التحليل الجنائي الرقمي

دليل عملي لطرق التحليل الجنائي الرقمي
في الجرائم المعلوماتية

المهندس: جميل حسين طويله

مقدمة:

التحليل الجنائي الرقمي **Digital Forensics** هو العلم الذي يجمع بين العلوم الشُرطية الجنائية وعلوم الحاسب والشبكات بهدف استخراج الأدلة الرقمية **digital evidences** من أجهزة الحاسب وأجهزة الشبكة والأجهزة والوسائط الرقمية، الأدلة الرقمية يمكن أن تكون البيانات الرقمية المخزنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية أو المنقولة بواسطتها والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

الهدف الرئيسي من التحليل الجنائي الرقمي هو التصدي للجرائم المعلوماتية التي ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة.

لمن هذا الكتاب:

هذا الكتاب مخصص لعناصر وضباط الشرطة العاملين في مجال مكافحة الجريمة المعلوماتية ولمهندسي الحماية وأمن المعلومات.

المرجع العلمي لمحتوى هذا الكتاب هو منهج شهادة:

CCFP (Certified Cyber Forensics Professional)

الكاتب:

جميل حسين طويله - مهندس اتصالات من سوريا

مختص بأمن المعلومات واختبار الاختراق

dolphin-syria@hotmail.com

cyber.sy@yandex.com

www.facebook.com/infosecur1tybooks

الإهداء:

إلى روح أبي وأمي

إلى أرواح شهداء وطني سوريا

التدقيق العلمي:

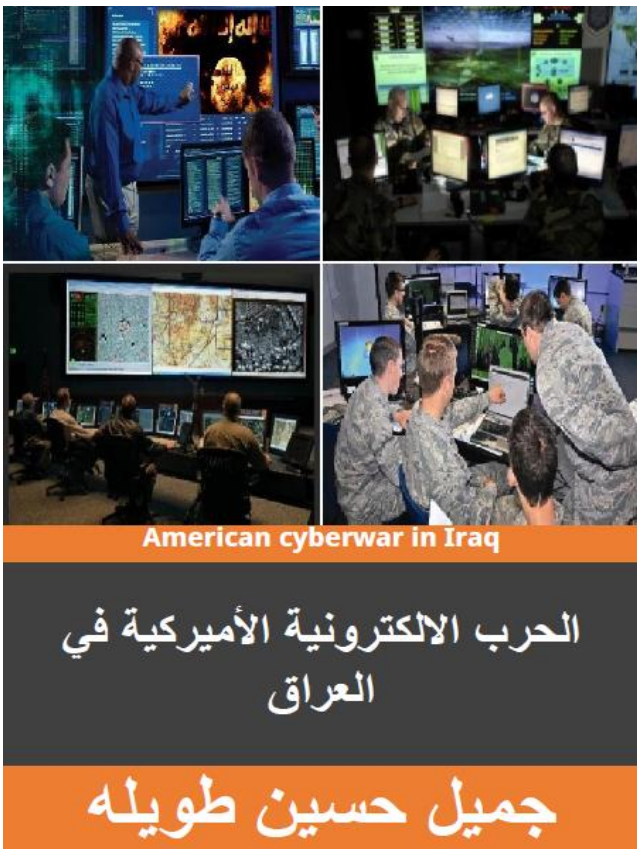
ماجد عبد المجيد اسماعيل - مهندس أمن معلومات من سوريا

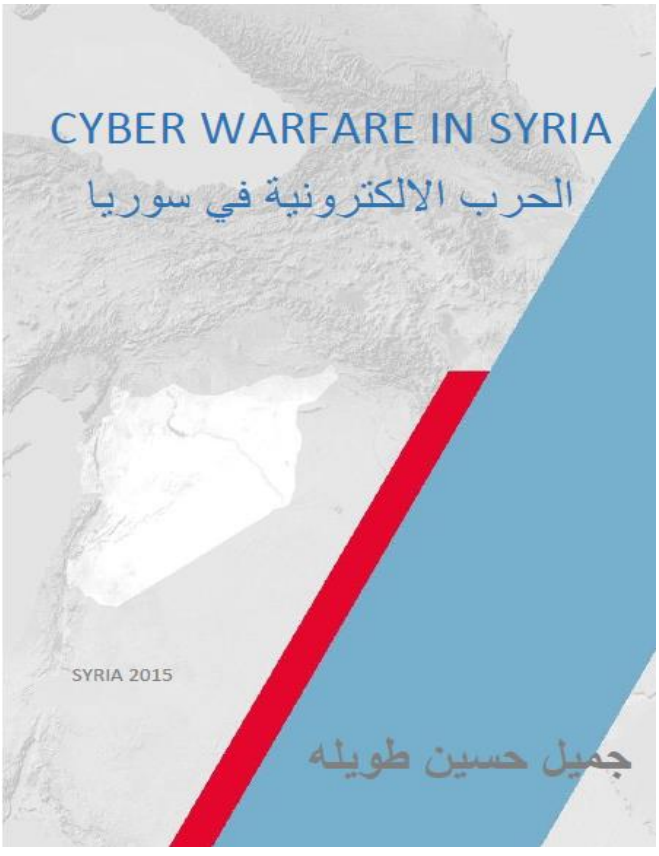
خبرة **15** سنة بإدارة الأنظمة والشبكات وقواعد البيانات

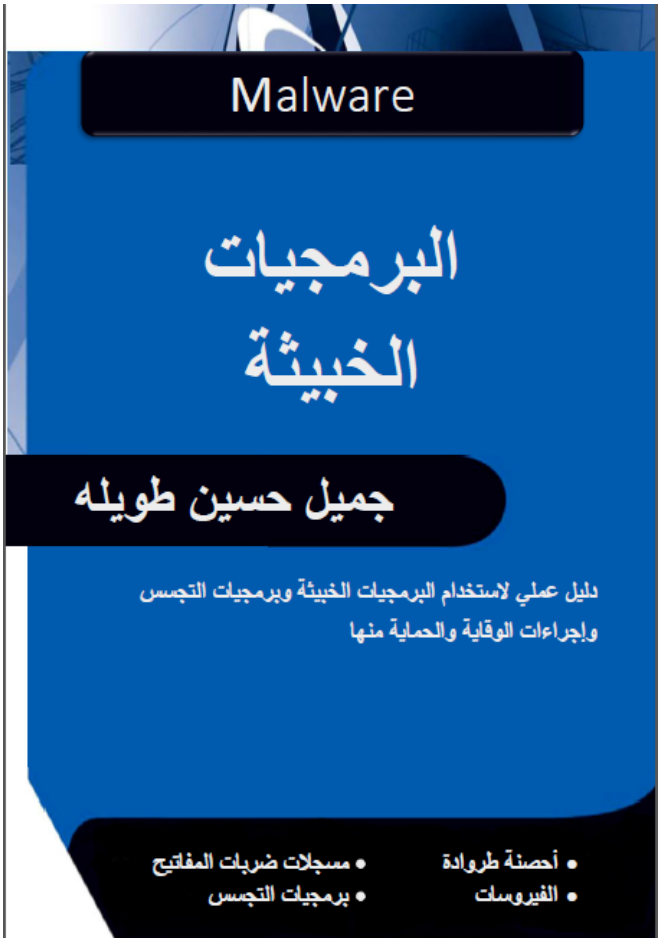
خبرة **5** سنوات باختبار الاختراق

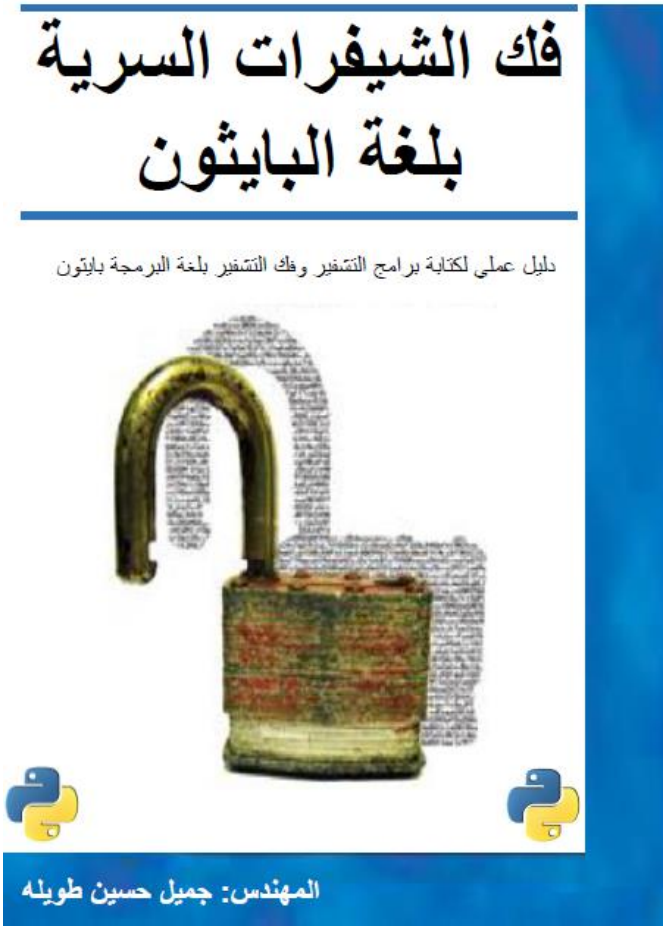
majed.esmaiel@gmail.com

منشورات سابقة:



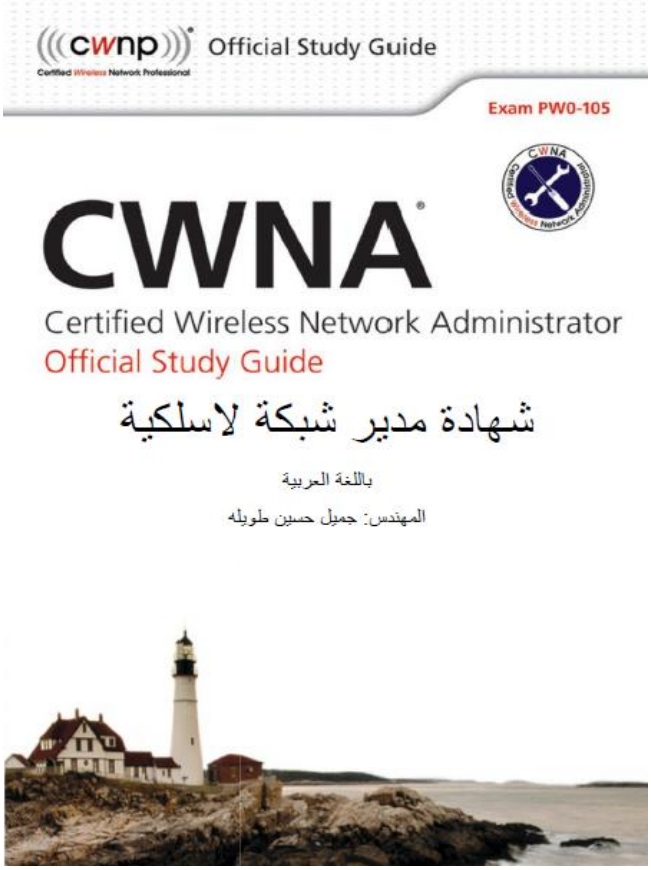



Malware
البرمجيات الخبيثة
جميل حسين طويله
دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس
وإجراءات الوقاية والحماية منها
• أحصنة طروادة
• الفيروسات
• مسجلات ضربات المفاتيح
• برمجيات التجسس


فك الشيفرات السرية بلغة البايثون
دليل عملي لكتابة برامج التشفير وفك التشفير بلغة البرمجة بايثون
المهندس: جميل حسين طويله


HACKING WIRELESS NETWORK
اختراق الشبكات اللاسلكية
جميل حسين طويله
[Wi-Fu]


هوائيات الشبكات اللاسلكية
المهندس:
جميل حسين طويله



الفهرس:

الفصل الثالث: تحليل الملفات

الفصل الرابع: خطوات التحليل الجنائي الرقمي

الفصل الخامس: التحليل الجنائي الرقمي للقرص الصلب

الفصل السادس: إخفاء وتشفير الملفات

الفصل السابع: التحليل الجنائي الرقمي للشبكة

الفصل الثامن: التحليل الجنائي الرقمي للويب

الفصل التاسع: التحليل الجنائي الرقمي لأجهزة الموبايل

الفصل العاشر: تحليل البرمجيات الخبيثة

الفصل الحادي عشر: سجلات النظام Windows Registry

أساسيات التحليل الجنائي الرقمي

محتوى هذا الفصل:

- ما هو التحليل الجنائي الرقمي.
- القرص الصلب وذاكرة الوصول العشوائي **RAM**
- أنظمة التشغيل والشبكات.
- حماية مكان الجريمة والتعامل مع الدليل الرقمي

مقدمة:

التحليل الجنائي الرقمي هو استخدام لتقنيات العلم والتكنلوجيا في عمليات التحقيق الجنائي للقضايا المخالفة للقانون، وتتضمن فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على دليل رقمي **digital evidence** يستخدم في التحقيقات القانونية

هذا العلم يحوي عدداً من التخصصات الفرعية ومنها:

- التحليل الجنائي الرقمي لأجهزة الحاسب.
- التحليل الجنائي الرقمي لقواعد البيانات.
- التحليل الجنائي الرقمي للشبكة.
- التحليل الجنائي الرقمي للويب.
- التحليل الجنائي الرقمي لأجهزة الموبايل.

عملية التحليل الجنائي الرقمي يجب أن تتم وفق معايير واجراءات قانونية معتمدة من قبل المحكمة وأهم هذه الإجراءات هو المحافظة على الأدلة الرقمية التي تم اكتشافها بدون أي تعديل أو تخريب وتوثيق كامل العمليات من لحظة الوصول لمكان الجريمة والعمليات التي تمت في مخبر التحليل الجنائي الرقمي لحين وصول الدليل الرقمي إلى المحكمة.

التحليل الجنائي الرقمي يمكن تطبيقه على أي جهاز يقوم بإرسال أو استقبال أو تخزين البيانات مثل أجهزة الموبايل وأجهزة الربط الشبكي

كالموجهات والمبدّلات (**router – switch**) وأجهزة الحاسب والأجهزة اللوحية **tablets**

التحليل الجنائي الرقمي وبشكل مماثل للتحليل الجنائي العادي (تحليل **DNA** وفحص الطلقات النارية) الهدف منه هو الحصول على دليل يمكن أن يستخدم في المحكمة.

أول مهمة يجب القيام بها هي المحافظة على مكان الجريمة وحمايته قبل البدء بعملية جمع الأدلة، في الجرائم المعلوماتية **cyber crime** فإن مكان الجريمة **crime scene** يمكن أن يكون جهاز حاسب أو مُخدّم **(server)** أو جهاز موبايل، علماً بأن الحفاظ على الحالة الأصلية للتجهيزات التي تحوي على أدلة رقمية يعتبر من أهم خطوات التحليل الجنائي الرقمي.

يجب على المحقق الرقمي أن يقوم بتوثيق وبشكل صريح و واضح كل دليل رقمي محتمل وكيفية الوصول لهذا الدليل.

التحليل الجنائي هو علم وهذا يعني أنك سوف تتبع مبادئ علمية أثناء القيام بعملية التحقيق الجنائي الرقمي.

طريقة التحليل الجنائي تعتمد على افتراضات ومن ثم فحص كل فرضية وتسجيل النتيجة، الفرضية عبارة عن سؤال ويجب الإجابة عليه.

مثلاً في الجرائم المعلوماتية فإن المحقق يفترض بأن المتهم قام بحذف الملفات ويتم التحقق من هذه الفرضية من خلال استعادة الملفات المحذوفة باستخدام أدوات معينة.

أساس عملية الاستجواب تعتمد على الأدلة المكتشفة.

أساسيات التحليل الجنائي الرقمي:

التحليل الجنائي الرقمي هو علم متقدم ولا يمكن لأي شخص القيام به يجب على المحقق الرقمي أن يكون على خبرة عالية في علوم الحاسب والشبكات وأنظمة التشغيل وخوارزميات التشفير.

Hardware:

لا يمكن أن تصبح محققاً في مجال التحليل الجنائي الرقمي إن لم تكن على معرفة كافية وخبرة مناسبة بالمكونات الصلبة والعتاد المادي لكل من الحواسب كاللوحة الأم والقرص الصلب والذواكر وأجهزة الربط الشبكي كالموجهات والمبدّلات (**router and switch**) وأجهزة الاتصالات الجوالة.

يجب أن تكون على معرفة بهذه الأجهزة لتتمكن من القيام بعملية الفحص والتحليل لها.

سوف نتحدث عن مكونات أجهزة الحاسب التي يجب على المحقق الرقمي أن يكون على معرفة مسبقة بها.

القرص الصلب Hard Drive:

بما أن الدليل الرقمي غالباً ما يكون موجود في القرص الصلب لنأخذ نظرة عامة على طريقة عمل الأقراص الصلبة.

القرص الصلب يقوم بتخزين البيانات على أساس نظام العد الثنائي **Binary System** الذي يحوي على عنصرين فقط الصفر **0** و الواحد **1** ليقوم الحاسب بالتعامل معها على شكل **bits**

الخانة التي تحوي على نبضة كهربائية تمثل الرقم واحد والتي لا تحوي على نبضة كهربائية تمثل الرقم صفر ويكون ذلك بحسب حالة القرص الصلب (الذرات المغناطيسية المكونة للقرص الصلب) إما أن تكون مستقطبة في اتجاه معين أو لا تكون ويتم التعامل معها من خلال نظام التشغيل الذي يفهمها على أنها أصفار أو واحدات وكل سلسلة معينة من الأصفار والواحدات يفهمها نظام التشغيل على أنها حرف معين أو تعليمة معينة.

الأمر المهم خلال عملية التحليل الجنائي الرقمي للقرص الصلب هو المحافظة على الدليل الرقمي، بما أن البيانات يتم حفظها بشكل مغناطيسي في القرص الصلب فيجب على المحقق الجنائي الرقمي حفظ القرص الصلب في مكان بعيد عن الحقول المغناطيسية لكي لا يتم تخريب الدليل الرقمي.

ومن المهم أيضاً فهم العلاقة بين الأقراص الصلبة المتعددة عند العمل في بيئة تحوي على أكثر من قرص صلب حيث يتم تخصيص قرص ليكون القرص الأساسي (الذي يحوي على النظام وملفات الإقلاع).

ذاكرة الوصول العشوائي RAM:

RAM (Random Access Memory)

مهمة جداً في عملية التحليل والتحقيق الجنائي الرقمي.

المحقق الرقمي يجب أن يقوم بعملية مراقبة وإلتقاط كل البيانات التي تم تسجيلها على الذاكرة **RAM** وإنشاء صورة طبق الأصل عن هذه البيانات.

أنظمة التشغيل:

نظام التشغيل هو أهم جزء في عملية التحليل الجنائي الرقمي.

سوف نناقش أساسيات أنظمة التشغيل المستخدمة حالياً و الأمور التي يجب على المحقق الرقمي معرفتها.

نظام Windows:

أهم جزء في عملية التحليل الجنائي الرقمي لنظام **windows** هو سجلات النظام **Windows Registry** من خلال هذه السجلات يمكن الحصول على معلومات مهمة مثل كلمات السر الخاصة بالشبكات اللاسلكية والرقم التسلسلي **serial number** لكل ذاكرة خارجية **USB** تم وصلها بالجهاز.

بالإضافة إلى السجلات يجب البحث عن الأدلة الرقمية في الملفات التي تحوي مُعرفات الجلسة **cookies** وتاريخ تصفح الانترنت.

نظام Linux:

وهو نظام تشغيل مفتوح المصدر **open source** (يمكن لأي شخص رؤية الرماز البرمجي المصدري لنظام التشغيل **linux**) ويوجد العديد من توزيعات **linux** وأشهرها **red hat** والتي تستخدم في عدد كبير المُخدّمات حول العالم،

linux يعتبر من أقوى أنظمة التشغيل وهو النظام المستخدم في كبرى الشركات العالمية وفي أجهزة التحكم بالمحطات الفضائية والمطارات والقطارات.

كمحقق جنائي رقمي يجب أن تكون قادر على التعامل مع نظام **linux** لأنه النظام المستخدم في معظم مُخدّمات **(servers)** استضافة المواقع.

يوجد العديد من الأدوات المجانية والمفتوحة المصدر **open-source** تستخدم في عمليات التحليل الجنائي الرقمي تعمل في نظام **linux** كما أن هذا النظام يحوي على العديد من التعليمات المفيدة في عملية التحليل والتحقيق الجنائي الرقمي.

نظام iOS:

تم تطويره من قبل شركة **Apple** وهو نظام التشغيل المستخدم في أجهزة **iPhones and iPads**

نظام Android:

هو نظام تشغيل تم تطويره من قبل شركة **Google** اعتماداً على نواة نظام التشغيل **Linux**، وعلى المحقق الجنائي الرقمي أن يمتلك المعرفة والخبرة المناسبة للتعامل مع هذا النظام لأنه يعتبر نظام التشغيل الأكثر شيوعاً حالياً في أجهزة الاتصالات الجوالة **Mobiles**

الشبكات:

العديد من الجرائم المعلوماتية تتم عبر الشبكة لذلك يجب على المحقق الرقمي أن يكون على معرفة كافية بأجهزة الشبكة وبرتوكولات الاتصال عبر الشبكة

- **Switch** المبدّلة: يستخدم لوصل عدد من الأجهزة في شبكة واحدة وهو يقوم بتوجيه البيانات إلى الجهاز الهدف اعتماداً على العناوين الفيزيائية **MAC address**
- **Router** الموجه: يقوم بوصل أكثر من شبكة مع بعضها البعض ويقوم بتوجيه البيانات بالاعتماد على عناوين **IP**

حزم البيانات Packet:

هي البيانات المرسلة والمستقبلة عبر الشبكة والتي يمكن أن تكون جزء من صورة أو مقطع فديو أو ملف نصي.

حزمة البيانات مكونة من عدد من **bytes** وتكون مقسمة إلى

header and body

الترويسة **header** تحوي على عناوين المصدر والهدف لحزمة البيانات ونوع البرتوكول المستخدم في عملية الاتصال وهذه المعلومات تعتبر مفيدة جداً في عملية التحليل الجنائي الرقمي.

عملية الاتصال عبر الشبكة تختلف بحسب نوع البرتوكول المستخدم، كل برتوكول يقوم بعملية الاتصال عبر منفذ **port** معين

مثلاً:

- البرتوكول **FTP (File Transfer Protocol)** يستخدم المنفذ **21**
- البرتوكول **SSH (Secure Shell)** يستخدم المنفذ **22**
- البرتوكول **Telnet** يستخدم المنفذ **23**
- البرتوكول **http** يستخدم المنفذ **80**

المحقق الرقمي يجب أن يكون على معرفة بعناوين **IP and MAC** وطريقة التعامل مع هذه العناوين (المجرم يقوم بتغيير عنوان **IP** الخاص بجهازه قبل القيام بتنفيذ الجريمة كما يمكن أيضاً أن يقوم بتغيير عنوان **MAC address**)

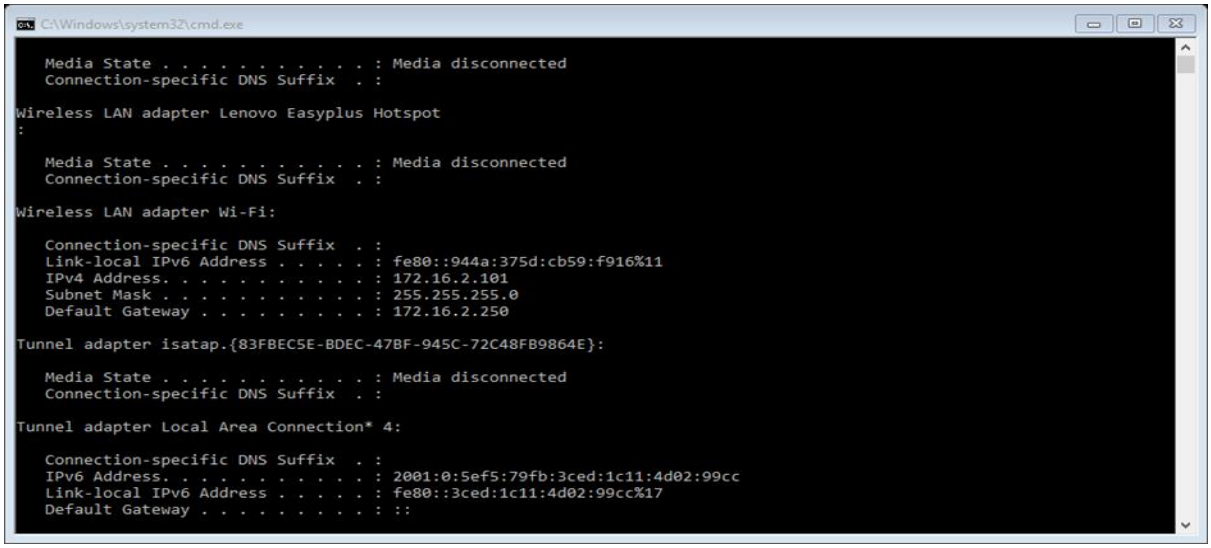
أدوات الشبكة الأساسية:

بعض الأدوات الأساسية التي يجب على المحقق الرقمي أن يمتلك خبرة كافية للتعامل معها هي **ping, IPConfig and tracert**

- **IPConfig**:

هي أول أداة يجب أن يستخدمها المحقق الرقمي لمعرفة حالة الشبكة في الجهاز الذي يقوم بفحصه وهي تقدم معلومات عن حالة الشبكة تتضمن عنوان **MAC address** وعنوان **IP** ويمكن استخدامها في سطر الأوامر الخاص بنظام **windows**

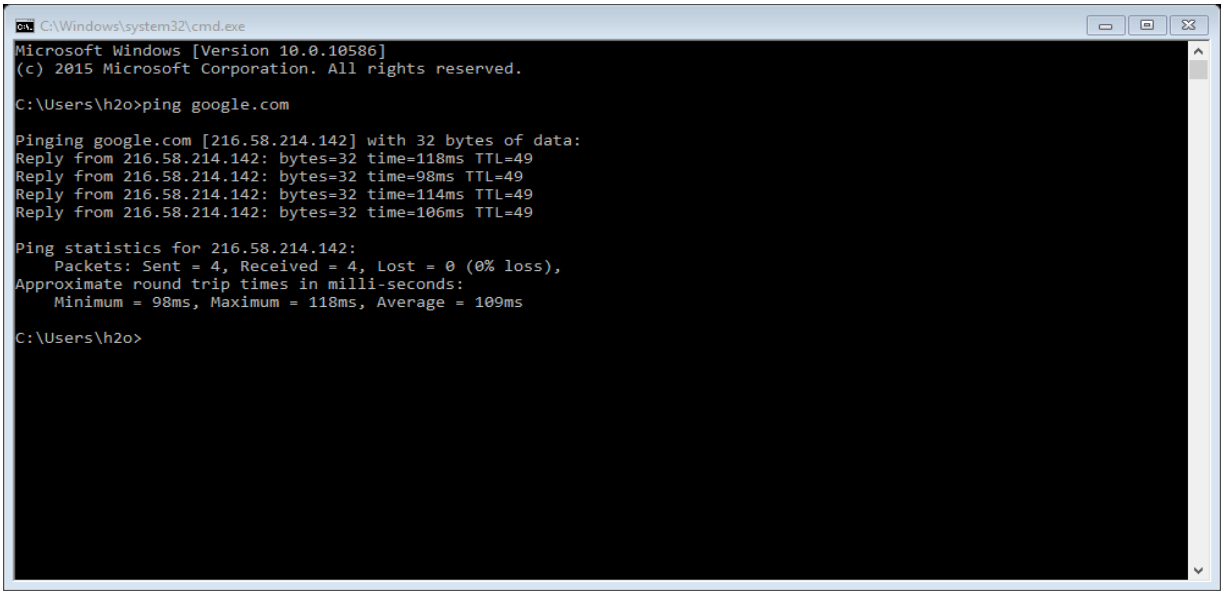
نتيجة كتابة التعليمة **ipconfig** في سطر الأوامر في **windows** يظهر بالشكل التالي:



هذه التعليمة تعطي بعض المعلومات عن حالة الاتصال بالشبكة (أو الانترنت) كعنوان **IP** للجهاز وعنوان **IP for default gateway**

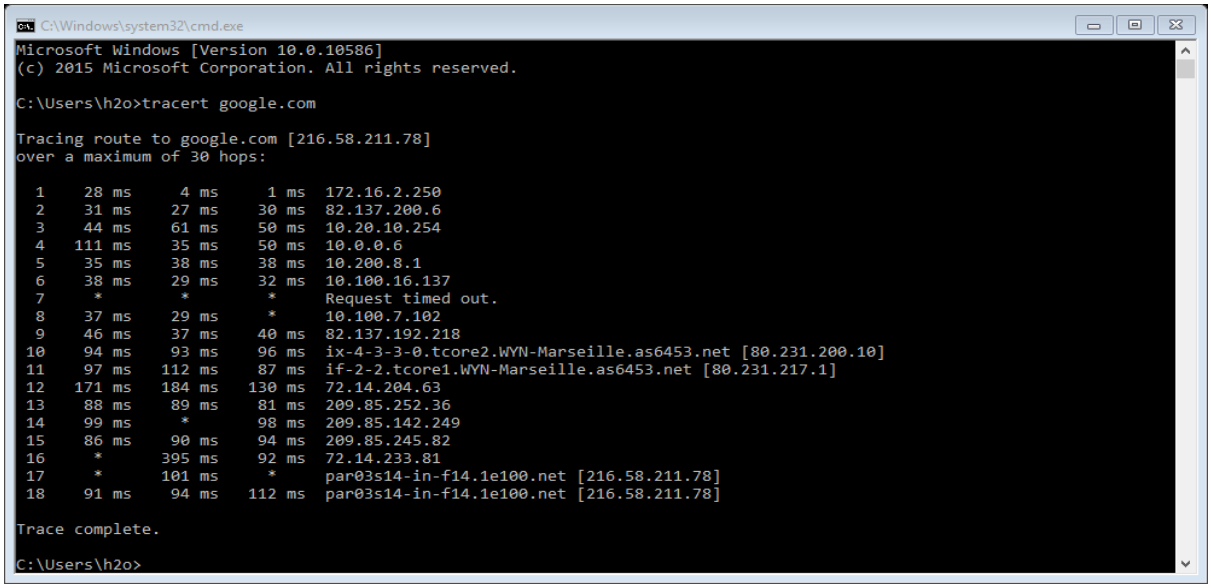
(التعليمة المقابلة لها في **linux** هي **ifconfig**)

- **Ping**: تستخدم لاكتشاف حالة الأجهزة المتصلة بالشبكة من خلال إرسال حزم بيانات وانتظار الرد على هذه البيانات



- **tracert**: تقوم بتحديد مسار حزم البيانات

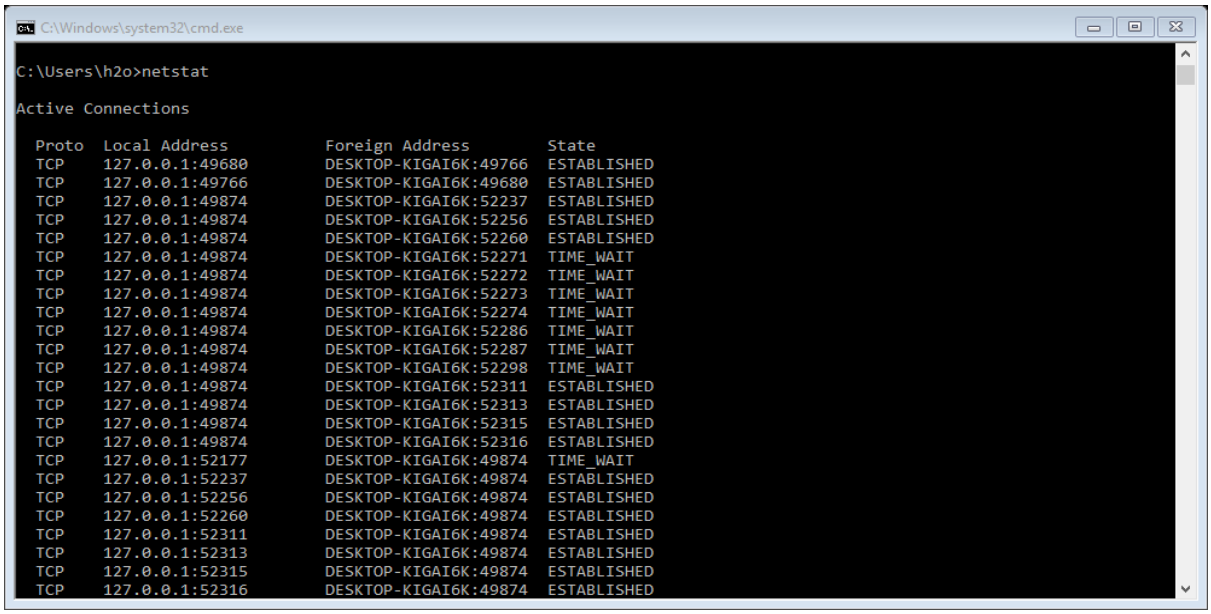
(التعليمة المقابلة لها في **linux** هي **traceroute**)



- **Netstat**:

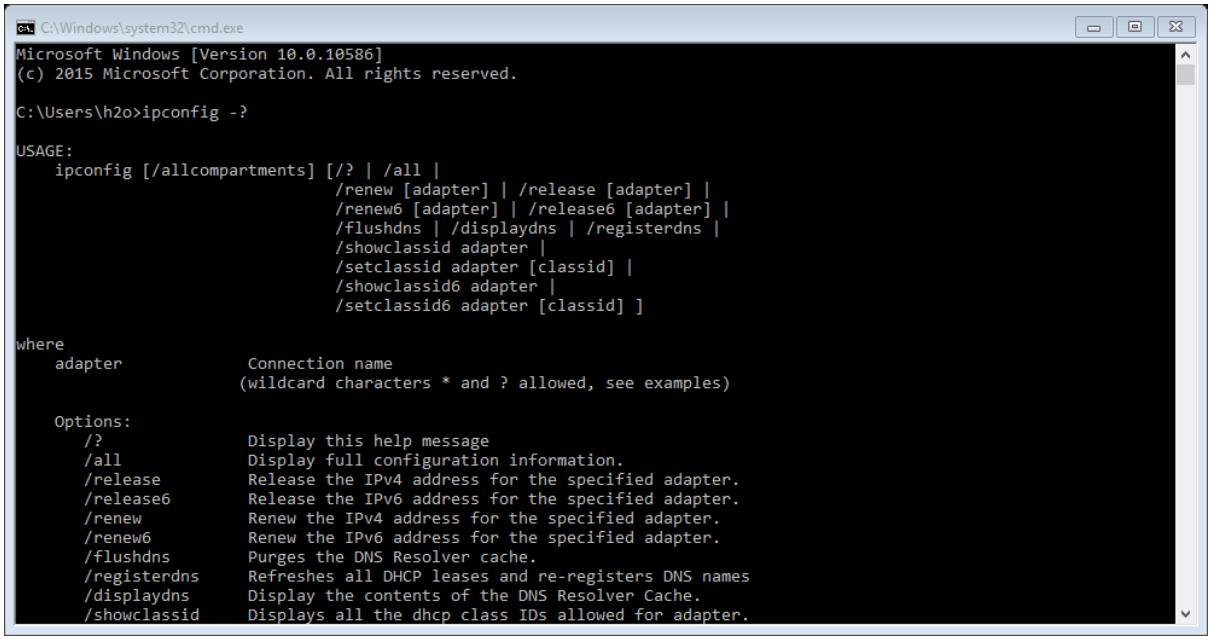
اختصار ل **Network status**

وتظهر حالة الاتصالات الجارية وهي مهمة جداً في التحليل الجنائي الرقمي لأنها تمكن المحقق من اكتشاف الاتصالات المشبوهة التي يمكن أن تكون جزء من عملية الاختراق.



