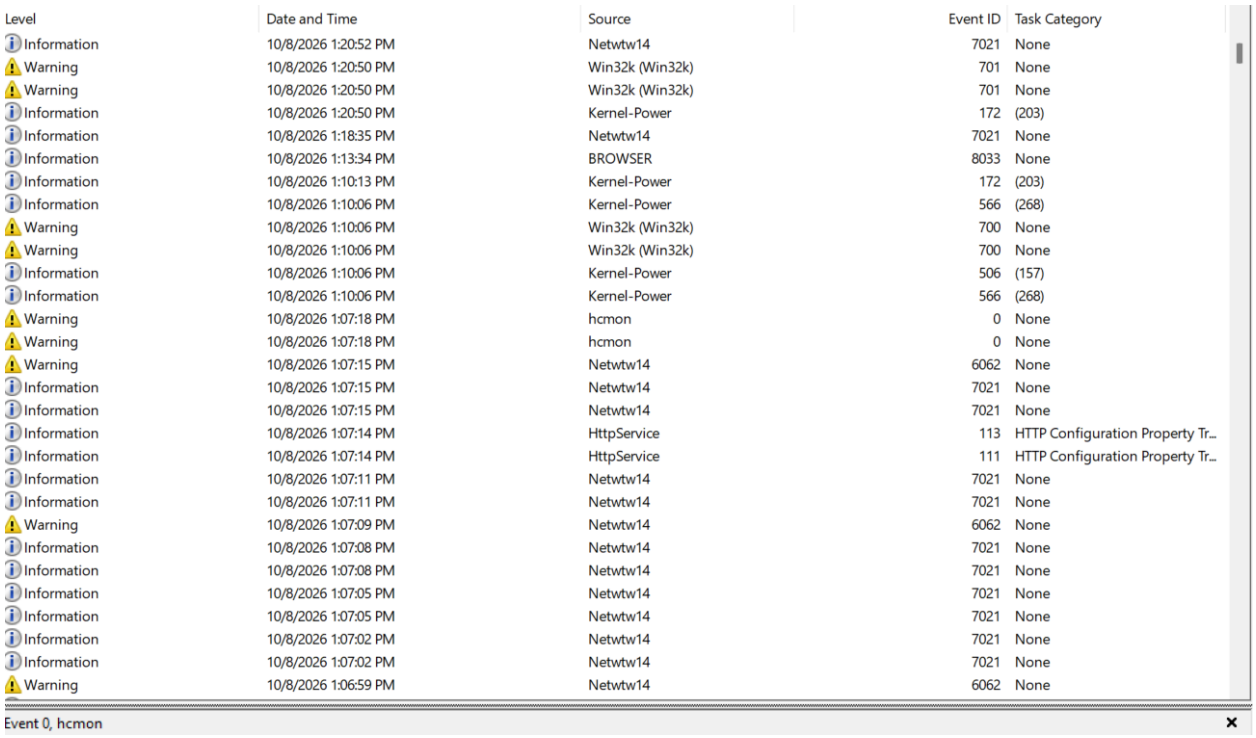
Level	Date and Time	Source	Event ID	Task Category
Error	8/16/2026 2:37:21 AM	AppReadiness	214	(1)
Error	9/17/2026 1:02:47 AM	AppReadiness	214	(1)
Error	8/24/2026 5:55:15 PM	Kernel-EventTracing	3	Session
Error	9/14/2026 2:32:35 AM	Kernel-EventTracing	3	Session
Error	4/13/2026 3:07:17 PM	Microsoft Office 16 Alerts	300	None
Warning	8/9/2026 1:28:56 PM	avp	4662	None
Warning	8/9/2026 1:28:56 PM	avp	4662	None





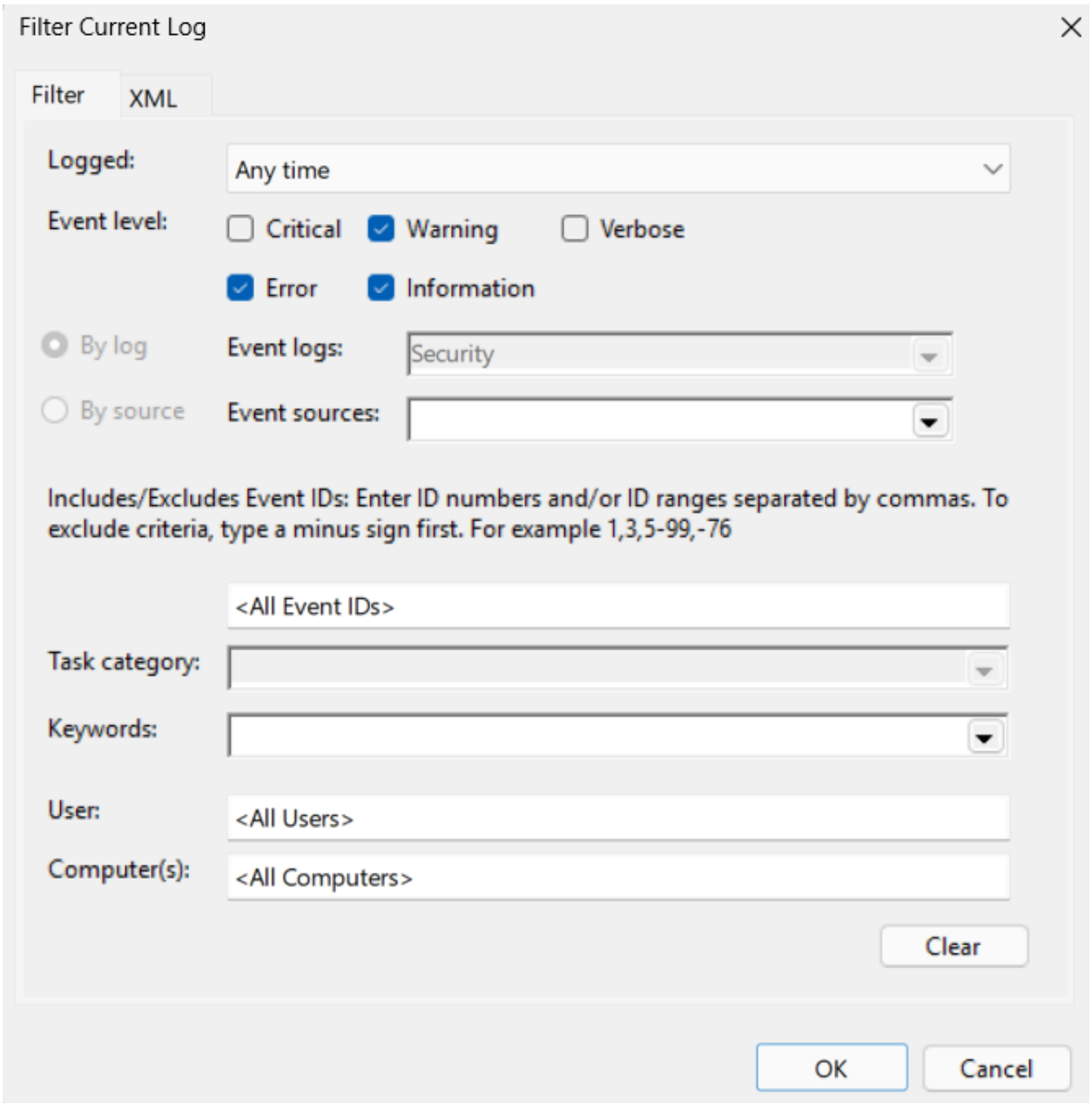
بما أن البرنامج يتطلب شراء ترخيص بعد انتهاء الفترة التجريبية، لدينا خيار لإكمال التكليف:

