﷽



**جامعة القدس المفتوحة**

**إجابة نشاط مقرر التحقيقات والأدلة الرقمية1462**

**إعـــــــــــــــــداد :هديل فؤاد فاروق حرب**

##### المشــــــــــــرف: أ.عيسى محمود عبد الله اسعد

**تحليل حادث اختراق باستخدام أدوات التحقيق الرقمي:**

##### 📝 تحليل أحداث الأمان باستخدام Event Viewer:

##### تم فتح أداة Event Viewer باستخدام البحث في Windows :

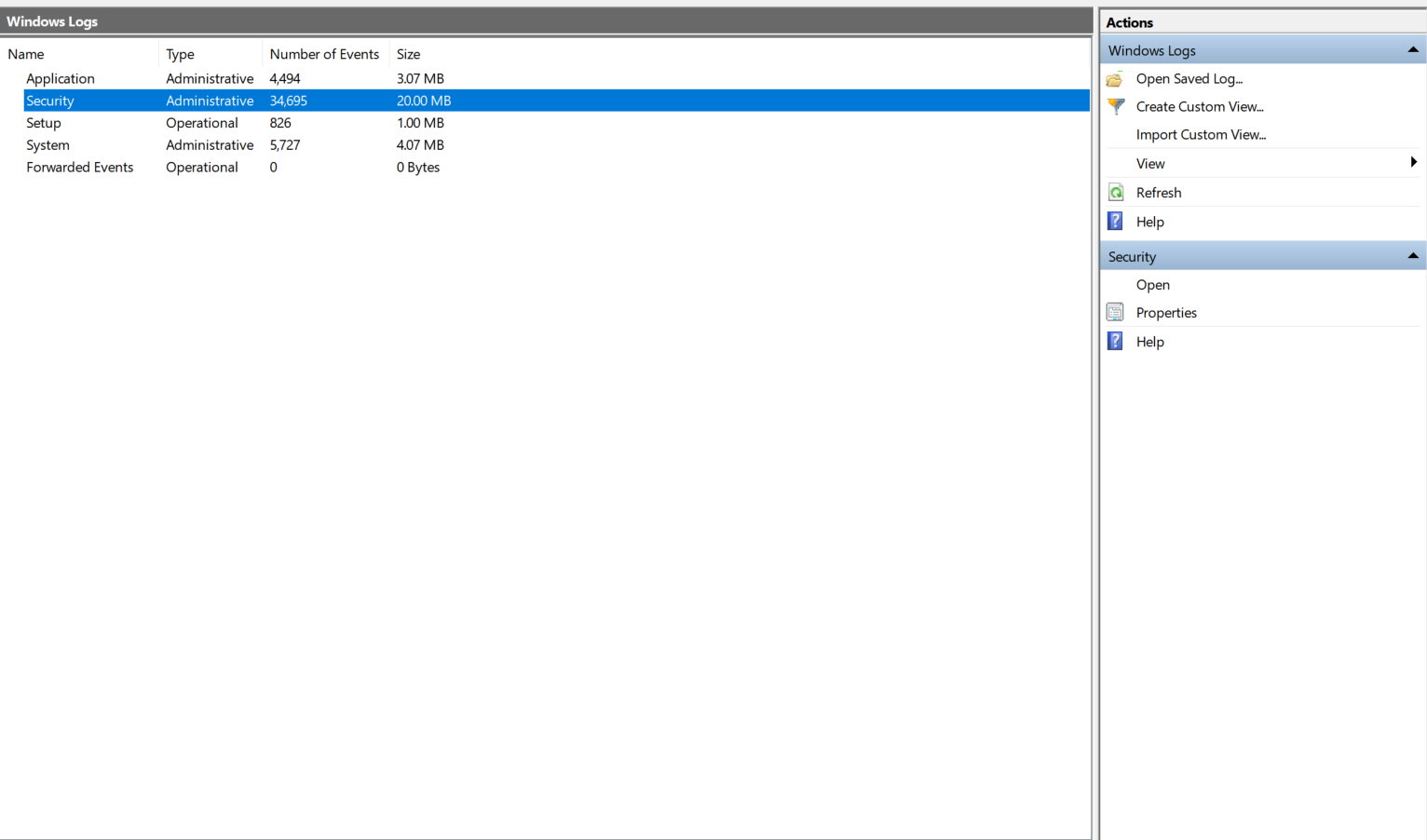