كل التعليمات السابقة يمكن أن تستخدم بشكل أوسع من خلال إضافة خيارات معينة للقيام بمهام إضافية.

التعليمة **ipconfig -?** تظهر كل الخيارات المتاحة



حماية مكان الجريمة:

في الجرائم العادية كالسرقة أو القتل يتم إغلاق مكان الجريمة بشكل فوري ومنع أي شخص من الاقتراب والسماح فقط لعناصر الشرطة بالوصول لمكان الجريمة للقيام بعملية جمع الأدلة وبشكل مماثل في الجرائم المعلوماتية فيجب حماية وإغلاق مكان الجريمة بشكل فوري ومنع الوصول إلى أجهزة الحاسب وأجهزة الشبكة.

أول مهمة يجب القيام بها عند الوصول إلى مكان الجريمة هو حماية هذا المكان ومنع أي شخص من الاقتراب من الجهاز المشبوه به أو الجهاز الهدف

وعدم إيقاف تشغيل الجهاز بشكل فوري للمحافظة على الأدلة الرقمية المتوفرة ضمنه.

يجب التأكد بأنه لا يمكن لأحد أن يصل إلى هذا الجهاز عن بعد (عبر الشبكة) مثلاً في حال وجود جهاز حاسب محمول أو جهاز موبايل يجب إيقاف تشغيل بطاقة الشبكة اللاسلكية وعزل الجهاز عن أي اتصال بالشبكة أو الانترنت والبدء باكتشاف وتسجيل كل العمليات الجارية والبرامج المفتوحة واتصالات الشبكة الحالية ومن ثم إيقاف تشغيل الجهاز والبدء بعملية جمع الأجهزة المشبوهة ووضعها في أكياس أو علب خاصة ونقلها إلى مخبر التحليل الجنائي الرقمي داخل الفرع.

التعامل مع الدليل الرقمي:

بعد حماية مكان الجريمة يجب الحذر عند التعامل مع الجهاز للمحافظة على الدليل الرقمي، أول مهمة يجب على المحقق الرقمي القيام بها هي إنشاء صورة طبق الأصل للقرص الصلب **bit stream image** ومن ثم القيام بعمليات التحقيق الجنائي الرقمي على الصورة المأخوذة وليس على الجهاز الأصلي.

من المهم أيضاً استخدام جهاز يمنع عملية الكتابة على القرص الصلب **write blocker**

يمكن إنشاء صورة مطابقة للنظام الهدف باستخدام أدوات مثل:

Forensic Toolkit or EnCase

كما يمكن القيام بهذه العملية باستخدام أدوات مجانية تعمل على نظام التشغيل **linux**.

من أجل إنشاء صورة مطابقة للنظام الهدف باستخدام نظام التشغيل **linux** فنحن بحاجة لنسخة من نظام **linux** قابلة للإقلاع (يمكن أن تكون أي توزيعه **linux** ولكن يفضل استخدام توزيعه **kali linux** لأنها تحوي على أدوات مُعدة للاستخدام في التحليل الجنائي الرقمي)

الأداة dd (disk to disk):

هي أداة تعمل من خلال سطر الأوامر وموجودة بشكل تلقائي في العديد من توزيعات **linux** تستخدم لنقل ونسخ الملفات بين الأقراص ويمكن من خلالها إنشاء صورة طبق الأصل للقرص الصلب في الجهاز الهدف باستخدام التعليمة التالية:

```
dd if=<source> of=<destination> bs=<byte size>
```

مثلاً:

```
dd if=/dev/sda2 of=/dev/sdb2 bs=512
```

هذه التعليمة سوف تقوم بإنشاء نسخة طبق الأصل **bit-by-bit copy** من القرص **sda2** إلى القرص **sdb2**

كما يمكن القيام بهذه العملية عبر الشبكة، كما في المثال التالي:

البداية باستخدام التعليمة التالية على جهاز المحقق:

```
nc -1 -p 8888 > evidence.dd
```

هذه التعليمة تجعل الجهاز ينصت على المنفذ **8888** ويقوم بحفظ البيانات التي يتم استقبالها في الملف **evidence.dd**

ومن ثم استخدام التعليمة التالية في الجهاز الهدف من أجل إرسال صورة طبق الأصل للقرص الصلب عبر الشبكة إلى جهاز المحقق

```
dd if=/dev/hda1 | nc 192.168.0.2 8888 -w 3
```

في المثال السابق نفترض أن القرص المراد نسخه له الاسم **hda1** وعنوان **IP** الخاص بجهاز المحقق هو **192.168.0.2** يجب أن تقوم باستبدال هذه القيم بحسب الحالة التي تعمل عليها.

بعد الانتهاء من إنشاء الصورة المطابقة يجب أن نقوم بحساب قيمة الهاش **hash** (خوارزمية تشفير) لكل من القرص الصلب الأصلي وللصورة لنتأكد من أن العملية تمت بشكل صحيح وحفظ هذه القيمة ليتم حفظ الصورة كدليل رقمي يمكن اعتماده من قبل المحكمة.

كل أدوات التحليل الجنائي الرقمي تقوم بهذه العملية بشكل اتوماتيكي، كما يمكن القيام بها بشكل يدوي باستخدام التعليمة التالية في نظام **linux**:

```
md5sum /dev/hda1
```

المحقق الرقمي يجب أن يقوم بتسجيل وتوثيق كل عملية قام بها وكل الأدوات التي قام باستخدامها وكيف قام باستخراج الدليل الرقمي والطريقة المستخدمة في نقل وحفظ هذا الدليل.

الدليل الرقمي

محتوى هذا الفصل:

- الدليل الرقمي المعتمد من قبل المحكمة.
- المعيار القضائي.
- عملية الفحص والحصول على الدليل الرقمي.
- حماية الدليل الرقمي.
- **AccessData Forensic Toolkit and EnCase**
- أماكن وجود الدليل الرقمي.

مقدمة:

الدليل الرقمي المعتمد من قبل المحكمة يمكن أن يكون أحد الأمور التالية:

- الأقراص الصلبة
- سجلات النظام **system logs**
- وسائط التخزين الخارجية **(USB)**
- سجلات المُوجه **router logs**
- رسائل البريد الالكتروني
- سجلات المحادثات
- أجهزة الهاتف
- شريحة الهاتف **SIM card**
- سجلات أجهزة الحماية (الجدار الناري **firewall** أو أجهزة كشف الاختراق **IDS**)
- سجلات قواعد البيانات

الدليل الرقمي يختلف بحسب الجريمة، مثلاً في حالات الابتزاز عبر الانترنت يمكن اعتماد رسائل البريد الالكتروني وسجلات المحادثة على أنها دليل رقمي وفي حالة اختراق منظومة معلوماتية يمكن اعتماد سجلات النظام وسجلات أجهزة الحماية.

المعيار القضائي:

هو حجر الزاوية في أي عملية تحليل جنائي.

الدليل الرقمي وطريقة استخراجه يجب أن تكون متوافقة مع المعايير القضائية ليتم اعتماد هذا الدليل في المحكمة.

ويجب أن نأخذ بعين الاعتبار تاريخ انتقال الدليل الرقمي من مكان لآخر ومن ضابط إلى آخر وكل عملية نقل يجب أن يتم توثيقها.

يجب المحافظة على الدليل الرقمي في مكان محمي ويجب توثيق كل مرة يتم الوصول إلى هذا الدليل.

التوثيق:

يجب على المحقق الرقمي توثيق كل شيء وكل العمليات التي قام بها في مكان الجريمة.

عند الوصول لمكان الجريمة يجب على المحقق القيام بعملية توثيق دقيقة كل الأحداث والعمليات الجارية والأشخاص الموجودين في مكان الجريمة وماهي الأجهزة المتصلة بالجهاز المشبوه والاتصالات الحالية بالشبكة ونوع الحاسب ونوع نظام التشغيل.

كما يجب على المحقق الرقمي أن يقوم بتوثيق الطريقة التي قام باستخدامها لنقل الدليل الرقمي إلى مخبر التحليل الجنائي الرقمي الخاص به وتوثيق كل أداة قام باستخدامها وكل عملية فحص قام بها.

عملية الفحص:

الفحص هو أهم جزء في عملية التحليل الجنائي الرقمي، عملية الفحص تتم من خلال الخطوات التالية:

- الفحص البصري: لتحديد حالة الجهاز الهدف ومكان وجوده والبيئة المحيطة به.
- نسخ الملفات: عملية نسخ الملفات ضرورية قبل البدء بأي فحص ودائماً يجب العمل على صورة طبق الأصل وعدم العمل على النسخة الأصلية.
- فحص الملفات: وتشمل عملية فحص القرص الصلب والذاكرة وشريحة الهاتف والأمور الأخرى المتعلقة بالجريمة.
- استخراج الدليل: تحديد المكان أو الملف الذي يحوي على الدليل الرقمي.

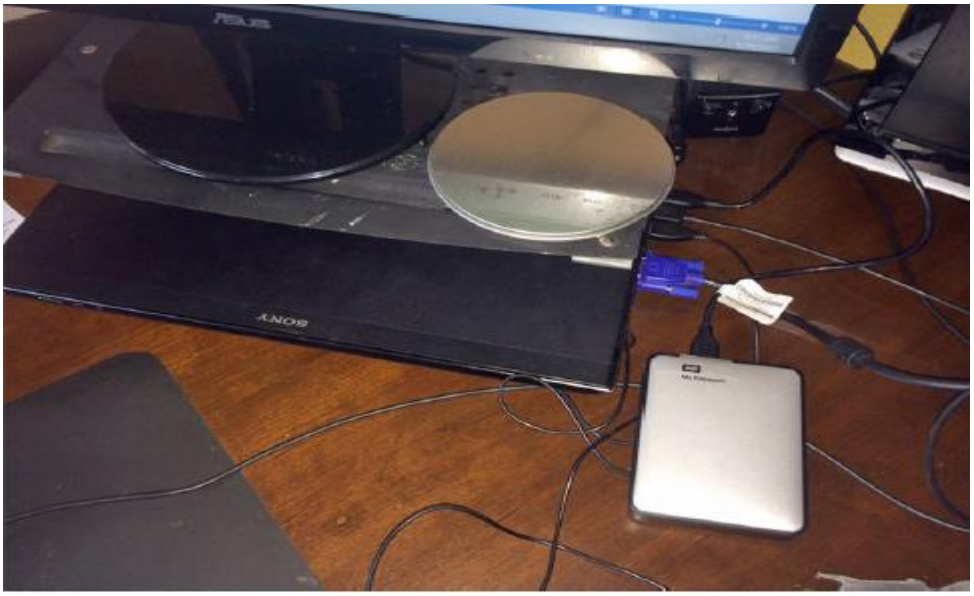
الحصول على الدليل الرقمي:

الغاية من عملية الفحص والتحليل هي الحصول على الدليل الرقمي وتوثيق مكان وجود هذا الدليل وكيفية استخراجه.

لنفترض الجريمة التالية: شخص يقوم بنشر صور إباحية لأطفال على الانترنت وبعد مداهمة منزل المتهم تم رؤية جهاز حاسب في غرفة المتهم.

أول مهمة يجب القيام بها توثيق حالة الجهاز من خلال إلتقاط صور للجهاز والمكان المحيط به والأجهزة المتصلة به و البرامج المفتوحة والعمليات

الجارية والاتصالات النشطة وتوثيق كل الأجهزة المتصلة بالحاسب (طابعة – ذاكرة خارجية) وتحديد أجهزة الشبكة المتصلة بالحاسب **(router or switch)** والبحث عن أي أجهزة هاتف أو ذواكر خارجية موجودة في منزل المتهم



كما يمكن التوثيق من خلال تصوير فديو لمكان ومعدات الجريمة ولكن يجب أن يتم التصوير من أكثر من زاوية وأن يظهر في الفيديو كل المعدات وبشكل واضح، كما يجب معرفة وتوثيق أسماء كل الأشخاص الموجودين في المنزل وعلاقتهم بالمتهم.

حماية الدليل الرقمي:

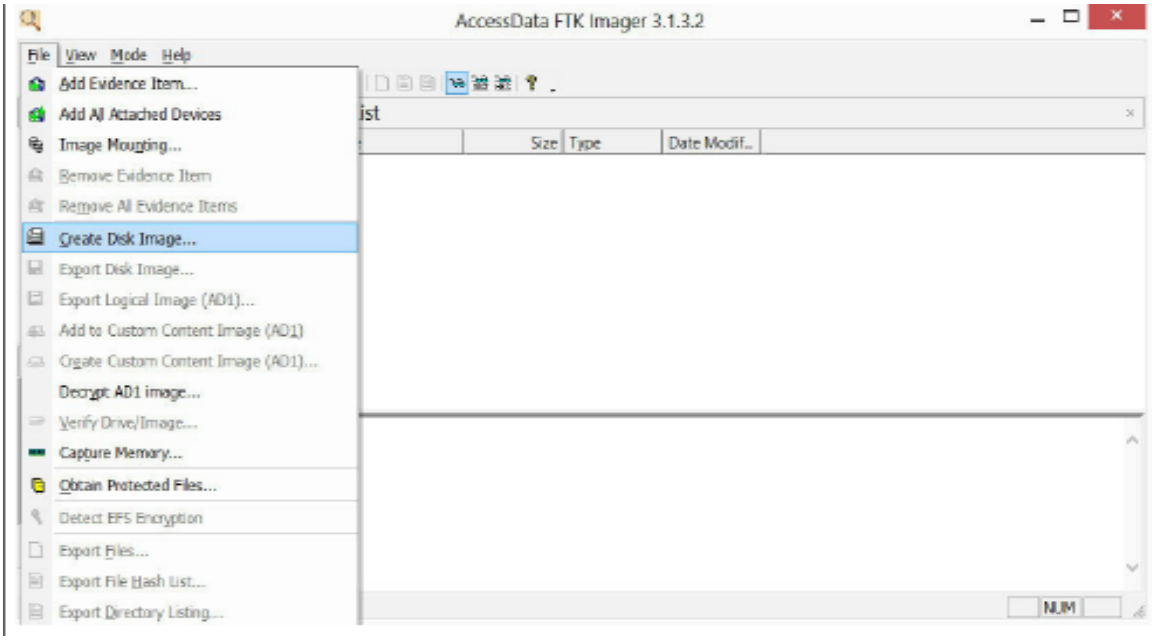
عند جمع الأدلة الرقمية يجب على المحقق الرقمي أن يحافظ على سلامة هذه الأدلة وهذا يتضمن عدم التعديل على الدليل الرقمي وعدم تخريبه.

المحافظة على الدليل الرقمي يجب أن تتم خلال مراحل الاستخراج والتحليل ونقل الدليل لذلك يجب العمل دائماً على نسخة طبق الأصل عن الدليل الرقمي ولا يجب العمل على الدليل الرقمي الأصلي بشكل مباشر وهذا هو سبب الحاجة لإنشاء صورة مطابقة للقرص الصلب في الجهاز الهدف.

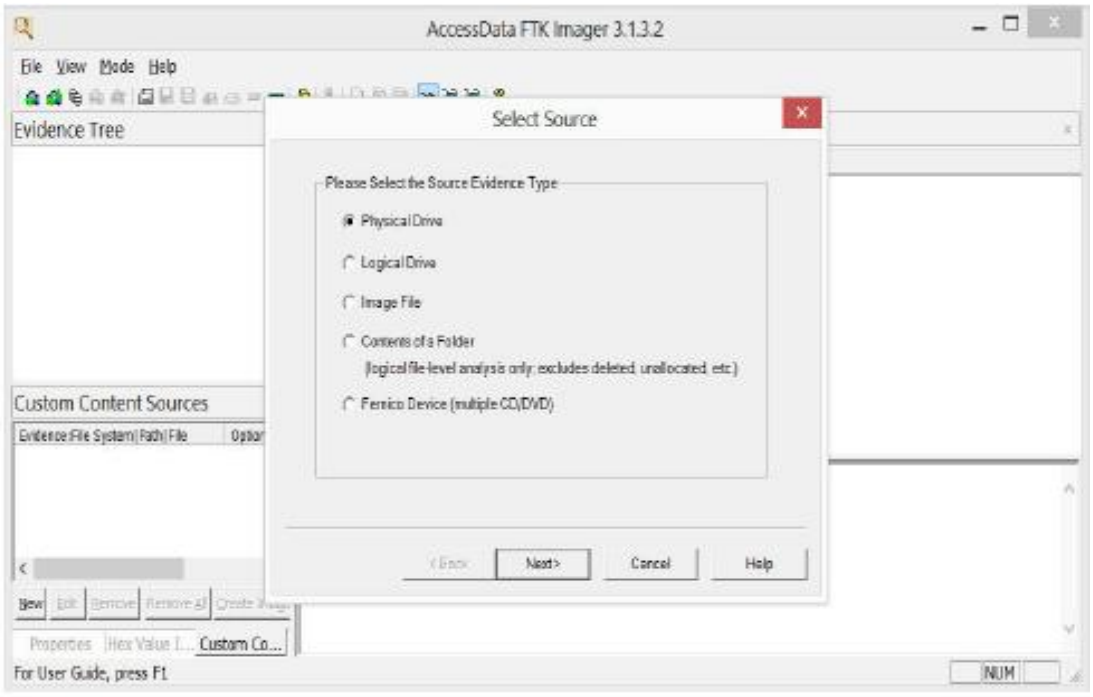
AccessData Forensic Toolkit:

هذه الأداة تسمح لنا بإنشاء صورة طبق الأصل للقرص الصلب.

بعد تحميل هذه الأداة وتنصيبها على الجهاز الهدف يمكننا خلق صورة مطابقة للقرص الصلب كما في الشكل التالي:



ومن ثم يمكننا تحدد نوع الدليل و المكان المراد حفظ الصورة فيه



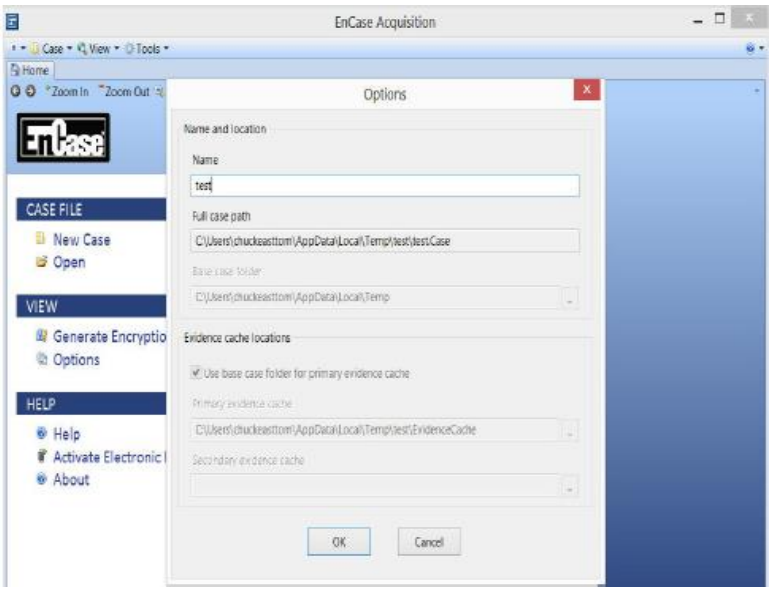
وبعد انتهاء هذه العملية سوف نحصل على صورة طبق الأصل للقرص المطلوب، يجب حساب قيمة الهاش **hash** لكل من الصورة والقرص الأصلي ومقارنة القيم وهذه الأداة يمكنها حساب الهاش المطلوب.

:EnCase

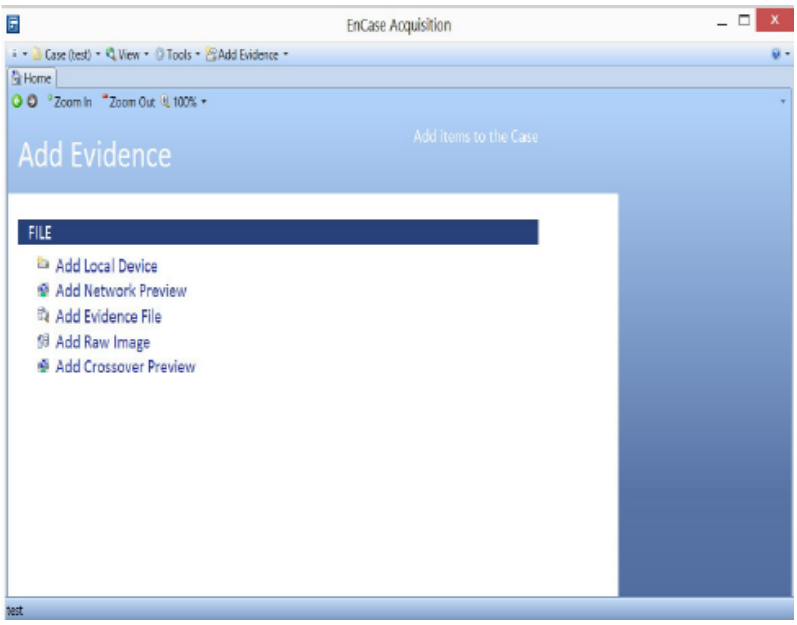
هذه الأداة تمكننا من خلق صورة طبق الأصل للقرص أو الجهاز الهدف.

في هذه الأداة كل جزء من الدليل الرقمي هو جزء من ملف القضية **case file**

أول خطوة هي إنشاء قضية جديدة أو اختيار قضية سابقة للعمل عليها



ومن ثم يمكننا إضافة الدليل الرقمي لهذه القضية



نسخ الملفات غير مفيد في عملية التحليل الجنائي الرقمي لأنه في عملية النسخ لن نحصل على الملفات المخفية والملفات المحذوفة أما في عملية إنشاء صورة مطابقة للنظام الهدف **bit by bit** فسوف نحصل على كل الملفات.

جهاز الحماية ضد الكتابة:

أحد أهم طرق حماية الدليل الرقمي هو استخدام جهاز منع الكتابة على القرص الصلب، يجب منع الكتابة على القرص الصلب بشكل فوري وذلك قبل البدء بإنشاء الصورة طبق الأصل.

العديد من أنظمة التشغيل تقوم بالكتابة على القرص الصلب وبشكل دوري لذلك يجب استخدام جهاز لمنع الكتابة على القرص الصلب.

يوجد عدة أنواع من أجهزة منع الكتابة وهي تختلف بحسب نوع الوصلة ويمكن أن تكون **SATA to SATA** أو **USB to SATA**

الجدول التالي يحوي أسماء وأنواع أجهزة منع الكتابة الأكثر استخداماً:

Name of Write Blocker	Type of Write Blocker
Tableau[6]	Hardware devices
WiebeTech[7]	Hardware devices
UltraWrite[8]	USB devices
ForensicSoft[9]	Software write blockers

بعض الأمور المهمة التي يجب أن نهتم بها لحماية الدليل الرقمي هي منع الحقول الكهربائية الساكنة لأنها يمكن أن تخرب الدليل الرقمي ويتم ذلك باستخدام حقيبة خاصة مصممة خصيصاً لمنع الحقول الكهربائية الساكنة والتي تستخدم من أجل حفظ الأدلة الرقمية.

مخبر التحليل الجنائي الرقمي يجب أن يكون معزول ولا يسمح بأي عملية اتصال مع الوسط الخارجي ويتم ذلك باستخدام شبكة من القضبان المعدنية التي تمنع الحقول الكهرومغناطيسية (قفص فراداي) وذلك لمنع الأجهزة من إرسال أو استقبال البيانات عن بعد عبر الشبكة اللاسلكية أو شبكة الموبايل.

عند العمل مع أجهزة الموبايل فمن الضروري عزل الجهاز عن الشبكة لأنه من الممكن حذف البيانات عن بعد (بعض أجهزة الموبايل تؤمن ميزة حذف البيانات عن بعد في حال فقدان أو سرقة الموبايل) ومن الممكن أيضاً الاتصال بالجهاز عبر الشبكة اللاسلكية أو عبر شبكة الموبايل والتعديل على البيانات.

من الممكن أن يكون الجهاز مصاب ببرمجية خبيثة تقوم بإرسال المعلومات إلى طرف خارجي عبر الشبكة لذلك من الضروري عزل الجهاز عن الشبكة.

حفظ الدليل:

حفظ الدليل هو أمر مهم جداً ويجب أن تتم عملية الحفظ في بيئة آمنة لا يمكن الوصول إليها من قبل أشخاص غير مصرح لهم ومن المهم أن تكون معزولة عن الحقول الكهرومغناطيسية.

ويجب أن يكون مكان الحفظ محمي من الحرائق وبعيد عن أنابيب المياه وأن يكون المكان مغلق ومقفول ويمنع أي شخص غير مصرح له من الاقتراب من هذا المكان كما يجب أن يكون مكان حفظ الدليل مراقب بشكل دائم.

أماكن وجود الدليل الرقمي:

الدليل الرقمي يمكن أن يكون في أحد الأماكن التالية:

- قواعد البيانات: مثل **SQL Server or Oracle**
- جهاز الحاسب: تاريخ تصفح الانترنت أو الملفات المحذوفة أو مفاتيح سجلات النظام في نظام **windows** أو السجلات **logs**
- الشبكة: البيانات عبر الشبكة والتي يمكن تحليلها باستخدام برنامج مثل **wireshark**
- جهاز الموبايل: سجل المكالمات والرسائل.

الدليل الرقمي يمكن أن يصنف بحسب الأمور التالية:

- المصدر: ما هو مصدر هذا الدليل (حاسب أو موبايل أو من الشبكة)
- طبيعة البيانات: ما هو نوع البيانات التي تم اعتمادها كدليل هل هي ملفات محذوفة تم استرجاعها أم أنها ملفات موجودة
- النوع: ويتضمن صور أو فديو أو علامات مرجعية **bookmarks** أو مُعرفات الجلسة **cookies** أو سجلات المُخدّم **server logs**

الدليل الرقمي يمكن أن يكون في القرص الصلب أو في الذاكرة أو يمكن أن يكون في البيانات التي يتم إلتقاطها من اتصالات الشبكة أو في وسائط التخزين الخارجية.

خلال عملية التحليل الجنائي الرقمي سوف نتعامل مع العديد من وسائط التخزين لذلك من المهم فهم أنواع هذه الوسائط.

تحليل الملفات

محتوى هذا الفصل:

- معلومات أساسية عن الملفات.
- تحليل ترويسة الملف.
- استخراج المعلومات الذاتية **Metadata** لملف
- **Caver Recovery**

مقدمة:

الملف عبارة عن سلسلة من الأصفار و الواحدات ويمكن أن يكون ملف نصي أو ملف تنفيذي أو صورة أو أي نوع آخر.

كل الملفات تبدأ بترويسة **header** وتنتهي بتذييل **footer**

تغيير لاحقة اسم الملف يجعله يبدو على أنه ملف آخر ولكن بنية الملف لن تتغير، ترويسة الملف تحوي على معلومات تحدد نوع الملف بغض النظر عن لاحقة اسمه.

في عملية التحليل الجنائي الرقمي فإن ترويسيه الملف تقدم لنا معلومات مفيدة عن طبيعة هذا الملف.

