Digital Forensics Lab Report

Lab 6 – KAPE **:Lab Name**

Digital Forensics Midterm Labs **:Course**

Eng. Abdulrazzaq Alsamawi **:Instructor**

Mohammed AL-Ma3mari **:Investigator / Student Name**

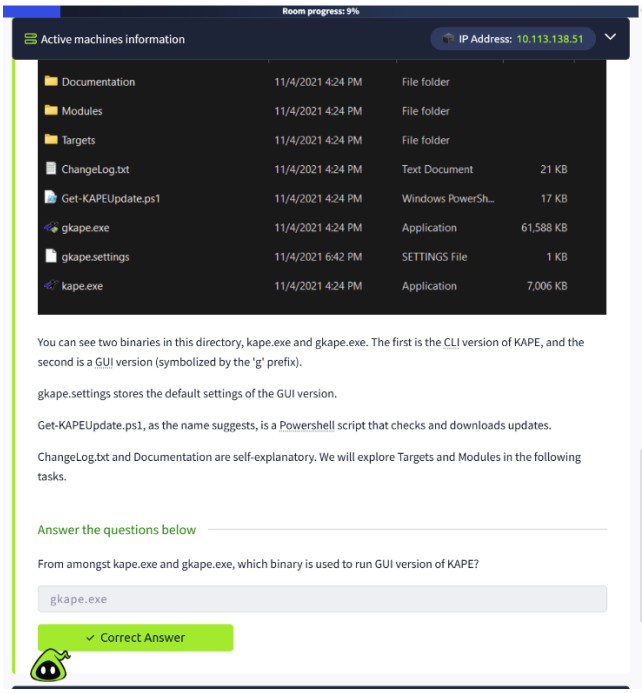
Al-Razi University **:University**

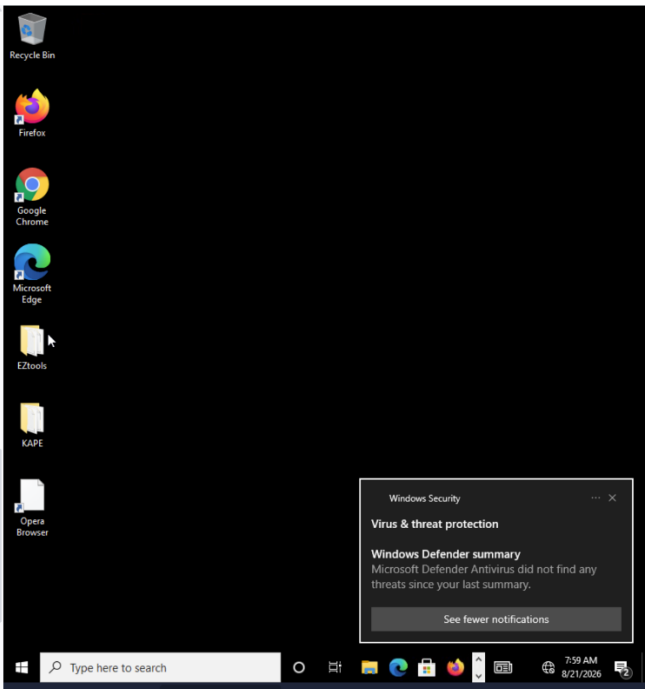
Objective .1

The primary objective of this laboratory is to utilize the Kroll Artifact Parser and Extractor (KAPE) to perform a rapid live forensic triage on a compromised Windows machine. The investigation involves configuring collection Targets, executing parsing Modules, and analyzing the extracted artifacts to uncover suspicious activities, external device connections, and execution .timelines