##### 

##### نافذة برنامج Event Viewer الرئيسية:

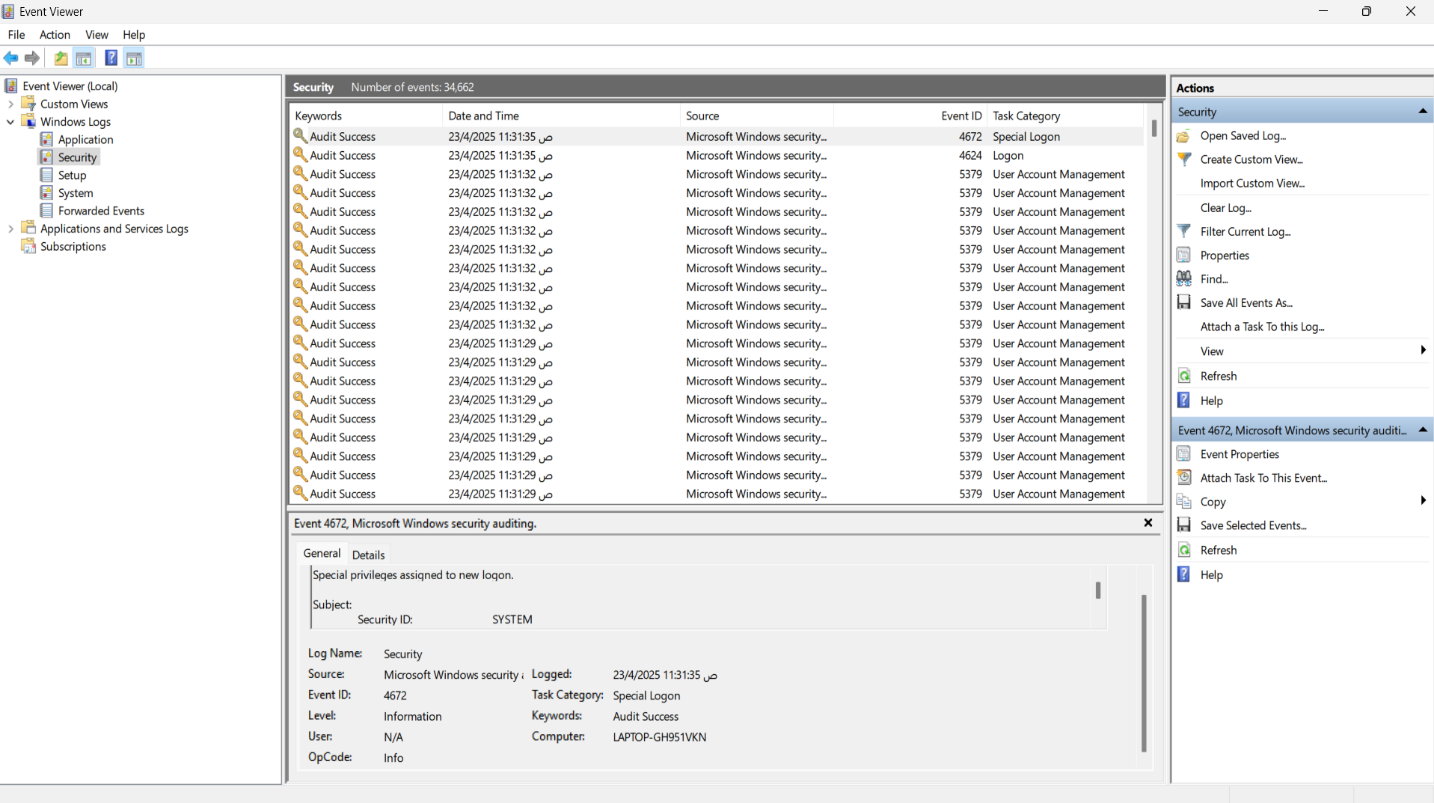
##### 

##### ثم الانتقال إلى: Windows Logs > Security

##### 



* أحداث سجل الأمان في **Event Viewer**:



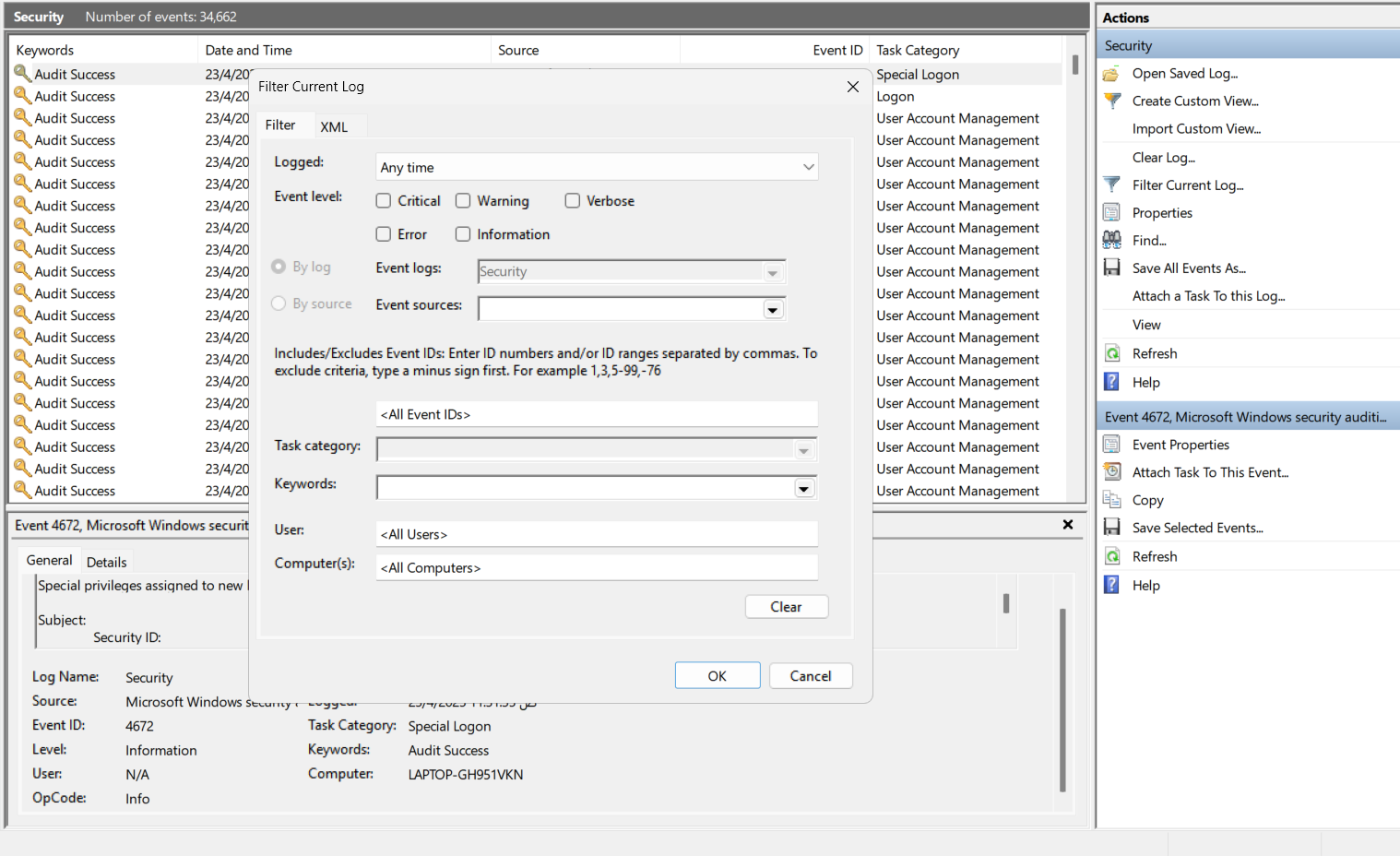
-حيث تم استعراض الأحداث الأمنية الخاصة بمحاولات الدخول واستخدام الصلاحيات.