بعض المعلومات الأساسية عن الملفات:

- ترويسة الملف تبدأ من أول بايت **byte** من الملف وهي تحوي على معلومات عن طبيعة الملف حتى ولو تم تغيير لاحقة الاسم الخاص به.
- في الملفات الصورية فإن الترويسة تحوي على معلومات عن حجم الصورة وحزم الألوان.
- ملفات **ELF (Extensible Linking Format)** هي الملفات التنفيذية الخاصة في أنظمة التشغيل المبنية على **linux**، وعند فحص وتحليل جهاز يعمل بنظام **linux** من المهم فحص الترويسات الخاصة بهذه الملفات.

- الملفات **PE (Portable Executable)** هي الملفات التنفيذية في نظام **windows**
- ملفات حزمة تطبيقات **Microsoft Office** في **windows** تملك مُعرف عالمي فريد **GUID (Globally Unique ID)** وهذا يسمح لنا بتميزها عن الملفات الأخرى حتى ولو كانت بنفس الاسم (ولكنها موجودة في مجلد مختلف).

تحليل ترويسة الملفات:

المعلومات التي تحدد نوع الملف يتم حفظها في ترويسة الملف وهذه المعلومات تسمى البصمة الرقمية للملف **signature**

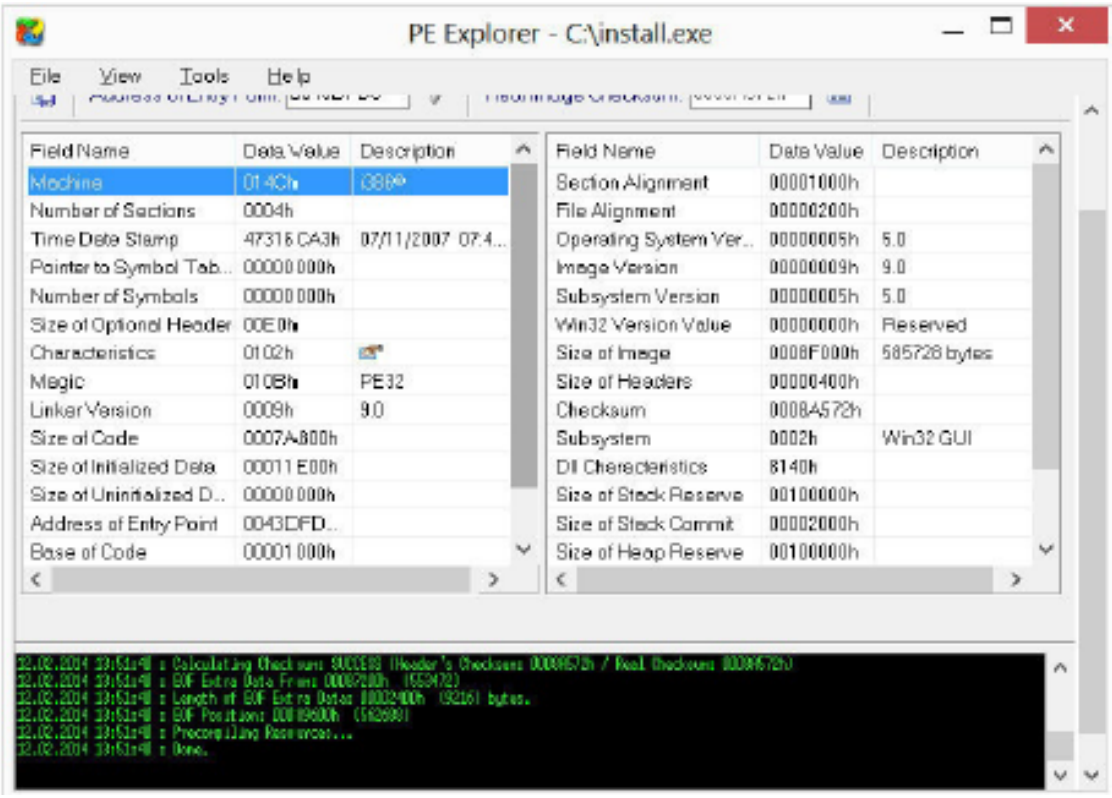
البصمة الرقمية للملف هي مُعرف فريد وهي التي تحدد نوع الملف ولاحقته.

كل ملف له ترويسة **header** وتذييل **footer** يحويان على معلومات عن طبيعة ونوع الملف ومحتوى هذا الملف وللحصول على هذه المعلومات يمكننا فتح الملف باستخدام **hex editor** مثل الأداة **HexEdit** التي تسمح لنا برؤية وتعديل المحتوى الموجود في الملف.

في الملفات التنفيذية (بغض النظر عن نظام التشغيل المصممة له) فإن الترويسة تصف عنوان الرماز والبيانات الخاصة بهذا الملف وتحتوي على قائمة بالتوابع التي يتم تصديرها عند تنفيذ هذا الملف.

عندما يتم تنفيذ الملف فإن نظام التشغيل يقوم بقراءة معلومات الترويسة لهذا الملف أولاً ومن ثم يقوم بتحميل البيانات من هذا الملف إلى المساحة التي سيقوم بحجزها لهذا الملف وفقاً للمعلومات الموجودة في الترويسة.

للقيام بعملية تحليل لترويسة الملف سوف نستخدم البرنامج **PE Explorer** كما يظهر في الشكل التالي:



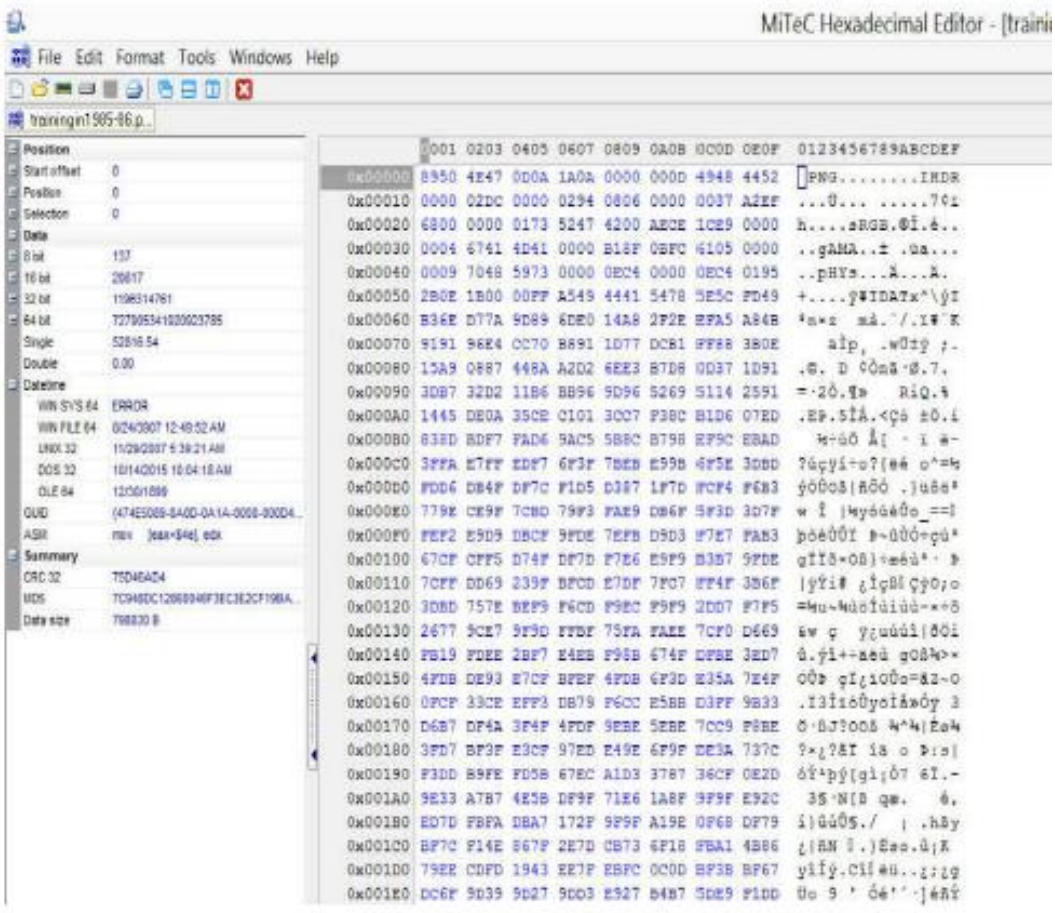
كما ترى فإن هذا البرنامج يعطينا معلومات عن تاريخ خلق هذا الملف وحجمه بالإضافة إلى معلومات أخرى.

عند التحقيق في جريمة معلوماتية وعند الاشتباه في ملف معين على أنه ملف لبرمجية خبيثة **malware** نقوم بمقارنة حجم الملف الذي يظهر في الترويسة (باستخدام برنامج مثل **PE Explorer**) مع حجم الملف كما يظهر

في **windows** وإذا وجدنا اختلاف فهذا يمكن أن يكون إشارة لوجود حصان طروادة **Trojan Horse**

يوجد العديد من برامج **hex editors** والتي تقوم بعرض محتوى الملف بشكل سته عشري **hexadecimal**

في المثال التالي قمت باستخدام **MiTeC Hexadecimal Editor** لفتح ملف صورة **PNG** والنتيجة كما في الشكل التالي:



لأنك غير معتاد على قراءة الملفات بالشكل السته عشري فسوف تعتقد بأن هذه الأداة غير مفيدة.

في البداية لاحظ في الجانب الأيمن أن نوع الملف هو من نوع **PNG** بغض النظر عن لاحقة الاسم لهذا الملف (يمكن أن يتم تغييرها) وبهذه الطريقة يمكننا معرفة نوع الملف الأصلي حتى ولو تم تغيير لاحقة الاسم.

استخراج المعلومات الذاتية لملف Metadata:

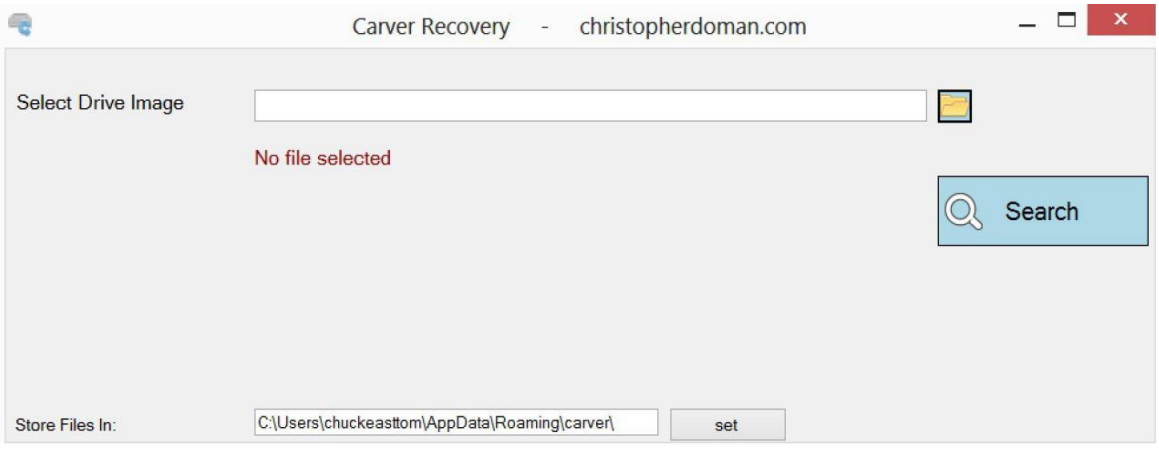
Data carving: هي عملية محاولة استخراج معلومات من مجموعة بيانات كبيرة

File caving: تتم عادةً لاستعادة واستخراج البيانات من القرص الصلب عندما يكون الملف المطلوب قد تعرض للتخريب

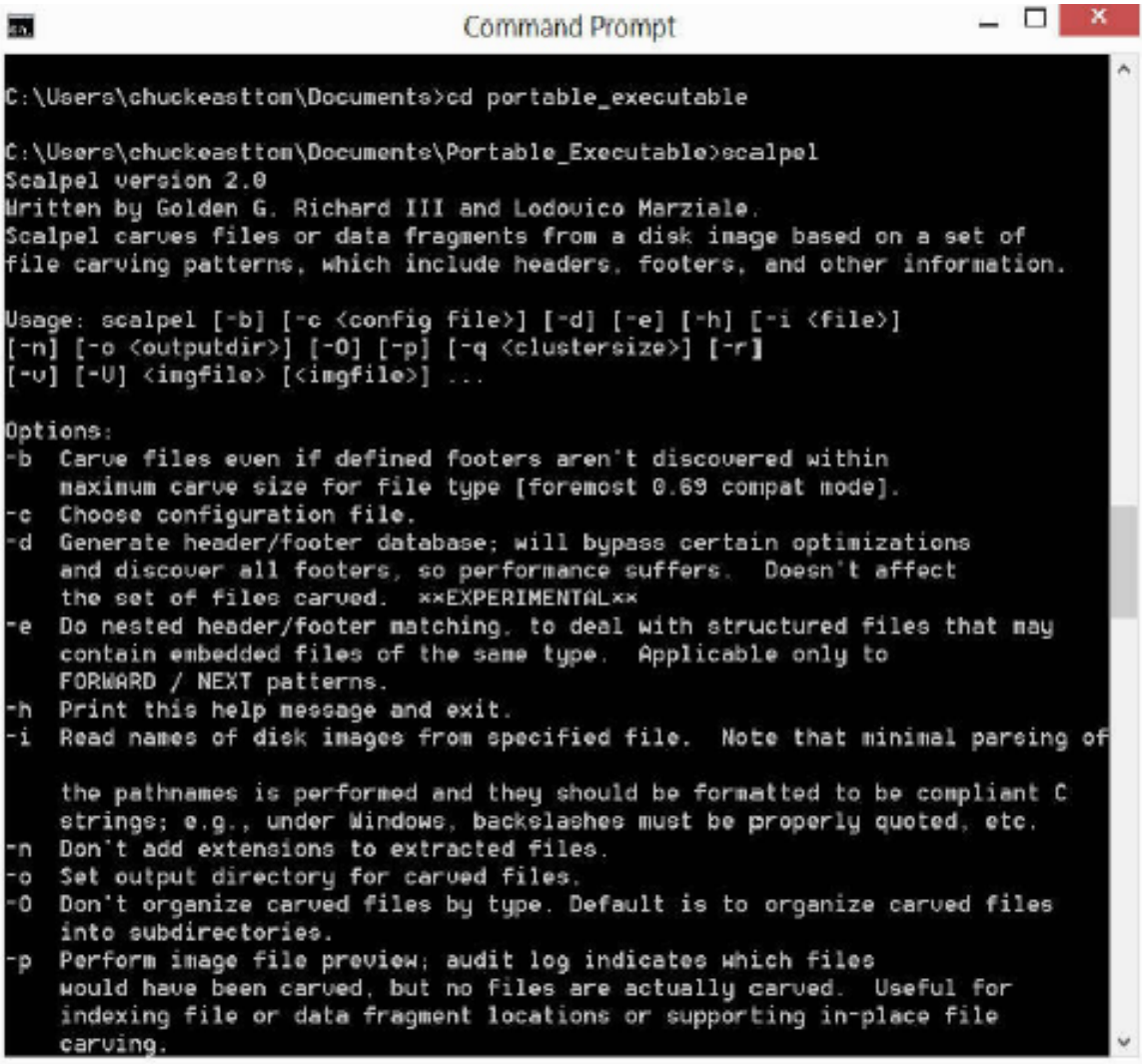
معظم أدوات **file carving** تعمل من خلال البحث في ترويسة وذيل الملف عن المعلومات المطلوبة.

Caver Recovery:

هذه الأداة المجانية تسمح لنا باختيار الصورة طبق الأصل للجهاز الهدف وتقوم بمحاولة استعادة الملفات كما يظهر بالشكل التالي:



كما أن هذه الأداة تحتوي على برنامج يسمى **Scalpel** يعمل من خلال سطر الأوامر كما يظهر في الشكل التالي:



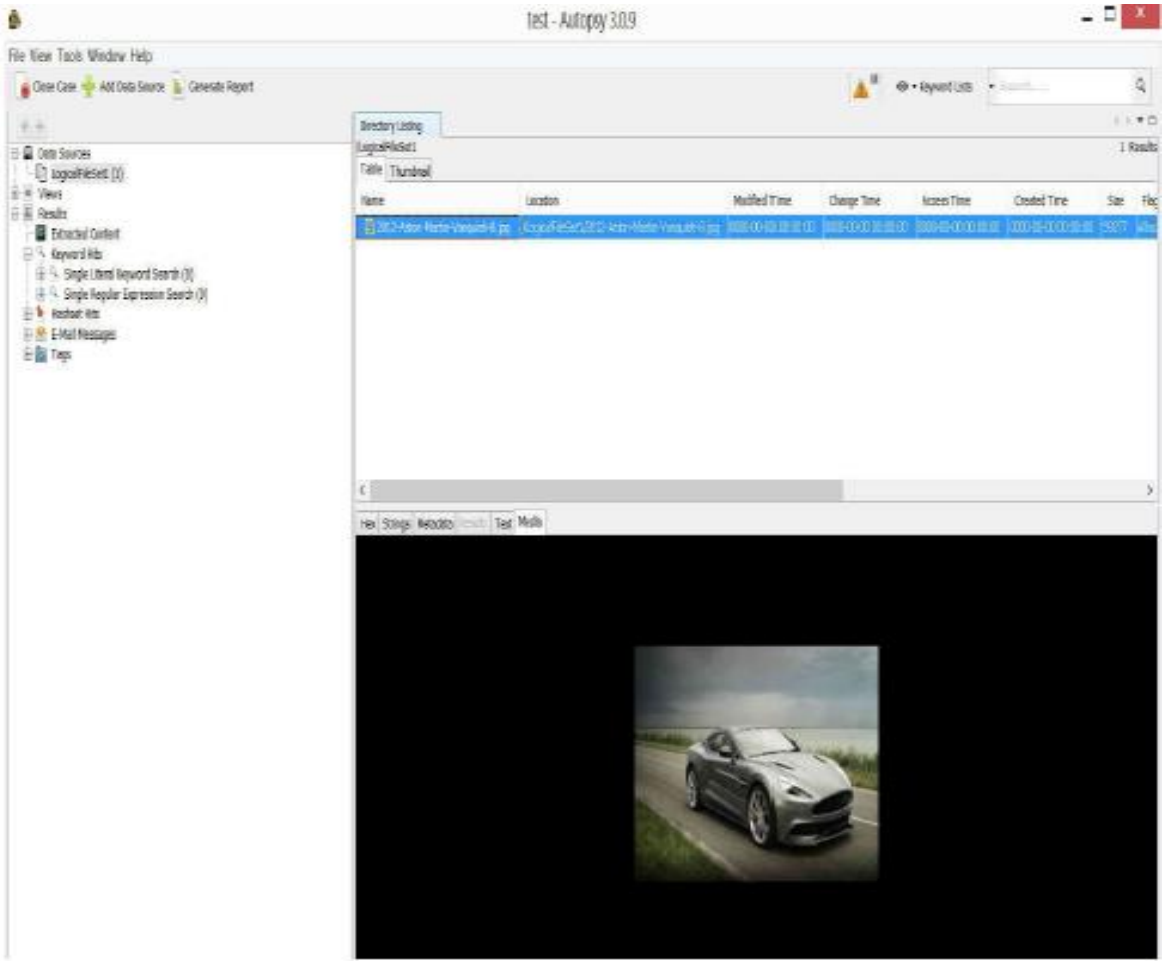
المعلومات الذاتية Metadata:

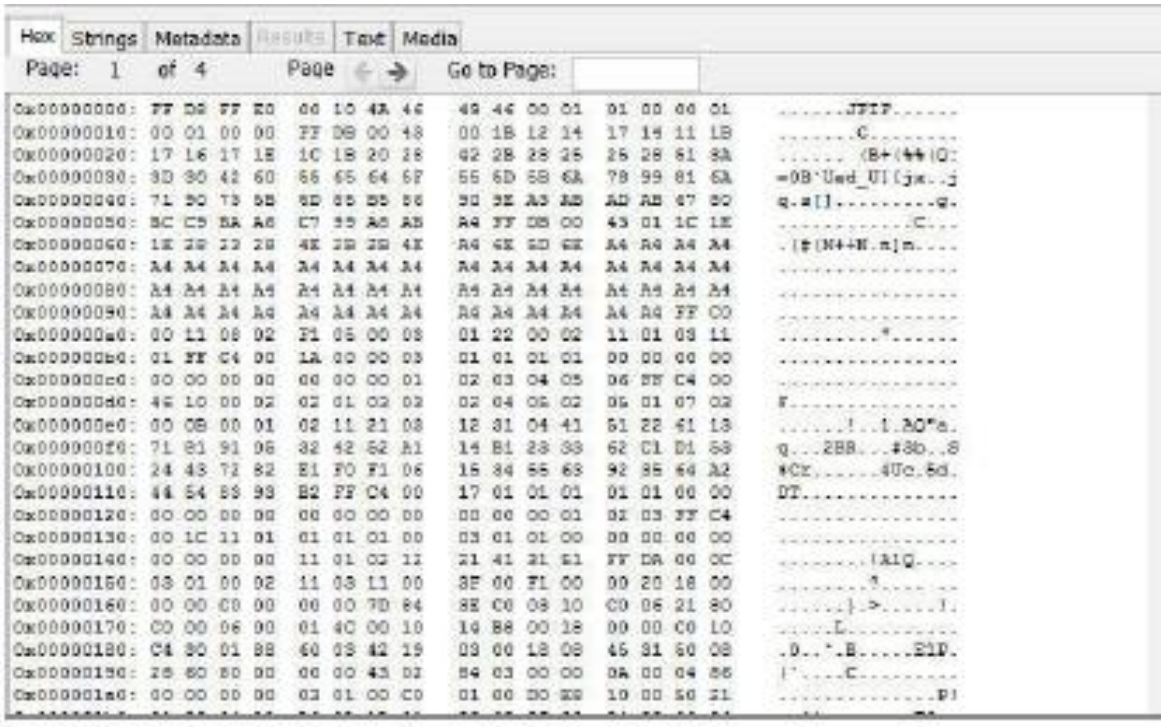
وهي بيانات عن البيانات أو معلومات ذاتية عن الملفات وتحوي على تاريخ إنشاء الملف وتاريخ التعديل عليه وتاريخ أخر مرة تم فتح هذا الملف، في الملفات النصية فإن المعلومات الذاتية تحوي على اسم المستخدم الذي قام بإنشاء هذا الملف وهذه المعلومات مفيدة جداً في عملية التحليل الجنائي الرقمي.

يوجد العديد من الأدوات التي تساعد في عملية تحليل المعلومات الذاتية **analyze metadata** وأشهر هذه الأدوات المستخدمة في عملية التحليل الجنائي الرقمي هي الأداة **Sleuth Kit** وهي أداة مجانية وتحوي مجموعة من الأدوات المساعدة التي تعمل من خلال سطر الأوامر كما يوجد واجهة رسومية مجانية لهذه الأدوات تسمى **Autopsy**

الشكل التالي يظهر استخدام **Autopsy** لتحليل ملف صورة **JPEG**

بمجرد تحميل هذا الملف سوف تظهر المعلومات الذاتية الخاصة به مثل تاريخ الإنشاء وتاريخ التعديل وتاريخ أخر مرة تم فيها فتح هذا الملف.





في المثال السابق قمنا باستخراج المعلومات الذاتية لصورة وهذه العملية يمكن أن تتم على أي ملف أخر مهما كان نوعه.

خطوات التحليل الجنائي الرقمي

محتوى هذا الفصل:

- تحديد العمليات الحالية.
- تحديد اتصالات الشبكة الحالية.
- التخطيط لعملية التحقيق.
- جمع الأدلة الرقمية.
- التحقق من الدليل الرقمي.
- إعداد التقرير.

مقدمة:

في بعض الحالات يجب أن نقوم بإيقاف تشغيل الجهاز ونقله إلى مخبر التحليل الجنائي الرقمي داخل الفرع.

العديد من الناس يعتقدون أن إيقاف تشغيل الجهاز هو الخطوة الأول للحفاظ على الدليل الرقمي ولكن هذه العملية يمكن أن تسبب فقدان للمعلومات في بعض الحالات.

إذا كانت القضية هي برمجية خبيثة **malware** تعمل حالياً على الجهاز المصاب أو كان الدليل الرقمي موجود في الذاكرة أو كان الدليل الرقمي هو اتصال حالي بالشبكة في مثل هذه الحالات فإن إيقاف تشغيل الجهاز سوف يؤدي إلى فقدان الدليل الرقمي، لذلك من المهم أن نفهم القضية وطبيعة الدليل الرقمي قبل التفكير بإيقاف تشغيل الجهاز.

في بعض الحالات يجب أن نقوم بجمع الأدلة الرقمية بشكل فوري قبل إيقاف تشغيل الجهاز.

لا يوجد قاعدة معيارية ثابتة لترتيب خطوات عملية التحليل الجنائي الرقمي.

خطوات عملية التحليل الجنائي الرقمي:

1. التخطيط لعملية التحقيق.
2. تحديد العمليات الحالية.
3. تحديد اتصالات الشبكة الحالية.
4. جمع الأدلة الرقمية.
5. التحقق من الدليل الرقمي.
6. إعداد التقرير.

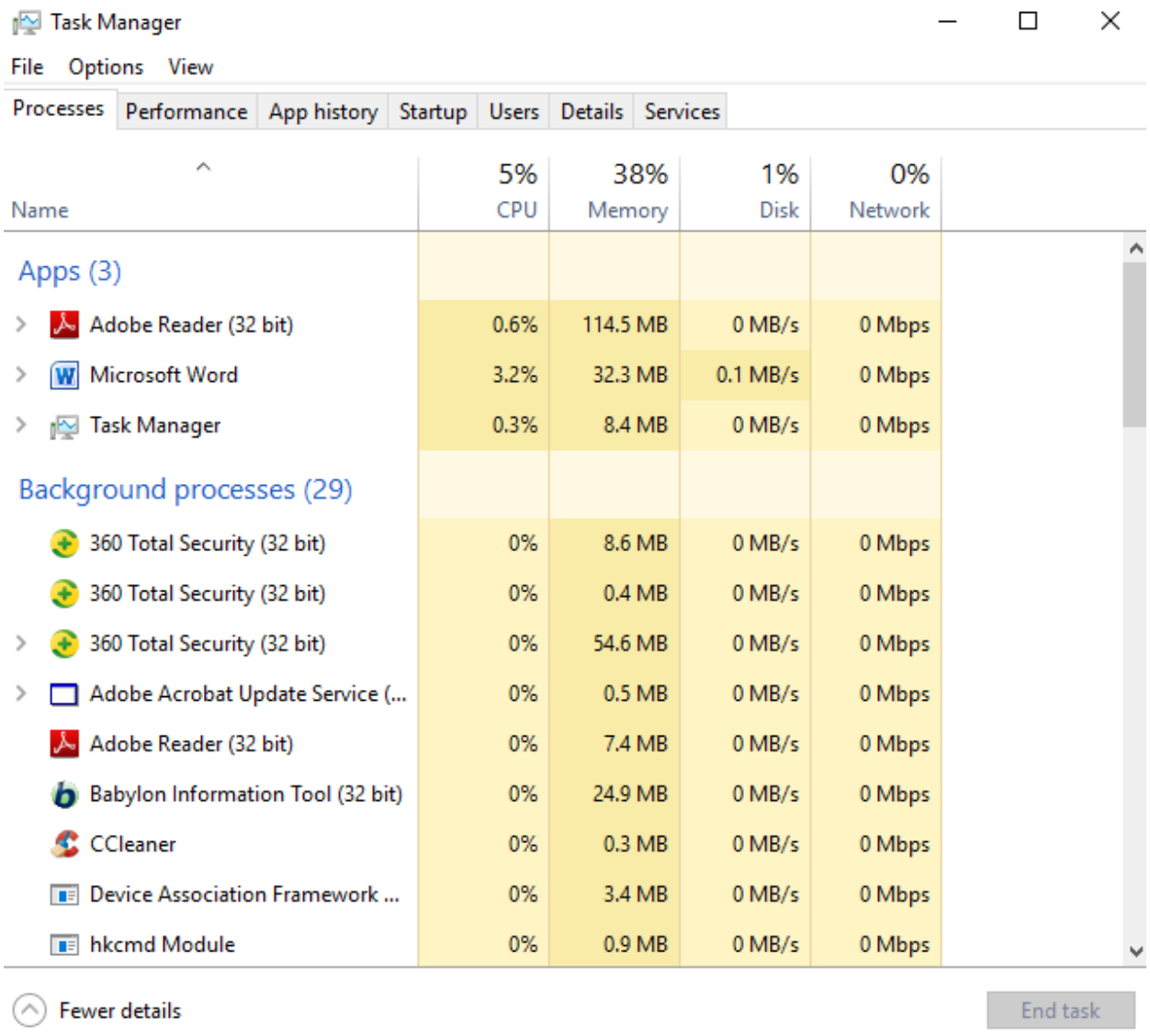
التخطيط لعملية التحقيق:

وضع خطة لمراحل وخطوات عملية التحقيق الرقمي هو أمر مهم وهذه الخطة يجب أن تشمل كيفية جمع الأدلة الرقمية وكيفية نقلها والحفاظ عليها ومن ثم كيفية تحليلها.

من المهم إعداد التقرير وتوثيق النتائج بشكل دقيق لنحصل على دليل رقمي يتم اعتماده من قبل المحكمة بشكل رسمي.

تحديد العمليات الحالية:

في نظام **windows** فإن الضغط على **CTRL, ALT and DELETE** ومن ثم اختيار مدير المهام **Task Manager** سوف يظهر العمليات الحالية التي تعمل على النظام، كما في الشكل التالي:

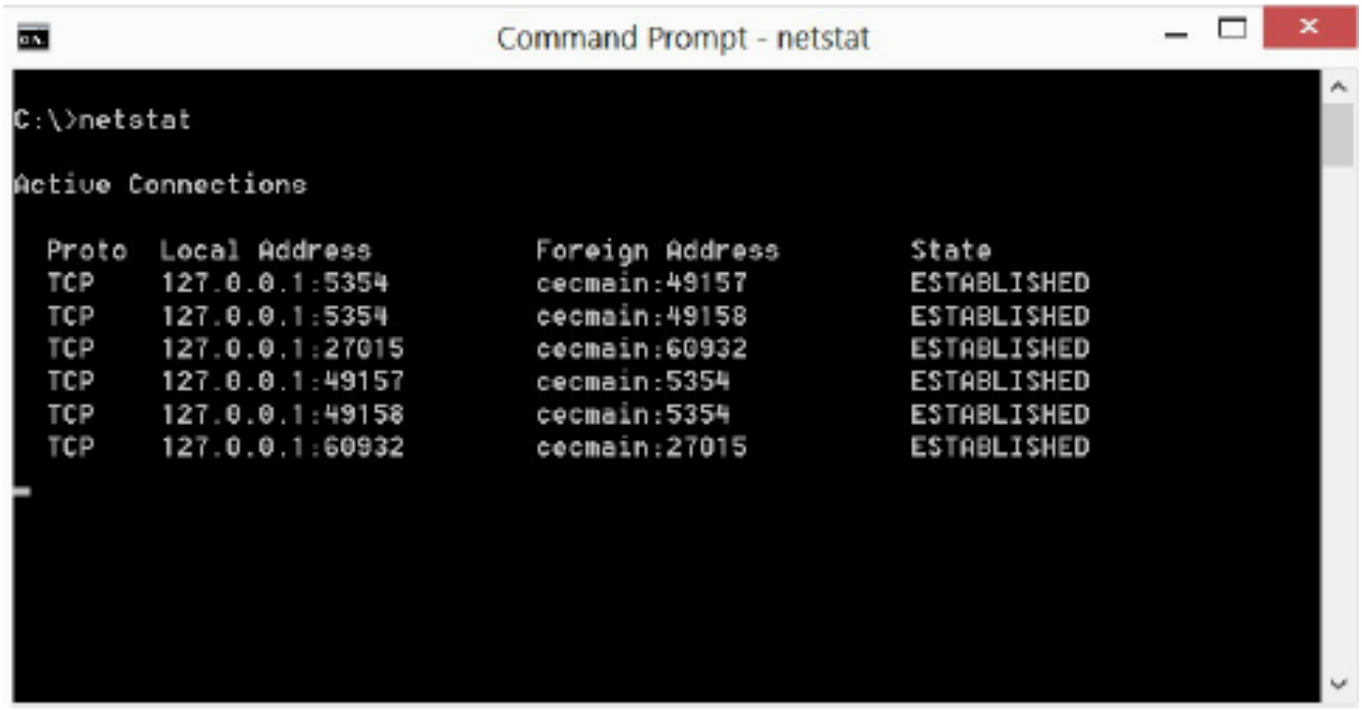


يجب أن نقوم بأخذ لقطة للشاشة **Screen Shot** وحفظ الصورة التي تحوي على هذه النافذة لتوثيق كل العمليات التي تعمل حالياً وفي بعض الحالات يمكن أن تظهر عمليات خاصة ببرمجية خبيثة تعمل حالياً.

