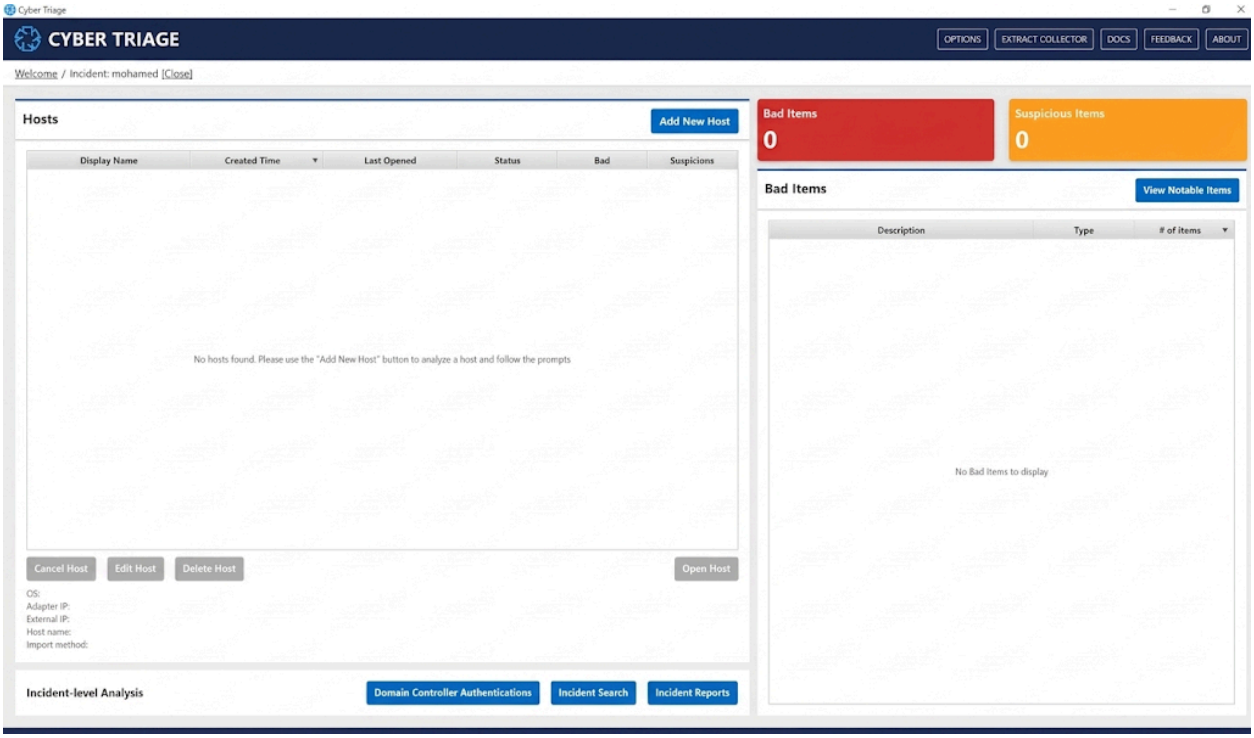
تقرير تحليل Cyber Triage

اسم الطالب: محمد حيدر مرشد ناصر المعمري

الصورة الأولى — الشاشة الرئيسية (لوحة Hosts)