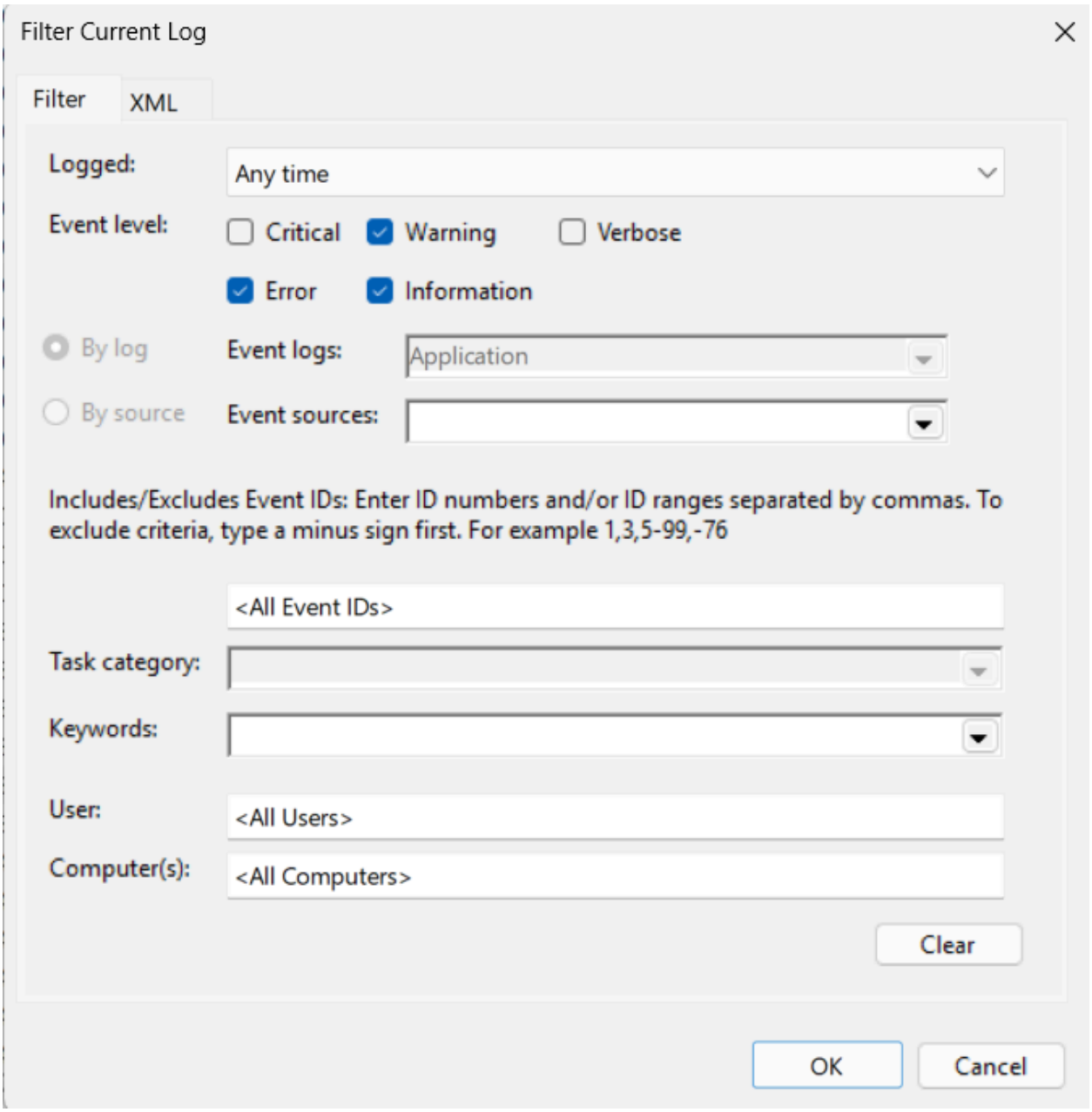

System Number of events: 38,015
Level Date and Time Source Event ID Task Category
Information 10/10/2026 3:23:36 PM Hyper-V-Hypervisor 1 None
Information 10/10/2026 3:23:36 PM Kernel-Boot 27 (33)
Information (32)
Information (101)
Information (31)
Information (58)
Information (57)
Information (62)
Information (12)
Filter Current Log
Filter XML
Logged: Any time
Event level: Critical Warning Verbose
Error Information
By log Event logs: System
By source Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
User: <All Users>
Computer(s): <All Computers>
Clear
OK Cancel
Event 0, hcmon
General Details
Detected unrecognized USB driver (\Driver\UsbDk).
Log Name: System
Source: hcmon
Event ID: 0
Level: Warning
User: N/A
OpCode: Info
Logged: 10/11/2026 12:00:49 AM
Task Category: None
Keywords: Classic
Computer: LAPTOP-V8SK0G0B