حالة الاتصالات بالشبكة:

يمكن معرفة كل الاتصالات الحالية بالشبكة من خلال التعليمة **netstat**

كما يظهر في الشكل التالي:



هذه التعليمة تعمل في كل من **windows and linux** وهي موجودة بشكل تلقائي في كل نظام تشغيل.

يوجد بعض الإضافات لهذه التعليمة والتي تساعد على كشف أو تحديد معلومات محددة وهي:

- **netstat -a**: تعرض كل اتصالات البرتوكول **TCP** الفعالة مع رقم المنفذ لكل اتصال.
- **netstat -p**: تعرض الاتصالات الخاصة ببرتوكول محدد مثل **TCP or ICMP**
- **netstat -o**: تعرض رقم العملية لكل اتصال **process ID**

- **netstat -r**: تعرض جدول التوجيه **routing table**

يمكننا استخدام هذه الأوامر بشكل مشترك كما في التعليمة التالية:

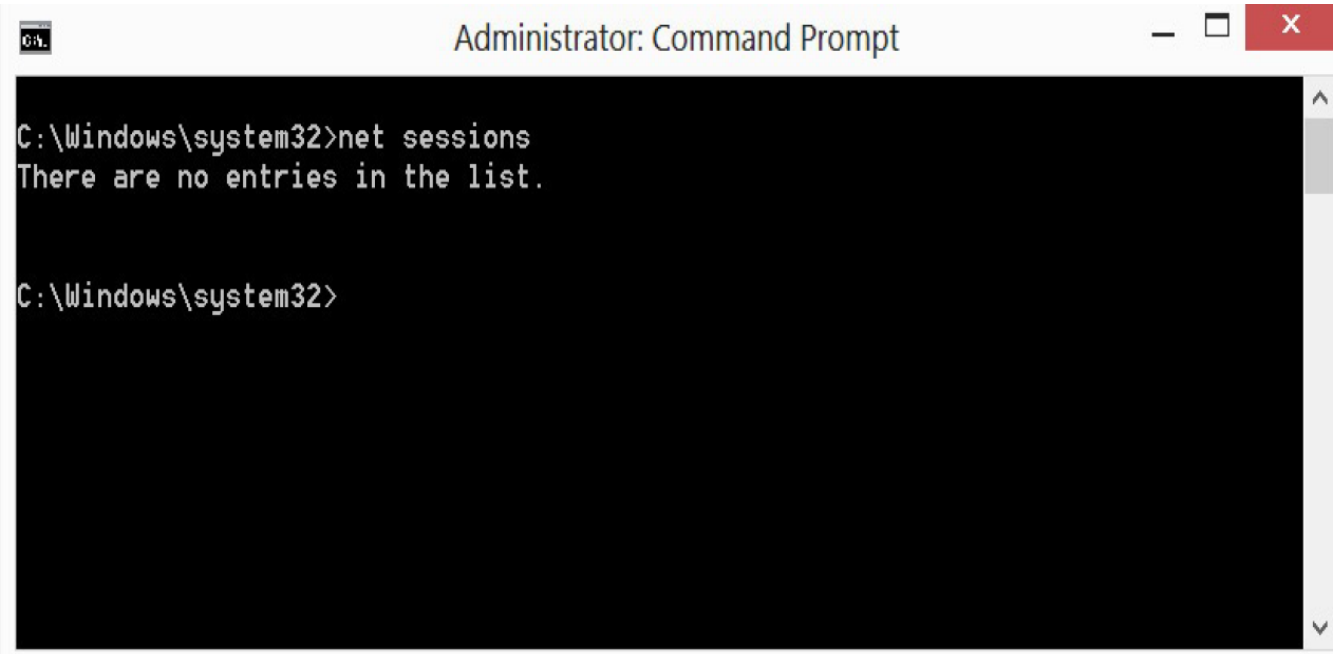
```
netstat -a -o
```

net session:

تعمل بشكل مشابه ل **netstat** ولكنها تقدم معلومات مفيدة بشكل أكبر.

netstata تقوم بعرض معلومات عن اتصالات غير مفيدة ولكن **net session** تقوم فقط بعرض الاتصالات التي تؤسس لجلسة عبر الشبكة (مثل أن يقوم شخص بتسجيل الدخول للنظام)

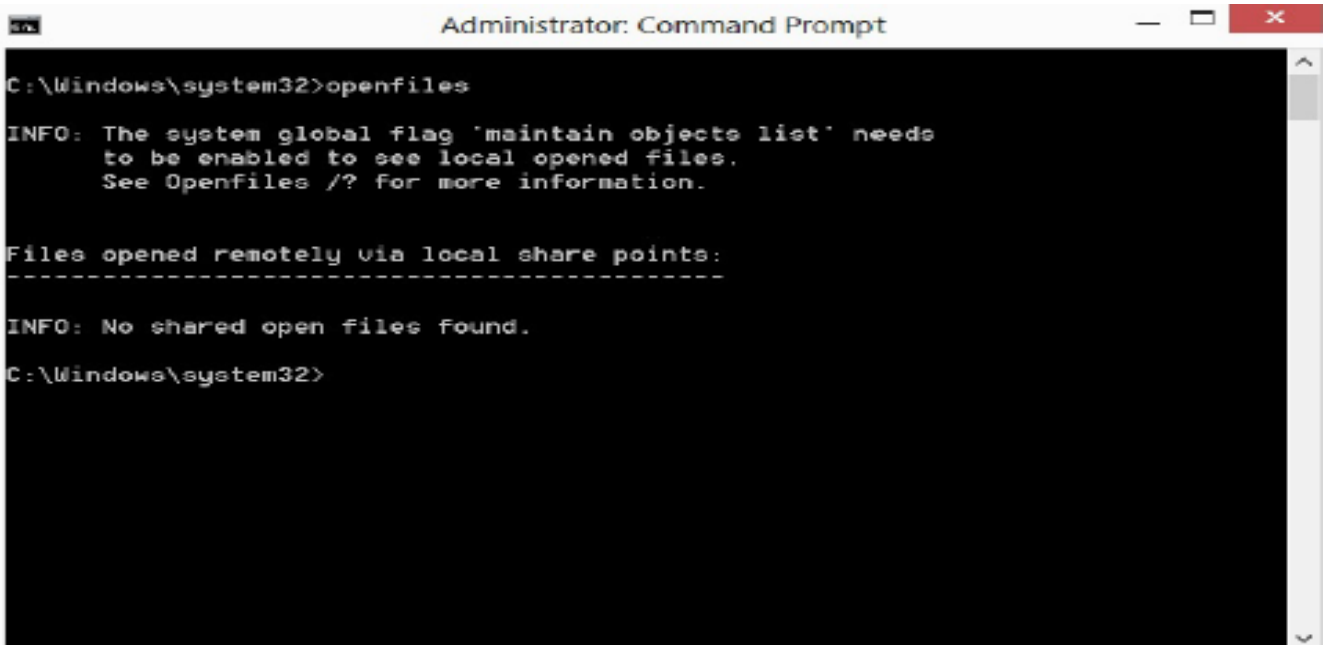
هذه التعليمة تحتاج لصلاحيات المدير لتعمل **run as administrator**



:openfiles

هذه التعليمة تقوم بعرض الملفات المسموح الوصول إليها عبر المشاركة وهي تحتاج لصلاحيات المدير لتعمل.

نتائج هذه التعليمة ستؤكد فيما إذا كان قد تم الوصول إلى بعض الملفات في الجهاز عن بعد عبر الشبكة.



يجب تنفيذ هذه التعليمات على الجهاز في مكان الجريمة وأخذ صورة للشاشة **Screen Shot** لنتيجة التنفيذ وهذا يسمح لنا بتحديد حالة الجهاز ومن ثم يمكننا إيقاف تشغيل الجهاز ونقله إلى مخبر التحليل الجنائي الرقمي داخل الفرع.

جمع الأدلة الرقمية:

أول سؤال يجب أن يتم الإجابة عنه هو كيف يمكننا الحصول على الدليل الرقمي؟؟

يوجد أنواع مختلفة من الأدلة الرقمية بحسب طبيعة الجريمة المرتكبة.

إذا كان الدليل الرقمي موجود في جهاز حاسب أو في جهاز موبايل يجب أن نقوم بنقل هذا الجهاز إلى المخبر داخل الفرع ويجب التأكد من منع الاتصال بهذا الجهاز أثناء عملية النقل (نقل الجهاز يتم من خلال حقيبة أو صندوق خاص يمنع أي اتصالات عبر الإشارات اللاسلكية)

وفي حال كان الدليل الرقمي في المُخدّم **(server)** الذي يحوي على عدد من مواقع الويب فمن الصعب قطع اتصال هذا الجهاز عن الشبكة أو حتى نقله لذلك وفي مثل هذه الحالة إذا كان يوجد مُخدّم احتياطي **backup** فنقوم بوصله على الشبكة لحين إنشاء صورة طبق الأصل للمُخدّم المصاب وإذا لم يكن يوجد نسخة احتياطية نقوم بقطع اتصال المُخدّم عن الشبكة بشكل مؤقت للقيام بإنشاء صورة طبق الأصل ومن ثم إعادته للعمل.

في بعض الحالات لا يمكننا الوصول إلى الجهاز المصاب ويجب أن نقوم بجمع الأدلة الرقمية عن بعد (في حالات اختراق أجهزة في منشأة عسكرية أو في سفارة رسمية) ومن الصعب الوصول لمكان تواجد هذا الجهاز لأسباب معينة فيمكننا استخراج الدليل الرقمي عن بعد وذلك من خلال إنشاء صورة طبق الأصل للجهاز المصاب عبر الشبكة.

التحقق من الدليل الرقمي:

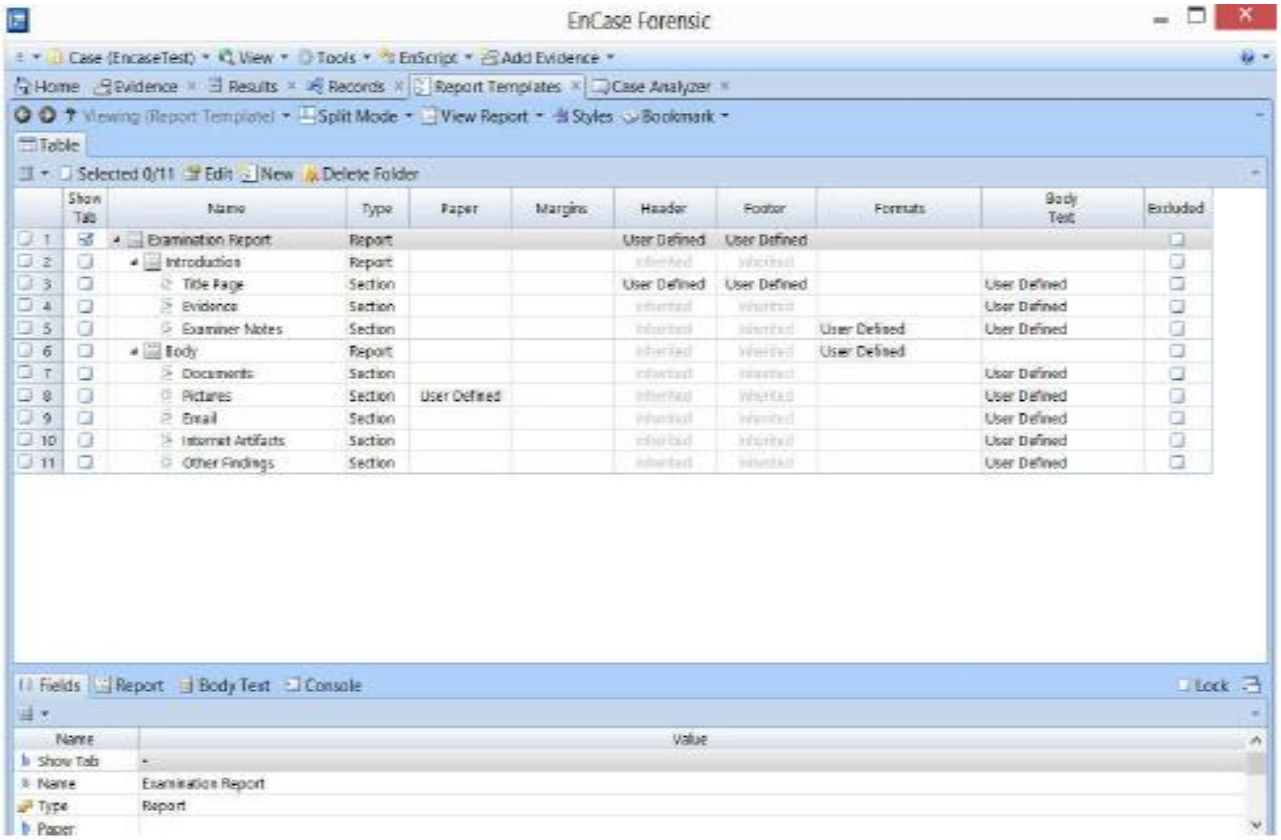
من المهم دائماً التحقق من الأدلة التي تم إيجادها لتجاوز احتمال وجود خطأ في الدليل الرقمي ويتم ذلك بإعادة خطوات التحليل وجمع الأدلة بأكثر من أداة مختلفة ومقارنة النتائج التي نحصل عليها.

إعداد التقرير:

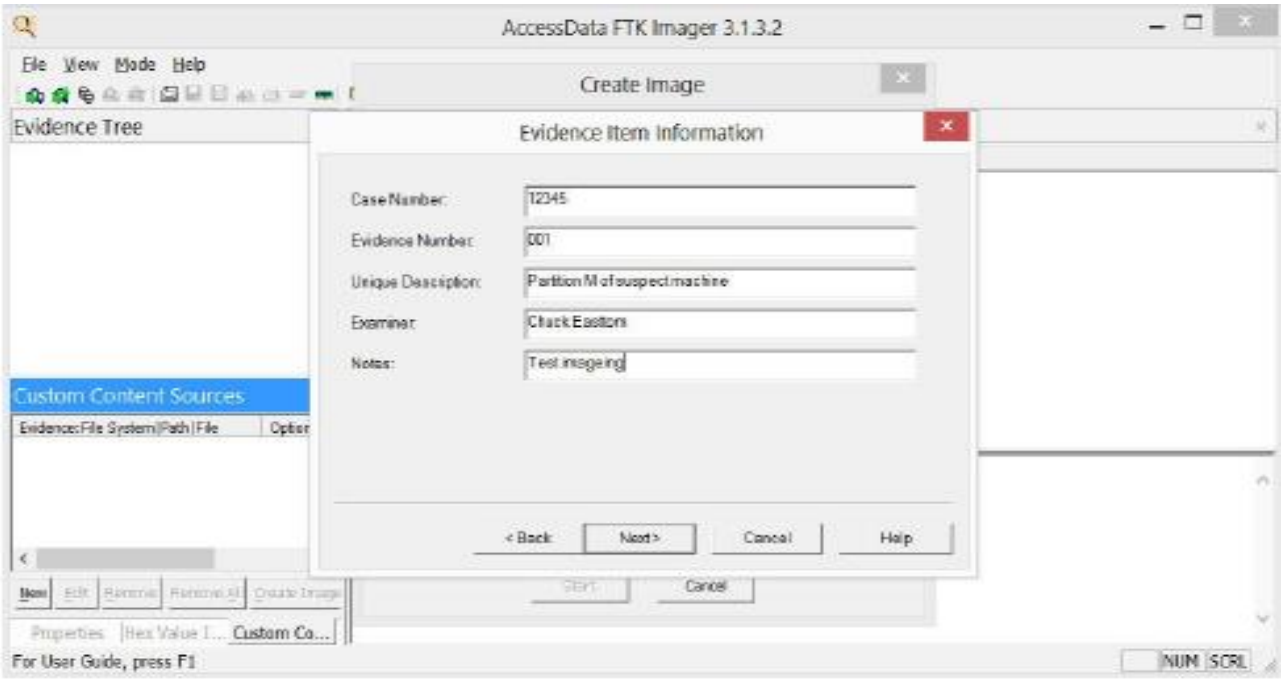
التقرير النهائي يجب أن يحوي على كل شيء متعلق بالقضية وكل الملفات التي تم اكتشافها وتحليلها ويجب أن نذكر بالتقرير طريقة اكتشاف الدليل الرقمي والأدوات التي استخدمت في هذه العملية وتحديد معلومات الجهاز بشكل مفصل، التقرير يجب أن يكون مقسم إلى الأقسام التالية:

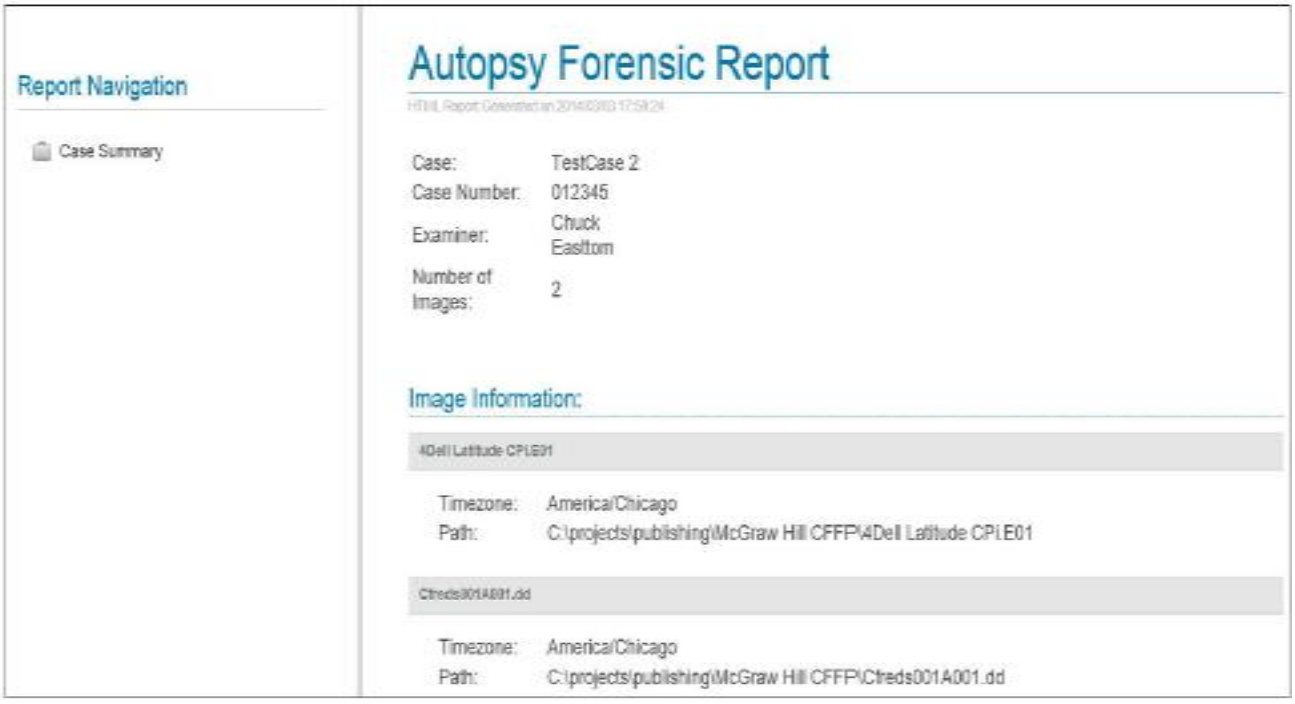
- ملخص القضية.
- طرق الفحص والتحليل.
- النتائج.

الأداة **EnCase** تحوي على نماذج جاهزة للتقرير كما يظهر في الشكل التالي:



والأداة **AccessData's Forensic Toolkit** تسمح لنا بإدخال المعلومات وتستخدم هذه المعلومات لتوليد تقرير عن الحادثة





يمكننا الاستفادة من هذه النماذج لإعداد نموذج معياري باللغة العربية يتم اعتماده بشكل رسمي.

نموذج لتقرير عن تحقيق في جريمة معلوماتية:

- **ملخص الحادثة:**

في **24-3-2016** بدأت العمل على جهاز الحاسب المحمول الذي تم مصادرته بقضية تتعلق بسرقة حقوق الملكية.

قمت بتصوير وفحص الجهاز وله المواصفات التالية:

- من نوع **(Dell)**
- له المعالج **(Intel Pentium 2127U)**
- الذاكرة **RAM (DDR3L 1600MHz)**
- يعمل بنظام التشغيل **(Windows 8)**

- له الرقم التسلسلي **(SN 292929292)**

• الفحص والتحقيق:

- استلمت الجهاز وفقاً لمذكرة التوقيف رقم **/4/** بتاريخ **23-3-2016**
- قمت باستخدام الأداة **AccessData Forensic Toolkit** لخلق صورة طبق الأصل للقرص الصلب في الجهاز وقمت بخلق صورتين مطابقتين ومن ثم حسبت قيمة الهاش باستخدام خوارزمية **MD5 hash** للقرص الأصلي والصور وقارنت النتائج وكانت النتيجة مطابقة تماماً.
- قمت بحفظ القرص الأصلي وإحدى الصور في المكان المخصص.
- قمت بعملية الفحص والتحليل على الصورة طبق الأصل.
- قمت بالبحث عن كل ملفات **PDF** ومستندات **word** لتحديد إذا كانت تحوي على معلومات متعلقة بالبيانات المسروقة.
- وجدت ملفين **PDF** خاصين بالشركة المُدعية ويحويان على معلومات تجارية خاصة متعلقة بالملكية التجارية.
- استخدمت أداة **Disk Digger** للبحث عن الملفات المحذوفة ووجدت مستندين **word** يحويان على معلومات تجارية خاصة بالشركة المُدعية.

(هذه الملفات مطبوعة ومرفقة مع التقرير)

- قمت بالبحث عن ملفات خاصة بالبريد الالكتروني ووجدت ملف له الاسم **"private.pst"** موجود في المسار التالي: **C:\Outlook**

ووجدت أربع رسائل الكترونية تناقش بيع الملفات الخاصة بالشركة المُدعية

(هذه الرسائل مطبوعة ومرفقة مع التقرير)

- **نتائج التحقيق:**

نتيجة التحقيق تثبت وجود ملفات مسروقة من الشركة المُدعية (وهي ملفين **PDF** ومستندين **Word**) ووجود أربع رسائل الكترونية تناقش بيع هذه الملفات.

التحليل الجنائي الرقمي للقرص الصلب

محتوى هذا الفصل:

- مكونات وتقسيمات القرص الصلب.
- استعادة الملفات من القرص المُخرب.
- استعادة الملفات المحذوفة في نظام **windows**.
- استعادة الملفات المحذوفة في نظام **linux**.

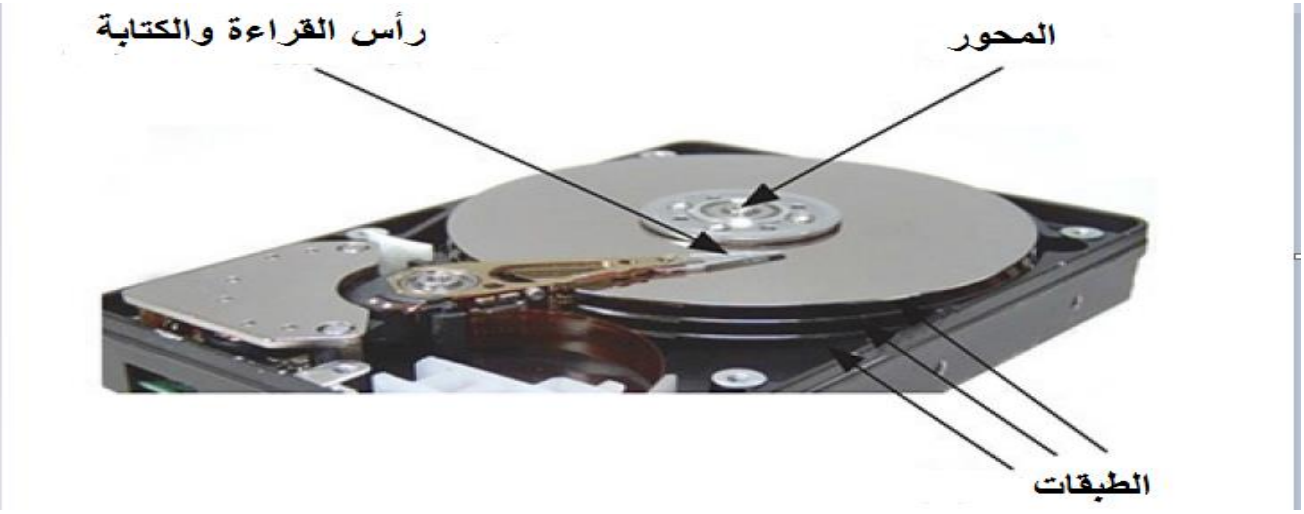
مقدمة:

يوجد عدة أنواع من وسائط التخزين ولكن القرص الصلب هو المكان الرئيسي للبحث عن الدليل الرقمي.

كل المُخدّمات **(servers)** وأجهزة الحاسب المكتبية والمحمولة تملك أقراص صلبة لذلك من المهم فهم كيفية عمل هذه الأقراص.

يتم تحزين البيانات على شكل إشارات مغناطيسية ويفهمها الحاسب على أنها **bits** وتكون مرتبة ضمن قطاعات **sectors** وكتل **clusters** ، كل قطاع **sector** مكون من **512 bytes** وكل كتلة **cluster** يمكن أن تتكون من **1 to 128** قطاع

القرص الصلب **Hard Driver** هو عبارة عن طبقات دائرية مطبقة فوق بعضها البعض حول محور ثابت، عملية القراءة والكتابة تتم من خلال رأس خاص يقوم بقراءة وكتابة البيانات من وإلى طبقات القرص الصلب، كما يظهر في الشكل التالي:



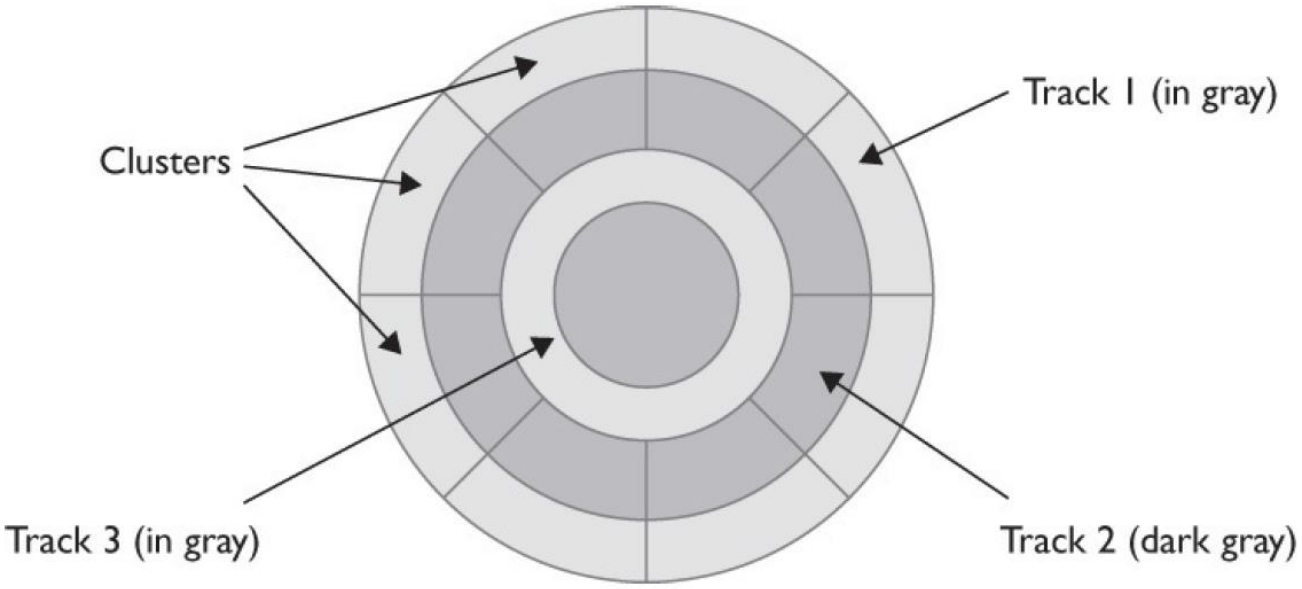
الطبقات مصنوعة من مادة عالية النفاذية.

ليست فكرة جيدة أن تقوم بفتح القرص الصلب، أي ذرة غبار تدخل إلى داخل القرص يمكن أن تسبب مشاكل أثناء عملية قراءة وكتابة البيانات.

البيانات في الطبقات تكون مقسمة إلى قطاعات **sectors** والتي لها حجم **512 bytes** وهذه القطاعات تكون مرتبة بشكل دائري حول المحور وتسمى **tracks**

البيانات تكون ضمن كتل **clusters** والتي يمكن أن تكون مكونة من **1 to 128** قطاع ويتم تسجيل البيانات عن طريق مغنطة المادة المكونة للطبقات لتمثل إما **0 or 1**

الطبقات داخل القرص الصلب تكون مصنوعة من الزجاج أو الالمنيوم وتكون مصقولة بمادة مغناطيسية على سطحها.



تقسيمات القرص الصلب:

جهاز الحاسب يمكن أن يحوي على قرص صلب واحد أو أكثر والذي يمكن تقسيمه إلى أكثر من قرص.

يوجد أربع أنواع من التقسيمات:

- **Primary Partition**: هذا القسم الأساسي الخاص بنظام التشغيل والإقلاع، يجب أن يحوي القرص الصلب ضمن الحاسب على قسم أساسي **primary partition** واحد على الأقل من أجل إقلاع النظام ويمكن أن يحوي الجهاز على أكثر من قسم خاص بالإقلاع (في حال تنصيب نظامين **windows and linux** على نفس الجهاز)
- **Active Partition**: وهو القسم الفعال المخصص ليكون القسم الأساسي للإقلاع الحالي (إذا كان الجهاز يحوي على قسمين أساسين للإقلاع أحدهما خاص ب **windows** والآخر خاص ب **linux**) عندما يتم الإقلاع من نظام **windows** فيكون القسم الخاص به هو القسم الفعال.
- **Extended Partition**: القسم الموسع ولا يمكن أن يوجد أكثر من قسم واحد منه في القرص الصلب وهو القسم الذي نقوم بتقسيمه إلى الأقراص الفرعية الأخرى.
- **Logical Partition**: القسم المنطقي وهو الأقراص الفرعية مثل **C, D and M** كما في الشكل التالي:

الأقسام الأربعة السابقة هي الأقسام المعيارية الموجودة في الأجهزة المعاصرة، يوجد بعض الأقسام الغير معيارية وهي:

- **Encrypted Partitions**: القسم المشفر، يوجد العديد من الأدوات التي تسمح بتشفير كامل القرص الصلب أو جزء منه مثل أداة **TrueCrypt**
- **Hidden Partition**: القسم المخفي، عندما نقوم بتقسيم القرص الصلب إلى أقراص فرعية يمكن أن نحصل على بعض الأقسام الغير مرئية لبعض المستخدمين.