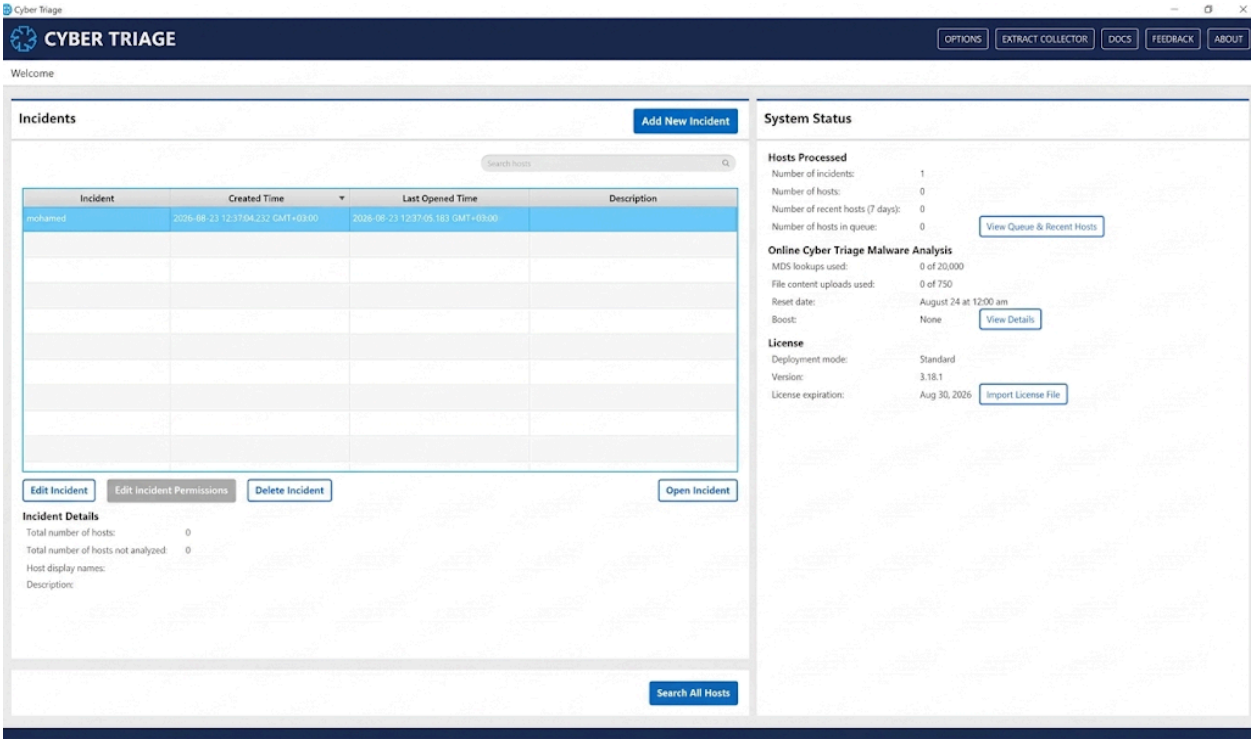


الشاشة الرئيسية — لوحة Hosts

> **الوصف:** تُظهر هذه الشاشة الواجهة الرئيسية لأداة Cyber Triage بعد فتح الحادثة المسماة **mohamed**. تحتوي اللوحة اليسرى على قائمة **Hosts** وهي فارغة في هذه المرحلة، مما يعني أنه لم يُضَف أي مضيف بعد للتحليل.
>
> **النقاط الرئيسية:**
>
> - عداد **Bad Items = 0** (باللون الأحمر) و**Suspicious Items = 0** (باللون البرتقالي) — الحادثة في بدايتها.
> - رسالة توجيهية تطلب من المحقق الضغط على زر **Add New Host** لبدء الإضافة.

- في أسفل الشاشة توجد أزرار تحليل على مستوى الحادثة: Domain Controller Authentications / Incident Search / Incident Reports.

الصورة الثانية — شاشة الحوادث (Incidents) وحالة النظام



شاشة Incidents وSystem Status

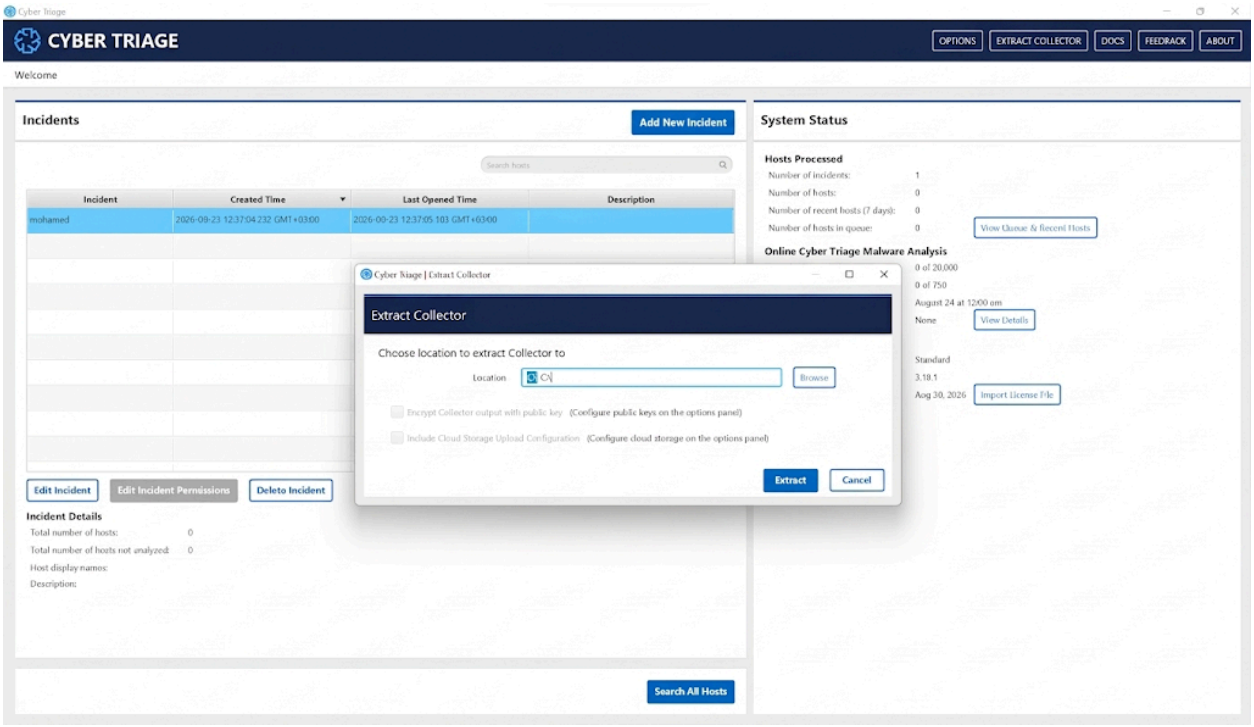
الوصف: تعرض هذه الشاشة قائمة الحوادث (Welcome Screen) في Cyber Triage، إلى جانب **System Status** على اليمين.