**✅ تعبئة نموذج Filter Current Log:**

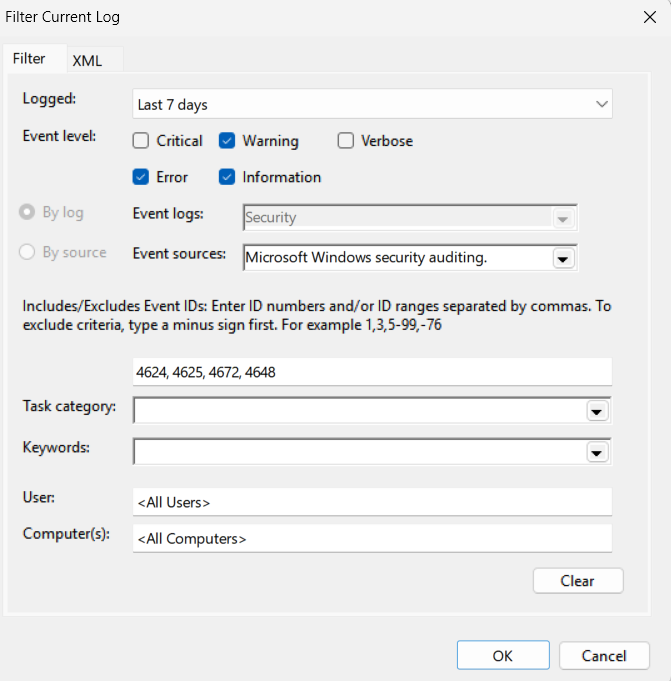
1. **Logged** :اختيار Last 7 days
2. **Event level**: تفعيل الخيارات التالية:
   * Information
   * Warning
   * Error
3. **Event sources**: اختيار Microsoft Windows security auditing
4. **Event Ids**: 4624, 4625, 4672, 4648
5. **Task Category**: تركها فارغة
6. **Keywords**: تركها فارغة
7. **User**: All Users
8. **Computer(s)**: All Computers

تم استخدام خيار  **( Filter Current Log**) لتصفية النتائج، وتم اختيار الأحداث ذات الأرقام:

* **4624** :تسجيل دخول ناجح
* **4625** : محاولة فاشلة لتسجيل الدخول
* **4672** :منح صلاحيات إدارية خاصة أو تعيين امتيازات خاصة لتسجيل دخول جديد
* **4648** : محاولة تسجيل دخول باستخدام بيانات اعتماد صريحة (غالبًا تظهر في هجمات)



تم تسجيل وتوثيق أهم الأحداث وتحليلها لتحديد مصدر الهجوم المحتمل.



##### 📄 توثيق الأحداث الأمنية المرتبطة بحادث الاختراق:

##### ✅ الحدث رقم 1:

##### 📅 التاريخ: 17/4/2025

##### 🕒 الوقت: 9:17:52 م

##### 🔢 رقم الحدث (Event ID): 4624

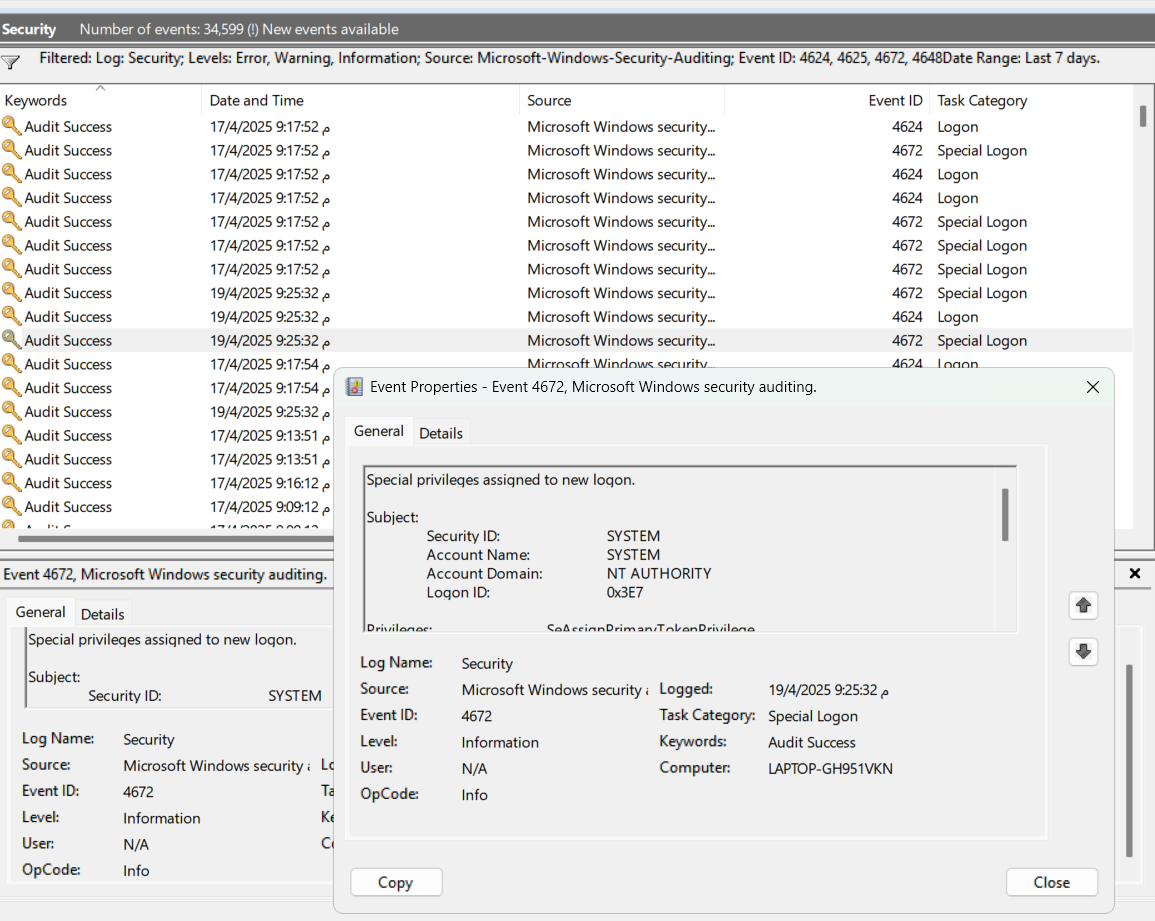
##### 📌 النوع: تسجيل دخول ناجح بعد عدة محاولات.

##### الوصف: تم تسجيل دخول ناجح للمستخدم بعد محاولات فاشلة. هذا السلوك قد يشير إلى أن المهاجم نجح في الوصول إلى كلمة المرور الصحيحة بعد عدة محاولات.