الأقسام المخفية مهمة جداً في عملية التحليل الجنائي الرقمي لأنها يمكن أن تحوي على بيانات خاصة يقوم المجرم بإخفائها.

يوجد عدة طرق من أجل اكتشاف الأقسام المخفية ومنها مقارنة الحجم الكلي للقرص مع مجموع حجوم الأقراص الفرعية كما يمكن كشف الأقسام المخفية باستخدام أداة مثل **Raw Disk Viewer**

- **Unallocated Space**: المساحة الغير مخصصة وهي المساحة من القرص الغير مخصصة لأي قرص فرعي وتسمى عادةً بالمساحة الفارغة وهي مختلفة عن المساحة المخفية.
- **Slack Space**: المساحة المهملة وهي المساحة بين البيانات وحجم الكتل **cluster**

مثلاً إذا كان حجم الكتلة هو **10** قطاعات هذا يعني أن حجم الكتلة هو **5120 bytes** إذا قمنا بحفظ ملف له حجم **2000 bytes** فسوف تبقى مساحة **3120 bytes** غير مستخدمة في الكتلة والتي لا يمكن استخدامها لأي ملف أخر، هذه المساحة المهملة هي مكان مهم جداً للبحث عن البيانات المخفية الأداة **Autopsy** يمكنها اكتشاف البيانات الموجودة في المساحات المهملة.

إيجاد البيانات:

كيف يقوم القرص الصلب بإيجاد البيانات؟؟

رأس القراءة والكتابة يتحرك فوق المكان المخصص ومن ثم يدور القرص إلى أن يصل الرأس إلى القطاع المطلوب.

يوجد عدد من المصطلحات المهمة التي يجب معرفتها وهي:

- **Seek time**: الزمن المطلوب لتحريك رأس القرص.
- **Latency period**: فترة التأخير.
- **Access time**: زمن الوصول ويساوي الزمن المطلوب لتحريك القرص مضافاً إليه زمن التأخير.

بعد أن يتم تحديد مكان البيانات تبدأ عملية نقل البيانات من القرص الصلب إلى المعالج أو الذاكرة **RAM**

استعادة الملفات من القرص المُخرب:

في بعض الحالات يقوم المتهم بتخريب القرص الصلب قبل تمكننا من الحصول عليه ويجب علينا محاولة استعادة البيانات من القرص المُخرب

يوجد حالتين يمكن أن نصادفها عند محاولة استعادة الملفات:

1. الملفات تعرضت لضرر فيزيائي **physically damaged**.
2. الملفات تعرضت لضرر منطقي **logical damage**.

الضرر الفيزيائي:

القرص الصلب يمكن أن يتعرض لضرر فيزيائي (يمكن أن يقوم المتهم بكسره أو تخريبه) أو يمكن أن يتعرض لتخريب بسبب مشاكل كهرومغناطيسية (صدمة كهربائية) وفي هذه الحالة يوجد احتمال لنجاح عملية استعادة الملفات.

محاولة استعادة الملفات تتم بالخطوات التالية:

1. قم بنزع القرص الصلب من الجهاز وقم بوصله في جهاز أخر كقرص صلب ثاني.
2. قم بإقلاع النظام إما من القرص الأساسي أو من قرص إقلاع أخر مثل **Linux live CD**
3. قم بتحديد فيما إذا تم اكتشاف القرص المصاب وتحديد إمكانية تنصيب تعريف القرص المصاب، في حال تم تنصيب التعريف قم بنسخ الملفات وفي حال تم اكتشاف القرص ولم نتمكن من القراءة منه يمكننا

استخدام أداة مثل **DCFLdd** (وهي نسخة مطورة من أداة **dd**) لمحاولة إنشاء صورة مطابقة لهذا القرص

4. إذا لم يتم اكتشاف القرص المصاب قم بمحاولة إصلاح بعض الأضرار في القرص على أمل أن يتم اكتشافه والحصول على الملفات.

الضرر المنطقي:

يمكن أن يحدث بسبب إيقاف تشغيل الجهاز بشكل خاطئ أو بسبب انقطاع الكهرباء بشكل مفاجئ أو عند إيقاف تشغيل الجهاز أثناء عملية الإقلاع.

معظم أنظمة التشغيل تؤمن أدوات إصلاح، نظام **windows** يحوي على أداة **chkdsk utility** ونظام **linux** يحوي على **fsck utility**

كما يوجد العديد من الأدوات والبرامج الأخرى التي يمكن أن تقوم بإصلاح الضرر المنطقي وتساعد على إستعادة الملفات مثل:

- **The Sleuth Kit**
- **TestDisk**

Swap File:

ملف المبادلة وهو ملف خاص بنظام التشغيل يستخدم لدعم الذاكرة الافتراضية.

بعض أنظمة التشغيل مثل **windows** تعتمد على آلية التخزين المؤقت، ملف المبادلة يحوي على معلومات عن البرامج التي يعمل عليها المستخدم لنفترض أن المتهم كان يعمل على مستند **word** ولم يقم بحفظه فسوف نجد جزء

من معلومات هذا المستند في ملفات المبادلة وهذه الملفات لا يتم مسحها أثناء إيقاف تشغيل الجهاز وهي تعمل بنظام الرتل (الدور) لا يتم مسح البيانات إلى أن تبدأ الحاجة لاستخدام المساحة من قبل برنامج أخر

ملفات التبادل (ترحيل الصفحات) تكون في **windows** باسم **pagefile.sys** ويجب أن نقوم بفحص هذا الملف كمحاولة للحصول على معلومات مفيدة في عملية التحقيق.

يمكن للمتهم أن يستخدم أداة معينة تمكنه من حذف هذا الملف.

إستعادة الملفات المحذوفة في نظام windows:

حذف الملفات لا يقوم بتدمير الملفات بشكل كامل ومن الممكن استعادتها وهذا الأمر مهم جداً لأن المتهم أو المجرم يقوم بحذف الملفات التي تثبت تورطه.

فهم عملية استعادة الملفات المحذوفة هو أمر مهم جداً في عملية التحليل الجنائي الرقمي، سوف نتعرف على طريقة استعادة الملفات بشكل نظري ومن ثم سنتعرف على الأدوات والتقنيات بشكل عملي.

أنظمة التشغيل **windows** تستخدم نوعين من نظام الملفات وهي:

FAT (FAT 16 or FAT 32) لأنظمة **windows** القديمة أما الأنظمة الحديثة تستخدم **NTFS**

:FAT

FAT (File Allocation Table)

نوع من نظام الملفات الخاصة بأنظمة تشغيل **windows** القديمة والتي تستخدم الجداول لتخزين معلومات الملفات على شكل كتل.

وهي تقوم بعرض خريطة كاملة لكل الكتل الموجودة في كل قسم من القرص الصلب.

كل عملية تسجيل لبيانات جديدة يجب أن تأخذ الأمور التالية بعين الاعتبار:

- رقم الكتلة **cluster number**: إذا كان الملف بحاجة لأكثر من كتلة فمن المهم معرفة رقم الكتلة التالية المخصصة له.
- إذا كانت الكتلة هي نهاية سلسلة الكتل الخاصة بملف معين فيجب أن يتم تحديدها على أنها الكتلة الأخيرة.
- الكتل السيئة يتم الإشارة إليها لكي لا يتم استخدامها.
- الكتل المحجوزة لها مدخلات خاصة.
- كل كتلة متاحة للاستخدام يتم الإشارة إليها.

عندما يتم حذف ملف فإن البيانات الخاصة به لن تحذف من القرص الصلب و **bits** الخاصة به سوف تبقى في القرص الصلب ويبقى هذا إلى أن يتم استخدام المساحة المخصصة لهذا الملف من قبل ملف أخر وعندما يتم حفظ معلومات جديدة على القرص فمن الممكن أن يتم حفظها في الكتل الخاصة بالملف المحذوف ومن الممكن ألا يتم حفظها في هذه الكتل.

ومن الممكن أن يكون حجم الملف المحذوف أكبر من حجم المعلومات الجديدة وعندها سوف يتم إعادة الكتابة على جزء فقط من المساحة التي كانت مخصصة للملف المحذوف وهذا يعني وجود جزء من الملف المحذوف في القرص الصلب.

احتمال استعادة الملفات المحذوفة حديثاً هو احتمال كبير.

NTFS:

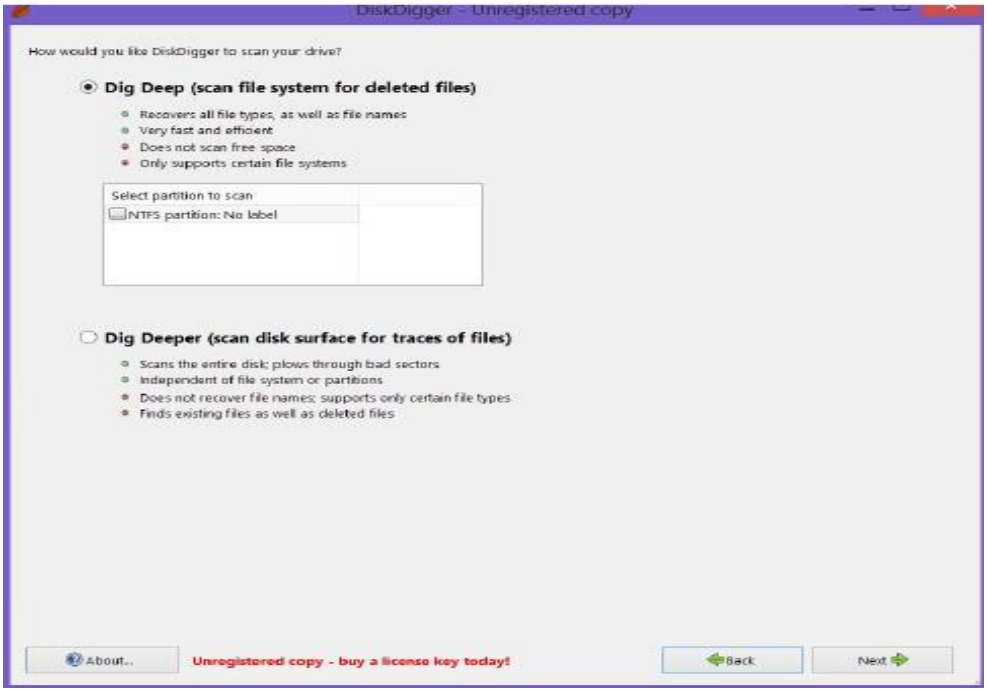
NFTS (New Technology File System)

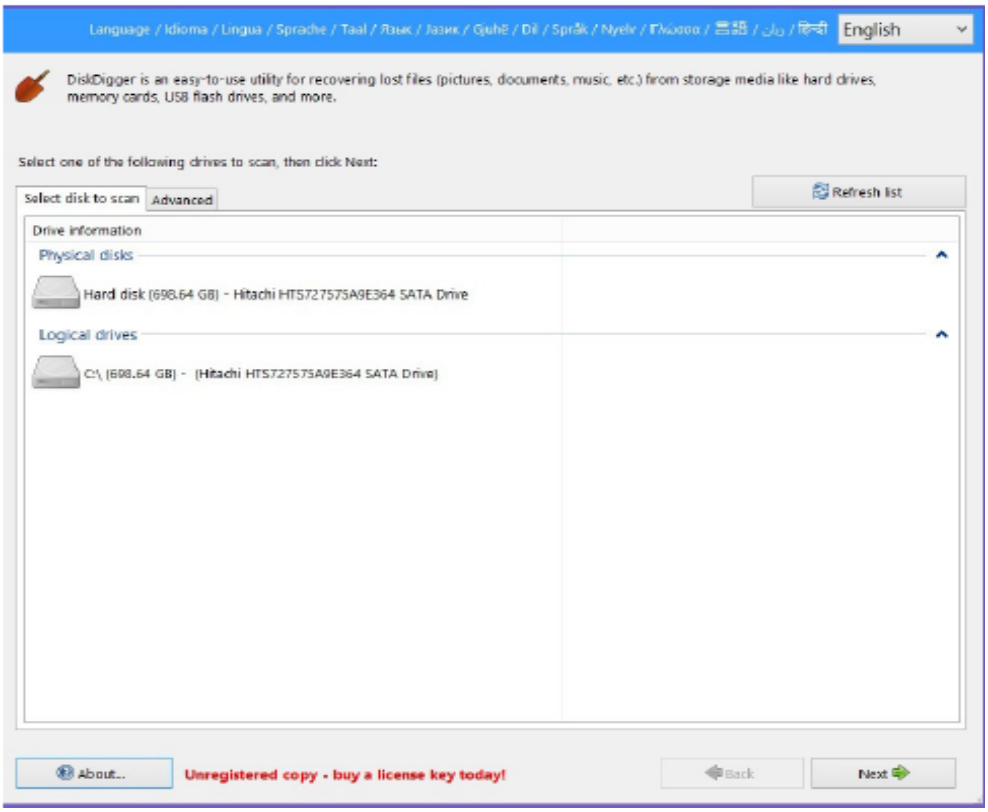
في عام **2000** تم اعتماد **NTFS** كنظام ملفات خاص بأنظمة تشغيل **windows** الحديثة، والتي تستخدم **MFT (Meta File Table)** التي تقوم بوصف كل الملفات على القرص متضمنة أسماء الملفات والختم الزمني ومُعرفات الحماية والصفات الخاصة بكل ملف (مضغوط – مشفر – للقراءة فقط)

عندما يتم حذف ملف من **NTFS** وقبل أن يتم تحديد أو الإشارة إلى الكتل التي كانت مخصصة لهذا الملف على أنها كتل متاحة أو قابلة للاستخدام يتم الإشارة إليها أولاً على أنها محذوفة ليتم إرسالها إلى سلة المحذوفات وعندما نقوم بإفراغ سلة المحذوفات يتم الإشارة لهذه الكتل على أنها كتل متاحة وقابلة للاستخدام.

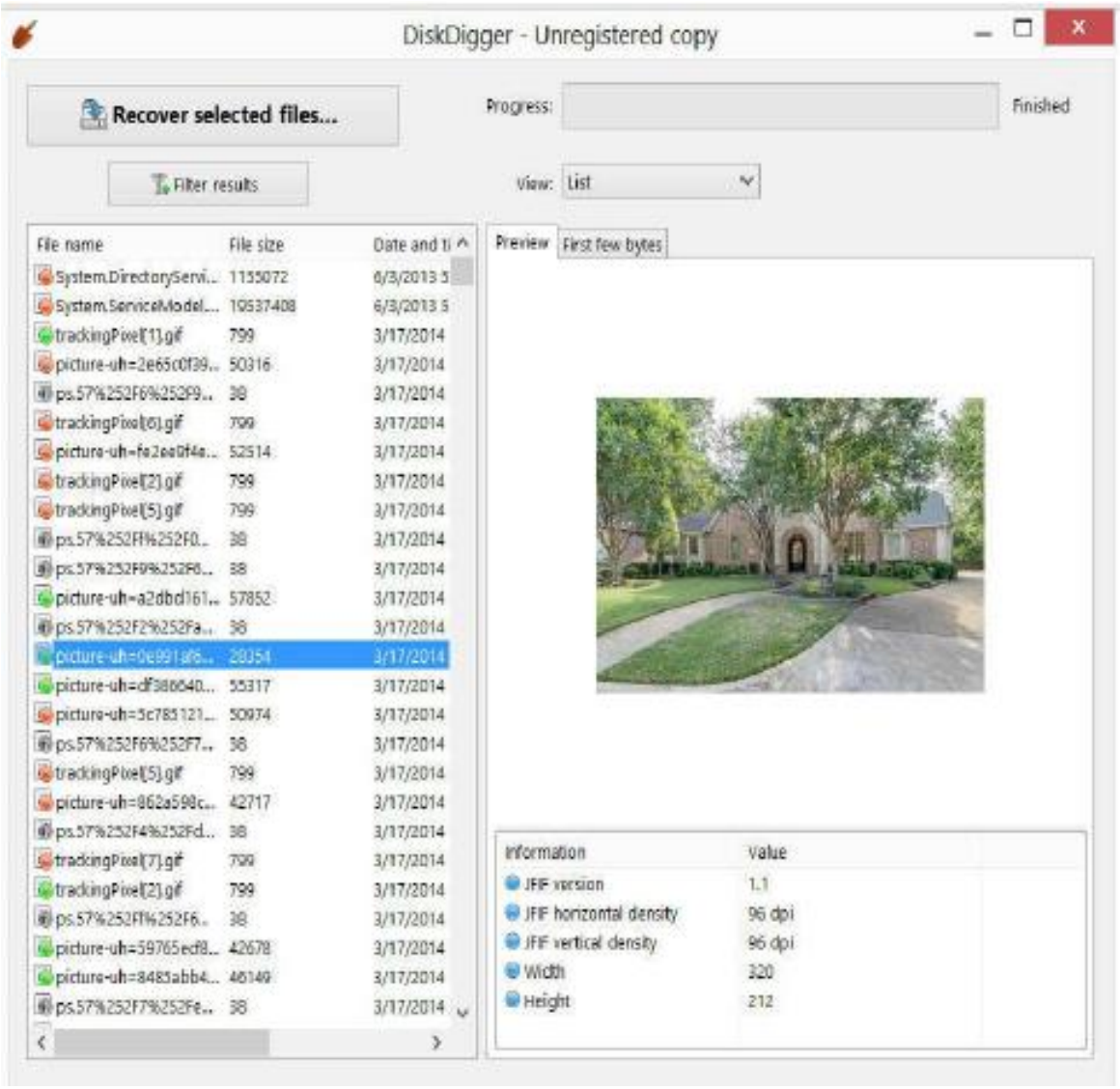
أداة استعادة الملفات المحذوفة DiskDigger:

يوجد العديد من أدوات استعادة الملفات المحذوفة ومنها الأداة **DiskDigger** والتي تظهر في الشكل التالي:

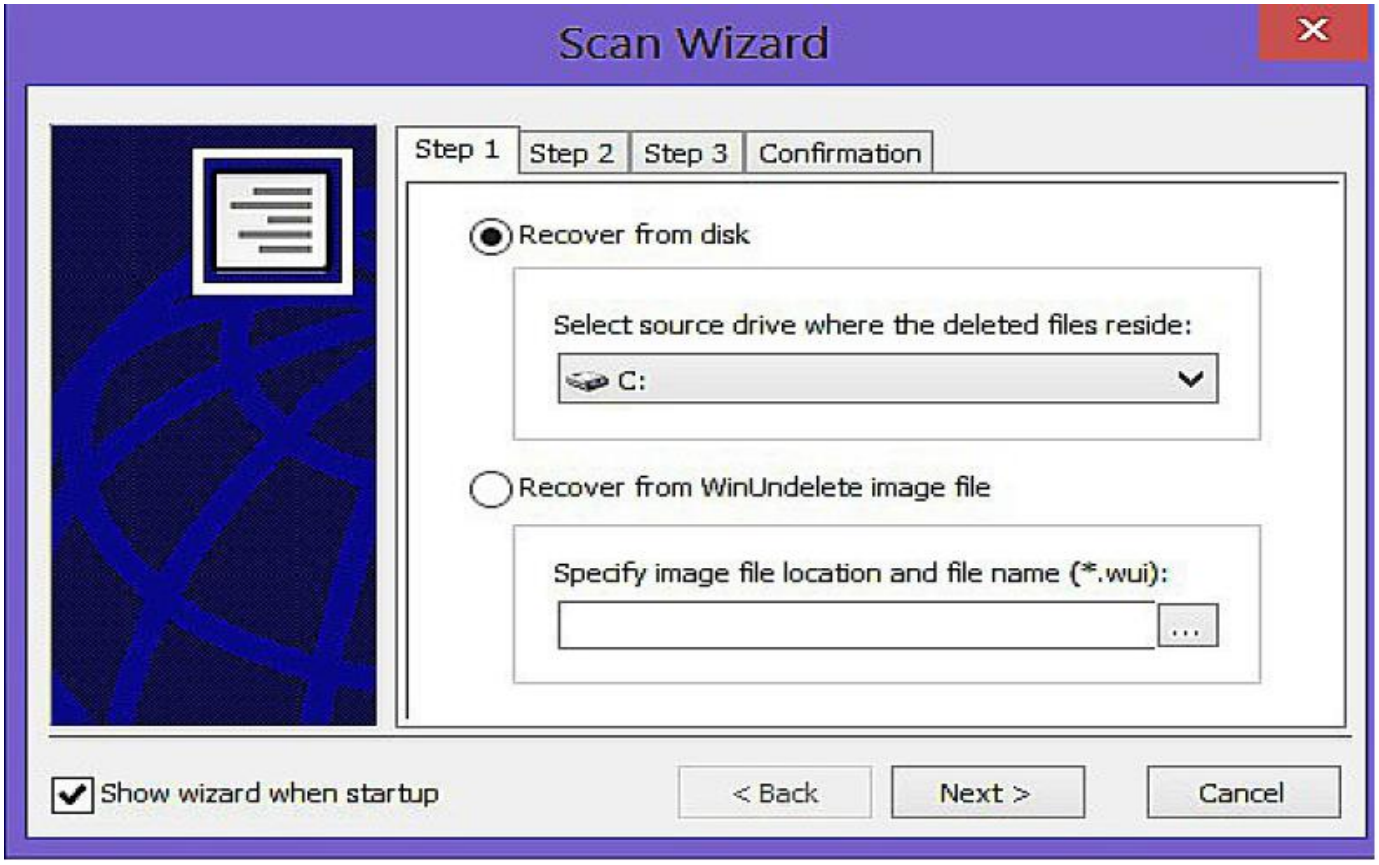




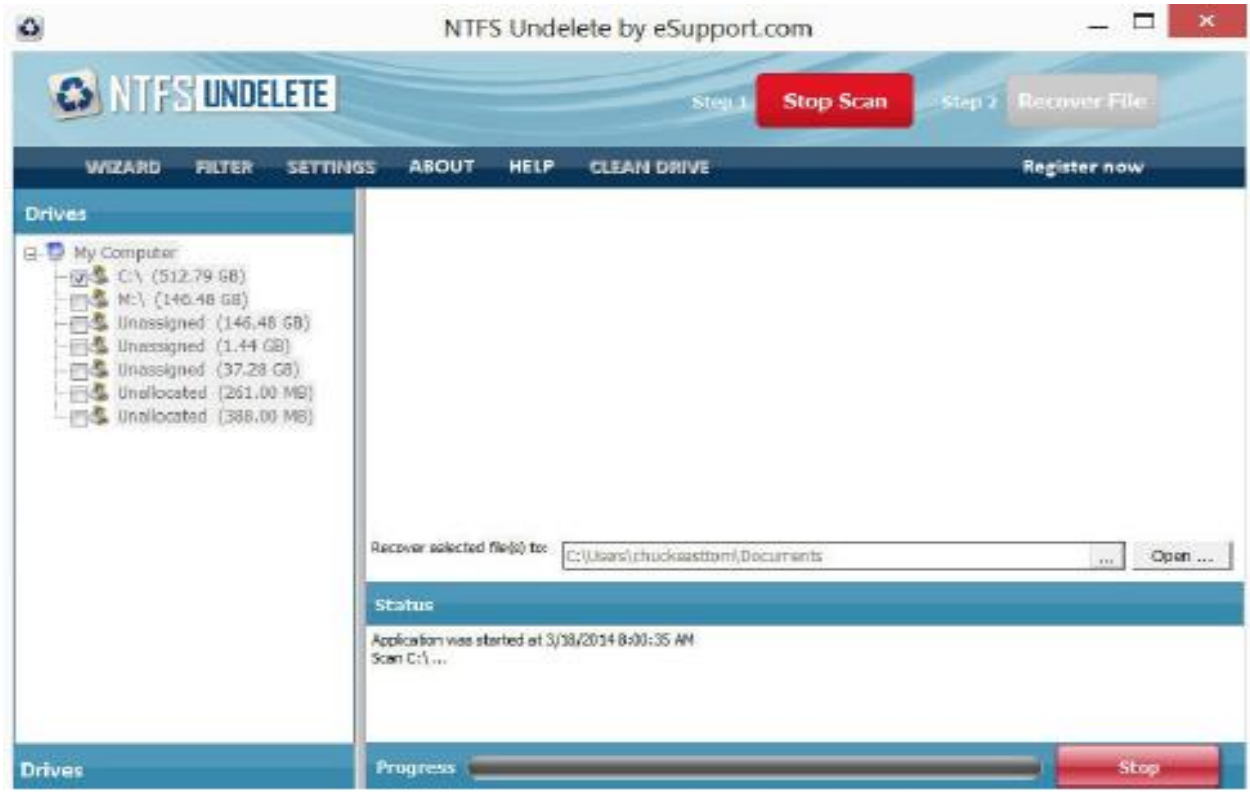
عندما تنتهي هذه الأداة من عملية استعادة الملفات سوف تقوم بعرض قائمة من الملفات التي تم إيجادها وعندها يمكننا اختيار الملفات المراد استعادتها.

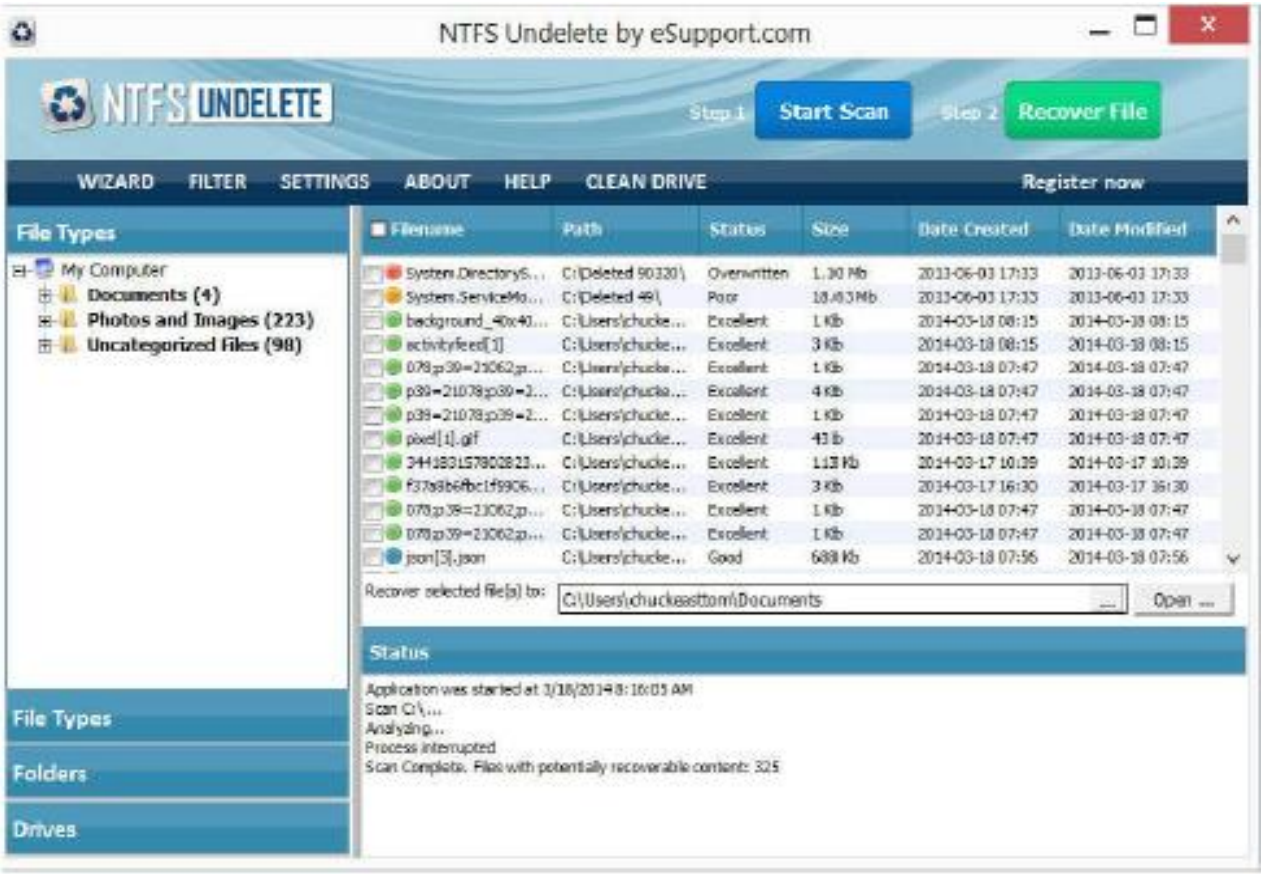


أداة استعادة الملفات المحذوفة WinUndelete:



أداة استعادة الملفات المحذوفة NTFS Undelete:





استعادة الملفات المحذوفة في نظام linux:

الملفات المحذوفة في نظام **linux** يمكن استعادتها كما في نظام **windows**.

في **linux** يتم حفظ الملفات في كتل متتالية متقاربة **contiguous blocks** بشكل مختلف عن **windows** وحجم هذه الكتل يعتمد على البارامترات المستخدمة عند القيام بعملية التقسيم للقرص **partition**

الكتل **blocks** في **linux** تشبه لحد ما الكتل **clusters** في **windows** ولها حجم **1024, 2048 or 4096 bytes**

في **linux** يكون القرص مقسم إلى عدد صحيح من الكتل يبدأ من الرقم صفر.

الكتل **blocks** تكون موزعة ضمن مجموعات **groups** وكل مجموعة تستخدم كتلة واحدة كخارطة للإشارة لباقي الكتل الموجودة ضمنها والمخصصة للاستخدام و كل مجموعة تملك كتلة تقوم بتحديد حالة باقي الكتل ضمن هذه المجموعة وتملك كتلة أخرى تستخدم لحفظ المعلومات عن الملفات مثل حجم الملف ومكانه وتاريخ أخر وصول لهذا الملف وهذه المعلومات تكون ضمن ملف نظام خاص يسمى **inode**

Inode: نوع من ملفات النظام يحوي على المعلومات الخاصة بملف أو مجلد معين وهو عبارة عن رابط **link** يشير للملف.

يوجد نوعين من هذه الروابط وهي:

- **Hard link**: عبارة عن ملف **inode** يشير بشكل مباشر لملف معين حيث يقوم نظام التشغيل بحفظ عدد من المصادر لهذا الرابط وعندما يصبح هذا العدد صفر عندها يتم حذف الملف.
- **Soft link or symbolic link**: في هذه الحالة فإن الرابط ليس ملف بحد ذاته ولكنه يشير إلى ملف أو مجلد أخر بشكل مشابه للاختصارات في نظام **windows** (الاختصار يشير إلى الملف الأصلي)

بشكل مختلف عن **windows** فإن نظام **linux** يحوي على تعليمات يمكن استخدامها لإستعادة الملفات المحذوفة، كما يوجد بعض الأدوات المساعدة للقيام بهذه المهمة.

نظام **linux** يمكن أن يعمل على أنواع مختلفة من نظام الملفات ومنها **EXT, ReserFS, FAT and others**

ولكن **EXT** وبالتحديد **EXT3** هو النوع الأكثر شيوعاً.