النقاط الرئيسية:

- الحادثة **mohamed** مُسجَّلة بتاريخ إنشاء `GMT+03:00 12:37:04 23-08-2026` وآخر فتح `-2026 GMT+03:00 12:37:05 23-08`.
- حالة النظام (System Status) توضح:
  - عدد الحوادث: **1**
  - عدد المضيفين: **0** (لم يُحلَّل بعد)
  - المُستخدَمة: MDS Lookups **0 من 20,000**

- File Content Uploads: **0 من 750**
  - وضع النشر: **Standard** | الإصدار: **3.18.1**
  - انتهاء الرخصة: **Aug 30, 2026**

الصورة الثالثة — استخراج Collector (Extract Collector)



نافذة Extract Collector

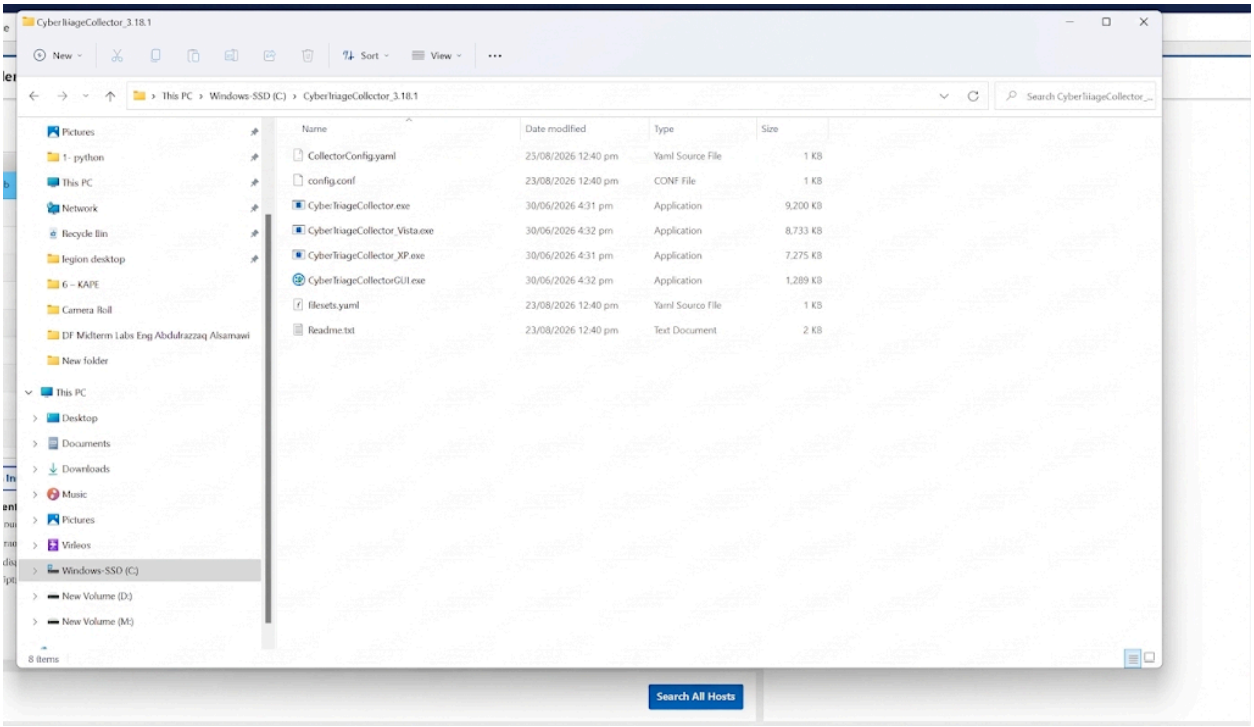
الوصف: تُظهر هذه الصورة نافذة **Extract Collector** التي تظهر عند الضغط على زر "Extract Collector" في شريط الأدوات العلوي. تُستخدم هذه الخطوة لاستخراج أداة الجمع (Collector) ووضعها في موقع محدد على القرص.

النقاط الرئيسية:

- حقل **Location** يحتوي على المسار `C:\` وهو القرص الجذر.
- خياران إضافيان (معطّلان في هذه الحالة):
  - **Encrypt Collector output with public key** — لحماية البيانات المجمَّعة.
  - **Include Cloud Storage Upload Configuration** — لرفع البيانات تلقائيًا إلى السحابة.

- زران للتنفيذ: **Extract** و **Cancel**.

الصورة الرابعة — ملفات CyberTriageCollector على القرص



محتويات مجلد CyberTriageCollector_3.18.1

الوصف: يعرض Windows File Explorer محتويات المجلد **CyberTriageCollector_3.18.1** الذي تم استخراجه في القرص `C:\`.