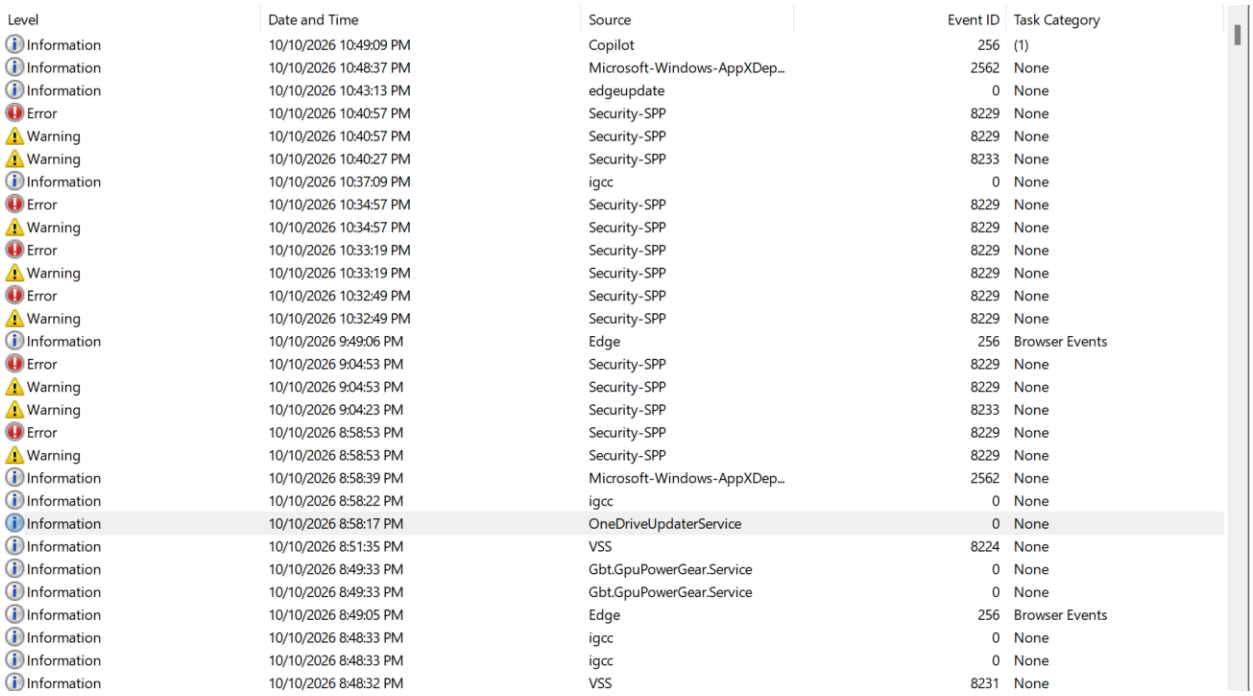


Level	Date and Time	Source	Event ID	Task Category
Information	10/8/2026 1:20:52 PM	Netwtw14	7021	None
Warning	10/8/2026 1:20:50 PM	Win32k (Win32k)	701	None
Warning	10/8/2026 1:20:50 PM	Win32k (Win32k)	701	None
Information	10/8/2026 1:20:50 PM	Kernel-Power	172	(203)
Information	10/8/2026 1:18:35 PM	Netwtw14	7021	None
Information	10/8/2026 1:13:34 PM	BROWSER	8033	None
Information	10/8/2026 1:10:13 PM	Kernel-Power	172	(203)
Information	10/8/2026 1:10:06 PM	Kernel-Power	566	(268)
Warning	10/8/2026 1:10:06 PM	Win32k (Win32k)	700	None
Warning	10/8/2026 1:10:06 PM	Win32k (Win32k)	700	None
Information	10/8/2026 1:10:06 PM	Kernel-Power	506	(157)
Information	10/8/2026 1:10:06 PM	Kernel-Power	566	(268)
Warning	10/8/2026 1:07:18 PM	hcmon	0	None
Warning	10/8/2026 1:07:18 PM	hcmon	0	None
Warning	10/8/2026 1:07:15 PM	Netwtw14	6062	None
Information	10/8/2026 1:07:15 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:15 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:14 PM	HttpService	113	HTTP Configuration Property Tr...
Information	10/8/2026 1:07:14 PM	HttpService	111	HTTP Configuration Property Tr...
Information	10/8/2026 1:07:11 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:11 PM	Netwtw14	7021	None
Warning	10/8/2026 1:07:09 PM	Netwtw14	6062	None
Information	10/8/2026 1:07:08 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:08 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:05 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:05 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:02 PM	Netwtw14	7021	None
Information	10/8/2026 1:07:02 PM	Netwtw14	7021	None
Warning	10/8/2026 1:06:59 PM	Netwtw14	6062	None

Event 0, hcmon


Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Security
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel


Filter Current Log
Filter
XML
Logged:
Any time
Event level:
Critical
Warning
Verbose
Error
Information
By log
Event logs:
Application
By source
Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
User:
<All Users>
Computer(s):
<All Computers>
Clear
OK
Cancel

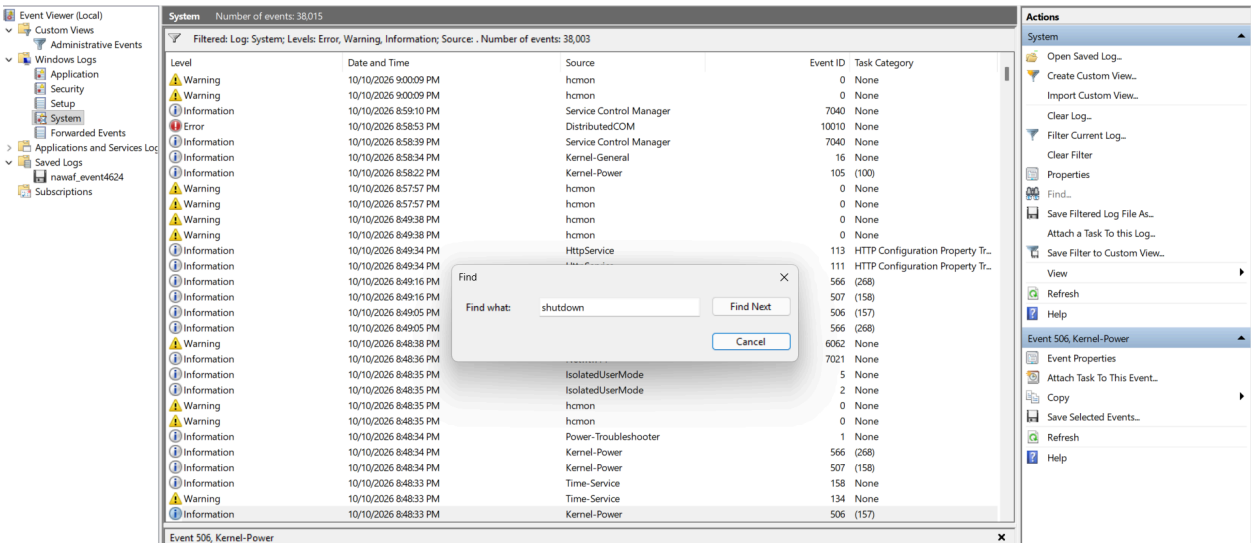


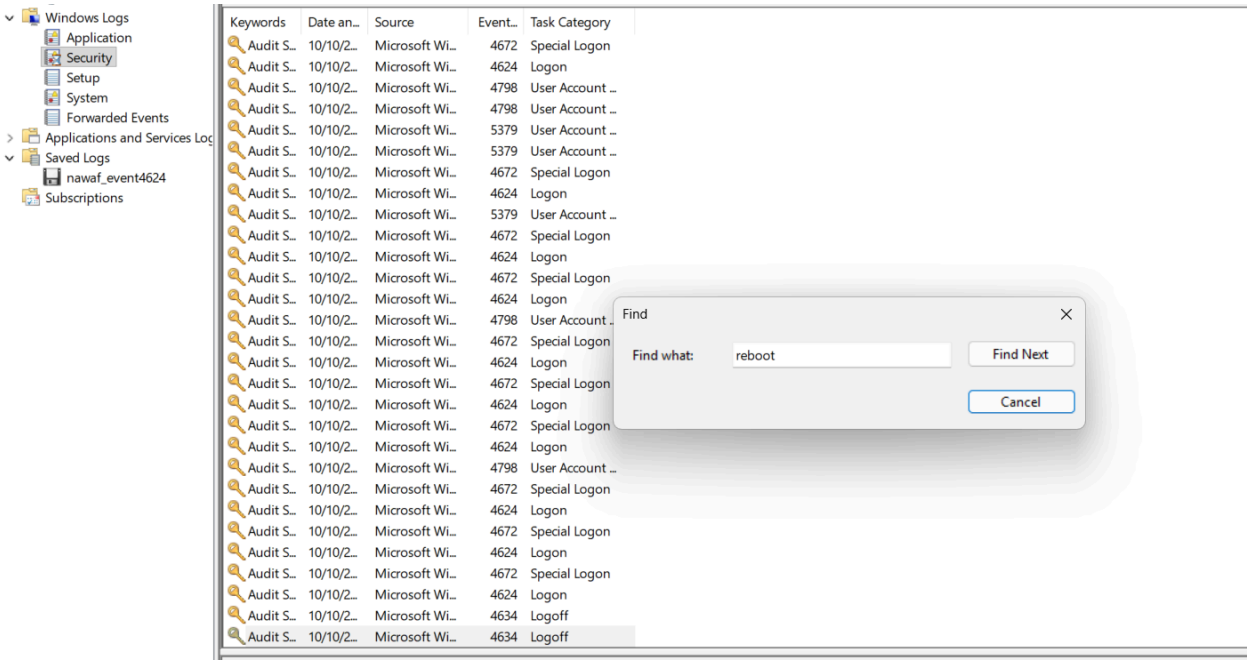
Level	Date and Time	Source	Event ID	Task Category
Information	10/10/2026 10:49:09 PM	Copilot	256	(1)
Information	10/10/2026 10:48:37 PM	Microsoft-Windows-AppXDep...	2562	None
Information	10/10/2026 10:43:13 PM	edgeupdate	0	None
Error	10/10/2026 10:40:57 PM	Security-SPP	8229	None
Warning	10/10/2026 10:40:57 PM	Security-SPP	8229	None
Warning	10/10/2026 10:40:27 PM	Security-SPP	8233	None
Information	10/10/2026 10:37:09 PM	igcc	0	None
Error	10/10/2026 10:34:57 PM	Security-SPP	8229	None
Warning	10/10/2026 10:34:57 PM	Security-SPP	8229	None
Error	10/10/2026 10:33:19 PM	Security-SPP	8229	None
Warning	10/10/2026 10:33:19 PM	Security-SPP	8229	None
Error	10/10/2026 10:32:49 PM	Security-SPP	8229	None
Warning	10/10/2026 10:32:49 PM	Security-SPP	8229	None
Information	10/10/2026 9:49:06 PM	Edge	256	Browser Events
Error	10/10/2026 9:04:53 PM	Security-SPP	8229	None
Warning	10/10/2026 9:04:53 PM	Security-SPP	8229	None
Warning	10/10/2026 9:04:23 PM	Security-SPP	8233	None
Error	10/10/2026 8:58:53 PM	Security-SPP	8229	None
Warning	10/10/2026 8:58:53 PM	Security-SPP	8229	None
Information	10/10/2026 8:58:39 PM	Microsoft-Windows-AppXDep...	2562	None
Information	10/10/2026 8:58:22 PM	igcc	0	None
Information	10/10/2026 8:58:17 PM	OneDriveUpdaterService	0	None
Information	10/10/2026 8:51:35 PM	VSS	8224	None
Information	10/10/2026 8:49:33 PM	Gbt.GpuPowerGear.Service	0	None
Information	10/10/2026 8:49:33 PM	Gbt.GpuPowerGear.Service	0	None
Information	10/10/2026 8:49:05 PM	Edge	256	Browser Events
Information	10/10/2026 8:48:33 PM	igcc	0	None
Information	10/10/2026 8:48:33 PM	igcc	0	None
Information	10/10/2026 8:48:32 PM	VSS	8231	None