##### 

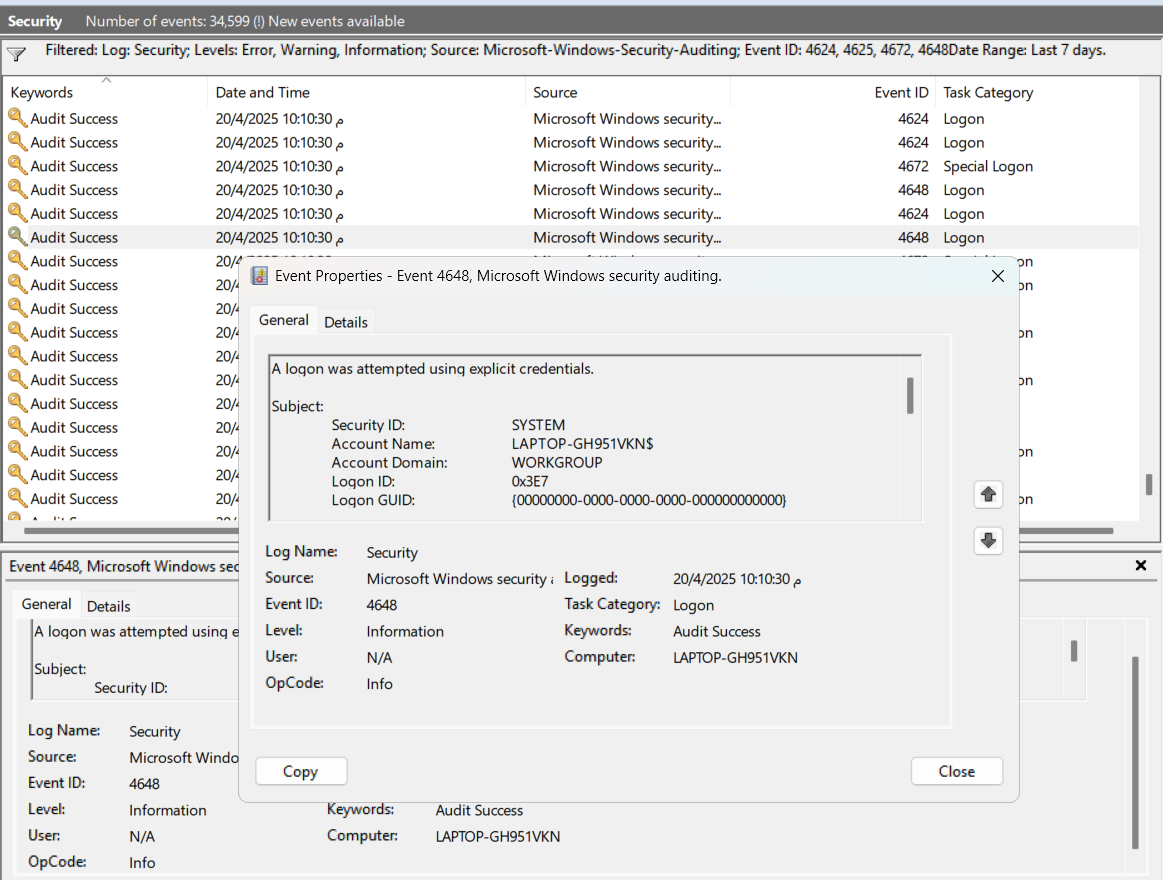
**✅ الحدث رقم 2**

* 📅ا**لتاريخ**: 19/4/2025
* 🕒**الوقت**: 9:25:32 م
* 🔢 **رقم الحدث** (**Event ID**): 4672
* 📌**النوع**: منح صلاحيات إدارية
* 📝**الوصف**: النظام منح صلاحيات خاصة للمستخدم مباشرة بعد تسجيل الدخول، قد يكون هذا مؤشراً على تصعيد صلاحيات المهاجم داخل النظام، مما يزيد من خطورة الوصول.



**✅ الحدث رقم 3**

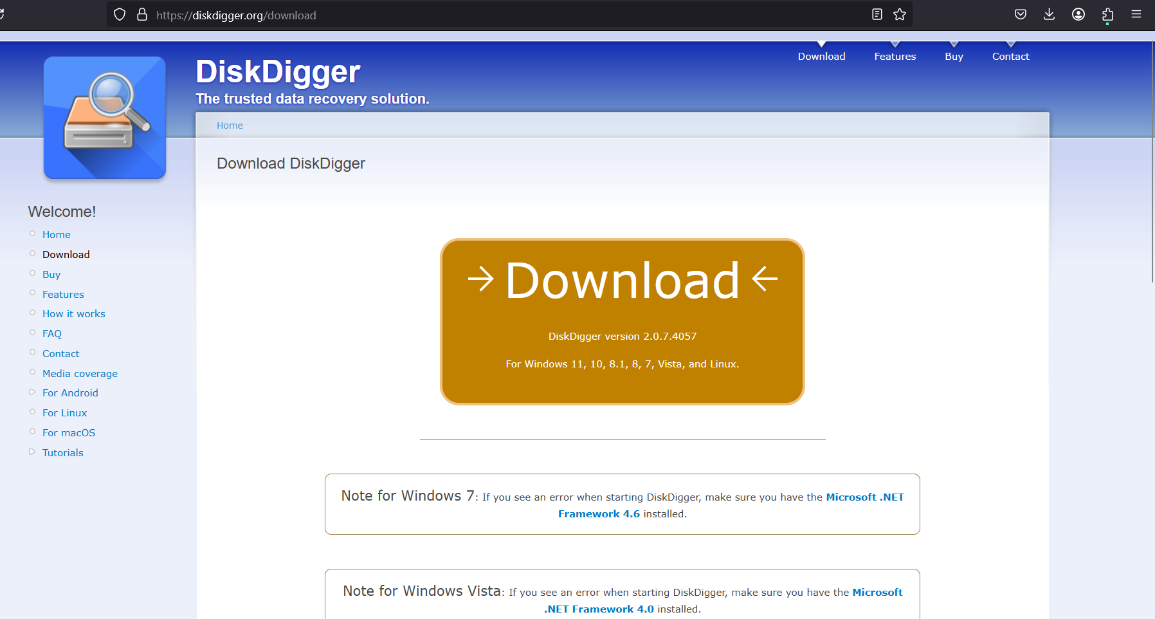
* 📅 **التاريخ**: 20/4/2025
* 🕒**الوقت** : 10:10:30 م
* 🔢**رقم الحدث** **(Event ID)** : 4648
* 📌ا**لنوع**: محاولة تسجيل دخول باستخدام بيانات اعتماد صريحة
* 📝 ا**لوصف**: تم تنفيذ طلب تسجيل دخول من خلال تقديم اسم المستخدم وكلمة المرور يدويًا. المستخدم حاول الوصول إلى العملية على الجهاز المحلي  
  هذا الحدث يشير إلى محاولة تسجيل دخول مباشرة، قد تكون من تطبيق خارجي أو سكربت يحاول استخدام بيانات دخول بشكل صريح.