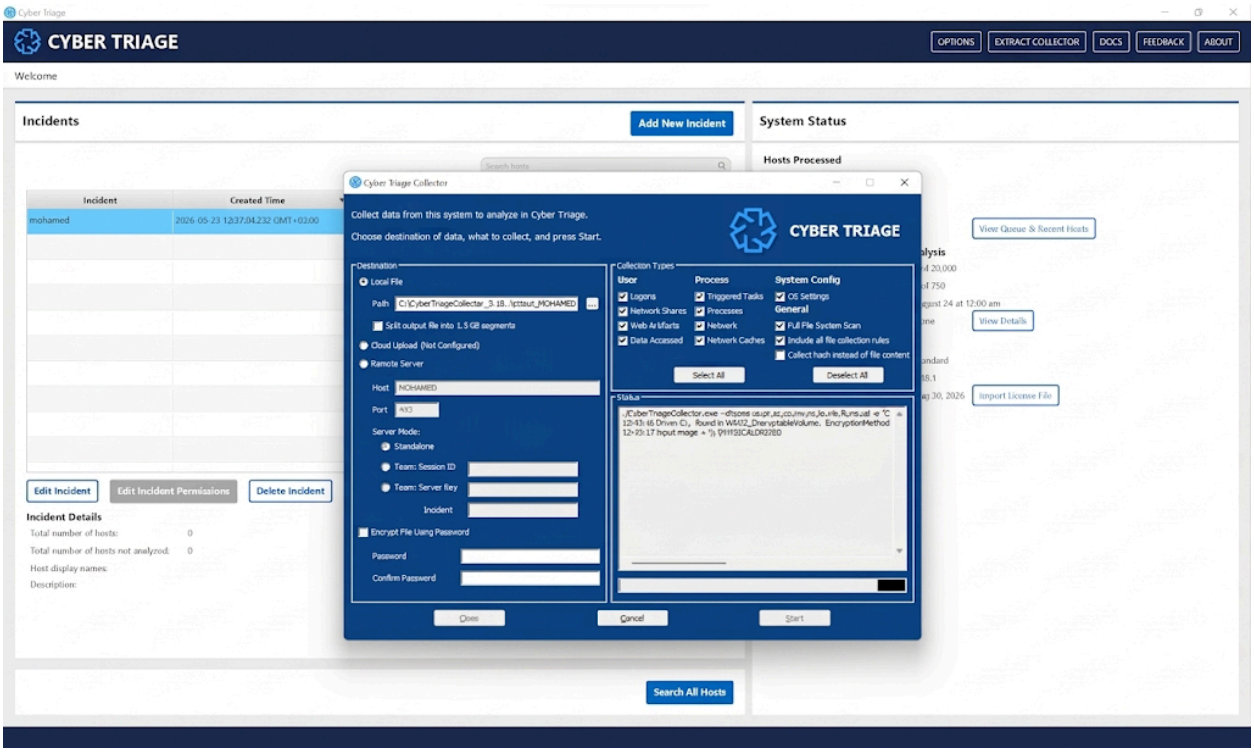
الملفات الموجودة:

اسم الملف	النوع	الحجم
CollectorConfig.yaml	Yaml Source File	1 KB
config.conf	CONF File	1 KB
CyberTriageCollector.exe	Application	9,200 KB
CyberTriageCollector_Vista.exe	Application	8,733 KB
CyberTriageCollector_XP.exe	Application	7,275 KB
CyberTriageCollectorGUI.exe	Application	1,289 KB
filesets.yaml	Yaml Source File	1 KB

الحجم	النوع	اسم الملف
2 KB	Text Document	Readme.txt

ملاحظة: توجد نسخ متعددة من الـ Collector لدعم أنظمة تشغيل مختلفة (XP، Vista، الإصدارات الحديثة).

الصورة الخامسة — إعداد وتشغيل عملية الجمع (Collection)



إعداد الجمع — نافذة Cyber Triage Collector

الوصف: تُظهر هذه الشاشة نافذة **Cyber Triage Collector** الرئيسية المُشغَّلة على الجهاز المستهدف، مع إعدادات الجمع الكاملة.

إعدادات الوجهة (Destination):

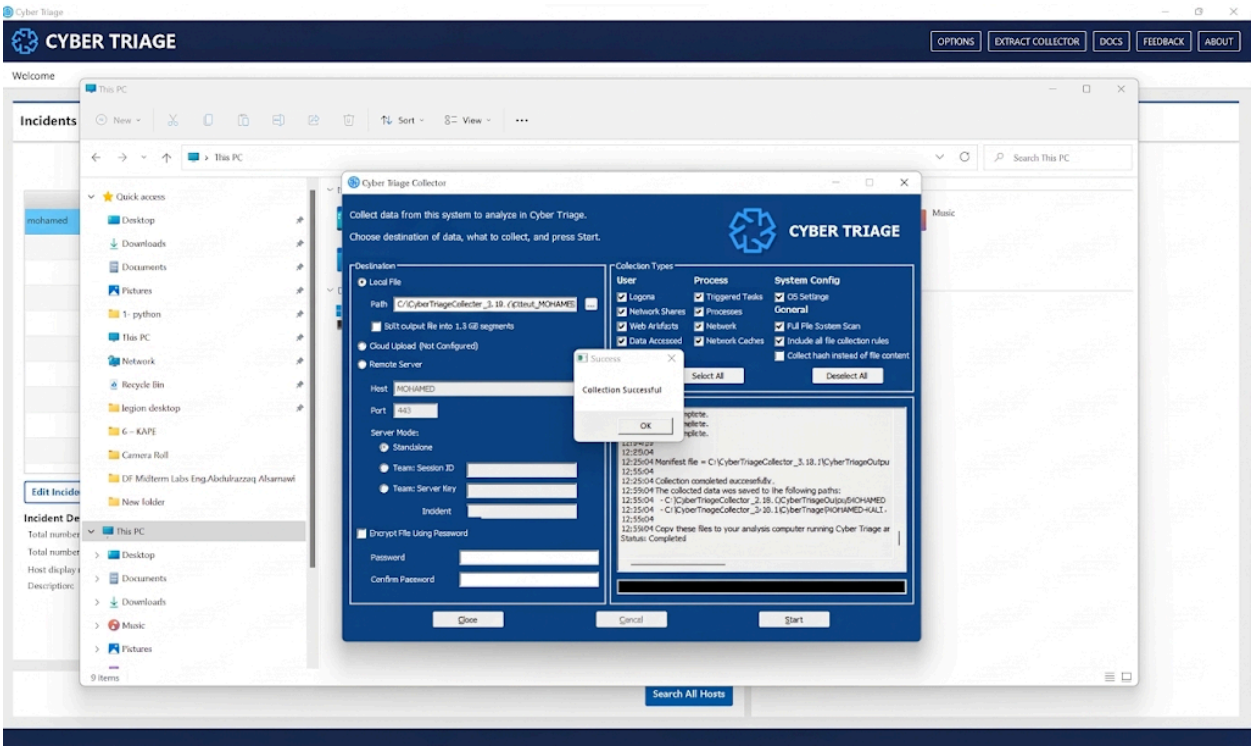
- ✅ **Local File** — مسار الحفظ محدد: `C:\CyberTriageCollector_3.18...\ctriout_MOHAMED`
- خيار تقسيم الملف إلى أجزاء 1.5 GB
- خيار Cloud Upload (غير مفعّل)
- خيار Remote Server مع الإعدادات: Host = MOHAMED، Port = 443