2. Configuration Analysis & Phase 1: KAPE Architecture

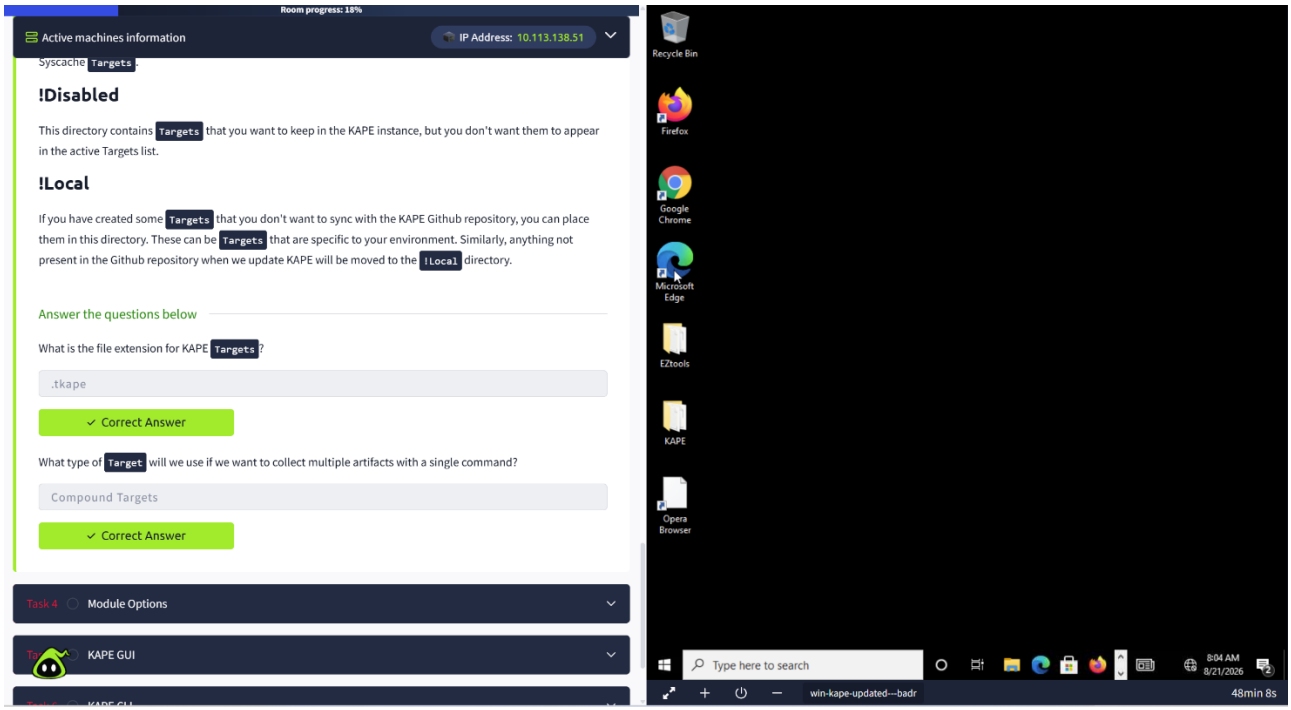
قبل البدء في عملية الجمع، كان من الضروري فهم هيكلية عمل الأداة لضمان استخراج الأدلة الصحيحة وعدم إتلاف بيانات النظام.