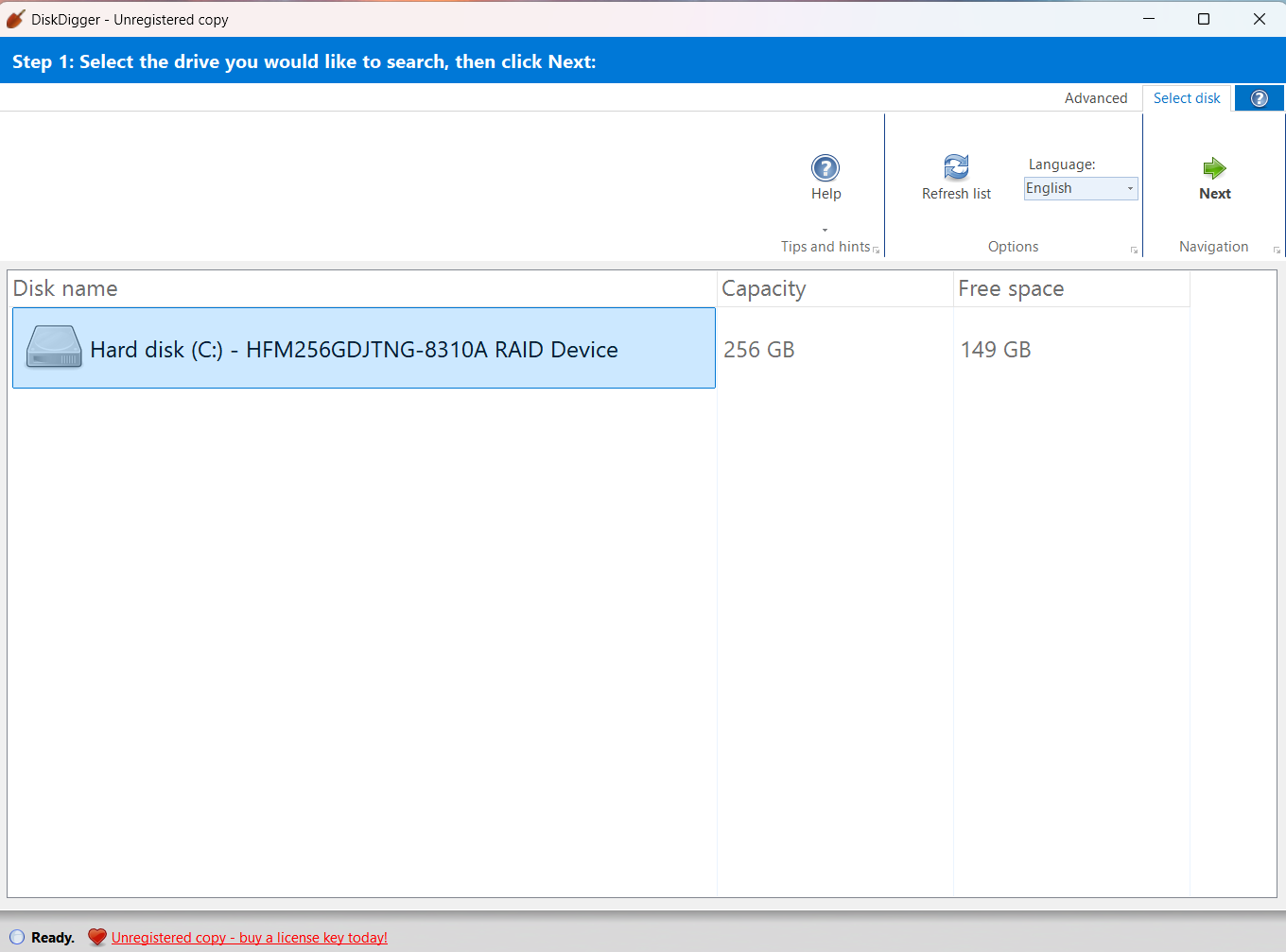
* **بعد استخدام الأدوات الرقمية وتحليل الأحداث على الجهاز LAPTOP-GH951VKN، تبين أن النشاطات التي تم رصدها ناتجة عن استخدام المستخدم الشرعي، ولا توجد مؤشرات قوية تدل على حدوث اختراق فعلي. ومع ذلك، فإن توثيق وتحليل هذه الأحداث يساهم في تعزيز الفهم العملي لأساليب التحقيق الرقمي ويُعتبر تدريباً واقعياً قيماً.**

**استرداد الملفات المحذوفة باستخدامDisk Digger:**

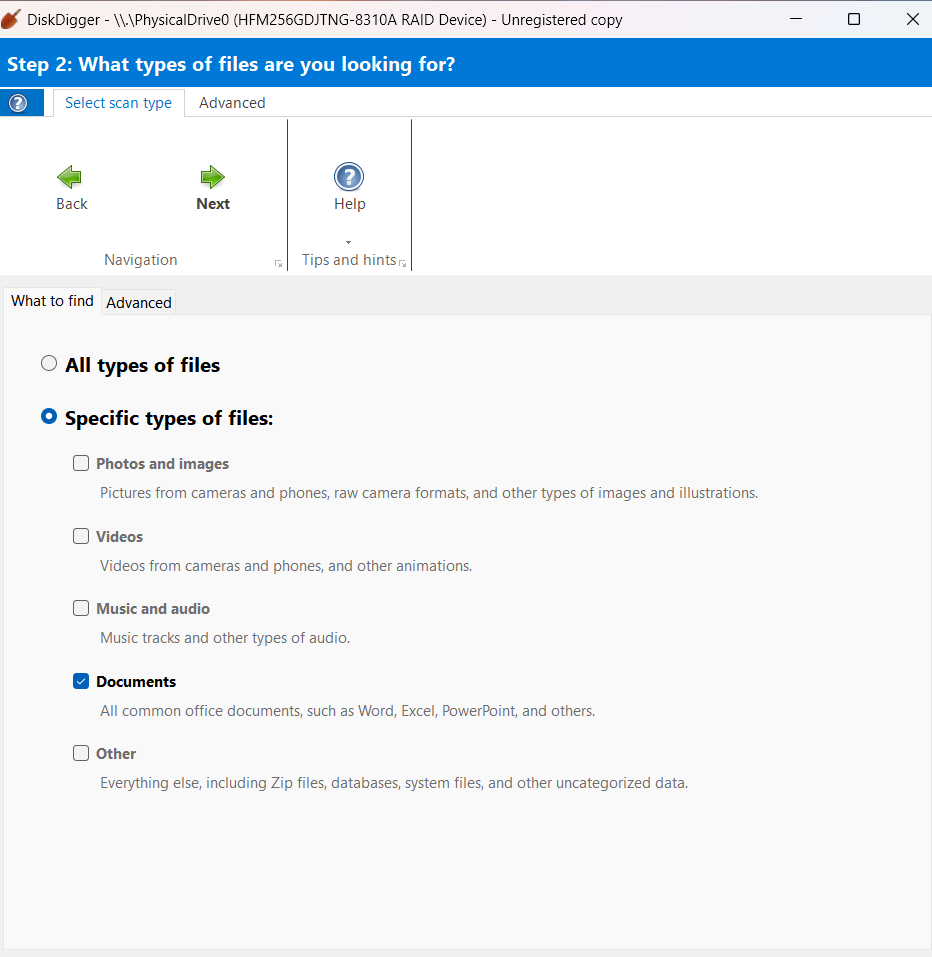
"-صفحة تنزيل برنامج استعادة الملفات من الموقع الرسمي Disk Digger" :