أنواع البيانات المجمَّعة (Collection Types):

- **User:** Logons ✅ | Network Shares ✅ | Web Artifacts ✅ | Data Accessed ✅
- **Process:** Triggered Tasks ✅ | Processes ✅ | Network ✅ | Network Caches ✅
- **System Config:** OS Settings ✅ | Full File System Scan ✅ | Include all file collection rules ✅ | Collect hash instead of file content ✅

سجل الحالة: يظهر في الجزء السفلي نشاط تنفيذ الأداة وتفاصيل طريقة التشفير المُكتشَفة.

الصورة السادسة — اكتمال عملية الجمع بنجاح



رسالة Collection Successful

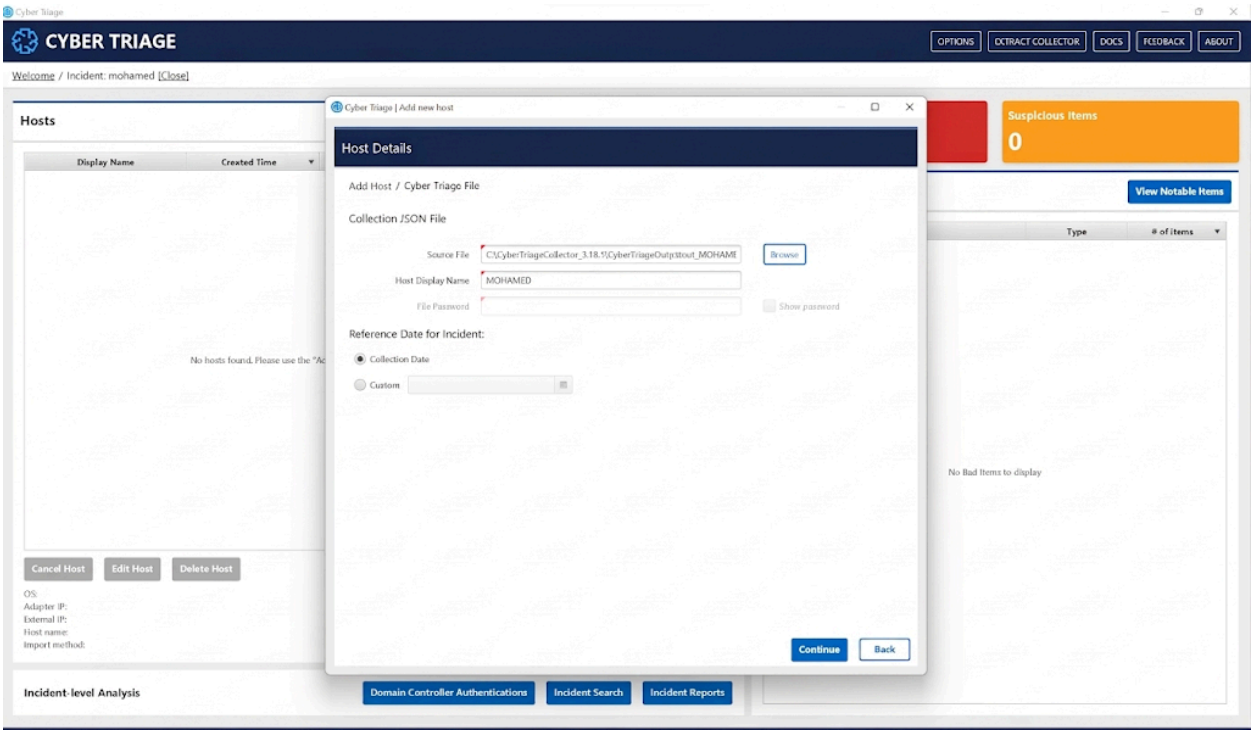
الوصف: تؤكد هذه الشاشة اكتمال عملية جمع البيانات من الجهاز المستهدف بنجاح، إذ تظهر نافذة منبثقة تقول **"Collection Successful"**.

