مقرر التحقيقات والأدلة ألرقمية - الجانب العملي

الادوات الاساسيه|:

شرح اداوات معرفة معلومات الشبكة على نظام الويندوز والكالي ومعرفه اهميه كل اداه من الادوات المذكورة وطريقه عملها .

مخرجات التعلم : Ipconfig / ifconfg / ping / trucert

* تنفيذ الامر ipconfig على موجه الاوامر cmd على نظام ويندوز ومعرفة معلومات الشبكة.
* تنفيذ الأمر ifconfig على نظام ويندوز ومعرفة عنون ip.
* تنفيذ الامر ping لمعرفة حالة الاتصال بالشبكة.
* تنفيذ الأمر trucert لإظهار المسارات التي مرت بها الحزمة حتى وصلت لوجهتها .
* القدره على فهم نتائج تنفيذ الادوات المذكورة سابقا.

البرنامج الثاني : windows sysinternals لتحليل البرمجيات الخبيثة .

يتناول شرح تحليل البرمجيات الخبيثة والتعرف على ادواته وطريقه عمل كل اداه .

مخرجات التعلم :

* تنفيذ اداة Procmon ومعرفة زمن تنفيذ كل عملية على الجهاز .
* تنفيذ الأداة Rammap ومعرفة كمية الذاكرة المستخدمة لكل برنامج على الجهاز.
* تنفيذ الأداة TCPview ورؤية بروتوكلات TCP /UDP وحالة الاتصال.
* تنفيذ الأداة Autorun ومراقبة البرامج التي تعمل تلقائيا عند تشغيل الجهاز.

البرنامج الثالث : event viewer

يتناول شرح برنامج event viewer احد مكونات نظام windows الذي يستخدم لعرض سجلات الاحداث .

مخرجات التعلم :

* تشغيل البرنامج من محرك البحث .
* التعرف على الواجهة الرئيسية للبرنامج.
* عرض الاحداث التي تخص الامان.
* تصفية الاحداث التي تظهر حسب المراد البحث عنه.

البرنامج الرابع : كيفيه تحميل اداه disk digger .

شرح كيفية تحميل اداه disk digger المهمة في استعادة الملفات المحذوفة .

مخرجات التعلم :

تحميل الأداة بالشكل الصحيح .

البرنامج الخامس : استعادة الملفات المحذوفة.

شرح كيفية استعادة الملفات التي تم حذفها من القرص .

مخرجات التعلم :

* التعامل مع البرنامج وفهم الواجهة الرئيسية .
* استعادة الملفات المحذوفة .

البرنامج السادس : ftk imager

شرح لبرنامج ftk imager الذي يعد احد خطوات التحليل الجنائي الرقمي يمكننا من اخذ نسخة عن القرص الصلب يحتوي على سيناريو لحيازة دليل ونسخه بواسطة البرنامج.

مخرجات التعلم :

* تنصيب البرنامج على الجهاز
* التعرف على اول الخطوات التي يقوم بها المحقق الجنائي
* معرفة كيفية نسخ القرص الصلب و تنفيذ سيناريو لنسخ دليل جنائي رابط الفيديو توضيحي : https://youtu.be/KGZEU91KsNU

البرنامج السابع : veracrypt

يتناول شرح لبرنامج veracrypt الذي يمكننا من تشفير الأقراص والأقراص الوهمية وحفظها.

مخرجات التعلم :

* تنصيب البرنامج .
* التعرف على الواجهة الرئيسية للبرنامج.
* معرفة الية تشفير القرص حسب الاحرف التي سيتم ربط القرص بها.
* تنفيذ تشفير لقرص وهمي او ملفات محددة .
* معرفة كيفية الوصول للملفات والأقراص التي تم تشفيرها وموقع حفظها .

رابط الفيديو التوضيحي :

https://youtu.be/hgCYu1eRckg

البرنامج الثامن : اداة wireshark

يتناول شرح لأداة الwireshark التي تعد اهم خطوات التحقيق الجنائي وتمكننا من التصنت على الاجهزة والشبكة بالإضافة لإمكانية تسريب المحادثة التي تم التصنت اليها التي يمكن من خلالها استخلاص معلومات مهمة جدا.

مخرجات التعلم :

* تنصيب برنامج ال wireshark.
* التعرف على الواجهة الرئيسية للبرنامج.
* تشغيل التقاط البيانات عبر الشبكة واخذ نسخة عنها.
* اظهار المعلومات الخاصة بالبروتوكلات و فهمها .
* حفظ نسخة من البيانات التي تم التقاطها و ارسالها.

رابط الفيديو للتوضيح : https://youtu.be/si0a2_JV27E

البرنامج التاسع :

برنامج Browser history exminar يتناول شرح برنامج Browser history exminar المهم في عمليه تحليل والتقاط سجلات المتصفحات.

مخرجات التعلم :

* تعلم كيفيه تحميل البرنامج.
* تنفيذ البرنامج والتعرف عليه .
* تعلم كيفيه التقاط البيانات المارة من الشبكه وتحليلها, ولالتقاط وتحليل سجلات التصفح .

رابط الفيديو(للتوضيح) : https://youtu.be/zChhtNX1d1o

البرنامج العاشر :

برنامج Encase: يتناول شرح اداه ال Encase التي تمكننا من خلق صوره طبق الاصل للقرص او جهاز الهدف.

مخرجات التعلم :

تنفيذ اداه Encase وإنشاء قضيه للعمل عليها .

رابط الفيديو(للتوضيح) :

https://youtu.be/tVFzXJY0PVo

البرنامج الحادي عشر :

اداة Nmap: التعرف على اداه تحليل حزم البيانات Nmap التي تفيد في معرفه المنافذ المفتوحة بالنظام والثغرات التي يمكن الدخول من خلالها .

مخرجات التعلم :

- تنفيذ اداه Nmap على الكالي .
- القدره على فهم ناتج تنفيذ الاداه .

البرنامج الثاني عشر :

برنامج PE explorer: شرح برنامج ال PE explorer للقيام بعمليه تحليل لترو يسه الملف .

مخرجات التعلم :

* تنفيذ برنامج PE explorer.

- القدره على فهم طريقه عمله.
- معرفه معلومات عن تاريخ خلق الملف وحجمه .