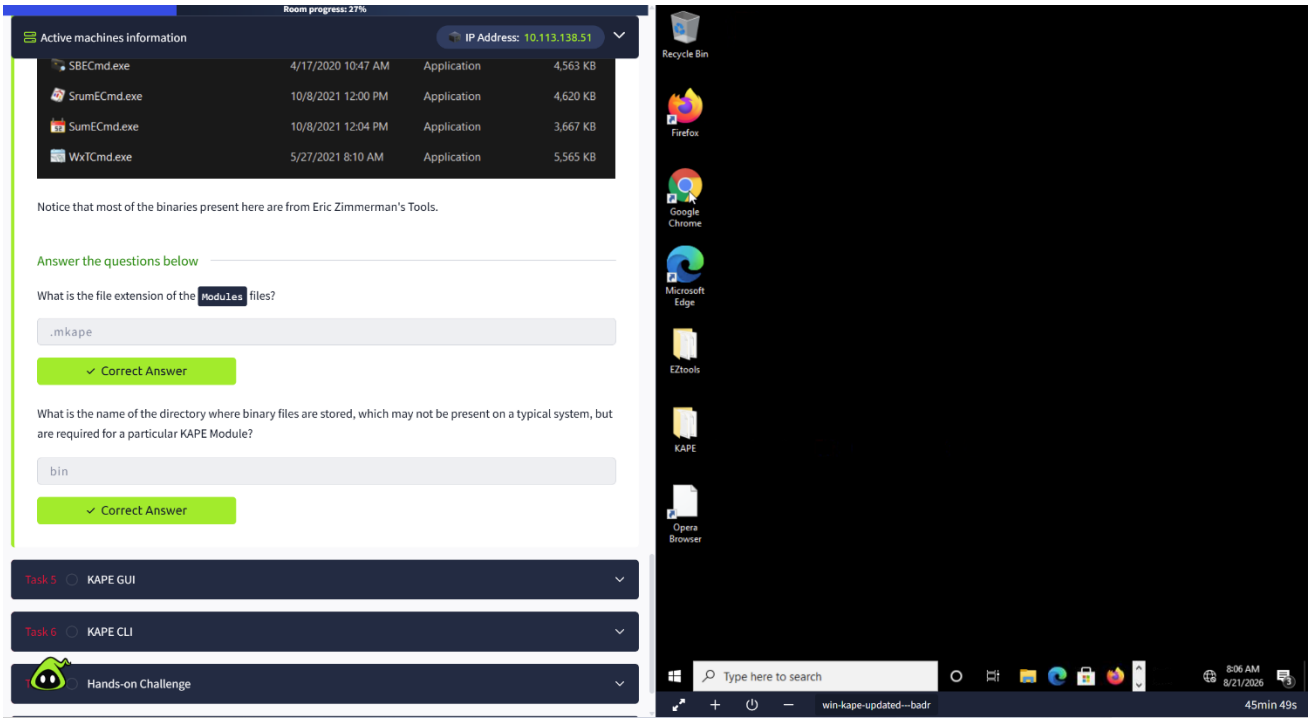
- **Analysis Step (GUI vs. CLI Validation):**

في هذه الخطوة، تم تحليل المجلد الجذري للأداة لتحديد الملفات التنفيذية الأساسية. تم تحديد gkape.exe كواجهة رسومية (GUI) تُسهل إعداد المتغيرات المعقدة، بينما يُستخدم kape.exe للتشغيل الصامت عبر سطر الأوامر (CLI) أثناء الاستجابة السريعة للحوادث.



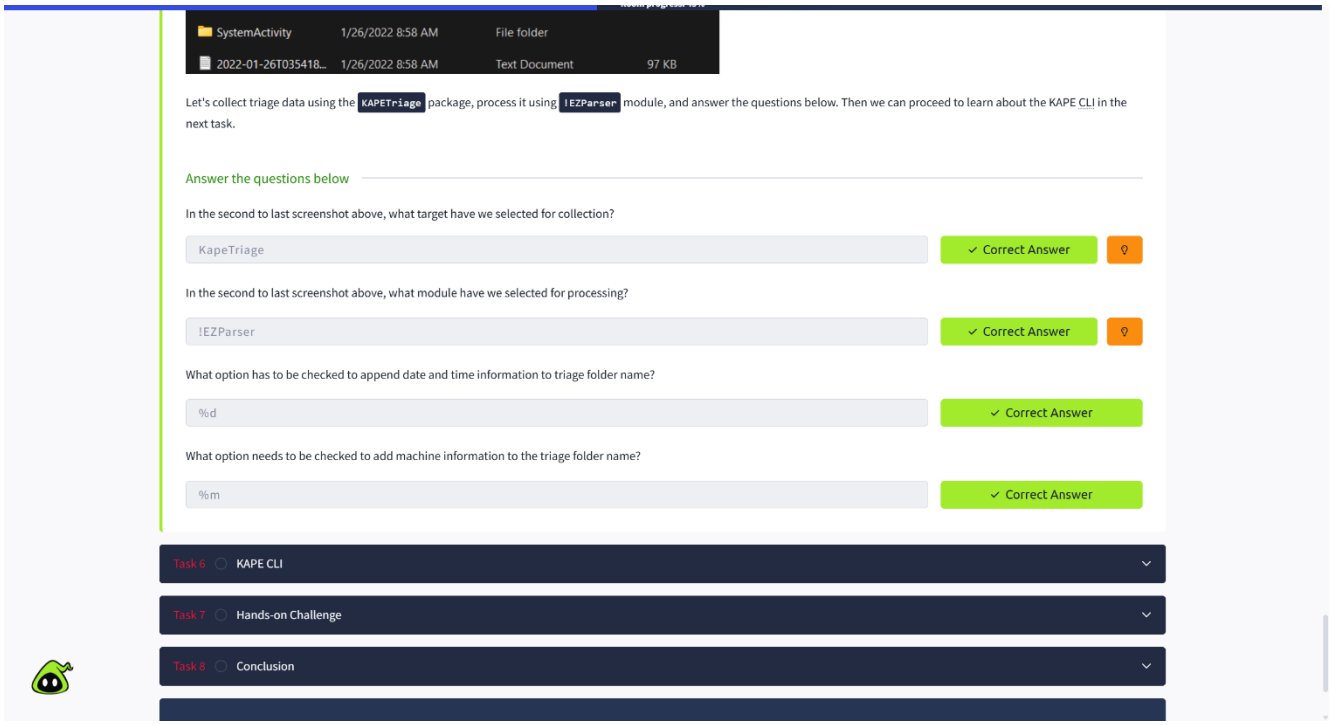
- **Analysis Step (Target Configurations):**