ما يكشفه سجل الحالة:

- تم إنشاء ملف Manifest في: `C:\CyberTriageCollector_3.18.1\CyberTriageOutput`

- **تم اكتمال الجمع بنجاح (Collection completed successfully)**
- تم حفظ البيانات في مسارَين:
  - `C:\CyberTriageCollector_3.18.1\CyberTriageOutput\MOHAMED`
  - `C:\CyberTriageCollector_3.18.1\CyberTriageOutput\MOHAMED-KALI-`
- التعليمات: انسخ هذه الملفات إلى جهاز التحليل الذي يعمل عليه Cyber Triage.
- الحالة النهائية: **Completed**

الصورة السابعة — إضافة مضيف جديد (Add New Host)



Cyber Triage إضافة ملف — نافذة Host Details

الوصف: تُظهر هذه الشاشة نافذة **Host Details** ضمن خاصية "Add Host / Cyber Triage File"، حيث يقوم المحقق باستيراد ملف البيانات المجمَّعة من الجهاز المستهدف إلى بيئة التحليل.

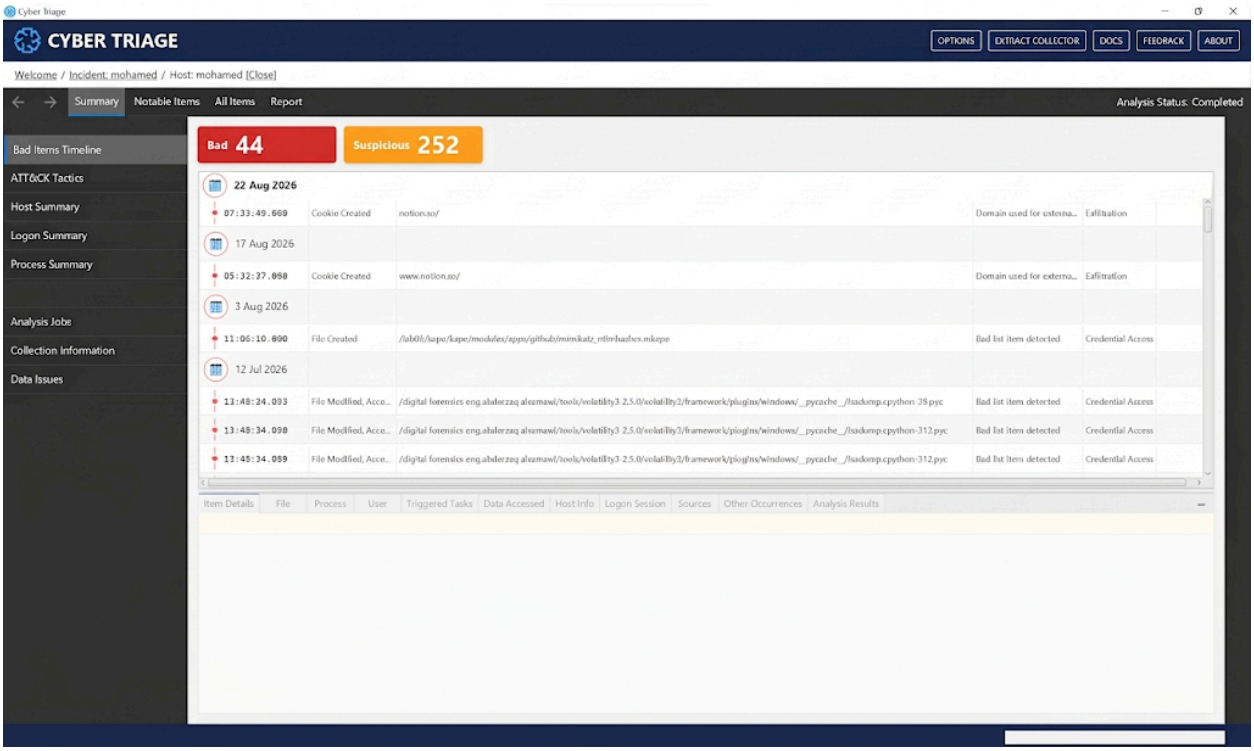
التفاصيل:

- **Source File:** `C:\CyberTriageCollector_3.18.1\CyberTriageOutput\ctriout_MOHAMED` (ملف JSON المُصدَّر)

- **Host Display Name:** MOHAMED
- **Reference Date for Incident:** ✅ Collection Date (تاريخ جمع البيانات)
- زر **Continue** للمتابعة إلى مرحلة التحليل.

الأهمية: هذه الخطوة تستورد البيانات المجمَّعة من الجهاز المشبوه إلى Cyber Triage لبدء التحليل الآلي.

الصورة الثامنة — ملخص نتائج التحليل (Summary)



لوحة Summary — Bad 44 | Suspicious 252

الوصف: تُعدّ هذه الشاشة من أهم الشاشات في التقرير، إذ تعرض **الجدول الزمني للعناصر الخطيرة (Bad Items Timeline)** بعد اكتمال التحليل.