- واجهة برنامج **Disk Digger** و تحديد القرص المراد فحصه:

****

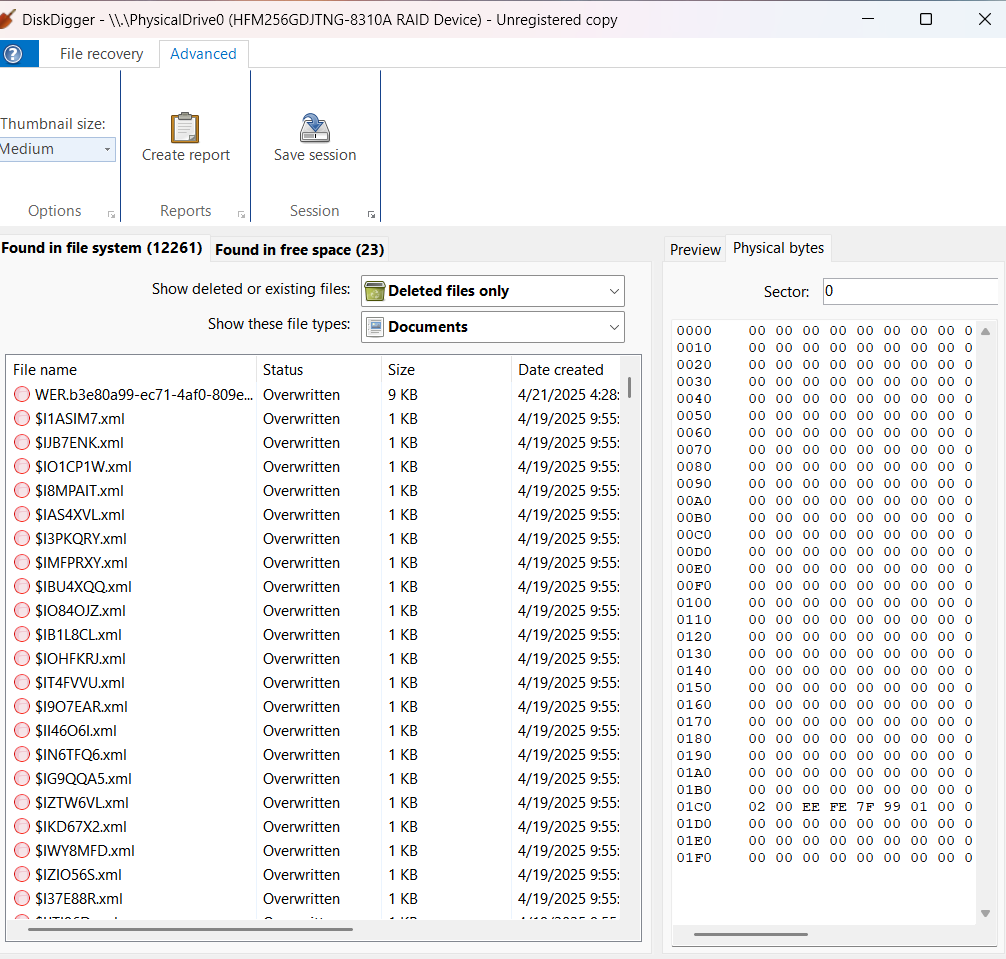
**-** اختيار أنواع الملفات المراد استرجاعها في برنامج **Disk Digger:**

****

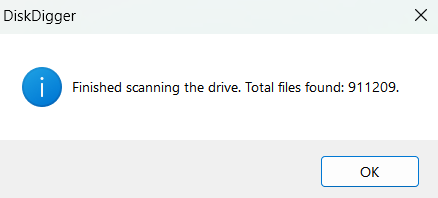
**-بعد تحديد محرك الأقراص C:\، تم اختيار البحث عن الملفات التالية:**

* مستندات (.docx, .txt, .pdf)

ثم تم بدء عملية الفحص من خلال النقر على "**Next**"  
الأداة بدأت في مسح القرص وتحليل الملفات المحذوفة التي ما زال بالإمكان استعادتها.