لضمان جمع الأدلة الدقيقة، تم تحليل بنية مجلد الأهداف (Targets). تم تحديد امتداد tkape. للملفات التي توجه الأداة لمسارات الأدلة داخل النظام. كما تم التأكيد على استخدام (Compound Targets) لجمع مسارات متعددة (مثل Registry و FileSystem) بأمر واحد لتقليل وقت التجميع.



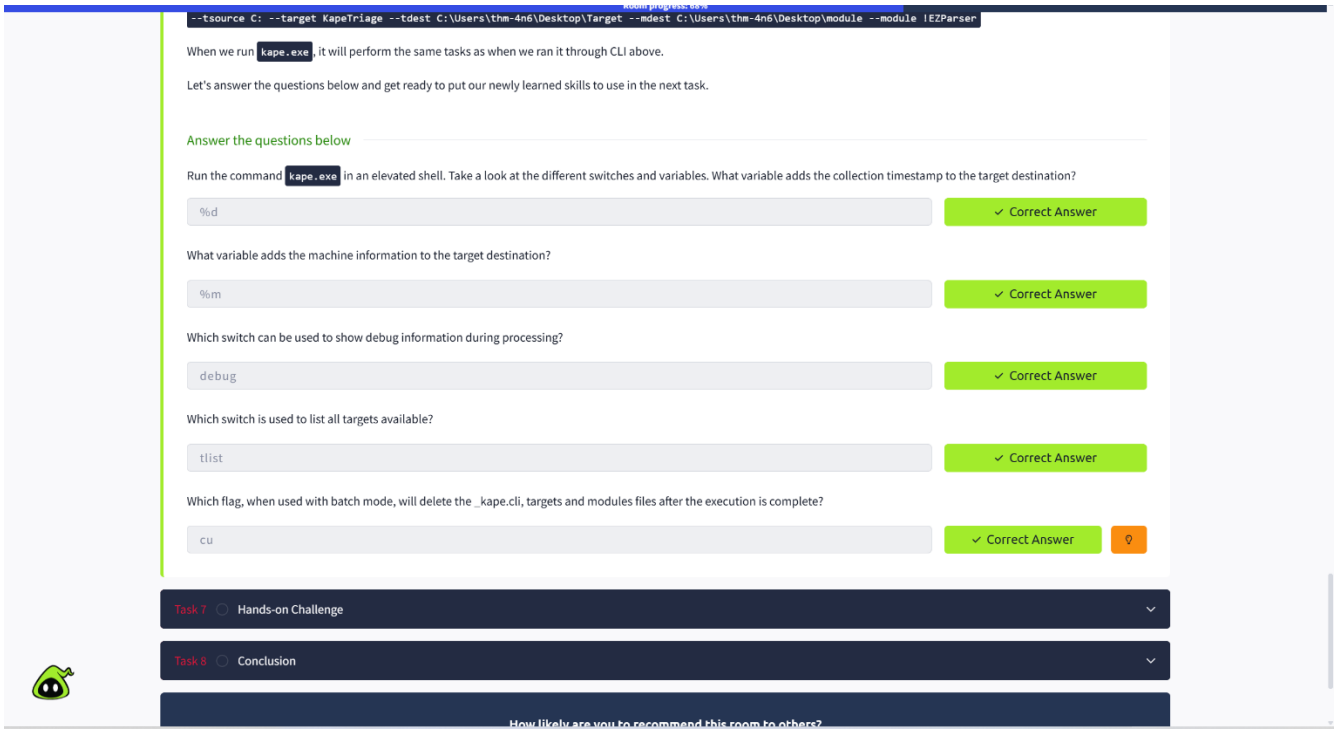
- **Binary Dependencies & Analysis Step (Modules):**