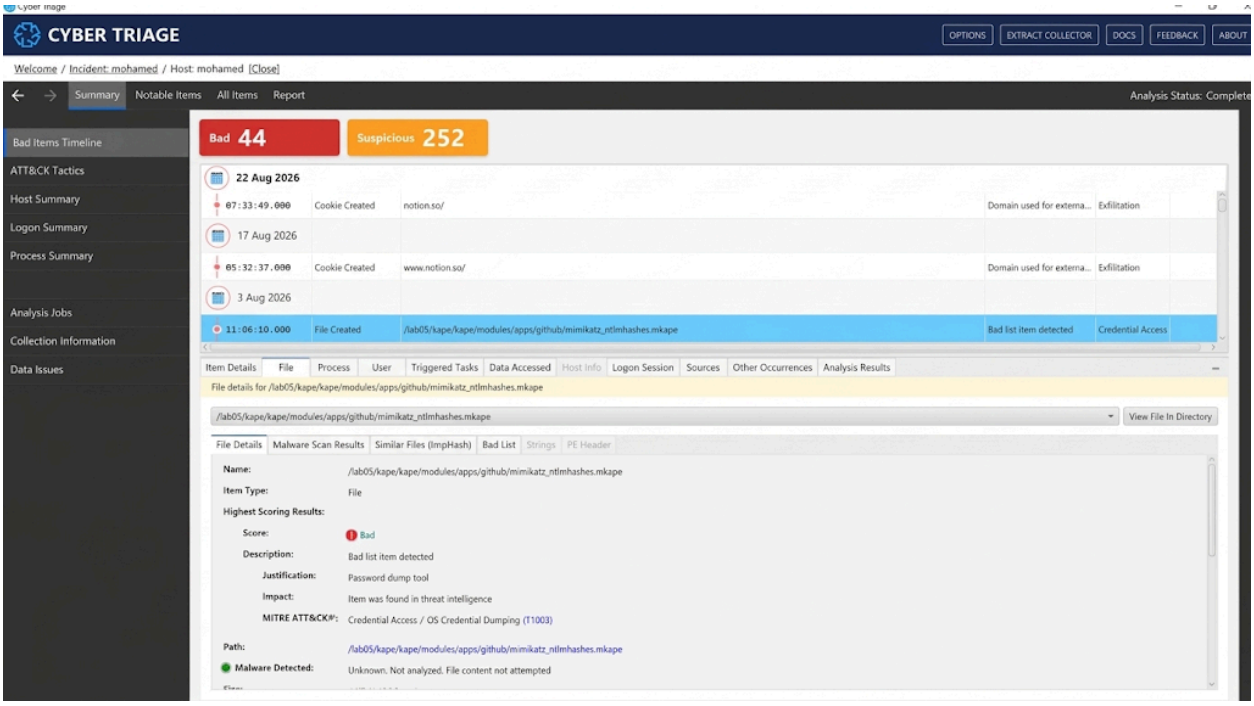
الأحداث الرئيسية المرصودة:

التصنيف	التفاصيل	
Domain used for Exfiltration	notion.so/	Created

	التفاصيل	التصنيف
Created	www.notion.so/	Domain used for Exfiltration
eated	/lab05/kape/modules/apps/github/mimikatz_ntlmhashes.mkape	Bad list item — Credential Access
dified	volatility3 framework plugins (متعددة)	Bad list item — Credential Access

القائمة الجانبية تتضمن: Bad Items Timeline | ATT&CK Tactics | Host Summary | Logon Summary | Process Summary | Analysis Jobs | Collection Information | Data Issues.

الصورة التاسعة — تفاصيل ملف Mimikatz



تفاصيل ملف mimikatz_ntlmhashes.mkape — File Details

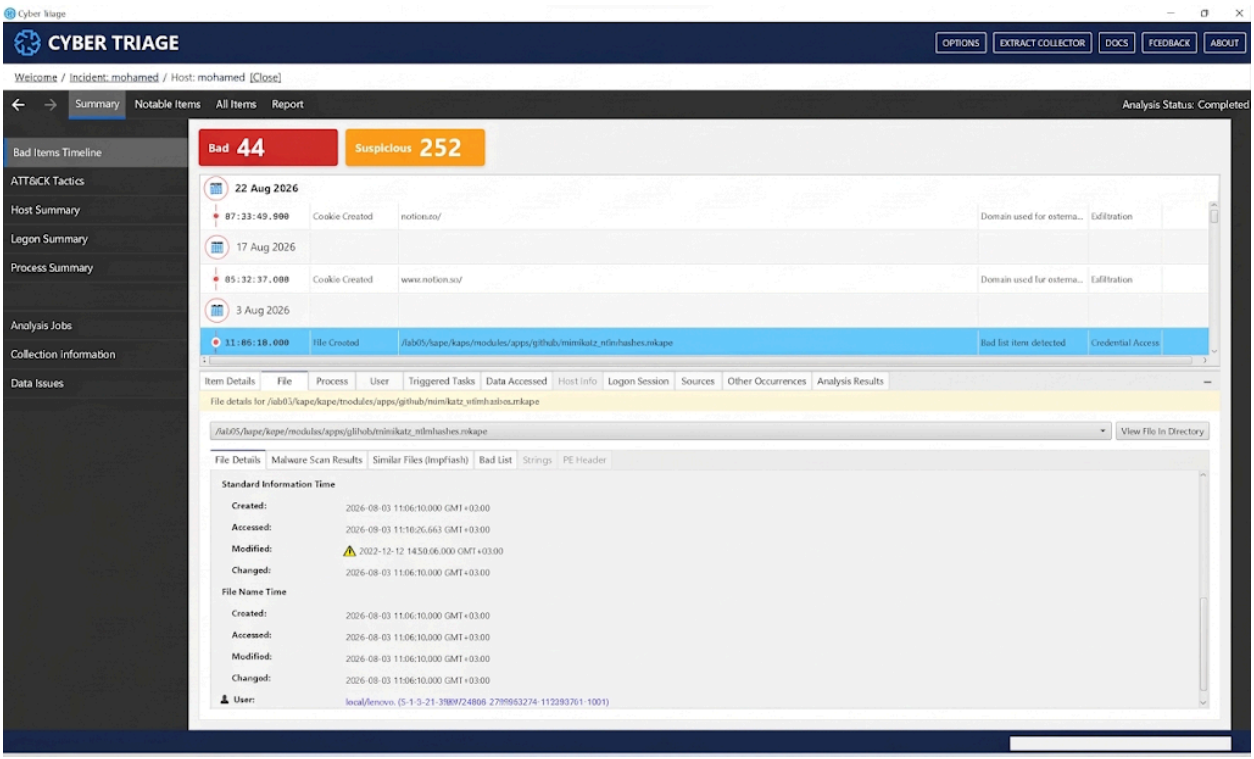
الوصف: تُظهر هذه الشاشة تفاصيل العنصر المحدد من الجدول الزمني، وهو ملف **mimikatz_ntlmhashes.mkape** الخطير.