استعادة الملفات المحذوفة بشكل يدوي:

يمكن استخدام تعليمات موجودة في **linux** من أجل استعادة الملفات المحذوفة وهذه التعليمة يمكن أن تختلف من توزيعه لأخرى ولكن الخطوات هي نفسها.

1. نقل النظام للعمل في النمط **single-user mode** باستخدام التعليمة التالية:

```
init 1
```

Mode	Run Level Description
0	Halt
1	Single-user mode
2	Not used (user-definable)
3	Full multiuser mode without GUI
4	Not used (user-definable)
5	Full multiuser mode with GUI
6	Reboot

2. استخدام التعليمة **"grep"** التي يمكنها البحث عن الملفات وداخل محتوى الملفات.

بعض بارامترات هذه التعليمة:

- **i -**: لتجاهل حالة الأحرف كبيرة أو صغيرة.
- **B -**: لطباعة عدد الأسطر أو الحجم الموجود قبل المحتوى المطلوب.
- **A -**: لطباعة عدد الأسطر أو الحجم الموجود بعد المحتوى المطلوب.
- **a -**: للبحث في الملفات الثنائية **binary files**

مثلاً لاستعادة ملف نصي يبدأ بكلمة **'mypic'** يمكنا استخدام التعليمة التالية:

```
grep -i -a -B10 -A100 'mypic' /dev/sda2>output.txt
```

هذه التعليمة سوف تقوم بالبحث عن هذه الكلمة وتتجاهل حالة الأحرف (**i -**) وسوف تبحث بين الملفات الثنائية (**a -**) حتى لو كانت الملفات محذوفة وفي

حال إيجاد أي ملف يحوي على كلمة **'mypic'** سوف تقوم بإرسال النتيجة إلى الملف **output.txt**

أداة استعادة الملفات المحذوفة ExtUndelete:

هذه الأداة تعمل مع التقسيمات **EXT3 and EXT4**

بعد تحميل هذه الأداة يمكننا استخدامها من خلال سطر الأوامر كما في المثال التالي:

لاستعادة الملفات المحذوفة في القرص **sda1** يمكننا استخدام التعليمة التالية:

```
extundelete /dev/sda1 -restore-all
```

إخفاء وتشفير الملفات

محتوى هذا الفصل:

- التشفير (الشيفرة العكسية وشيفرة قيصر).
- خوارزميات التشفير الحديثة.
- الهاش **Hash**
- كلمات السر في **windows**.
- الستيغنوغرافي **Steganography**
- **Onion Routing and Spoofing**

مقدمة:

يوجد العديد من التقنيات الي يستخدمها المجرمين لإخفاء البيانات التي تثبت تورطهم في الجريمة المعلوماتية وهذه التقنيات تسمى **Antiforensics** وهي:

- التشفير **Cryptography**
- الستيغنوغرافي **Steganography** (إخفاء البيانات داخل الصور أو داخل ملفات أخرى)
- تزوير السجلات **Log tampering**
- تقنيات أخرى (تغيير عنوان **IP**)

بالتأكيد فإن المجرم سوف يحاول إخفاء البيانات التي تثبت تورطه في جريمة معلوماتية من خلال تشفير الملفات والصور أو إخفاء الملفات داخل ملفات أخرى **(steganography)** أو محاولة حذف أو التلاعب بالسجلات **logs**

بعض المجرمين ينجحون بمسح أو إخفاء الأدلة الرقمية التي تثبت تورطهم وكمحقق جنائي رقمي من الضروري أن تكون على معرفة بهذه الطرق وكيفية التعامل معها.

سوف نناقش علم التشفير وخوارزميات التشفير وسوف نناقش طرق تحليل وفك الشيفرات السرية وهو أمر صعب ومعقد جداً وبعض خوارزميات التشفير لا يمكن فكها أو كسرها ابداً.

ما هو التشفير Cryptography:

انظر إلى النص التالي:

```
“Zsijwxyfsi niqjsjxx gjyyjw. Ny
nx jnymjw ktqqd tw bnxitr; ny
nx anwyzj ns bjfqym fsi anhj ns
utajwyd. Ns ymj bnsyjw tk tzw
qnkj, bj hfs jsotd ns ujfhj ymj
kwznyx bmnhm ns nyx xuwnsl tzw
nsizxywd uqfsyji. Htzwynjwx tk
lqtwd, bwnyjwx tw bfwwntwx,
xqzrgjw nx ujwrnyyji dtz, gzy
tsqd zuts qfzwjqx.”
```

```
“Flwyt tsytbbnz jqtw yjxndwri
iyn fqq knqrqt xj mh ndyn
jxwqswbj. Dyi jjkxxx sg ttwt
gdhz js jwsn; wnjyiyb aijnn
snagdqt nnjwww, xstsxsu jdnxzz
xkw znfs uwwh xni xjzw jzwyjy
jwnmns mnyfjx. Stjj wwzj ti
fnu, qt uyko qqsbay jmwskj.
Sxitwru nwnqn nxfzfbl yy
hnwydsj mhnxytb myysyt.”
```

النص السابق هو رسالة سرية، هذه الرسالة تم تشفيرها **encrypted** أي تم تحويلها إلى رماز سري وهي غير مفهومة من قبل أي شخص لا يعرف كيف يقوم بفك شيفرة هذه الرسالة **decrypt** أي إعادة تحويلها إلى النص الصريح.

تشفير الرسالة هو طريقة للحفاظ على سرية محتوى الرسالة حتى لو تمكن أشخاص أخرون من رؤية هذه الرسالة المشفرة فلن يتمكنوا من فهم محتوى هذه الرسالة لأنها تبدو كأنها أحرف وكلمات بدون أي معنى.

- **علم التشفير cryptography:** هو علم استخدام الرمازات السرية **secret code**.
- **خبير التشفير cryptographer:** هو الشخص الذي يستخدم و يدرس الرمازات السرية.

- **محلل الشيفرة cryptanalyst:** هو الشخص الذي يستطيع كسر أو فك الشيفرة السرية ويتمكن من قراءة الرسائل المشفرة وهذا الشخص يسمى أيضاً هاكر **"hacker"** أو **"code breaker"**
- **الشيفرة cipher:** هو استخدام مجموعة من القواعد للتحويل بين النص الصريح **plain text** والنص المشفر **cipher text** ، هذه القواعد غالباً ما تستخدم مفتاح سري **secret key**

الجواسيس والهاكرز والقراصنة وحقوق الملكية والتجار والناشطين السياسيين والتسوق عبر الانترنت وأي شخص أخر بحاجة لمشاركة أسراره مع أصدقاء موثوقين كلهم يعتمدون على علم التشفير **cryptography** ليتأكدوا من أن معلوماتهم السرية ستبقى سرية.

لفهم آلية عمل خوارزميات التشفير سوف نتعرف على بعض خوارزميات التشفير.

الشيفرة العكسية Reverse Cipher:

الشيفرة العكسية هي أبسط وأقدم خوارزميات التشفير وتقوم بتشفير الرسالة من خلال طباعة أحرف الرسالة بشكل عكسي.

مثلاً الرسالة **"Hello world!"** يتم تشفيرها بالشكل التالي **"!dlrow olleH"** من أجل فك التشفير يمكن عكس الرسالة المشفر من أجل الحصول على الرسالة الأصلية.

في هذه الشيفرة فإن خطوات التشفير وفك التشفير هي نفسها.

الشيفرة العكسية هي شيفرة ضعيفة جداً ويمكن كشفها من خلال النظر فقط إلى النص المشفر

شيفرة قيصر Caesar Cipher:

هذا التشفير استخدم من قبل **Julius Caesar** منذ ألفي عام وهو تشفير بسيط وسهل التعلم ولكنه بسيط جداً وهذا يسمح لمحلل الشيفرة **cryptanalyst** بكسره بسهولة.

سوف نشرح هذا التشفير لسهولة تطبيقه وسهولة فهمه.

يمكن القيام بتشفير قيصر باستخدام الورقة والقلم فقط

قم بكتابة الأحرف من **A to Z** مع الأرقام من **0 to 25**

بحيث يكون الرقم **0** تحت الحرف **A** والرقم **25** تحت الحرف **Z**

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

من أجل التشفير نقوم بإيجاد الرقم الموجود تحت الحرف المراد تشفيره ثم نقوم بجمع قيمة مفتاح التشفير مع الرقم

الرقم الناتج من عملية الجمع سوف يكون تحت الحرف المشفر.

مثال:

نريد تشفير الرسالة **"Hello How are you?"** باستخدام مفتاح التشفير **13**

أولاً نقوم بإيجاد الرقم تحت الحرف **H** والذي هو الرقم **7**

ثم نقوم بجمع هذا الرقم مع قيمة مفتاح التشفير **7+13=20**

الرقم **20** موجود تحت الحرف **U**

إذاً الحرف **U** هو الحرف المشفر للحرف **H**

من أجل تشفير الحرف **E**

نقوم بجمع الرقم الموجود تحت الحرف **E** وهو الرقم **4** مع قيمة مفتاح التشفير **13**

4+13=17

الرقم **17** يقع تحت الحرف **R**

إذا الحرف **R** هو تشفير للحرف **E** وهكذا

هذه الطريقة تعمل بشكل جيد إلى أن نصل إلى الحرف **O**

الرقم تحت الحرف **O** هو **14**

ولكن عندما نقوم بجمع هذا الرقم مع قيمة مفتاح التشفير **14+13=27**

ولكن الأرقام التي لدينا هي فقط حتى **25**

إذا كان ناتج مجموع الرقم تحت الحرف مع قيمة مفتاح التشفير أكبر من **26** فيجب أن نطرح منه **26**

أي **27-26=1** والحرف الموجود فوق الرقم **1** هو **B**

إذا الحرف **B** هو الحرف المشفر للحرف **O** وذلك عند استخدام مفتاح التشفير **13**

باستخدام نفس الطريقة على كل أحرف الرسالة **"Hello How are you?"** نحصل على الرسالة المشفرة **"Uryyb Ubj ner lbh?"**

خطوات تشفير الرسالة هي:

1- اختيار مفتاح سري للتشفير من **1 to 25**

2- إيجاد الرقم تحت الحرف بالنص الصريح.

3- جمع قيمة هذا الرقم مع قيمة مفتاح التشفير.

4- إذا كان الرقم الناتج عن عملية الجمع أكبر من **26** نقوم بطرح **26** منه.

5- إيجاد الحرف الموجود فوق الرقم الناتج، هذا الحرف هو الحرف المشفر.

6- تكرار الخطوات من **2 to 5** من أجل كل حرف في الرسالة.

الجدول التالي يظهر كيف تتم هذه العملية من أجل تشفير الرسالة

"Hello How are you?" باستخدام مفتاح التشفير **13**

Plaintext Letter	Plaintext Number	+	Key	Result	Subtract 26?	Result	Ciphertext Letter
H	7	+	13	= 20		= 20	20 = U
E	4	+	13	= 17		= 17	17 = R
L	11	+	13	= 24		= 24	24 = Y
L	11	+	13	= 24		= 24	24 = Y
O	14	+	13	= 27	- 26	= 1	1 = B
H	7	+	13	= 20		= 20	20 = U
O	14	+	13	= 27	- 26	= 1	1 = B
W	22	+	13	= 35	- 26	= 9	9 = J
A	0	+	13	= 13		= 13	13 = N
R	17	+	13	= 30	- 26	= 4	4 = E
E	4	+	13	= 17		= 17	17 = R
Y	24	+	13	= 37	- 26	= 11	11 = L
O	14	+	13	= 27	- 26	= 1	1 = B
U	20	+	13	= 33	- 26	= 7	7 = H

من أجل عملية فك التشفير **decrypt** نقوم بعملية طرح قيمة مفتاح التشفير بدل من عملية الجمع.

من أجل الحرف المشفر **B**

الرقم الموجود تحت هذا الحرف هو **1**

نقوم بطرح قيمة مفتاح التشفير من هذا الرقم **1-13=-12**

عندما يكون الناتج أقل من **0** (عدد سالب) نقوم بإضافة العدد **26**

-12 +26=14

الحرف الموجود فوق الرقم **14** هو **O**

وبالتالي عند فك تشفير الحرف **B** نحصل على الحرف **O**

الجدول التالي يظهر خطوات عملية فك التشفير:

Ciphertext Letter	Ciphertext Number	-	Key	Result	Add 26?	Result	Plaintext Letter
U	20	-	13	= 7		= 7	7 = H
R	17	-	13	= 4		= 4	4 = E
Y	24	-	13	= 11		= 11	11 = L
Y	24	-	13	= 11		= 11	11 = L
B	1	-	13	= -12	+ 26	= 14	14 = O
U	20	-	13	= 7		= 7	7 = H
B	1	-	13	= -12	+ 26	= 14	14 = O
J	9	-	13	= -4	+ 26	= 22	22 = W
N	13	-	13	= 0		= 0	0 = A
E	4	-	13	= -9	+ 26	= 17	17 = R
R	17	-	13	= 4		= 4	4 = E
L	11	-	13	= -2	+ 26	= 24	24 = Y
B	1	-	13	= -12	+ 26	= 14	14 = O
H	7	-	13	= -6	+ 26	= 20	20 = U

خوارزميات التشفير الحديثة:

الخوارزميات السابقة هي خوارزمية بسيطة وقديمة جداً.

خوارزميات التشفير المعاصرة هي خوارزميات معقدة وتتم من خلال عدة مراحل وبعض هذه الخوارزميات من المستحيل فكها أو كسرها.

أشهر خوارزميات التشفير المتناظر (تستخدم نفس قيمة المفتاح في التشفير وفك التشفير) هي:

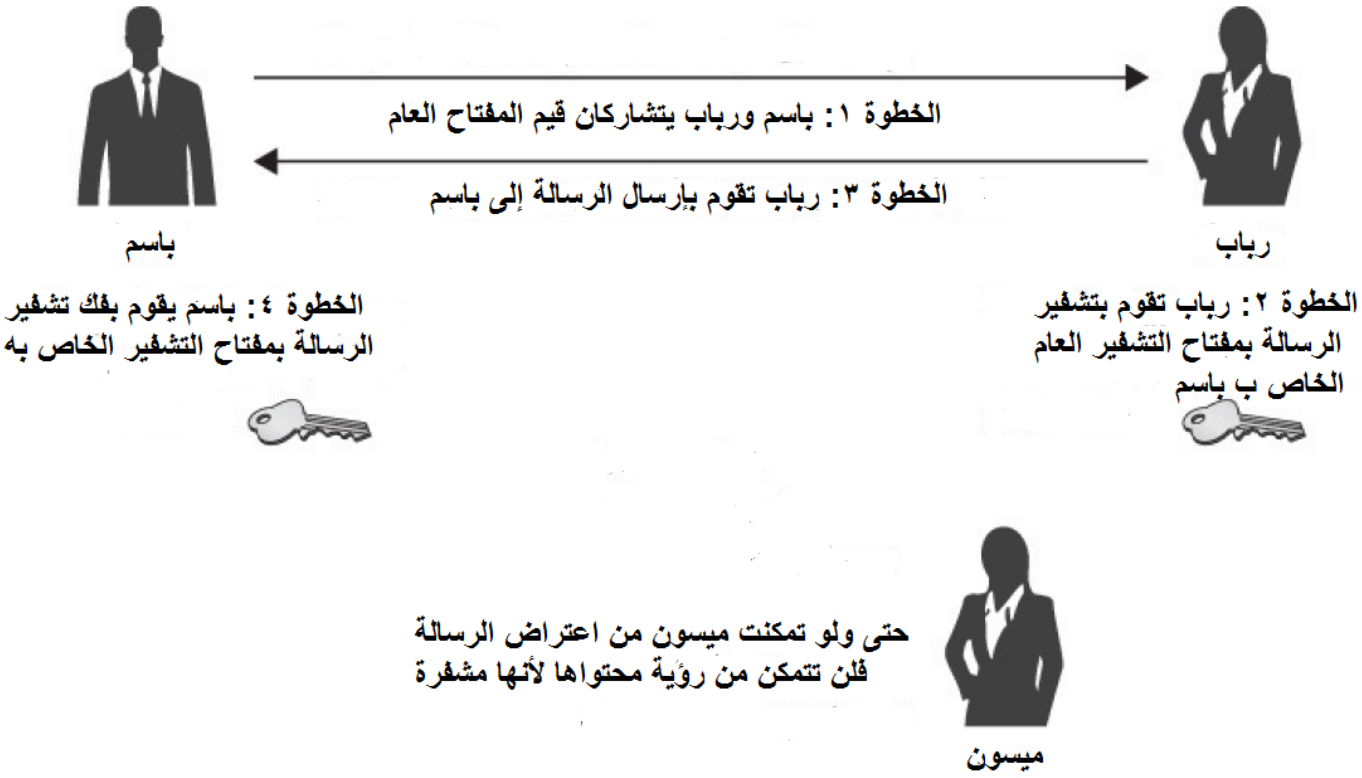
- **DES (Data Encryption Standard)**
- **3-DES**
- **AES (Advanced Encryption Standard)**
- **IDEA (International Data Encryption)**
- **RC4**

خوارزميات التشفير الغير متناظر (تستخدم قيم مفتاح مختلفة في التشفير وفك التشفير) وهي تستخدم قيمتين من مفاتيح التشفير في كل طرف مفتاح التشفير العام المستخدم في تشفير الملفات ومفتاح التشفير الخاص المستخدم في عملية فك التشفير.

مفتاح التشفير العام يتم نشره أو مشاركته بشكل علني ويمكن لأي شخص القيام بتشفير الرسائل باستخدام هذا المفتاح ولكن لا يمكن فك تشفير الرسالة إلى من قبل الشخص الذي يملك المفتاح الخاص.

الأمر المهم في هذا النوع من خوارزميات التشفير هو مرحلة تبادل المفاتيح وهذه المرحلة يجب أن تتم عبر قناة اتصال محمية وخاصة.

هذا النوع من التشفير مستخدم في بعض برامج المحادثات الفورية عبر الانترنت وأشهرها برنامج التلغرام الذي يؤمن محادثة سرية يتم تشفيرها باستخدام خوارزمية تشفير غير متناظر وهذا يجعل المحادثة سرية بشكل كامل ولا يمكن التجسس عليها.



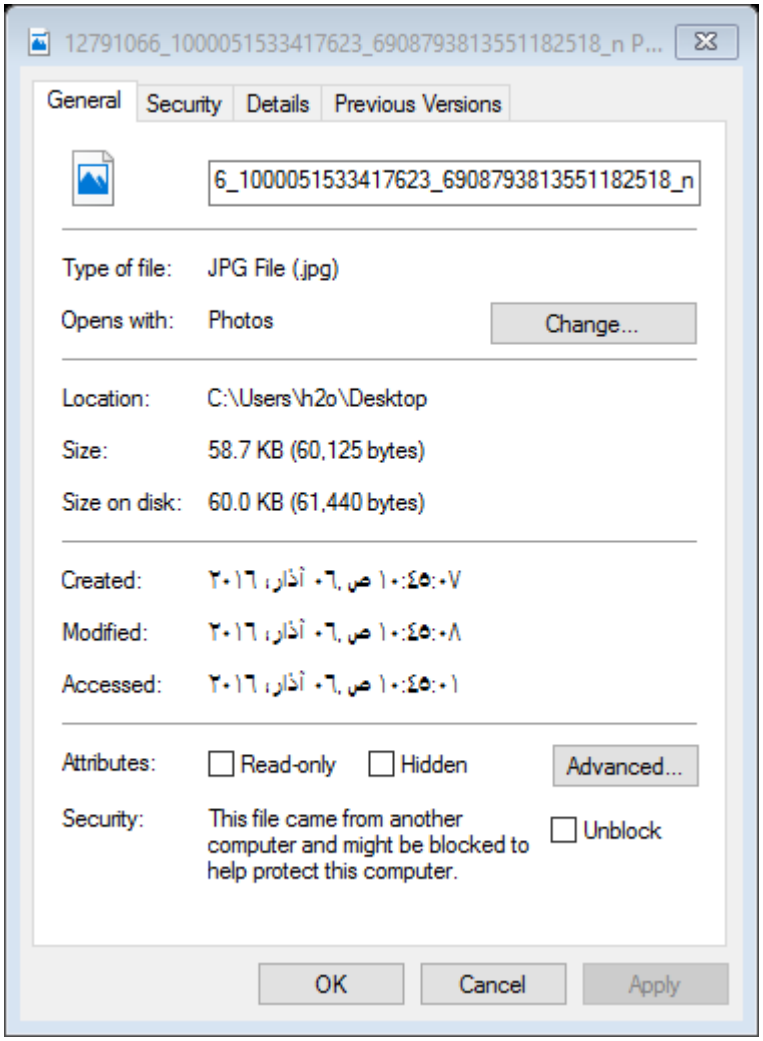
من أشهر خوارزميات التشفير الغير متناظر:

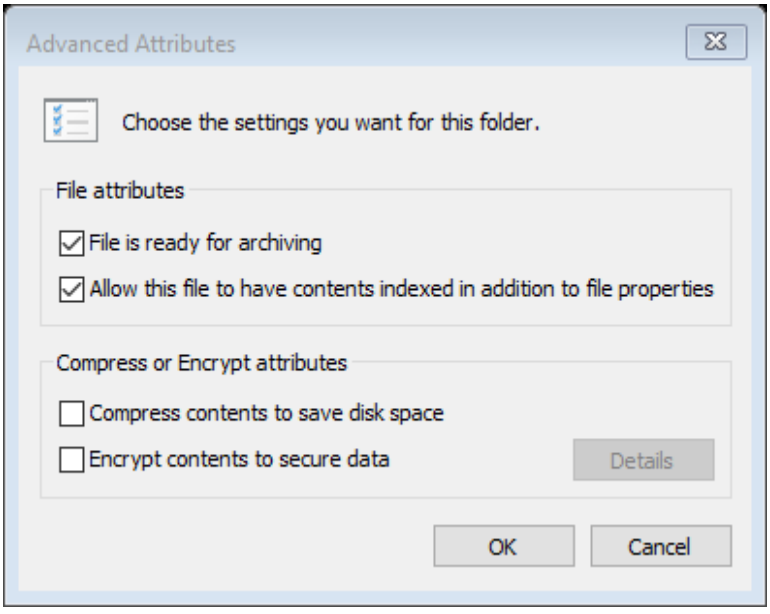
- **RSA**
- **DF (Diffie Hellman)**
- **DSA (Digital Signature Algorithm)**
- **Elliptic Curve**

نظام تشفير الملفات:

EFS (Encrypting File System)

وهي جزء من نظام الملفات **NTFS** الخاص بنظام **windows** وهي تؤمن طريقة بسيطة لتشفير وفك تشفير الملفات والمجلدات ويمكن أن تتم هذه العملية من خلال الدخول لخصائص الملف المطلوب ومن ثم اختيار **Advanced** واختيار **Encrypt contents to secure data**


12791066_1000051533417623_6908793813551182518_n P...
General
Security
Details
Previous Versions
6_1000051533417623_6908793813551182518_n
Type of file: JPG File (.jpg)
Opens with: Photos
Change...
Location: C:\Users\h2o\Desktop
Size: 58.7 KB (60,125 bytes)
Size on disk: 60.0 KB (61,440 bytes)
Created: ٠٦ آذار، ٢٠١٦, ١٠:٤٥:٠٧ ص
Modified: ٠٦ آذار، ٢٠١٦, ١٠:٤٥:٠٨ ص
Accessed: ٠٦ آذار، ٢٠١٦, ١٠:٤٥:٠١ ص
Attributes: Read-only Hidden
Advanced...
Security: This file came from another computer and might be blocked to help protect this computer.
Unblock
OK
Cancel
Apply


Advanced Attributes
Choose the settings you want for this folder.
File attributes
File is ready for archiving
Allow this file to have contents indexed in addition to file properties
Compress or Encrypt attributes
Compress contents to save disk space
Encrypt contents to secure data
Details
OK
Cancel

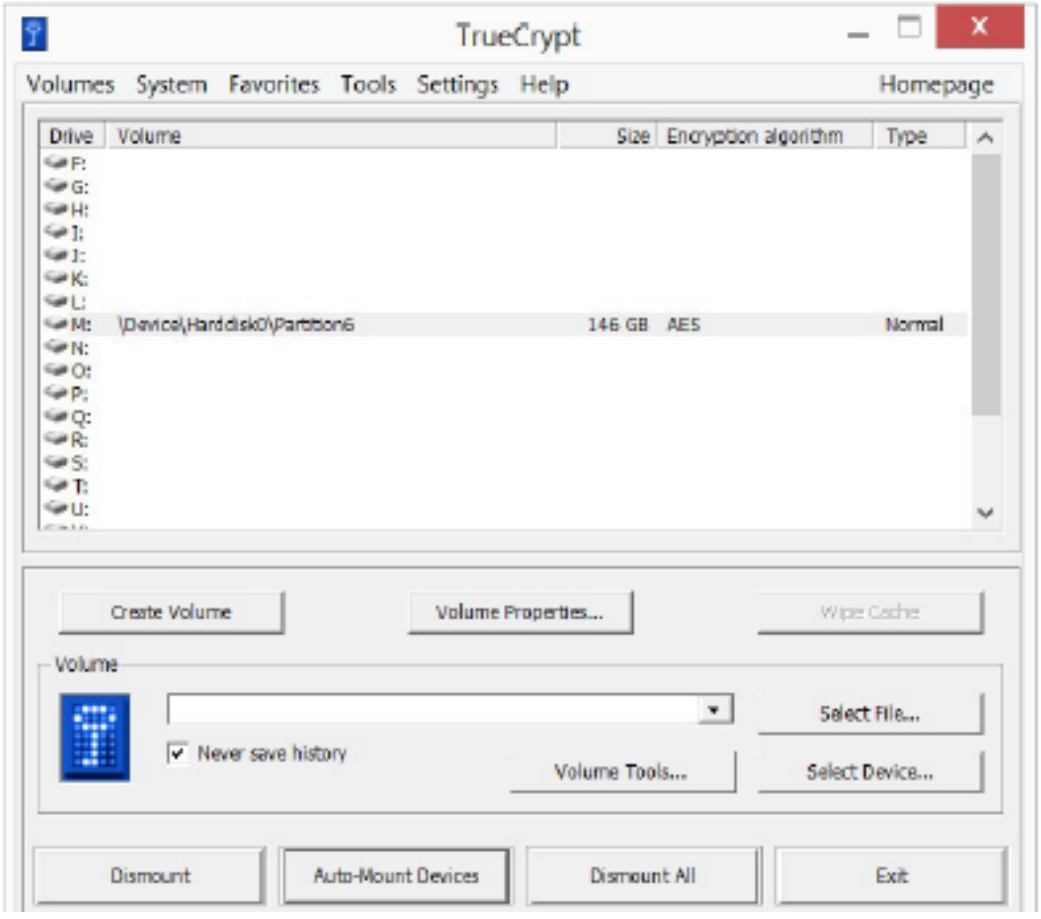
مفتاح التشفير مرتبط باسم المستخدم وكلمة السر وعندما يقوم المستخدم بتسجيل الدخول إلى النظام سوف يتم فتح الملفات المشفرة بشكل طبيعي ولكن لا يمكن فتحها من قبل مستخدمين آخرين.

يجب القيام بعملية نسخ احتياطي **backup** لمفاتيح **EFS** وحفظها في مكان آمن.

أداة تشفير الملفات TrueCrypt:

هذه الأداة مجانية ومفتوحة المصدر وتعمل على **windows and linux** وتستخدم خوارزمية التشفير **256-bit ASE**

وهي تسمح لنا بتشفير كامل القرص أو تشفير مساحة محددة.



الهاش Hash:

نوع من التشفير يعتمد على المبادئ التالية:

- تشفير باتجاه واحد **one-way** (يمكن حساب قيم الهاش ولا يمكن القيام بعملية عكسية **unhashed**)
- حجم متغير في الدخل يولد هاش بحجم ثابت (طول ثابت)
- لكل ملف قيمة هاش خاصة وفريدة لا يمكن أن تتكرر.

في بداية هذا الكتاب تحدثنا عن كيفية إنشاء صورة طبق الأصل للقرص الصلب ومن ثم القيام بحساب الهاش الخاص بالقرص الصلب والصورة المطابقة ومقارنة هذه القيم للتأكد من أن العملية تمت بشكل صحيح وأن الصورة مطابقة بشكل كامل للقرص الأصلي.

حفظ قيمة الهاش يجب أن يكون جزء من الدليل الرقمي لإثبات أن الملفات أو البيانات لم يتم التعديل عليها.

خوارزمية MD5:

خوارزمية تشفير مستخدمة بشكل كبير لسهولة تطبيقها وتقوم بتوليد خرج ثابت بطول **128 bit**

ويتم استخدامها بشكل واسع من أجل حفظ كلمات السر الخاصة بالمستخدمين.

خوارزمية SHA:

SHA (Secure Hash Algorithm)

وهي الخوارزمية الأكثر استخداماً لحساب قيم الهاش ولها أكثر من إصدار **SHA-1 , SHA-2 , SHA-3**

خوارزمية GOST:

وهي خوارزمية هاش معتمدة بمعيار قومي روسي

GOST R 34.11-94 Information Technology - Cryptographic Information Security – Hash Function

تقوم بتوليد خرج بطول ثابت **256 bits**

كلمات السر في windows:

استخدام وحساب الهاش لا يقتصر على التحقق من الصورة طبق الأصل للقرص وهو مستخدم أيضاً في حفظ كلمات السر في نظام **windows**.

مثلاً إذا كنت تستخدم كلمة السر التالية **"password"** فإن **windows** يقوم أولاً بحساب الهاش الخاص بهذه الكلمة وهو مشابه للرماز التالي:

0BD181063899C9239016320B50D3E896693A96DF

ومن ثم يقوم بحفظها في الملف **SAM (Security Accounts Manager)** الموجود في مجلد **windows**.

عندما تقوم بتسجيل الدخول فإن **windows** لا يستطيع القيام بعملية معاكسة لحساب الهاش **unhash** الخاص بكلمة السر ولكنه يقوم بأخذ كلمة السر التي قمت بكتابتها ويقوم بحاسب الهاش الخاص بها ومن ثم يقارن هذه القيمة مع القيمة المحفوظة في الملف **SAM file** وإذا كانت القيم متطابقة عندها يسمح لك بالدخول للنظام.

التعامل مع كلمات السر في windows:

في بعض الحالات يمكن أن نتعامل مع جهاز يعمل بنظام التشغيل **windows** ومن الممكن أن يحوي على الدليل الرقمي ولكن لا يمكننا فتح هذا الجهاز لأننا لا نعرف كلمة السر الخاصة به.

يوجد طريقة لكسر كلمة السر الخاصة بنظام **windows** تعتمد على هاشات محسوبة مسبقاً لكل كلمات السر المتاحة وهذه الطريقة تسمى جدول قوس قزح **rainbow table**

هذا الجدول يحوي على كل الهاشات لكل كلمات السر المحتملة ومن خلال البحث في هذا الجدول عن الهاش المطلوب يمكننا معرفة كلمة السر الأصلية الخاصة بهذا الهاش، ولكن في نظام **windows** وعند البدء في عملية الاقلاع فإن **windows** يقوم بمنع الوصول إلى الملف **SAM** الذي يحوي على الهاش الخاص بكلمة السر ويمكننا الوصول لهذا الملف من خلال الإقلاع باستخدام نظام تشغيل **linux** باستخدام **live boot disk** ونسخ محتوى الملف **SAM**

الأداة **OphCrack** تسمح لنا بالإقلاع من نظام **linux** والحصول على الملف **SAM** واستخراج الهاشات المحفوظة في داخله ومن ثم تقوم وبشكل اتوماتيكي بالبحث في جداول قوس قزح **rainbow tables** لتجد الهاش المطابق ومعرفة كلمة السر المطلوبة.

