المطلوب العملي

التحقيقات والأدلة الرقمية



أولا

• تحميل جهاز افتراضي مع أي نظام تشغيل



ثانيا

• عمل نسخة من القرص الصلب على الجهاز الافتراضي باستخدام أي أداة من المذكورة في الكتاب ثم مطابقة القرص مع القرص الأصلي وحساب الهاش (سكرين شوت لكل خطوة وعمل تقرير)



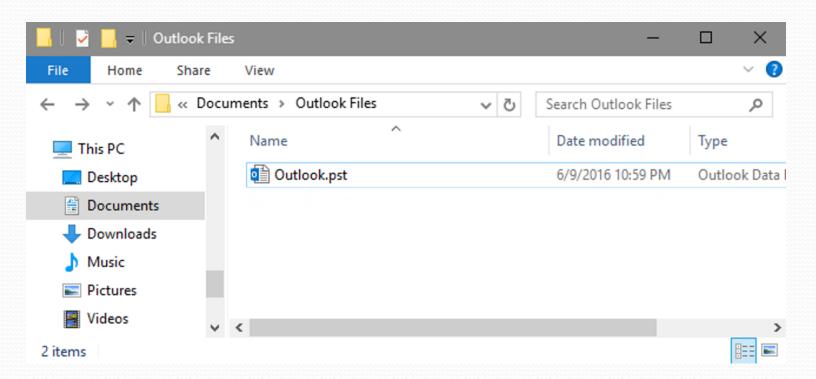
ثالثا

• عمل استرداد لبعض بيانات القرص الصلب بواسطة أداة Disk digger • وتصنيف البيانات حسب الأهمية (سكرين شوت لكل خطوة وعمل تقرير)



رابعا

• استرداد الملف الخاص بالبريد الاليكتروني pst مع (سكرين شوت لكل خطوة وعمل تقرير)



خامسا

اختيار ملف من الملفات المستردة وفحص ترويسته باستخدام أي أداة من الأدوات المذكورة بالمقرر واظهارها مع (سكرين شوت لكل خطوة وعمل تقرير)

PE Explorer - C:\TEST\malicious.exe View Tools Help HEADERS INFO Address of Entry Point: 00447380 Real Image Che Field Name Data Value Description Machine 014Ch 1386® Number of Sections 0008h Time Date Stamp 24425E19h 19/06/1992 22:22:17 Pointer to Symbol Table 900000000h Number of Symbols 000000000h Size of Optional Header 00E0h Characteristics 818Eh 15

سادسا

جمیع ما سبق یتم وضعه کقضیة افتراضیة بسیناریو من اختراعك وتوضع
النتائج كتقریر في برنامج Encase مع (سكرین شوت لكل خطوة و عمل
تقریر)