تفاصيل الملف:

- **Name:** `/lab05/kape/kape/modules/apps/github/mimikatz_ntlmhashes.mkape`
- **Item Type:** File
- **Score:** 🔴 Bad
- **Description:** Bad list item detected
- **Justification:** Password dump tool (أداة تفريغ كلمات المرور)
- **Impact:** Item was found in threat intelligence (موجود في قواعد بيانات التهديدات)
- **MITRE ATT&CK®:** `Credential Access / OS Credential Dumping (T1003)`
- **Path:** `/lab05/kape/kape/modules/apps/github/mimikatz_ntlmhashes.mkape`
- **Malware Detected:** Unknown — Not analyzed (لم يتم تحليل محتوى الملف)

الخلاصة: Mimikatz هي أداة شهيرة لسرقة بيانات الاعتماد من ذاكرة Windows، وتُعدّ وجودها على الجهاز مؤشرًا قويًا على نشاط مهاجم متمرس.

الصورة العاشرة — التوقيتات الزمنية لملف Mimikatz (Timestamps)



تحليل التوقيتات — Standard Information Time vs File Name Time

الوصف: تعرض هذه الشاشة تفاصيل التوقيتات (Timestamps) لملف Mimikatz من نافذة **File Details**، وهي من أهم المؤشرات الجنائية الرقمية.

Standard Information Time ($STANDARD_INFORMATION):

الحدث	التوقيت
Created	2026-08-03 11:06:10.000 GMT+03:00
Accessed	2026-08-03 11:06:26.663 GMT+03:00
Modified	⚠️ 2022-12-12 14:50:06.000 GMT+03:00
Changed	2026-08-03 11:06:10.000 GMT+03:00

File Name Time ($FILE_NAME):

الحدث	التوقيت
Created	2026-08-03 11:06:10.000 GMT+03:00
Accessed	2026-08-03 11:06:10.000 GMT+03:00
Modified	2026-08-03 11:06:10.000 GMT+03:00
Changed	2026-08-03 11:06:10.000 GMT+03:00

> **المستخدم:** `local\lenovo` (SID: S-1-3-21-3989724808-2799963274-112280761-1001)
>
> **التحليل الجنائي:** تاريخ Modified في `STANDARD_INFORMATION$` يعود إلى **12-12-2022** بينما بقية التواريخ في **03-08-2026**، وهذا يُشير بقوة إلى عملية **Timestomping** — وهي تقنية يستخدمها المهاجمون لتعديل توقيت الملف وإخفاء أثرهم، مما يجعل الملف يبدو أقدم مما هو عليه.

الخلاصة والنتائج الرئيسية

تم رصد نشاط خبيث واضح على الجهاز MOHAMED. النتائج تشير إلى مهاجم متمرس نفّذ عدة تقنيات هجومية موثّقة في إطار MITRE ATT&CK.

التهديدات المرصودة

1. **سرقة بيانات الاعتماد (Credential Dumping — T1003)**
   - وجود ملف (`mimikatz_ntlmhashes.mkape`) Mimikatz بتاريخ 3 أغسطس 2026.
   - أداة متخصصة في استخراج كلمات المرور وhashes من ذاكرة Windows.
2. **تسريب البيانات (Exfiltration)**
   - رصد cookies مرتبطة بنطاق `notion.so` بتاريخَي 17 و22 أغسطس 2026.
   - يُحتمل استخدام Notion كقناة لتسريب البيانات (Data Exfiltration over Web Service).
3. **التلاعب في التوقيتات (Timestomping)**
   - تاريخ تعديل ملف Mimikatz يعود إلى 2022 رغم أن الملف أُنشئ في 2026.
   - تقنية إخفاء الأثر الزمني لتضليل المحققين.
4. **استخدام أدوات تحليل جنائي (Forensics Tools — KAPE & Volatility3)**
   - وجود ملفات Volatility3 framework في مجلدات KAPE.
   - يُشير إلى أن المهاجم استخدم أدوات جنائية للتحقق من البيئة أو جمع معلومات إضافية.

الإحصائيات النهائية

المؤشر	القيمة
إجمالي العناصر الخطيرة	🔴 44
إجمالي العناصر المشبوهة	🟠 252
تقنيات ATT&CK المُرصَدة	Credential Access (T1003) + Exfiltration
الأداة الأخطر	Mimikatz
المستخدم المشبوه	local\lenovo