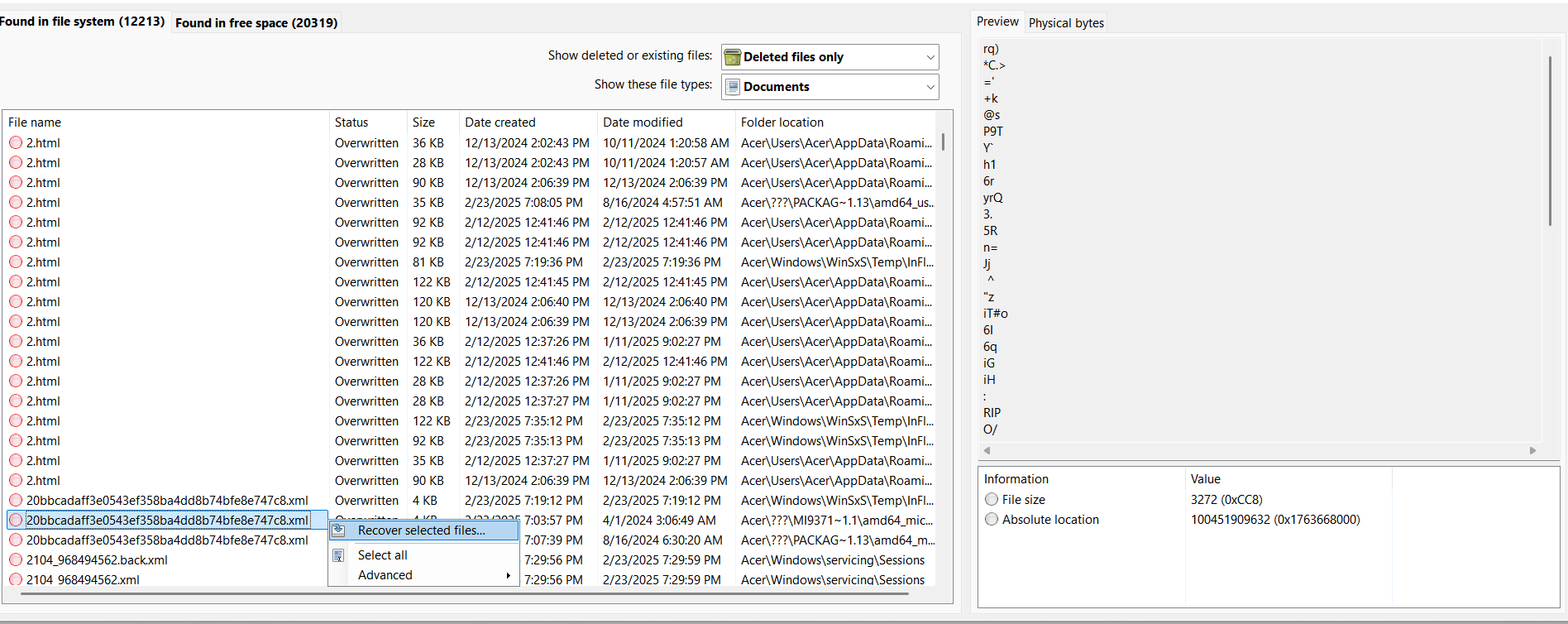
- اكتمال فحص القرص بواسطة **Disk Digger**



📝 توثيق ملفات مرتبطة بحادث اختراق:

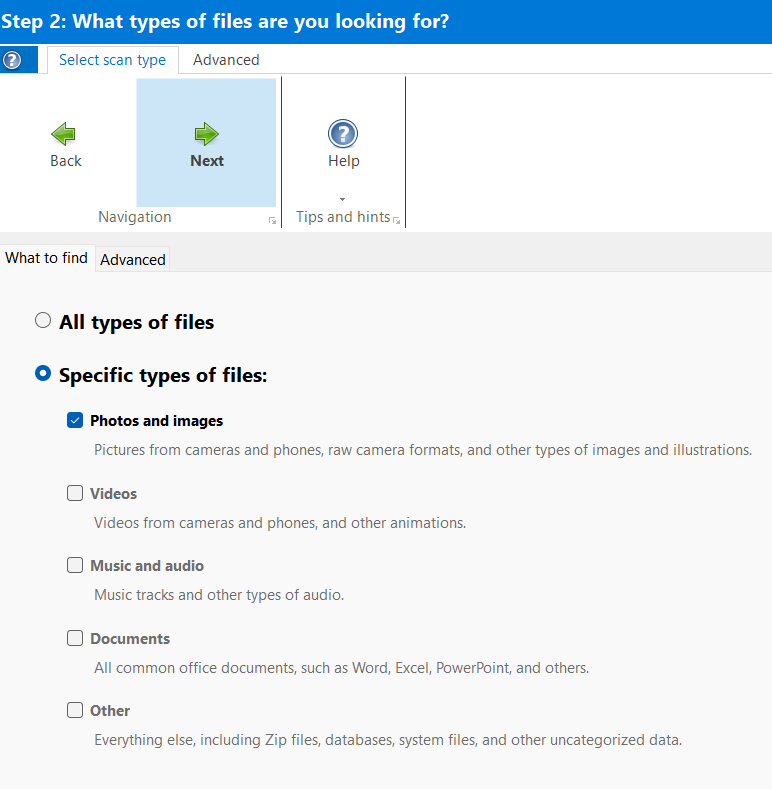
**📌 الملف الأول:**

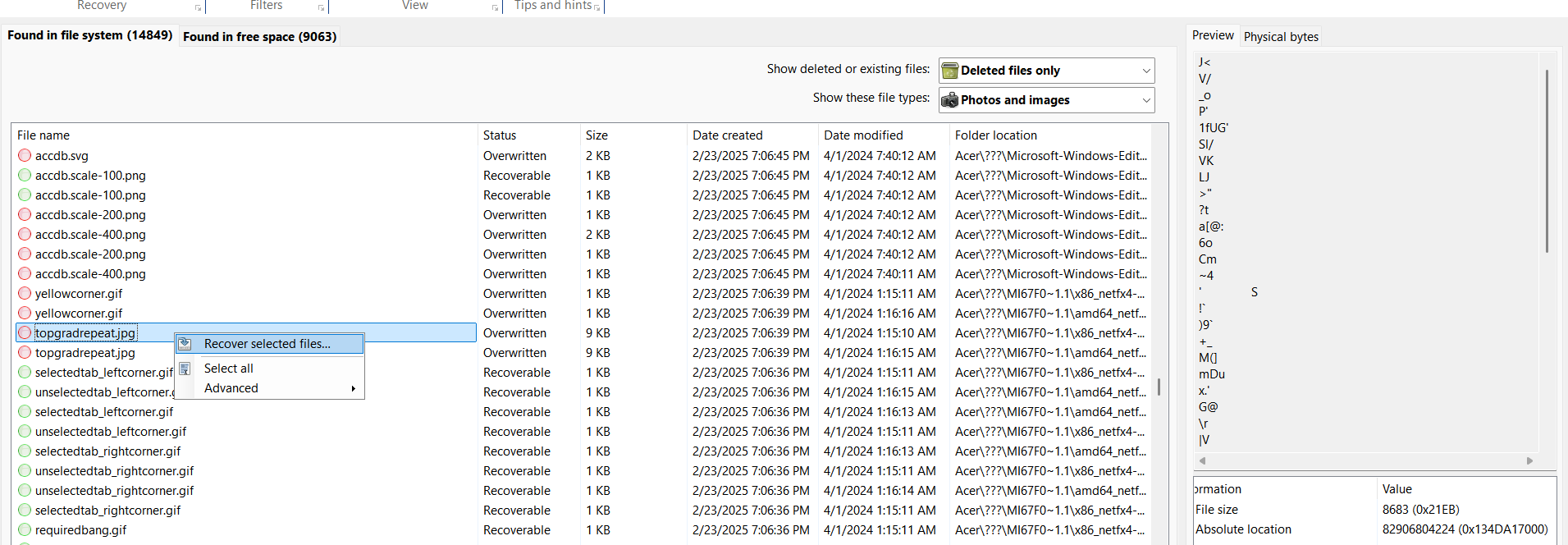
* 📄 **الاسم** : 20bbcadaff3e0543ef358ba4dd8b74bfe8e747c8.xml
* 📁 **الموقع**: Acer\{???}\MI9371~1.1\amdf64\_mic...
* 📅 **تاريخ الإنشاء** 23-02-2025: الساعة 7:00 م
* 📅 **تاريخ التعديل** 01-04-2025: الساعة 3:00 ص
* 📏 **الحجم**4 KB:
* 📌 الوصف: ملف بصيغة XML يحتوي على محتوى غير مفهوم يتضمن رموزاً وحروفاً عشوائية لا تتطابق مع بنية ملفات XML العادية. توقيت التعديل تم خلال فترة غير اعتيادية، ويُشتبه في أن الملف ناتج عن أداة خارجية أو يحتوي على بيانات مشفرة.
* التحليل: بناءً على توقيت الإنشاء والتعديل والمحتوى الغريب، يُرجّح أن هذا الملف قد يكون جزءاً من محاولة اختراق أو نشاط غير مصرح به.