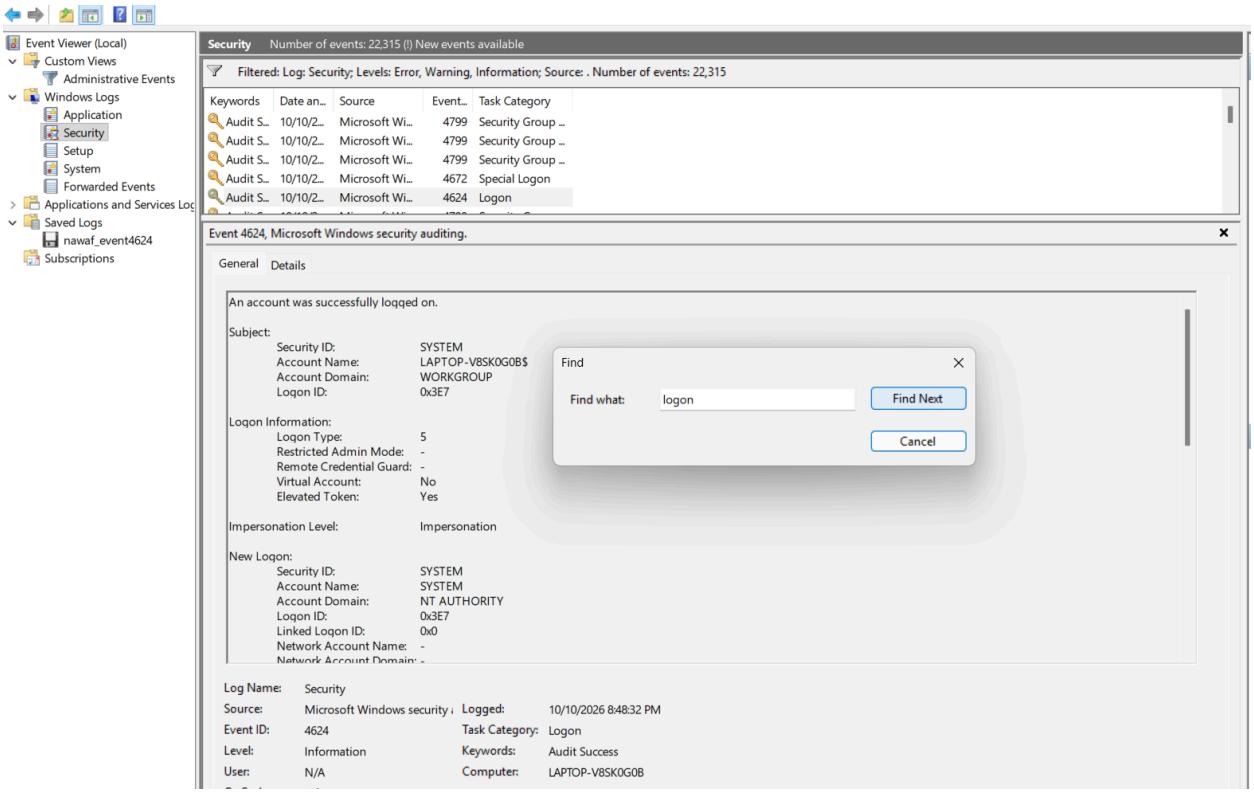
2. البحث عن الكلمات المفتاحية والنتائج التشغيلية

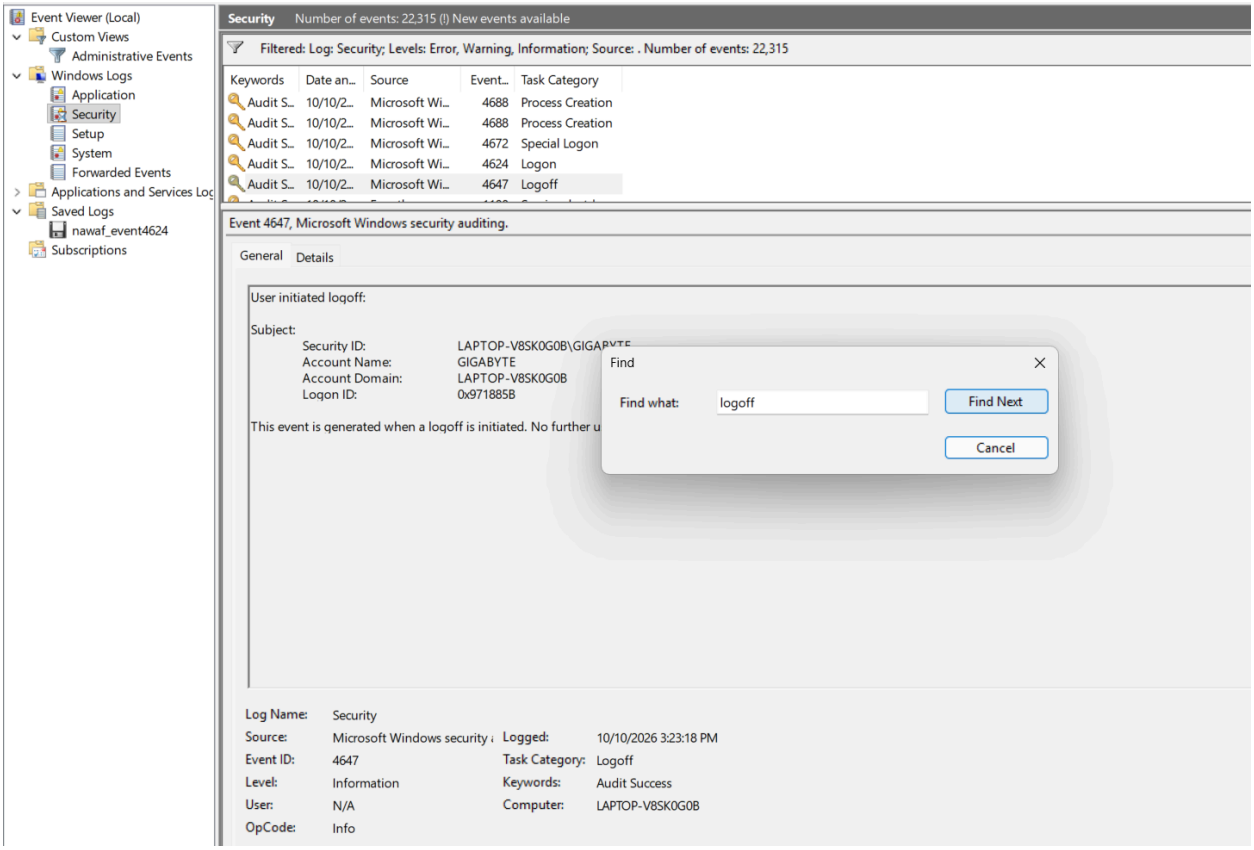
تم إجراء بحث مخصص عبر السجلات المستوردة للكلمات المفتاحية المطلوبة:

- **`logon` / `logoff`:** تم رسم التايملاين الزمني لجلسات المستخدمين وتحديد أوقات بدء ونهاية الأنشطة.
- **`reboot` / `shutdown`:** تم تحديد الطوابع الزمنية الدقيقة التي صَدرت فيها أوامر إيقاف أو إعادة التشغيل ومعرفة اسم العملية المسؤولة.
- **`uninstall`:** تتبع عمليات إزالة البرامج وتعديل إعدادات البرمجيات في النظام.


Event Viewer (Local)
Custom Views
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Saved Logs
nawaf_event4624
Subscriptions
System Number of events: 38,015
Filtered: Log: System; Levels: Error, Warning, Information; Source: . Number of events: 38,003
Level Date and Time Source Event ID Task Category
Warning 10/10/2026 9:00:09 PM hcmon 0 None
Warning 10/10/2026 9:00:09 PM hcmon 0 None
Information 10/10/2026 8:59:10 PM Service Control Manager 7040 None
Error 10/10/2026 8:58:53 PM DistributedCOM 10010 None
Information 10/10/2026 8:58:39 PM Service Control Manager 7040 None
Information 10/10/2026 8:58:34 PM Kernel-General 16 None
Information 10/10/2026 8:58:22 PM Kernel-Power 105 (100)
Warning 10/10/2026 8:57:57 PM hcmon 0 None
Warning 10/10/2026 8:57:57 PM hcmon 0 None
Warning 10/10/2026 8:49:38 PM hcmon 0 None
Warning 10/10/2026 8:49:38 PM hcmon 0 None
Information 10/10/2026 8:49:34 PM HttpService 113 HTTP Configuration Property Tr...
Information 10/10/2026 8:49:34 PM 111 HTTP Configuration Property Tr...
Information 10/10/2026 8:49:16 PM 566 (268)
Information 10/10/2026 8:49:16 PM 507 (158)
Information 10/10/2026 8:49:05 PM 506 (157)
Information 10/10/2026 8:49:05 PM 566 (268)
Warning 10/10/2026 8:48:38 PM 6062 None
Information 10/10/2026 8:48:36 PM 7021 None
Information 10/10/2026 8:48:35 PM IsolatedUserMode 5 None
Information 10/10/2026 8:48:35 PM IsolatedUserMode 2 None
Warning 10/10/2026 8:48:35 PM hcmon 0 None
Warning 10/10/2026 8:48:35 PM hcmon 0 None
Information 10/10/2026 8:48:34 PM Power-Troubleshooter 1 None
Information 10/10/2026 8:48:34 PM Kernel-Power 566 (268)
Information 10/10/2026 8:48:34 PM Kernel-Power 507 (158)
Information 10/10/2026 8:48:33 PM Time-Service 158 None
Warning 10/10/2026 8:48:33 PM Time-Service 134 None
Information 10/10/2026 8:48:33 PM Kernel-Power 506 (157)
Event 506, Kernel-Power
Find
Find what: shutdown
Find Next
Cancel
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Event 506, Kernel-Power
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help


Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Saved Logs
nawaf_event4624
Subscriptions
Keywords Date an... Source Event... Task Category
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4798 User Account ...
Audit S... 10/10/2... Microsoft Wi... 4798 User Account ...
Audit S... 10/10/2... Microsoft Wi... 5379 User Account ...
Audit S... 10/10/2... Microsoft Wi... 5379 User Account ...
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 5379 User Account ...
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4798 User Account ...
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4798 User Account ...
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4634 Logoff
Audit S... 10/10/2... Microsoft Wi... 4634 Logoff
Find
Find what: reboot
Find Next
Cancel


Event Viewer (Local)
Custom Views
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Saved Logs
nawaf_event4624
Subscriptions
Security Number of events: 22,315 (!) New events available
Filtered: Log: Security; Levels: Error, Warning, Information; Source: . Number of events: 22,315
Keywords Date an... Source Event... Task Category
Audit S... 10/10/2... Microsoft Wi... 4799 Security Group ...
Audit S... 10/10/2... Microsoft Wi... 4799 Security Group ...
Audit S... 10/10/2... Microsoft Wi... 4799 Security Group ...
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Event 4624, Microsoft Windows security auditing.
General Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: LAPTOP-V8SK0G0B$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Information:
Logon Type: 5
Restricted Admin Mode: -
Remote Credential Guard: -
Virtual Account: No
Elevated Token: Yes
Impersonation Level: Impersonation
New Logon:
Security ID: SYSTEM
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7
Linked Logon ID: 0x0
Network Account Name: -
Find
Find what: logon
Find Next
Cancel
Log Name: Security
Source: Microsoft Windows security Logged: 10/10/2026 8:48:32 PM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: LAPTOP-V8SK0G0B