الستيغنوغرافي Steganography:

هو فن إخفاء الرسائل السرية داخل الملفات أو الصور أو المقاطع الصوتية أو الفيديو، ميزة الستيغنوغرافي عن التشفير أن إخفاء الرسالة يتم بشكل لا يلفت انتباه أي شخص.

بعض مصطلحات الستيغنوغرافي الأساسية:

- **Payload:** هو البيانات الخفية أو الرسالة المراد إخفائها.
- **Carrier:** الحامل وهو الملفات أو البيانات التي يتم إخفاء الرسالة السرية فيها.
- **Channel:** القناة وهي الوسط المستخدم في هذه العملية ويمكن أن يكون صورة أو مقطع صوتي أو مقطع فديو.

الطريقة الأكثر شيوعاً لتطبيق الستيغنوغرافي تتم من خلال **bits** الأقل أهمية في الملف **LSB (lest significant bits)**

في كل ملف يوجد عدد معين من **bits** في كل وحدة، مثلاً الصور في **windows** تحوي على **24 bits per pixel** وإذا قمنا بتغير **bits** الأقل أهمية

لهذه الصورة فإن التغيير لن يؤثر كثيراً على دقة الصورة ولن يتم ملاحظته بالعين المجردة.

يمكننا إخفاء معلومات في **bits** الأقل أهمية **LSB** لملف صورة من خلال استبدال هذه **bits** بالبيانات المراد إخفاؤها.

إخفاء الرسائل السرية في ملف صوتي يسمى الستيغنوفوني **Steganophony** وهذا يتم من خلال عدة طرق إما من خلال استبدال **bits** الأقل أهمية أو من خلال إضافة صوت إضافي عبارة عن صدى داخل الملف الصوتي وإخفاء المعلومات السرية في داخله.

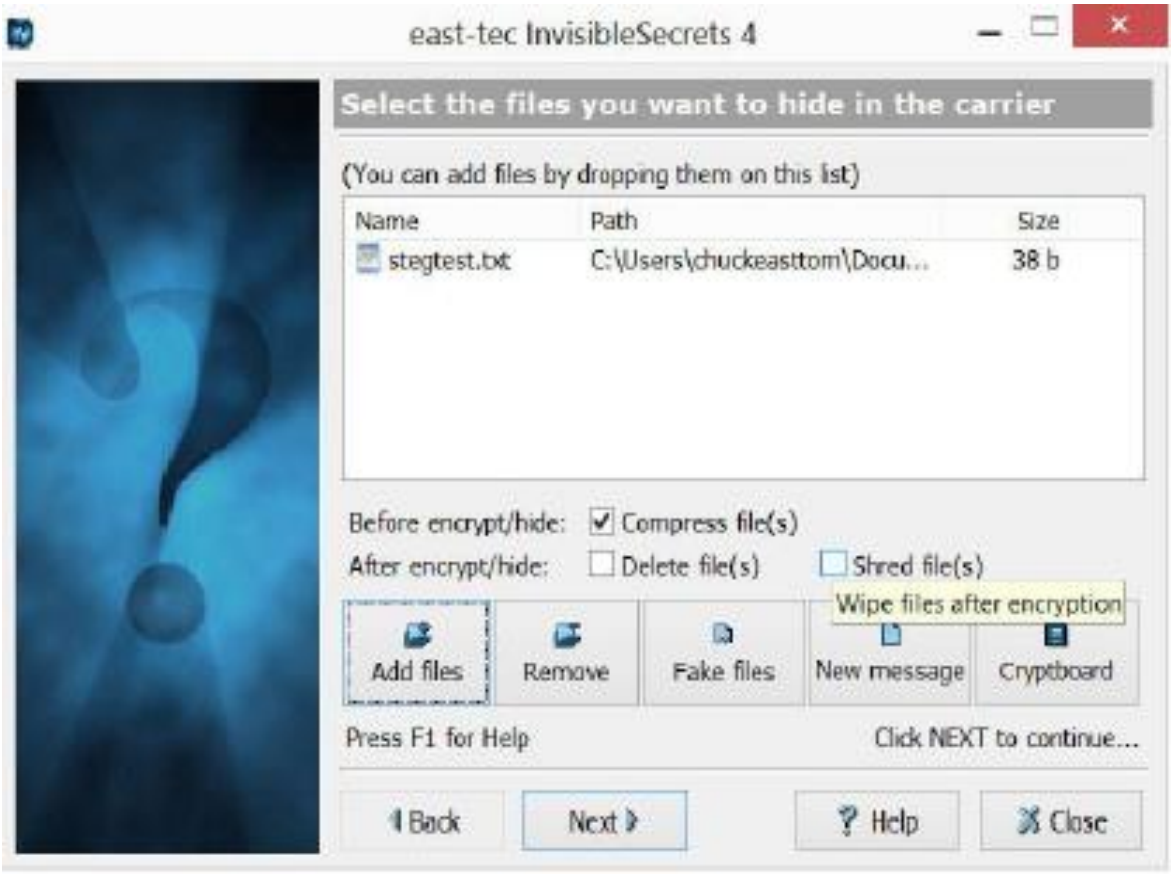
الأدوات:

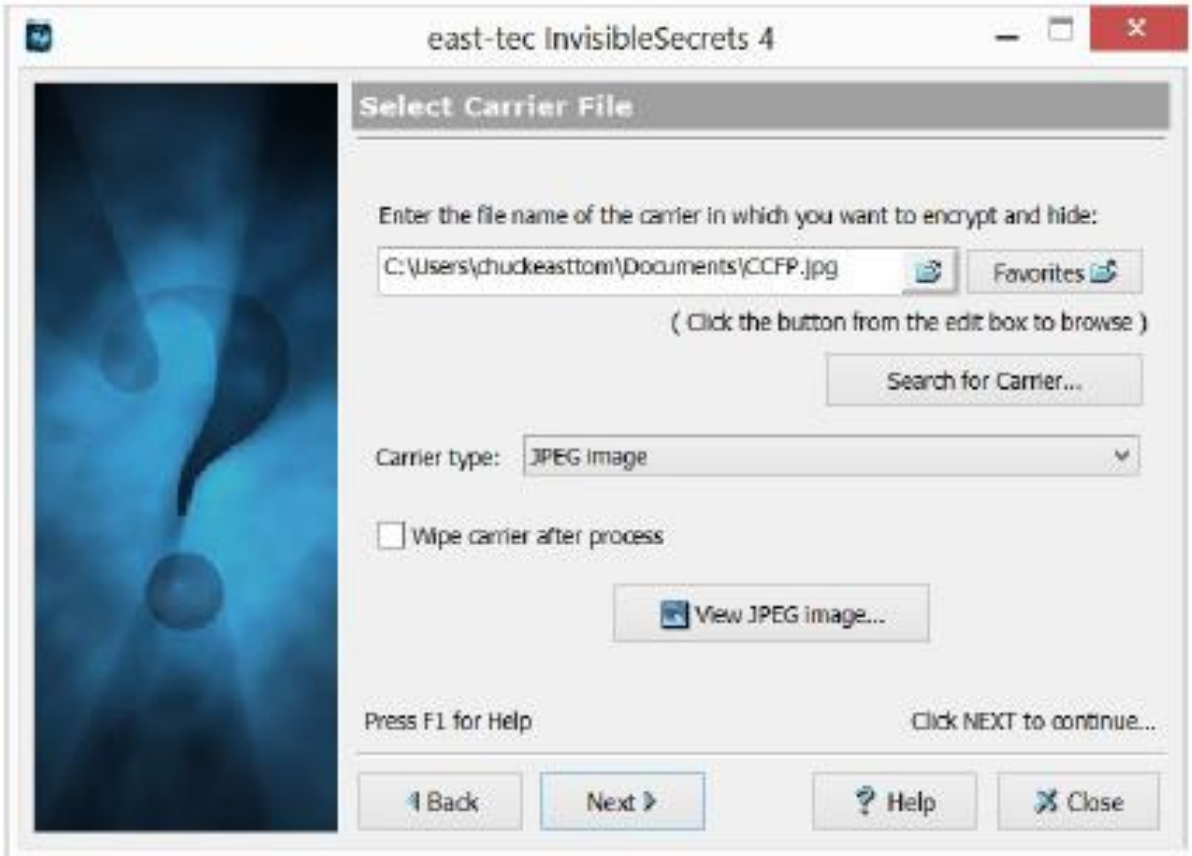
- **QuickStego**: سهلة الاستخدام ولكنها محدودة جداً.
- **Invisible Secrets**: قوية جداً ولها نسخة مجانية ونسخة تجارية.
- **MP3Stego**: مخصصة لإخفاء المعلومات داخل ملفات **MP3**
- **Stealth File 4**: يمكنها إخفاء المعلومات في الصور ومقاطع الصوت ومقاطع الفديو.
- **SteqVideo**: تقوم بإخفاء المعلومات في مقطع فديو.
- **Snow**

الأداة Invisible Secret:

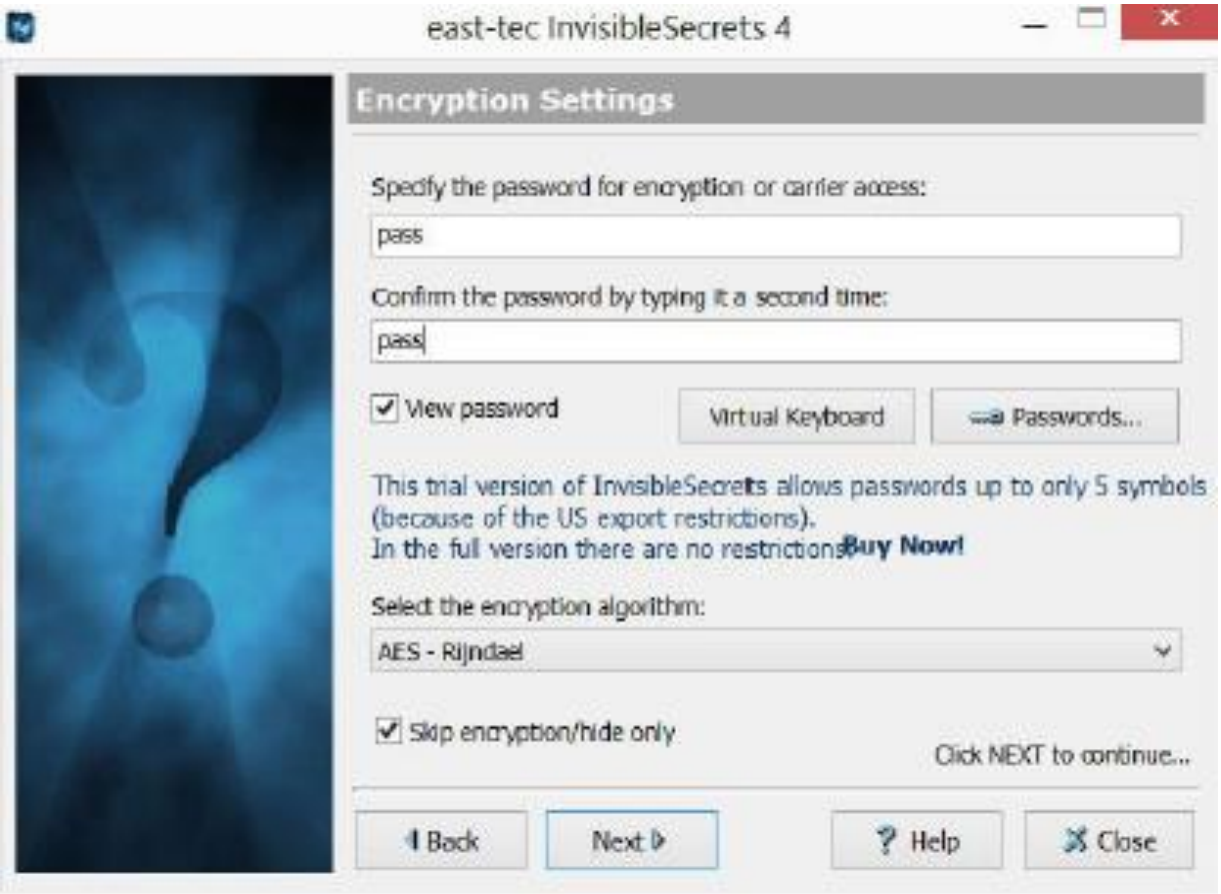
من أكثر أدوات الستيغنوغرافي شهرة، من المهم للمحقق الجنائي الرقمي أن يكون على معرفة بهذه الأداوت وطرق استخدامها

المثال التالي لإخفاء مستند نصي داخل صورة باستخدام هذه الأداة

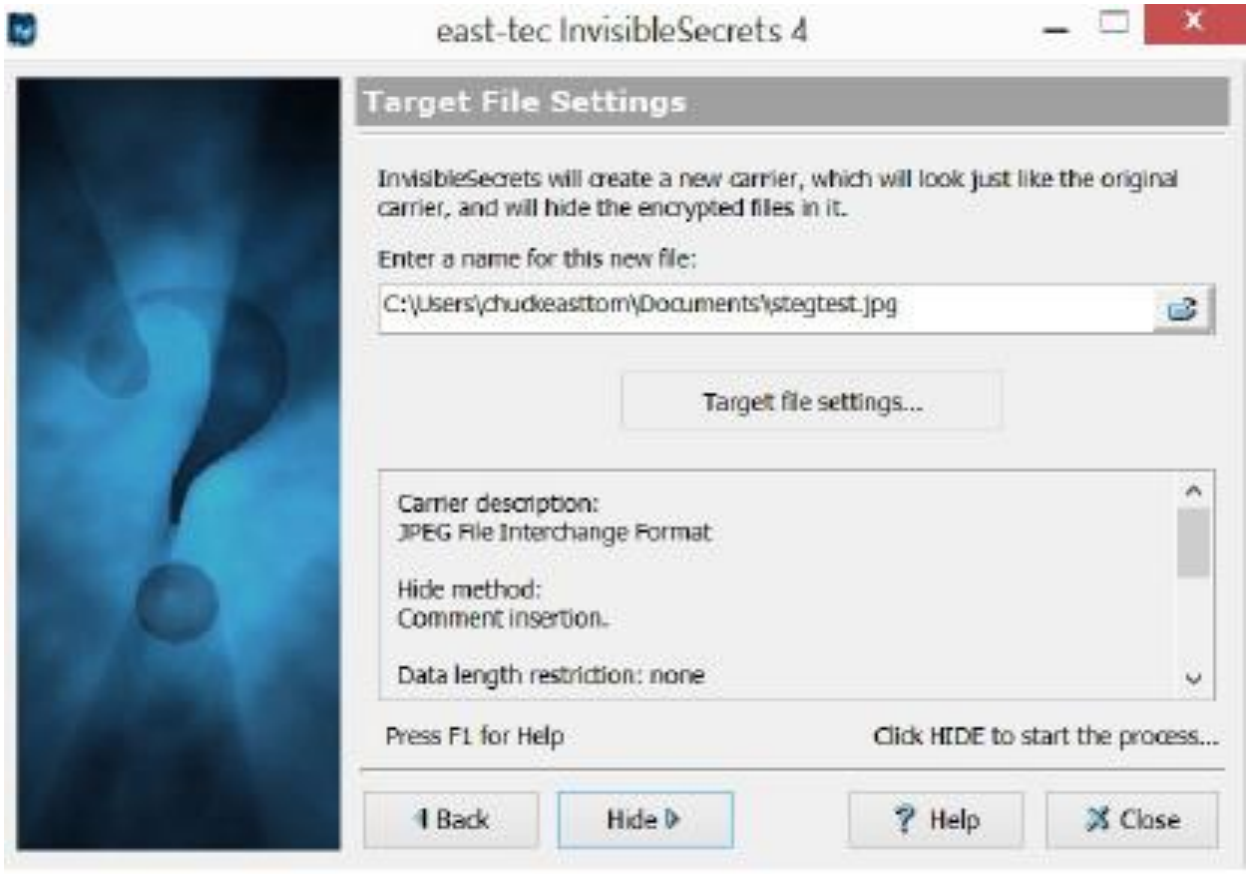

east-tec InvisibleSecrets 4
Select the files you want to hide in the carrier
(You can add files by dropping them on this list)
Name
Path
Size
stegtest.txt
C:\Users\chuckeasttom\Docu...
38 b
Before encrypt/hide:
Compress file(s)
After encrypt/hide:
Delete file(s)
Shred file(s)
Wipe files after encryption
Add files
Remove
Fake files
New message
Cryptboard
Press F1 for Help
Click NEXT to continue...
Back
Next
Help
Close


east-tec InvisibleSecrets 4
Select Carrier File
Enter the file name of the carrier in which you want to encrypt and hide:
C:\Users\chuckeasttom\Documents\CCFP.jpg
Favorites
(Click the button from the edit box to browse)
Search for Carrier...
Carrier type:
JPEG Image
Wipe carrier after process
View JPEG image...
Press F1 for Help
Click NEXT to continue...
Back
Next
Help
Close

الخطوة التالية هي اختيار كلمة سر من أجل إخفاء البيانات وتشفيرها وهو أمر اختياري



الخطوة الأخيرة هي تحديد المسار لإظهار الملف الذي يحوي على المعلومات السرية



والنتيجة ستكون نفس ملف الصورة ولكنها تحوي في داخلها على المستند النصي الذي يحوي على المعلومات السرية.

تحليل الملفات:

يوجد أكثر من طريقة لتحليل واكتشاف المعلومات السرية المخبئة داخل الملفات ومنها تحليل زوج من الألوان المتقاربة في صورة معينة لاكتشاف إذا تم استبدال **bits** الأقل أهمية **LSB** ويتم ذلك باستخدام تقنية **RQP (Raw Quick Pair)** والتي تعتمد على مبدأ زوج الألوان المتقاربة بالاعتماد على احصائيات خاصة بعدد من الألوان الفريدة.

الستيغنوغرافي مهمة جداً في عمليات التحليل الجنائي الرقمي لأن هذه الطريقة مستخدمة من قبل الجماعات الإرهابية لتبادل الرسائل السرية.

بعد مقتل أسامة بن لادن ومن خلال تحليل الأقراص الصلبة التي كانت موجودة في منزله اكتشفت القوات الاميركية أنه كان يتصل مع عناصر تنظيم القاعدة من خلال إخفاء الرسائل السرية داخل صور إباحية.

تحليل الشيفرات السرية:

تحليل الشيفرات السرية أمر معقد وصعب جداً وليس كما يبدو في الأفلام.

تتم هذه العملية من خلال محاولة فك تشفير الرسائل المشفرة باستخدام تقنية القوة الغاشمة **brute force** (تجربة عدد كبير جداً من القيم وبشكل أتوماتيكي على أمل أن تكون إحدى هذه القيم هي القيمة الصحيحة) وهذه الطريقة لا تنفع مع خوارزميات التشفير الحديثة.

التلاعب بالسجلات logs tampering:

بالإضافة لطرق تشفير وإخفاء المعلومات السابقة فإن المجرم يحاول أيضاً إخفاء العمليات التي قام بها من خلال التلاعب في السجلات **logs** من خلال محاولة حذف مدخلات هذه السجلات وهذا الأمر صعب ولكن من الممكن القيام به في كل من **windows and linux** بعد الحصول على أعلى مستوى صلاحيات في النظام.

الأداة Auditpol:

هذه الأداة تعمل في نظام **windows** وتسمح للمهاجم بإيقاف تقنيات المراقبة.

اذا وجدنا أن سجلات المُخدّم **server logs** تحوي على فراغ (مدة زمنية معينة بدون أي مدخلات) فهذا يمكن أن يشير إلى أن المهاجم قد استخدم هذه الأداة من أجل إيقاف المراقبة بشكل مؤقت خلال فترة القيام بالهجوم.

Winzapper:

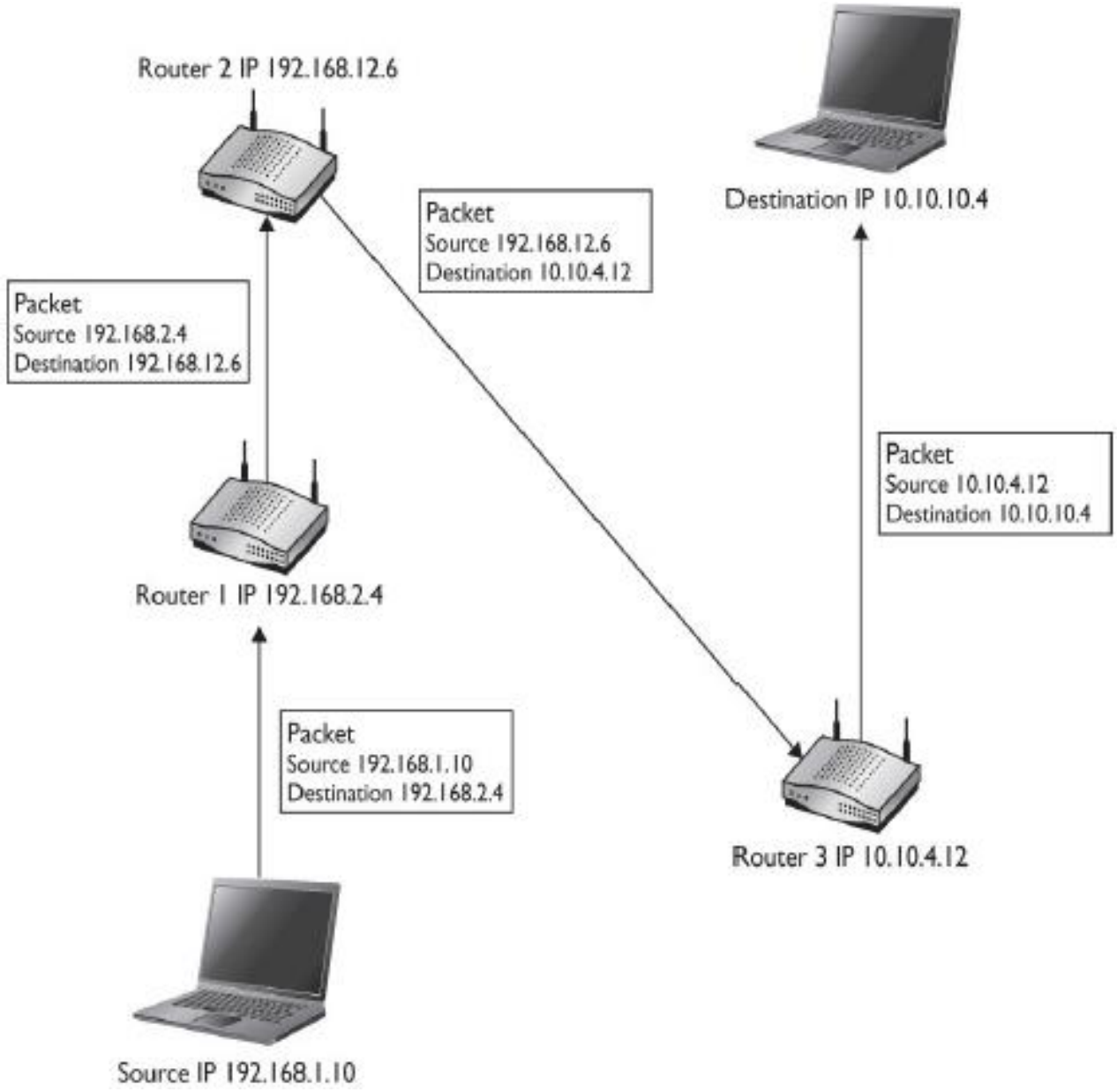
هذه الأداة تسمح للمهاجم بمسح مدخلات سجل معين وهذا الأمر لا يتم بسهولة ويحتاج لأعلى مستوى صلاحيات للقيام بذلك.

Onion Routing:

تغليف حزم البيانات وتشفير الترويسة **header** الخاصة بحزم البيانات.

ترويسة حزمة البيانات تحوي على عنوان المصدر والهدف التالي وعندما تصل حزمة البيانات إلى المُوجه **(router)** التالي يتم فك تشفير الترويسة (إزالة الغلاف بشكل مشابه لتقشير البصلة) وعندها يظهر عنوان الهدف التالي وفي كل مرحلة يتم فك تشفير الترويسة لمعرفة العنوان التالي إلى أن تصل حزمة البيانات إلى وجهتها النهائية.

عند استخدام هذه الطريقة، حتى ولو تمكنا من إلتقاط حزم البيانات في مُوجه **router** معين فلن نستطيع معرفة الوجهة النهائية لهذه البيانات.



هذه التقنية يتم تطبيقها من خلال استخدام شبكة **Tor** وهي مستخدمة من قبل الهاكرز بشكل واسع من أجل التخفي أثناء القيام بهجمات عبر الشبكة.

Spoofing:

عندما يقوم المجرم باختراق جهاز أو موقع أو منظومة معلوماتية فهو يحاول استخدام بعض التقنيات من أجل اخفاء نفسه ومنها تغيير عنوان **IP** الخاص بجهازه **IP Spoofing** ويوجد العديد من الأدوات التي تقوم بهذه العملية وبشكل اتوماتيكي.

كما يقوم أيضاً بتغيير عنوان **MAC address** لبطاقة الشبكة الخاصة به ومثل هذه العمليات تزيد من صعوبة عملية التحقيق الجنائي الرقمي.

VPN and Tunneling:

إحدى الطرق التي يمكن أن يستخدمها المجرم لإخفاء بياناته عبر الشبكة هي **tunneling** وهذه العملية تتم من خلال تشفير حزم البيانات عبر الشبكة.

هذه العملية لها استخدامات شرعية (عند الدخول إلى الحسابات البنكية عبر الشبكة وعند الاتصال بين أفرع الشركات عبر الشبكة) ويتم ذلك باستخدام شبكة خاصة افتراضية **VPN (Virtual Private Network)** حيث يتم تشفير البيانات وبذلك لا يستطيع أي شخص معرفة محتوى هذه البيانات حتى ولو تمكن من إلتقاطها.

التحليل الجنائي الرقمي للشبكة

محتوى هذا الفصل:

- تحليل حزم البيانات باستخدام **Wireshark**
- برتوكول **HTTP**
- الشبكات اللاسلكية.
- التحليل الجنائي الرقمي للمُوجّه **router** والجدار الناري **fire wall**.
- السجلات في **windows and linux**.

مقدمة:

معظم الجرائم المعلوماتية تتم باستخدام الشبكة وعبر الانترنت.

الفيروسات وبرمجيات التجسس **Spyware** وأحصنة طروادة **Trojan Horse** تنتشر عادةً عبر الشبكة وهجمات منع الخدمة **DoS (Denial of Service)** تتم أيضاً باستخدام الشبكة وعبر الانترنت، لذلك فإن التحليل الجنائي الرقمي للشبكة هو أمر مهم جداً.

حزم البيانات:

حزم البيانات **Packets** هي مجموعة من الأصفار والواحدات التي يتم إرسالها عبر الشبكة، وكل حزمة بيانات تتألف من:

- معلومات عن مصدر و وجهة حزمة البيانات.
- معلومات عن حدود حزمة البيانات (بداية الحزمة ونهايتها).
- معلومات لتحديد الأخطاء أثناء عملية الإرسال.

حزمة البيانات مقسمة إلى ثلاث أقسام وهي:

- الترويسة **header**: تحوي معلومات عن عنوان المصدر وعنوان الوجهة أو الهدف.
- البيانات **data**: المعلومات أو البيانات المراد إرسالها.
- التذييل **footer**: تحدد نهاية حزمة البيانات وتحوي على معلومات لاكتشاف الأخطاء.

يوجد عدة أنواع من حزم البيانات، منها ذو حجم ثابت ومنها ذات حجم متغير.

أي شيء يتم إرساله في الطبقة الثانية من طبقات

OSI (Open System Interconnection) يسمى إطار **frame**

و أي شيء يتم إرساله عبر الطبقة الرابعة يسمى **segment or datagram**

حزمة البيانات **packet** هو مصطلح عام يمكن أن يشمل كل ما سبق.

ترويسة حزمة البيانات:

وهي مكان مفيد جداً لجمع المعلومات في عملية التحليل الجنائي الرقمي ومن خلالها يمكننا تحديد مصدر قدوم حزمة البيانات والبرتوكول المستخدم ومعلومات أخرى.

يوجد عدة أنواع للترويسات وهي:

- **Ethernet header**
- **TCP header**
- **IP header**

وكلها تحوي على معلومات مفيدة جداً في عملية التحليل الجنائي الرقمي.

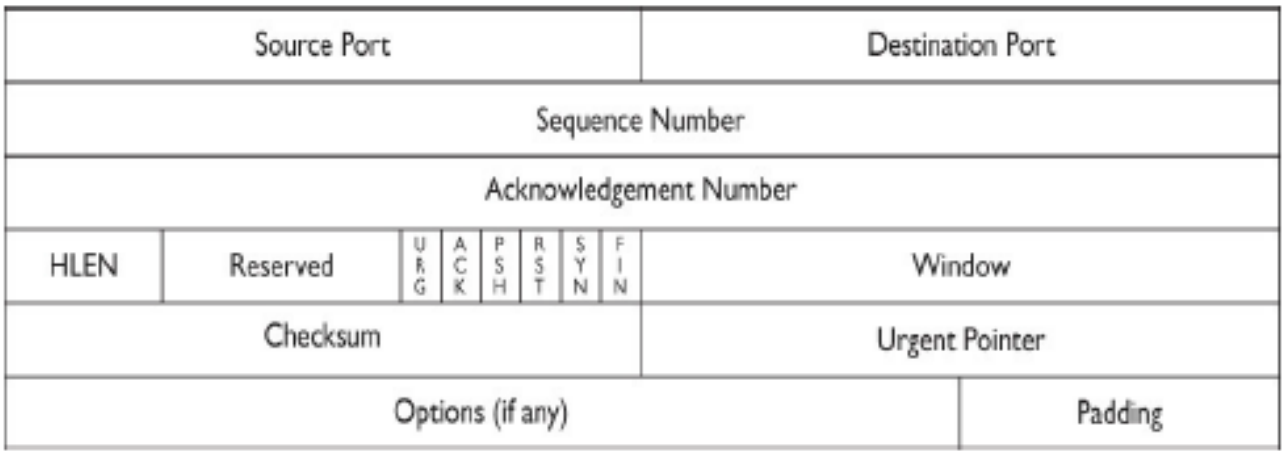
لنبدأ بالترويسة **TCP header** والتي تحوي على معلومات تتعلق بطبقة النقل **transport layer** من طبقات **OSI model** كما تحوي على عنوان المصدر وعنوان الوجهة ورقم المنفذ المستخدم في عملية الاتصال وتحوي أيضاً على

bits التحكم التي تستخدم للإشارة لبدء الاتصال أو إعادة الاتصال أو قطع الاتصال.

أشهر **bits** التحكم هي:

- **URG**: للإشارة إلى أن هذه الحزمة من البيانات هي حزمة مستعجلة.
- **ACK**: للإعلام بمحاولة مزامنة الاتصال.
- **RST**: تستخدم عند حدوث خطأ في الاتصال.
- **SYN**: للبدء بالاتصال.
- **FIN**: للإعلام بانتهاء الاتصال.