تتطلب الأدلة الخام التي يتم جمعها معالجة لتصبح مقروءة. توضح هذه الخطوة إعدادات الـ Modules ذات الامتداد .mkape. كما تم تحديد مجلد bin كحاوية أساسية للبرمجيات المساعدة (مثل أدوات Eric Zimmerman) التي تعتمد عليها KAPE لفك تشفير وتحليل السجلات (Parsing).



- **Analysis Step (Triage Parameter Setup):**

تم هنا إعداد خطة الهجوم الجنائي. تم اختيار الهدف KapeTriage لجمع أهم الأدلة الحيوية (MFT, Logs, Registry)، وتم ربطه بوحدة المعالجة !EZParser لتحويل البيانات إلى جداول CSV. بالإضافة إلى إعداد متغيرات حفظ الأدلة بإضافة التاريخ والوقت d% واسم الآلة m% للحفاظ على التسلسل الهرمي الجنائي (Chain of Custody).

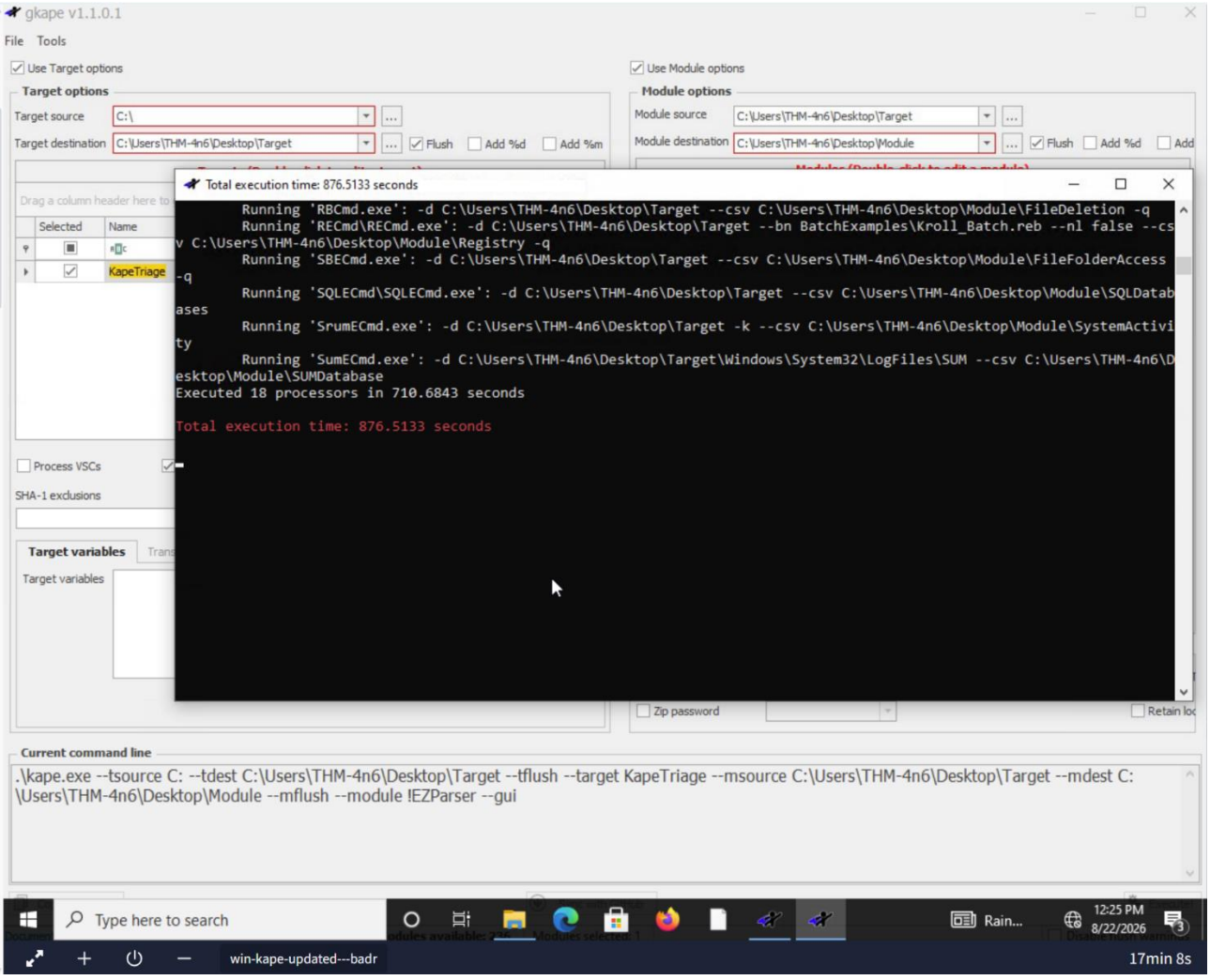


- **Analysis Step (Command-Line Switches Optimization):**

توثق هذه الخطوة الفهم العميق لأوامر الشاشة السوداء (CLI) الخاصة بالأداة. تم إعداد متغيرات التنظيف الآلي --cu لحذف الملفات المؤقتة بعد الانتهاء، وتفعيل وضع -- debug لمراقبة الأخطاء أثناء معالجة ملفات النظام المعقدة والمقفلة.

3. Phase 2: Live Forensic Triage Execution

هذه هي المرحلة الأهم والأكثر استهلاكاً لموارد النظام، حيث تم إطلاق الأداة للعمل الفعلي داخل النظام المصاب.