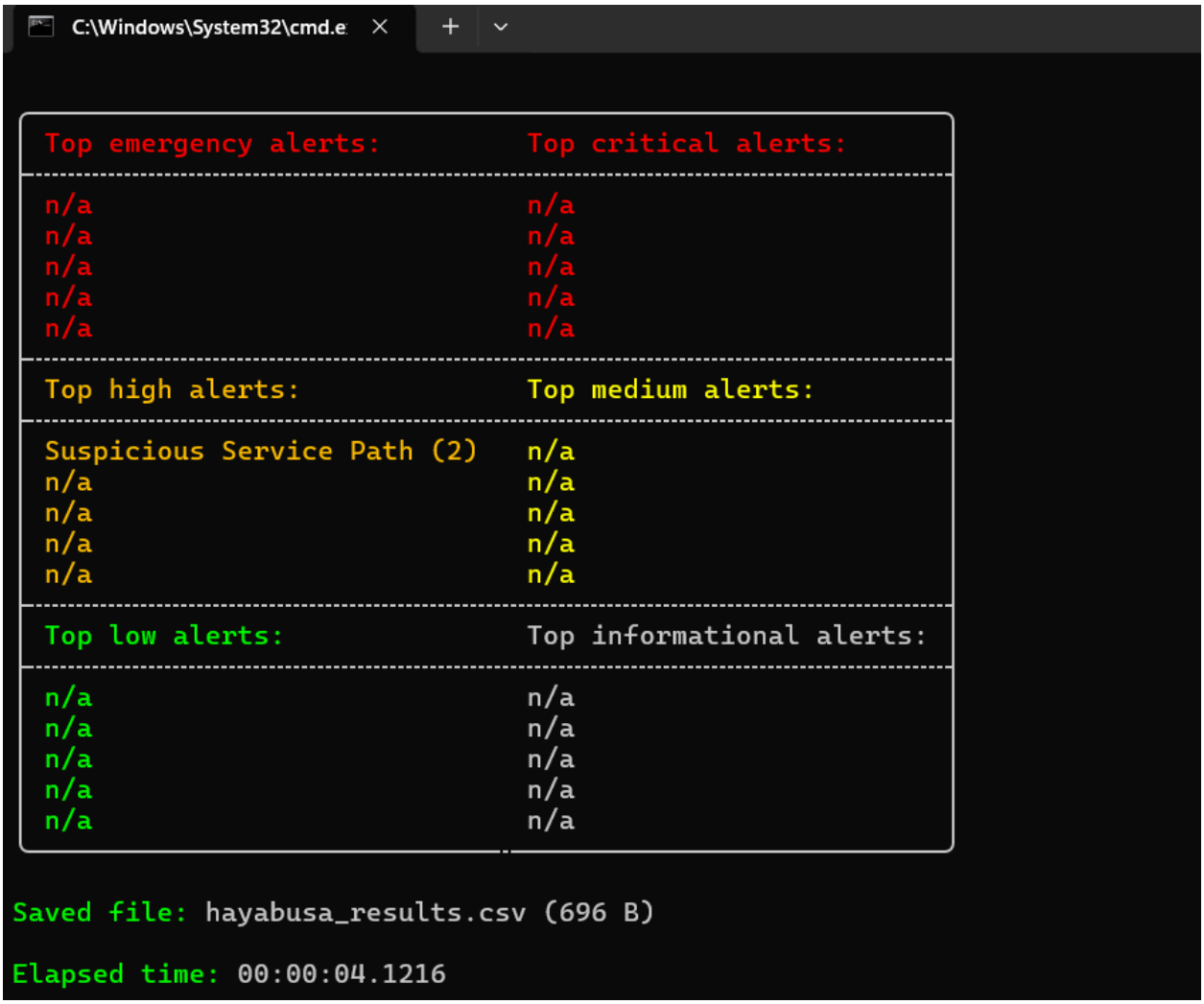

Event Viewer (Local)
Custom Views
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Saved Logs
nawaf_event4624
Subscriptions
Security Number of events: 22,315 (!) New events available
Filtered: Log: Security; Levels: Error, Warning, Information; Source: . Number of events: 22,315
Keywords Date an... Source Event... Task Category
Audit S... 10/10/2... Microsoft Wi... 4688 Process Creation
Audit S... 10/10/2... Microsoft Wi... 4688 Process Creation
Audit S... 10/10/2... Microsoft Wi... 4672 Special Logon
Audit S... 10/10/2... Microsoft Wi... 4624 Logon
Audit S... 10/10/2... Microsoft Wi... 4647 Logoff
Event 4647, Microsoft Windows security auditing.
General Details
User initiated logoff:
Subject:
Security ID: LAPTOP-V8SK0G0B\GIGABYTE
Account Name: GIGABYTE
Account Domain: LAPTOP-V8SK0G0B
Logon ID: 0x971885B
This event is generated when a logoff is initiated. No further u
Find
Find what: logoff
Find Next
Cancel
Log Name: Security
Source: Microsoft Windows security Logged: 10/10/2026 3:23:18 PM
Event ID: 4647 Task Category: Logoff
Level: Information Keywords: Audit Success
User: N/A Computer: LAPTOP-V8SK0G0B
OpCode: Info

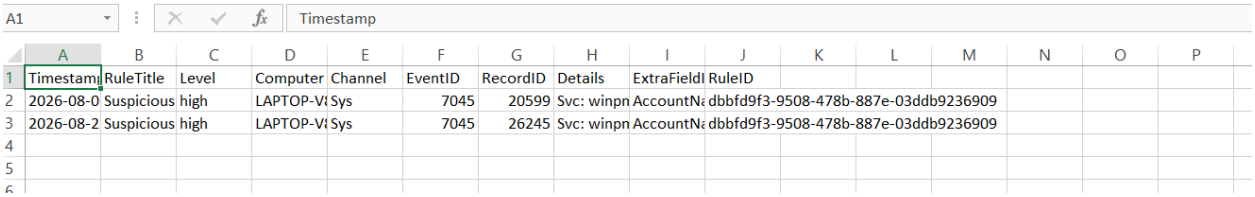
الجزء الثالث: صيد التهديدات والتايملاين عبر Hayabusa (Part C)

1. منهجية العمل وتنفيذ الأمر

تم تشغيل أداة **Hayabusa** على مجلد السجلات المصدّرmohamed_hedar للقيام بصيد التهديدات الآلي استناداً إلى قواعد Sigma وبناء تايملاين زمني جنائي.







الجزء الرابع: تحدي السجلات - التحقيق في هجوم برمجية خبيثة (Part D)

1. تحليل سيناريو الحادثة

أبلغ أحد الموظفين أن جهازه ينطفئ فوراً بعد كل عملية تسجيل دخول مع ظهور نافذة سوداء لـ CMD. وقد تبين أن المشكلة ناتجة عن برمجية خبيثة تم تثبيتها من الإنترنت وأنشأت آلية استمرارية لتنفيذ أمر الإيقاف تلقائياً.

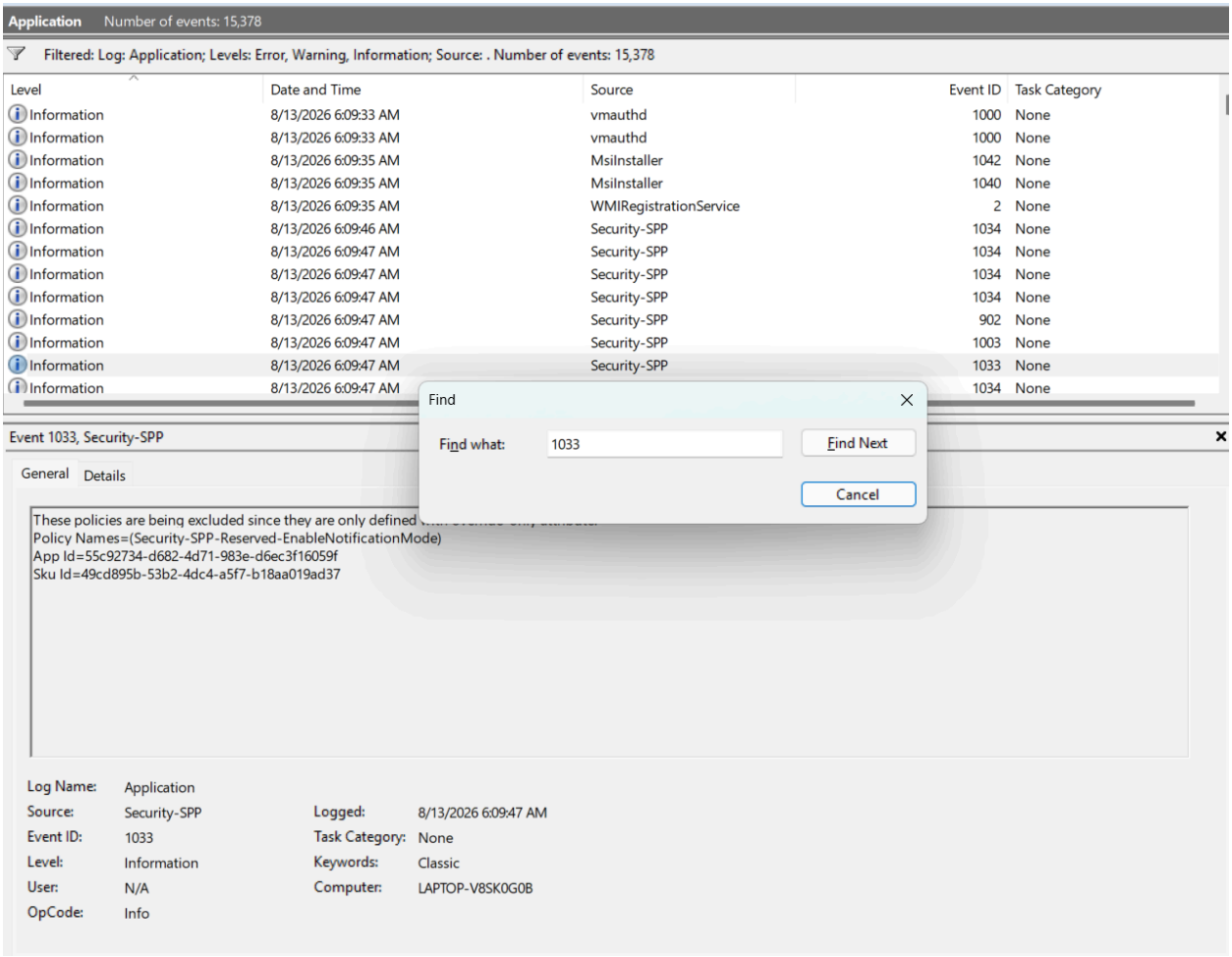
2. خطوات التحقيق الجنائي واستخراج الأدلة