**📌 الملف الثاني :**

* 📄**الإسم** topgradrepeat.jpg:
* 📁**الموقع** Acer\MI67F0~1.1\x86\_netfx4-..:
* 📅 **تاريخ الإنشاء** : 23-02-2025 الساعة 7:06 م
* 📅**تاريخ التعديل** : 01-04-2024 الساعة 1:15 ص
* 📏**الحجم**:9 KB
* 📌**الوصف** : صورة بصيغة JPG محفوظة في مسار برمجي غير معتاد مرتبط بمكتبات النظام وتاريخ التعديل أقدم من تاريخ الإنشاء، مما يشير إلى أنه تم نسخه من مصدر خارجي ،لا يوجد ما يدل على أنه ملف خبيث، لكن توقيته وموقعه يجعلان منه ملفًا يحتمل الشك.





**تحليل الأدلة وتحديد مصدر الهجوم**:

**🔎 أولًا: تحليل السجلات من Event Viewer**

أظهرت أداة **Event Viewer** عدة أحداث أمنية متكررة، من أبرزها:

* **4625 :محاولات فاشلة لتسجيل الدخول** باستخدام أسماء مستخدمين عامة ، في أوقات مختلفة.
* **:4624تسجيل دخول ناجح** لاحقًا لحساب مما قد يدل على نجاح أحد الأطراف في الوصول إلى الحساب بعد عدة محاولات.
* **:4672منح صلاحيات خاصة** بعد تسجيل الدخول مباشرة، مما يُرجّح أنه قد حدث تصعيد للصلاحيات.
* **:4648 محاولة تسجيل دخول باستخدام بيانات اعتماد صريحة**، وهو نمط يُستخدم غالبًا في هجمات أو سكربتات خارجية.

هذه الأحداث مجتمعة تُشير إلى سلسلة نشاطات قد تدل على **محاولة اختراق حساب إداري داخل النظام**.

**💾 ثانيًا: تحليل الملفات المستردة من Disk Digger**

تم استرجاع عدد من الملفات المشبوهة أو محل الشك، من بينها:

**20bbcadaff3e0543ef358ba4dd8b74bfe8e747c8.xml-:**

* ملف **XML** يحتوي على رموز مشفّرة وغير مفهومة، تم تعديله في وقت متأخر من الليل، ما يزيد من احتمالية كونه ناتج عن أداة مشبوهة.

: **topgradrepeat.jpg-**

* ملف صورة محفوظ في مجلد غير معتاد يخص مكتبات النظام. لا يحتوي على شفرة ظاهرة، لكن توقيت التعديل والموقع يجعله ملفًا يستحق التدقيق.

**🔗 ثالثًا: الأنماط والارتباطات بين الأحداث الأمنية والملفات**

1. بدأت السجلات الأمنية بتسجيل **محاولات فاشلة لتسجيل الدخول(4625(**، ما يدل على محاولة تخمين كلمة مرور أو اختبار صلاحيات مستخدم.
2. مباشرة بعد ذلك، تم **تسجيل دخول ناجح(4624(** بنفس الحساب، مما يُشير إلى نجاح المحتال في الوصول للنظام بعد تكرار المحاولات.
3. بعد تسجيل الدخول، ظهر **حدث تصعيد صلاحيات (4672(**، وهو مؤشر على أن المستخدم حصل على صلاحيات إدارية موسعة، مما يُعتبر خطوة كلاسيكية في الهجمات لإكتساب سيطرة أكبر على الجهاز.
4. بالتزامن مع هذه الأحداث، تم رصد **ملف XML بإسم مشفّر (20bbcadaff3e...)** في مجلد غير واضح، ويحتوي على محتوى غير مقروء، ما يدل على احتمال استخدامه لتخزين أو تنفيذ أوامر بطريقة غير مباشرة.
5. كما تم استرجاع ملف صورة باسم **topgradrepeat.jpg** محفوظ داخل مجلد يخص مكتبات النظام (netfx4) وهو مكان غير منطقي لوجود ملف صورة، مما يُرجح أنه إما تم إخفاؤه هناك أو تم نقله بواسطة أداة خارجية.
6. أيضًا سُجّلت **محاولة استخدام بيانات اعتماد صريحة(4648(**، وهي طريقة تُستخدم عادة من قبل أدوات خارجية أو سكربتات للوصول للنظام دون المرور بالطريقة التقليدية.

**رابعاً: تحديد المصدر المحتمل للهجوم**

من خلال الربط بين توقيت الأحداث والملفات المستردة، يُرجّح أن **المصدر الرئيسي للهجوم هو حساب مستخدم إداري** الذي تم تسجيل الدخول به بعد عدة محاولات فاشلة، ثم تم منحه صلاحيات موسعة.

-وقد يكون الاختراق ناتجًا عن:

* **تسريب بيانات الدخول الخاصة بالمستخدم الإداري**أو**دخول من طرف داخلي لديه معرفة سابقة بالحساب**، لا تظهر أدلة على وجود برنامج خبيث فعّال، لكن تسلسل الأحداث يُشير إلى **هجوم داخلي مخطط أو استخدام غير مشروع لحساب** أو على الأقل استخدام خاطئ لحساب بصلاحيات عالية