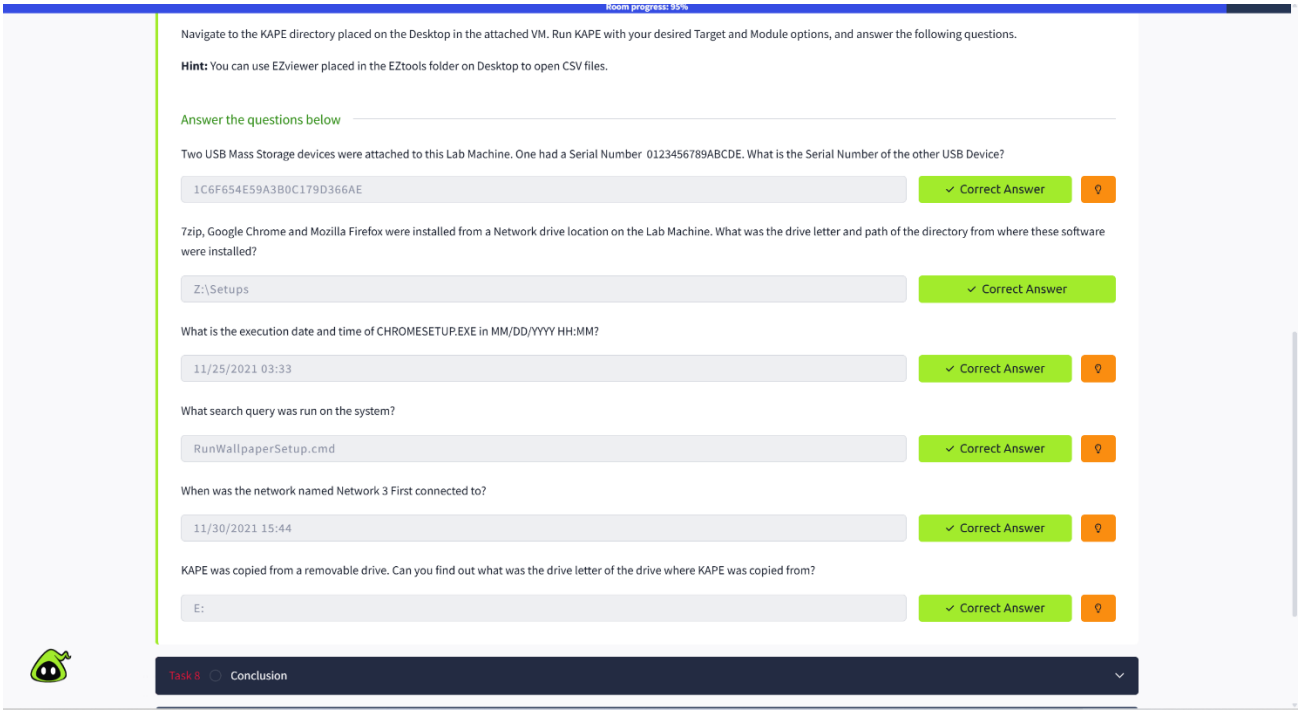


- **Processing Details & Execution:**

تُظهر هذه الصورة عملية المعالجة الحية (Live Triage) قيد التنفيذ. استغرقت العملية جهداً مكثفاً من النظام (Total execution time: 876.5133 seconds)، حيث قامت الأداة بتشغيل 18 معالجاً مختلفاً بشكل متوازٍ. تضمنت هذه العملية فك تشفير سجلات النظام (Registry Hives)، واستخراج بيانات شبكة الاتصال، وتحليل ملفات الـ Prefetch و Amcache لرصد النشاطات المشبوهة، مما يدل على حجم البيانات الضخم الذي تمت معالجته واستخراجه من الآلة

4. Evidence Analysis & Phase 3: Forensic Findings

بعد انتهاء معالجة الأدلة وتحويلها إلى تقارير مقروءة، تم تحليل النتائج للإجابة على التساؤلات الجنائية حول الاختراق.