الخطوة الأولى: تحليل تثبيت البرنامج (Event ID 1033)

- عند فحص سجلات التثبيت، تبين وجود تثبيت لبرنامج مشبوه تضمن في تفاصيله نصاً مشفراً بصيغة Base64:

```
==cGljb0NURntFdjNudF92aTN3djNyXw
```

- **فك التشفير (الجزء الأول):** `_picoCTF{Ev3nt_vi3wv3r`



الخطوة الثانية: كشف آلية الاستمرارية في الريجستري (Event ID 4657)

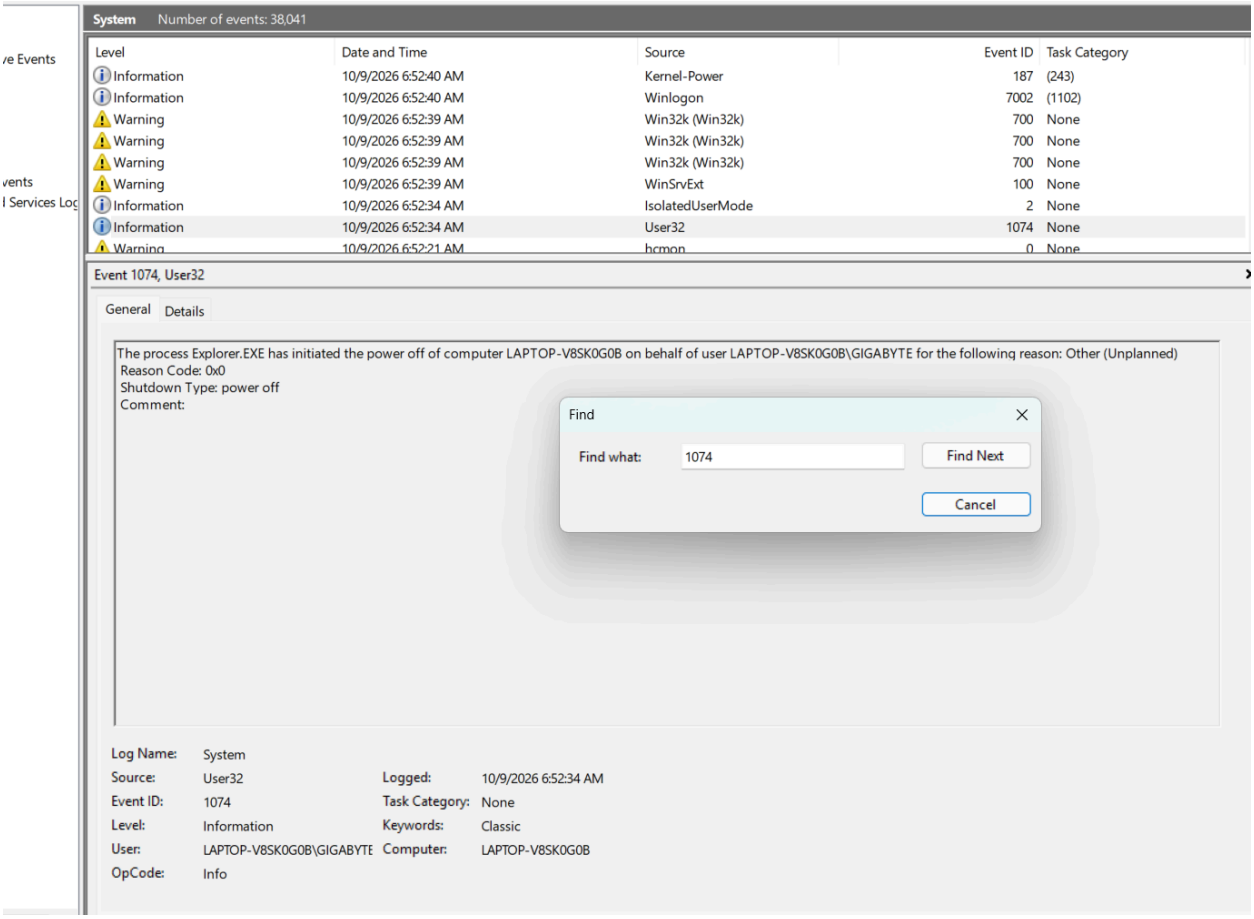
- بالفحص باستخدام **Event ID 4657**، تم رصد تعديل في مفتاح الاستمرارية للريجستري (`CurrentVersion\Run`) باسم `Immediate Shutdown` وقيمة مشفرة:

```
==MXNfYV9wcjN0dHlfdXMzZnVsXw
```

الخطوة الثالثة: تحليل حدث الإيقاف (Event ID 1074)

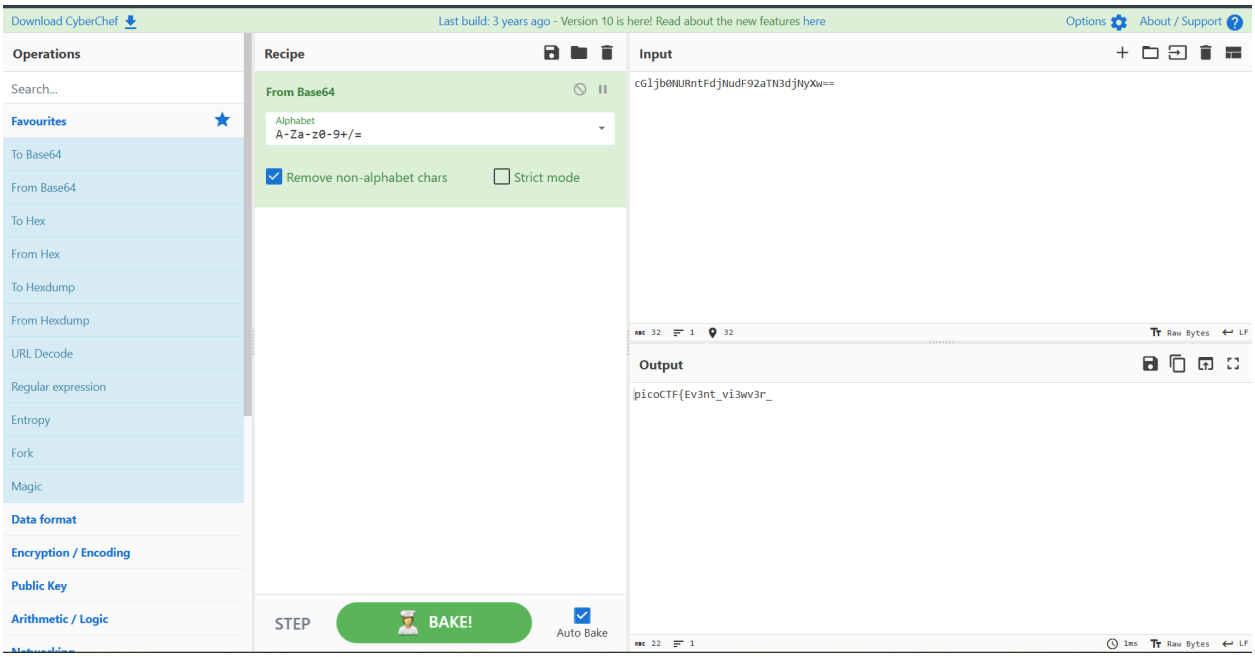
- أظهر الحدث **1074** تنفيذ ملف `custom_shutdown.exe` لأمر إيقاف التشغيل، مع وجود الجزء الثالث والأخير في خانة الملاحظات:

`=dDAwbF84MWJhM2ZlOX0`

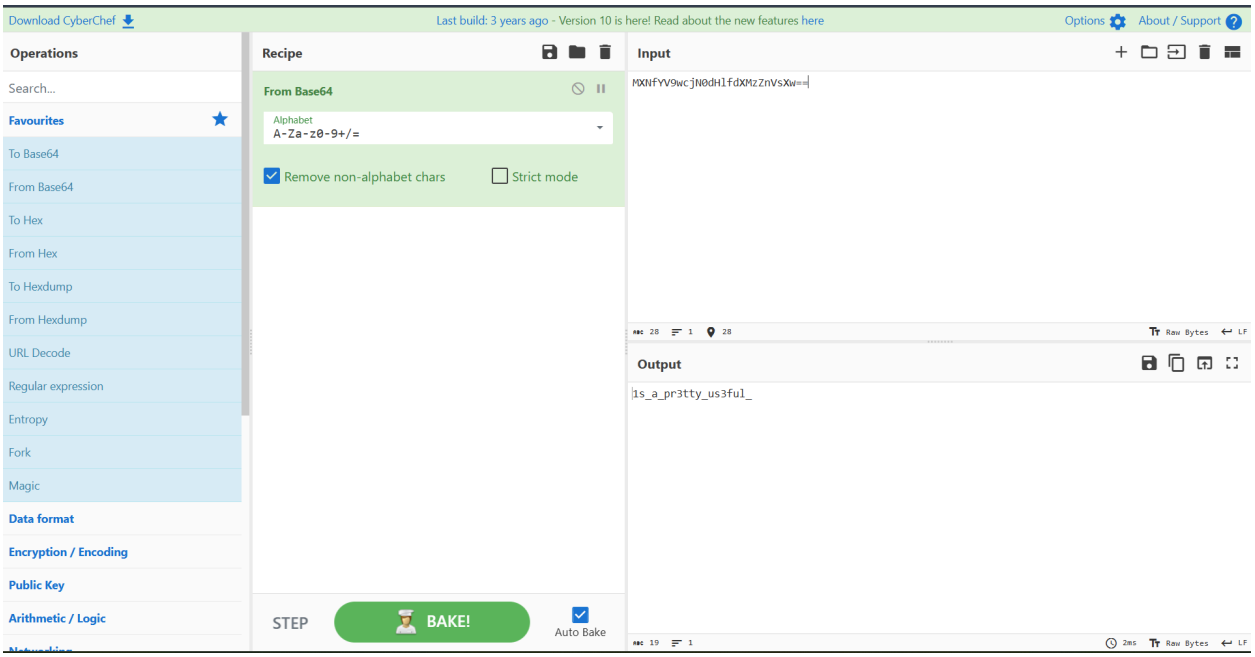


تم فك التشفير الثلاث الاحداث تبع الفلاج عن طريق اداه الcyber chif

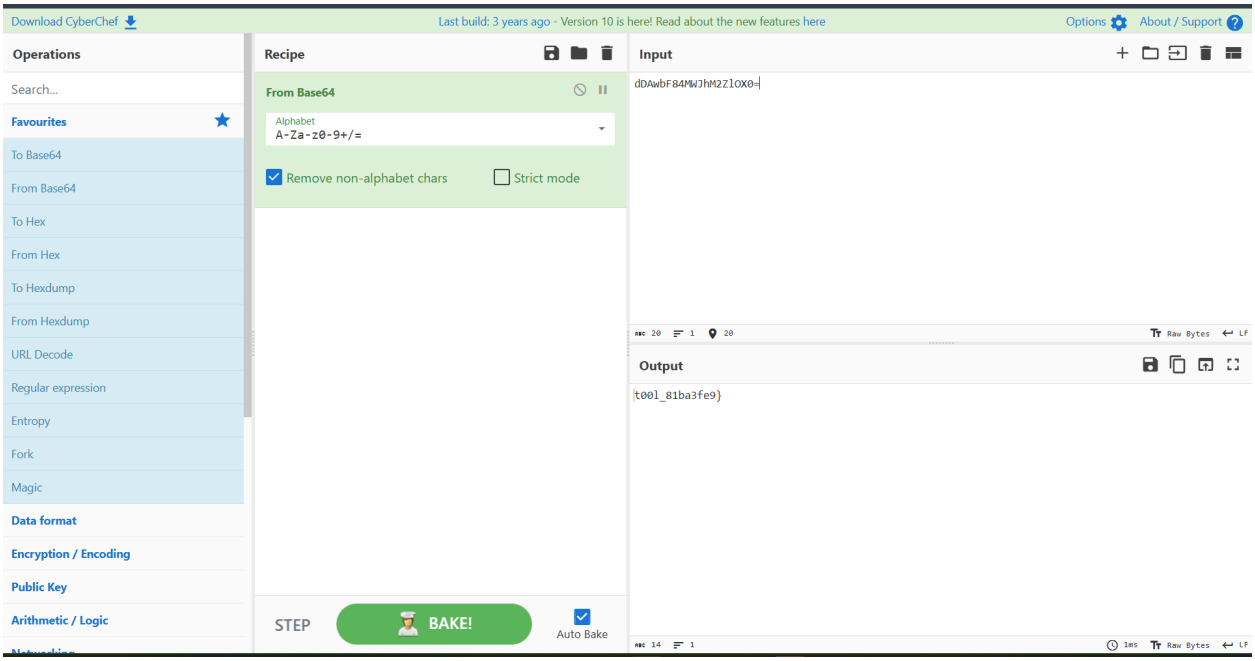
الاول



الثاني



الثالث



3. الفلاج النهائي (The Flag)

بعد تجميع الأجزاء الثلاثة المفكوكة من ترميز Base64، نحصل على الفلاج النهائي للتحدي:

`picoCTF{Ev3nt_vi3wv3r_1s_a_pr3tty_us3ful_t00l_81ba3fe9}`

4. التوصيات ومعالجة الحادثة

1. تشغيل الجهاز في **الوضع الآمن (Safe Mode)**.
2. حذف القيمة الخبيثة من مفتاح الريجستري في المسار:
   `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
3. إزالة مجلد التطبيق الضار نهائياً من مسار التثبيت.