- **Recovered Artifacts & Key Findings:**

بناءً على التقارير المستخرجة، تم الوصول إلى الاستنتاجات الجنائية التالية:

1. **USB Forensics:** تم تحديد الرقم التسلسلي للفلاشة المتصلة بالجهاز وهو (C6F654E59A3B0C179D366AE1).

2. **Software Execution:** تم إثبات أن البرامج أُعدت للتثبيت من مسار الشبكة (Z:\setups).

3. **Execution Timeline:** تم رصد وقت تنفيذ ملف CHROMESETUP.EXE بدقة في تاريخ 2021/25/11 03:33.

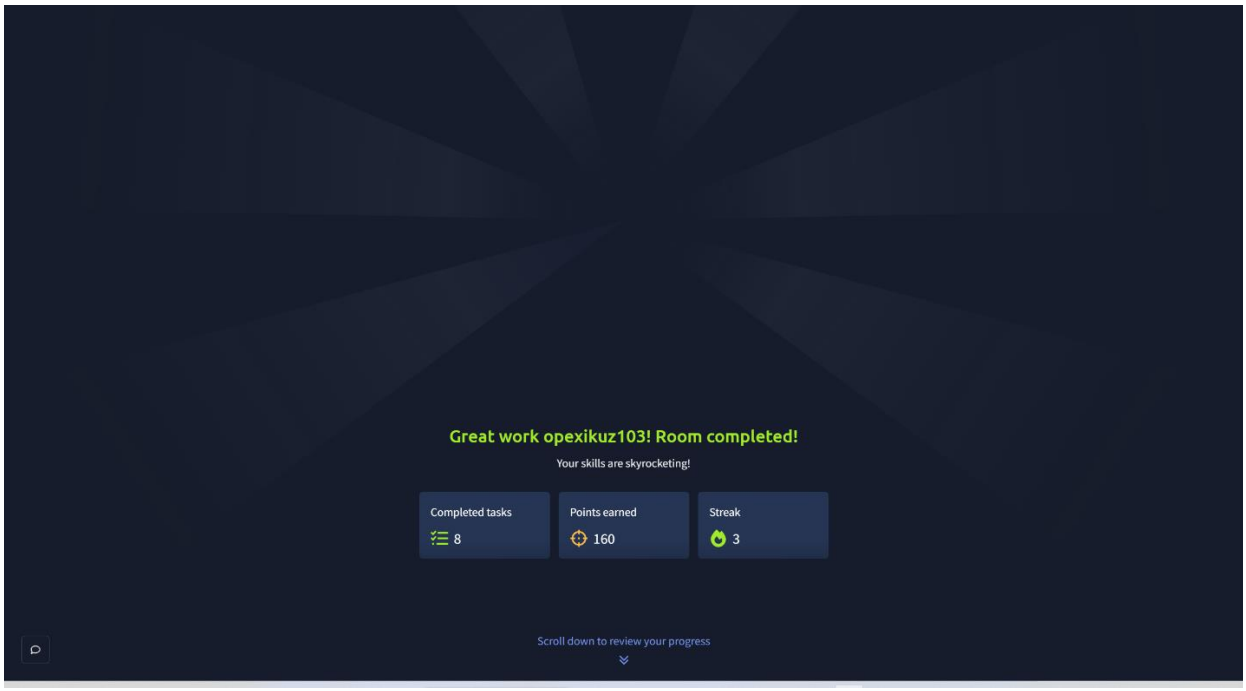
4. **Malicious Activity/Queries:** من خلال تحليل سجلات النشاط، تم اكتشاف أن المهاجم/المستخدم قام بتشغيل الاستعلام (RunWallpaperSetup.cmd).

5. **Network Forensics:** تم تحديد تاريخ أول اتصال بشبكة (Network 3) في 2021/30/11 15:44.

6. **Data Exfiltration/Tools:** تم التأكد من أن أداة KAPE تم تشغيلها ونسخها من محرك الأقراص (E:).

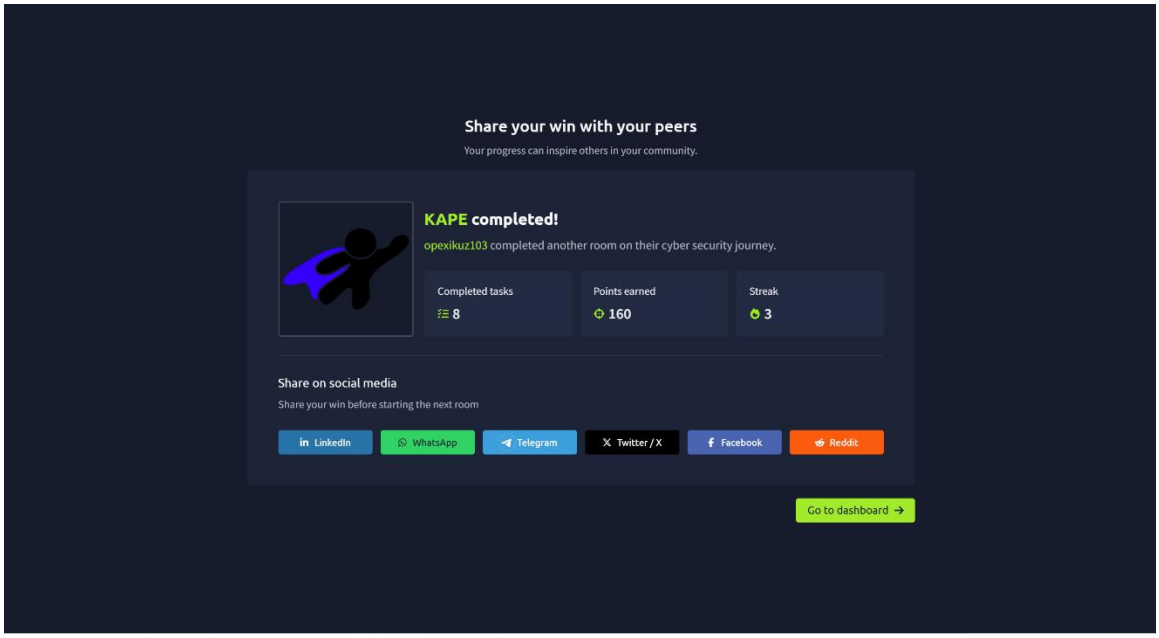
5. Verification & Conclusion

تم إنجاز كافة متطلبات التحقيق الجنائي بنجاح.



- **Task Completion:**

إثبات إتمام جميع المهام الثمانية (Tasks 8) الخاصة بالغرفة، مما يؤكد اجتياز الجانبين النظري التأسيسي والعملي التطبيقي بالكامل.



- **Room Certification:**

شهادة اكتمال الغرفة (KAPE Completed) عبر منصة TryHackMe بنسبة 100% للمحقق، مما يوثق الجهد المبذول في إنهاء المعمل.