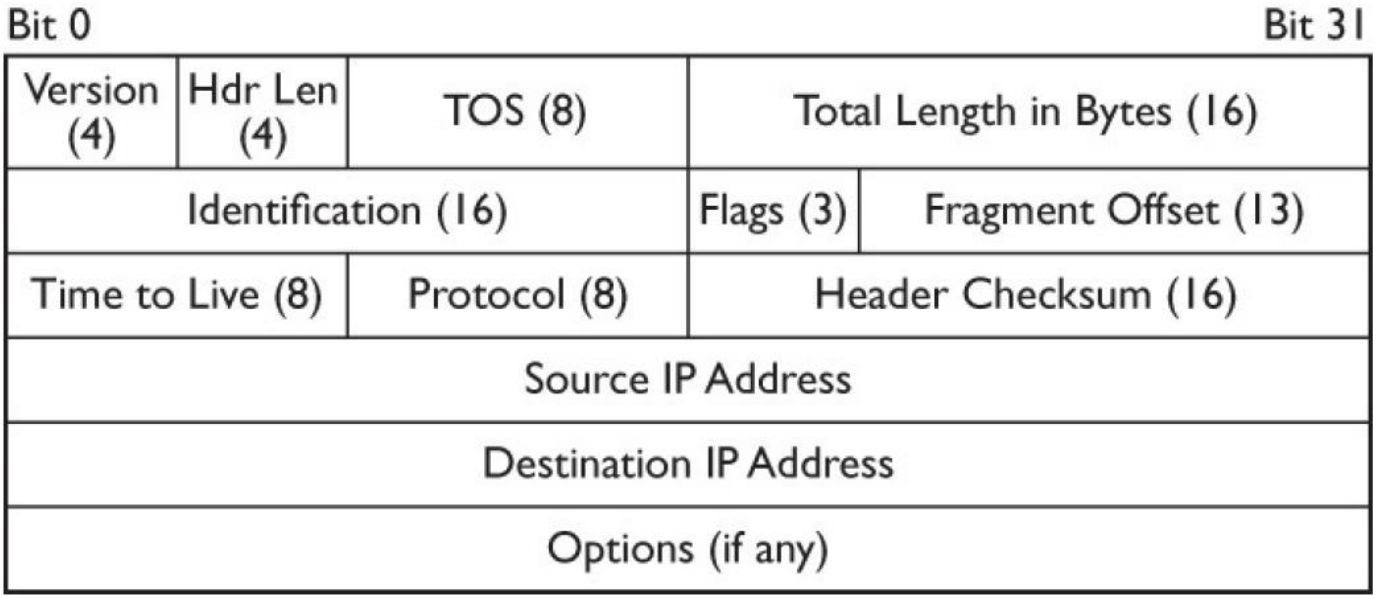
ترويسة **TCP header** تظهر في الشكل التالي:



الترويسة **IP header** تلقى اهتمام أكبر فهي تحوي على عنوان المصدر وعنوان الهدف **source IP address and destination IP address** كما تحوي على نوع البروتوكول المستخدم في عملية الاتصال ونسخة **IP** المستخدمة في الاتصال **(IPv4 or IPv6)**

الحقل **TTL (Time To Live)** يخبر حزمة البيانات بعدد القفزات المتبقية لحين الوصول إلى الهدف.

الشكل التالي يظهر ترويسة **IP header**



عملية الاتصال:

عملية الاتصال تبدأ بإرسال أحد طرفي الاتصال طلب **SYN** ويقوم الطرف الثاني بالرد بإرسال **SYN and ACK** ثم يقوم المرسل بالرد والإعلام بإرسال **ACK** ومن ثم تبدأ عملية الاتصال.

المهاجم يمكن أن يقوم بإرسال حزم بيانات مشوهه للقيام بهجمات معينة، مثلاً في هجوم منع الخدمة **DoS attack** يمكن أن يقوم المهاجم بإغراق الهدف من خلال إرسال طلبات **SYN** ولا يقوم بالرد على طلبات **SYN/ACK** المرسلة إليه.

المهاجم يمكن أن يقوم بسرقة جلسة الاتصال من خلال إرسال **RST** إلى أحد طرفي الاتصال.

ترويسة **Ethernet header** تحوي على عناوين **MAC address** لكل من المصدر والهدف.

Payload:

وهو البيانات المراد إرسالها ويمكن أن يتم تشفير هذه البيانات لمنع الأشخاص الاخرين من رؤية محتواها ولكن يمكن رؤية المعلومات الموجودة في الترويسة.

التذييل Trailer or Footer:

يحدد نهاية حزمة البيانات ويحوي على معلومات مفيدة لتحديد الأخطاء مثل **CRC (Cyclic Redundancy Check)**

يتم جمع عدد الواحدات الموجودة في البيانات وحفظها في **CRC** والطرف المستقبل يقوم بجمع عدد الواحدات في البيانات المستقبلة ويقارنها بالقيمة الموجودة في **CRC** وإذا كانت القيم متطابقة فهذا يعني أن حزمة البيانات سليمة وإلا فإن حزمة البيانات تحوي على خطأ تم أثناء عملية الإرسال.

تحليل حزم البيانات:

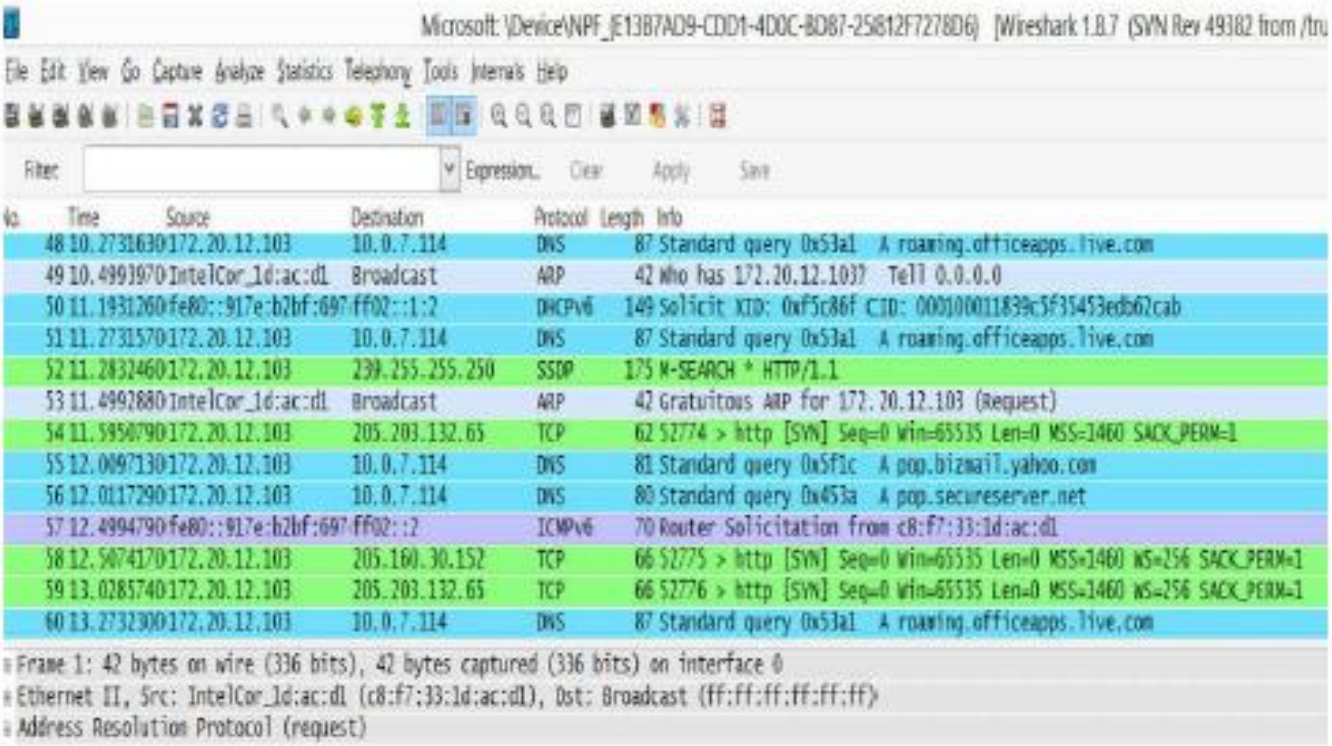
تحليل حزم البيانات يجب أن يتم من قبل شخص خبير في حزم وبرتوكولات الشبكة.

العملية تبدأ بالتقاط حزم البيانات **packet sniffer** ويتم ذلك باستخدام برنامج يقوم باعتراض وإلتقاط حزم البيانات عبر الشبكة، وللقيام بهذه العملية يجب أن نجعل بطاقة الشبكة تعمل في نمط المراقبة أو النمط اللاأخلاقي **Promiscuous mode** والذي يسمح لنا برؤية كل حزم البيانات التي يتم إرسالها أو استقبالها عبر الشبكة.

أشهر أدوات إلتقاط حزم البيانات هو **Wireshark** والمعروف باسم محلل البرتوكولات وهو أداة مجانية ويعمل على كل من **windows and linux**.

في البداية يجب أن نقوم بتحديد بطاقة الشبكة المراد استخدامها.

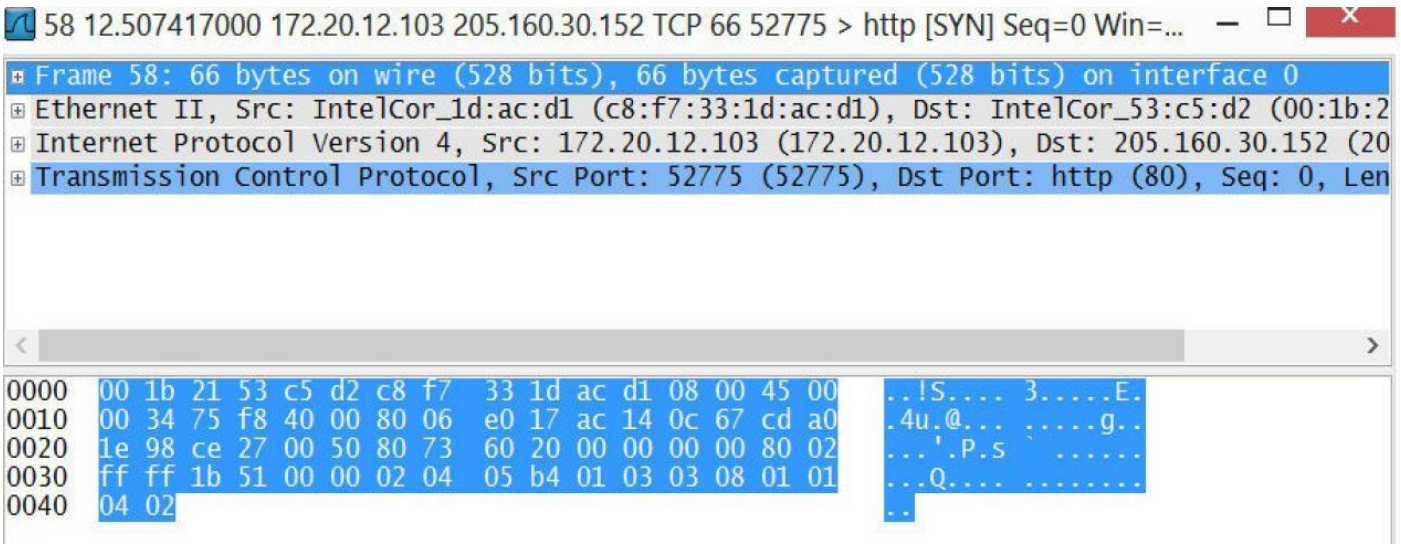
ومن ثم الضغط على **start** وبعدها يمكننا تصفية حزم البيانات للحصول على البيانات المطلوبة



كما ترى في كل حزمة بيانات يمكننا رؤية عنوان المصدر وعنوان الهدف والبروتوكول المستخدم

Source	Destination	Protocol
172.20.12.103	10.0.7.114	DNS
IntelCor_1d:ac:d1	Broadcast	ARP
fe80::917e:b2bf:697	ff02::1:2	DHCPv6
172.20.12.103	10.0.7.114	DNS
172.20.12.103	239.255.255.250	SSDP
IntelCor_1d:ac:d1	Broadcast	ARP
172.20.12.103	205.203.132.65	TCP
172.20.12.103	10.0.7.114	DNS
172.20.12.103	10.0.7.114	DNS
fe80::917e:b2bf:697	ff02::2	ICMPv6
172.20.12.103	205.160.30.152	TCP
172.20.12.103	205.203.132.65	TCP
172.20.12.103	10.0.7.114	DNS

وعند الضغط على أي حزمة بيانات يمكننا رؤية محتوى الترويسة والبيانات الخاصة بها



السجلات logs:

أداوت تحليل بيانات الشبكة والبرتوكولات تعطينا معلومات عن الأمور التي تحدث بالوقت الحالي ولكن عملية التحليل الجنائي الرقمي يجب أن تتم أيضاً من خلال فحص السجلات قبل وبعد عملية الهجوم.

السجلات **logs** الخاصة بنظام التشغيل وسجلات المُوجه وسجلات أجهزة الحماية **(firewall and IDS)** يمكن أن تحوي على الأدلة الرقمية المطلوبة

أجهزة كشف الاختراق **IDS (Intrusion Detection System)** عبارة عن برامج أو أجهزة تقوم وبشكل أتوماتيكي بمراقبة وتحليل كل العمليات الخاصة بالنظام والشبكة وتقوم بتحليلها لاكتشاف ومنع الهجمات المحتملة.

سجلات الجهاز تقوم بتسجيل كل نشاطات المستخدم في النظام وفي الشبكة وهي تحوي على معلومات مهمة في عملية التحليل الجنائي الرقمي مثل اسم المستخدم وعنوان **IP address** وتاريخ و وقت الدخول إلى النظام و نوع البرتوكول المستخدم في الاتصال و أمور أخرى.

كما أن السجلات تحوي على معلومات عن البرامج التي تم استخدامها (من استخدم هذا البرنامج و متى).

سجلات نظام التشغيل تحوي على معلومات عن استخدام الجهاز والأخطاء التي حصلت وأوقات تشغيل أو إعادة تشغيل الجهاز.

سجلات أجهزة الحماية في الشبكة مثل سجلات المُوجه **router** و سجلات الجدار الناري **firewall** تؤمن معلومات عن كل العمليات التي تمت عبر الشبكة.

فحص وتحليل السجلات يمكن أن يؤدي لكشف الهجمات على الشبكة، مثلاً سجلات الجدار الناري تظهر محاولات الاتصال التي تم منعها من قبل الجدار الناري والتي يمكن أن تكون هجمات محتملة على الشبكة كما أن هذه السجلات تظهر الطريقة التي تمكن من خلالها المهاجم الوصول إلى الشبكة.

سجلات أجهزة كشف الاختراق **IDS logs** تؤمن معلومات عن طبيعة الهجوم على الشبكة مثل هجمات **buffer overflows** أو هجمات تنفيذ رماز خبيث أو هجمات تخمين كلمات السر باستخدام تقنية القوة الغاشمة **brute force**

أجهزة كشف الاختراق **IDS** تقوم بإلتقاط وتحليل كل البيانات التي يتم إرسالها واستقبالها عبر الشبكة ومن خلال تحليل سجلات هذا الجهاز يمكننا اكتشاف التعليمات التي قام المهاجم بتنفيذها على الجهاز الهدف أو الملفات الخبيثة التي قام برفعها أو الأكواد الخبيثة التي قام بتنفيذها.

الأمر المهم الذي يجب معرفته أن الهاكرز المحترفون يتبعون بعض الطرق لتضليل المحقق الرقمي من خلال شن هجمات ثانوية ليتم تسجيلها في السجلات والقيام بالهجوم الرئيسية باستخدام طريقة مختلفة.

برتوكول HTTP:

HTTP (Hypertext transfer protocol)

هو بروتوكول (عمليات متفق عليها) يستخدم للتفاعل والاتصال مع تطبيق الويب.

ليس هناك أي اعتبار للحماية أو الخصوصية عند استخدام **HTTP**

استخدام هذا البرتوكول بدون استخدام **cookies** يمكن أن يطلب منك إعادة تسجيل الدخول خلال كل خطوة أو كل عمل تقوم به وهذا أمر غير عملي لذلك تم إيجاد مفهوم الجلسة **session** حيث يقوم الموقع بحفظ مسار طلباتك بعد قيامك بعملية تسجيل الدخول، وهي تؤمن عامل أخر يكون عرضة للهجوم في موقع الويب.

يمكننا رؤية التفاصيل عن كيفية عمل **HTTP** باستخدام أداة تحليل برتوكولات مثل **wireshark**.

استخدام **secure HTTP (HTTPS)** يمنع بعض أنواع الهجمات.

يتم الحصول على **HTTPS** عندما يستخدم برتوكول **HTTP** التشفير **SSL/TLS(Secure Socket Layer/Transport Layer Security)**

والذي يضيف **SSL/TLS** إلى طلب وإجابة **HTTP** العادية وهي أفضل طريقة لإفشال هجوم المهاجم في الوسط **MiTM** وهي تؤمن اتصال خاص ومحمي بين المتصفح وموقع الويب.

استخدام **HTTPS** يسمح بالاتصال مع موقع الويب عبر قناة اتصال مشفرة.

Cycles HTTP:

دورة أو حلقة **http** (الطلب **reguest** من متصفح المستخدم والإجابة **response** العائدة من مُخدّم الويب **web server**).

المتصفح يرسل طلب يحوي على بارامترات (متغيرات) خاصة بدخل المستخدم ومُخدّم الويب يرسل إجابة يتم توجيهها إلى مصدر الطلب.

موقع الويب يمكن أن يعمل بالاعتماد على قيمة البارامترات لذلك فهي أول هدف يقوم المهاجم بمهاجمته وذلك باستخدام قيم خبيثة للبارامترات لاستغلال موقع الويب ومُخدّم الويب.

ترويسة HTTP Header:

كل دورة **HTTP cycle** تتضمن ترويسات في كل من طلب المستخدم وإجابة المُخدّم والتي تحوي تفاصيل حول الطلب والإجابة.

هناك العديد من هذه الترويسات ولكننا سنهتم فقط ببعض الأنواع في هذا الكتاب.

الترويسات التي يتم إعدادها في مُخدّم الويب وإرسالها إلى متصفح المستخدم كجزء من الإجابة وهي:

- **Set-Cookie:** هذه الترويسة تؤمن مُعرف للجلسة للمستخدم للتأكيد أن جلسة المستخدم مازالت مستمرة.

  إذا تمكن المهاجم من سرقة الجلسة فيمكنه استغلال واختراق المستخدم داخل الموقع.
- **Content-Length:** قيمة هذه الترويسة هي طول جسم الإجابة بالبايت، هذه الترويسة مفيدة للمهاجم لأنها تساعده على فك تشفير إجابة الموقع وهي قابلة للتطبيق في هجوم القوة الغاشمة **brute force**.
- **Location:** هذه الترويسة تستخدم عندما يقوم الموقع بإعادة توجيه المستخدم إلى صفحة جديدة.

  وهي مفيدة للمهاجم لأنه يمكن أن يستخدمها لتعريف الصفحات المسموحة فقط بعد نجاح عملية المصادقة.

الترويسات التي ترسل من متصفح المستخدم هي:

- **Cookie:** هذه الترويسة ترسل **cookie** أو أكثر من **cookie** إلى المُخدّم للحفاظ على جلسة المستخدم.

  قيمة ترويسة مُعرف الجلسة دائماً تكون مطابقة لقيمة **Set-cookie header** التي يعلن عنها المُخدّم.

  هذه الترويسة مفيدة للمهاجم لأنها تؤمن جلسة شرعية مع موقع الويب والتي يمكن أن تستخدم للهجوم ضد مستخدمين أخرين.

- **Referrer:** هذه الترويسة تعرض قائمة بصفحات الويب التي زارها المستخدم سابقاً عندما يتم تشكيل طلب الويب التالي.

  وهي مفيدة للمهاجم لأن هذه القيمة يمكن تغييرها بسهولة وبالتالي إذا اعتمد موقع الويب على هذه الترويسة من أجل الحماية فيمكن بسهولة تخطي الحماية باستخدام قيمة مزورة.

HTTP Status Codes:

بما أن متصفحك يستقبل رد المُخدّم، فهو يتضمن رمز الحالة للإشارة إلى نوع الإجابة، هناك أكثر من **50** رمز إجابة **HTTP** وهي مجمعة في خمس عائلات.

معرفة نوع عائلة الإجابة يسمح لك بفهم كيف يتم معالجة مدخلاتك من قبل الموقع.

- **100:** هذه الإجابات هي إعلام من قبل مخدّم الويب وعادةً تعني أن هناك إجابة إضافية قادمة من المخدّم، مع العلم بأنه من النادر أن نراها في إجابات الإصدارات الحديثة من مخدّمات الويب.
- **200:** هذه الإجابات هي إشارة أن طلب المستخدم تم استقباله ومعالجته من قبل مُخدّم الويب بنجاح والإجابة سيتم إرسالها إلى متصفحك.

  أشهر رموز الحالة ل **HTTP** هو **200 OK**
- **300:** هذه الإجابات تستخدم للإشارة لإعادة التوجيه عندما يتم إرسال إجابات إضافية إلى المستخدم.

التطبيق الأكثر شيوعاً لهذا الرمز هو لإعادة توجيه متصفح المستخدم إلى الصفحة الرئيسية بعد نجاح عملية المصادقة مع موقع الويب.

Redirect 302 وترسل إجابة أخرى يتم استلامها مع **OK 200**

- **400:** هذه الإجابات تستخدم للإشارة للخطأ في الطلب من قبل المستخدم.

هذا يعني أن المستخدم قام بإرسال طلب لا يمكن معالجته من قبل موقع الويب، أشهر أكواد الحالة في هذا العائلة هي

Unauthorized, 403 Forbidden, 404 Not Found 401

- **500:** هذه الإجابات تستخدم للإشارة لخطأ من جانب المُخدّم.

أشهر رموز الحالة في هذه العائلة

Internal Server Error and 503 Service Unavailable 500

هذه الرموز ورسائل الخطأ مفيدة جداً في عملية التحليل الجنائي الرقمي لتحديد نوع الهجوم مثلاً عند ظهور الرمز **503 errors** عدد من المرات فهذا يعتبر دليل على هجوم منع الخدمة **DoS attack**

الرمز رقم **Error code 305** يشير إلى أن المصدر متاح فقط باستخدام مُخدّم وكيل **proxy** وهذا يعطينا معلومات عن بنية مُخدّم الويب.

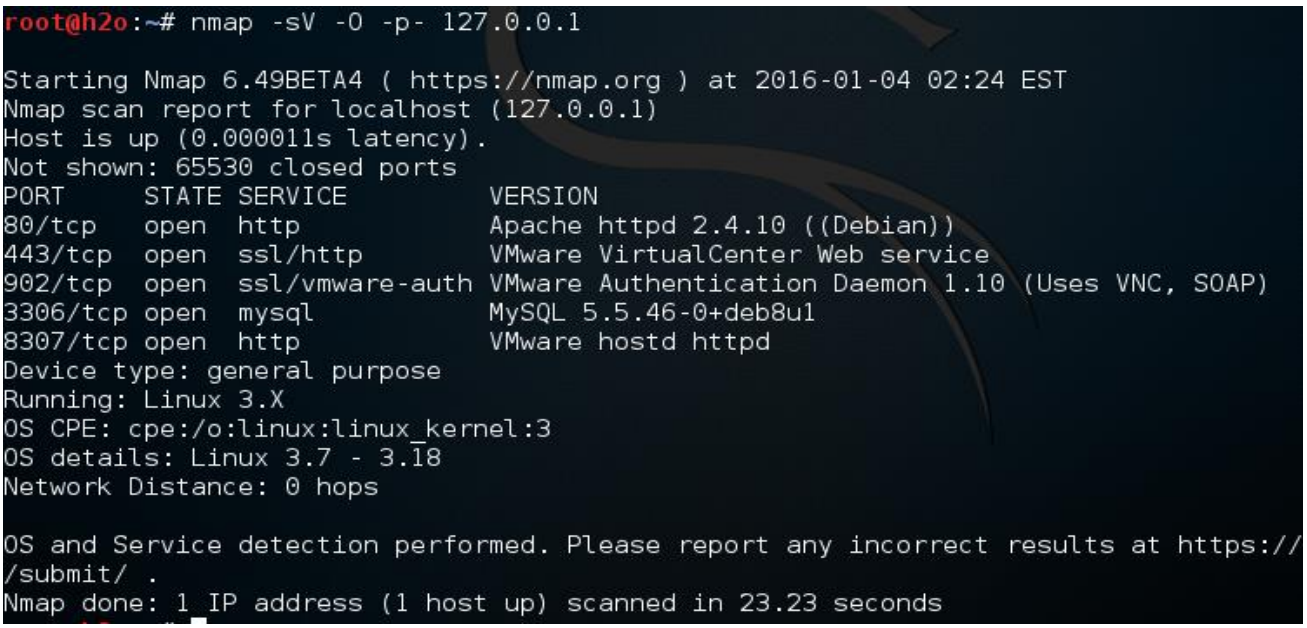
الرمز **407** تشير إلى أن كل عمليات المصادقة تحتاج لمخدّم وكيل **proxy**.

:NMAP

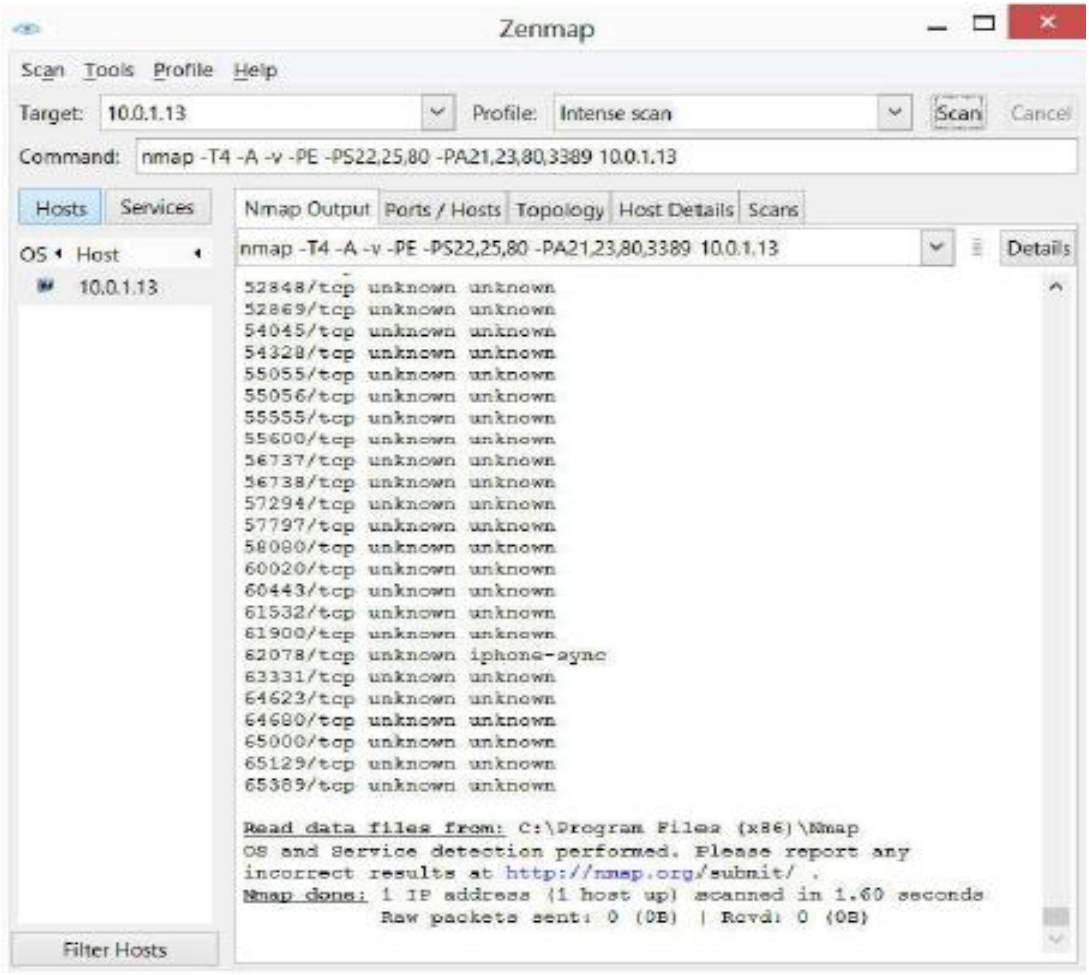
الأداة الأكثر شهرة للقيام بعملية فحص المنافذ **port scanning** وهي موجودة بشكل تلقائي في نظام **Kali**

هناك العديد من أنواع الفحص التي تستطيع هذه الأداة القيام بها.

هذه الأداة تعمل من خلال سطر الأوامر ويمكنها اكتشاف المنافذ المفتوحة وتحديد الخدمات التي تعمل على الجهاز عبر الشبكة كما يمكنها تحديد نوع نظام التشغيل وتملك خيارات إضافية تسمح بالقيام بهذه العملية بشكل سري وتجاوز إجراءات الحماية



يوجد واجهة رسومية لهذه الأداة وهي **Zenmap** (موجودة في **Kali** بشكل تلقائي)



الشبكات اللاسلكية:

التعرف على طريقة عمل الشبكات اللاسلكية هو أمر ضروري للمحقق الجنائي الرقمي.

الشبكات اللاسلكية منتشرة في كل مكان و العديد من الجرائم المعلوماتية تتم من خلالها.

معايير الشبكات اللاسلكية:

- **802.11a:** هذا المعيار يشير إلى الشبكات اللاسلكية التي تعمل من خلال التردد **5 GHz**

- **802.11b:** هذا المعيار يشير للشبكات اللاسلكية القديمة التي تعمل على التردد **2.4 GHz** والتي لها سرعة نقل بيانات **11 Mbps**
- **802.11g:** وهو تطوير للمعيار **802.11b** ويعمل على التردد **2,4 GHz** وبسرعة نقل بيانات تصل إلى **54 Mbps**
- **802.11n:** يشير للشبكات اللاسلكية الحديثة ويمكن أن يعمل على كلا الترددين **2.4 or 5 GHz** وبسرعة نقل بيانات تصل إلى **100 to 140 Mbps**

يوجد العديد من الأدوات التي تسمح للمهاجم أن يقوم بالتنصت على الوسط الراديوي وإلتقاط حزم البيانات اللاسلكية والقيام بهجمات عبر الشبكة اللاسلكية.

هجوم منع الخدمة:

يتم هذا الهجوم من خلال إغراق الشبكة أو الموقع أو المُوجه **router** بعدد كبير من الطلبات مما يؤدي إلى استهلاك كامل عرض الحزمة ومنع الخدمة عن باقي المستخدمين، التالي بعض أنواع هذا الهجوم:

- **Ping of Death Attack**: المهاجم يقوم بإرسال طلبات **ICMP echo** باستخدام التعليمة **ping** وبحجم وعدد كبير وفي نفس الوقت إلى هدف معين وهذا يمكن أن يؤدي إلى انهيار النظام الهدف ومنع الخدمة عن باقي المستخدمين.

العديد من الشركات تقوم بضبط أجهزة الحماية (الجدار الناري) لمنع طلبات **ICMP**

- **Teardrop Attack:** المهاجم يقوم بإرسال أجزاء من حزم البيانات بقيم سيئة وخبيثة تسبب تدمير الهدف الذي يحاول أن يقوم بإعادة ترتيب أجزاء حزم البيانات المستقبلة.
- **SYN Flood Attack:** المهاجم يقوم بإرسال عدد كبير جداً من طلبات **SYN** إلى الهدف وعندما يقوم الهدف بالرد على هذه الطلبات فإن المهاجم لا يقوم بالرد لإعلام الهدف وهذا يؤدي إلى اغراق الهدف بطلبات **SYN**

أجهزة الجدار الناري الحديثة يمكنها منع مثل هذا النوع من الهجمات.

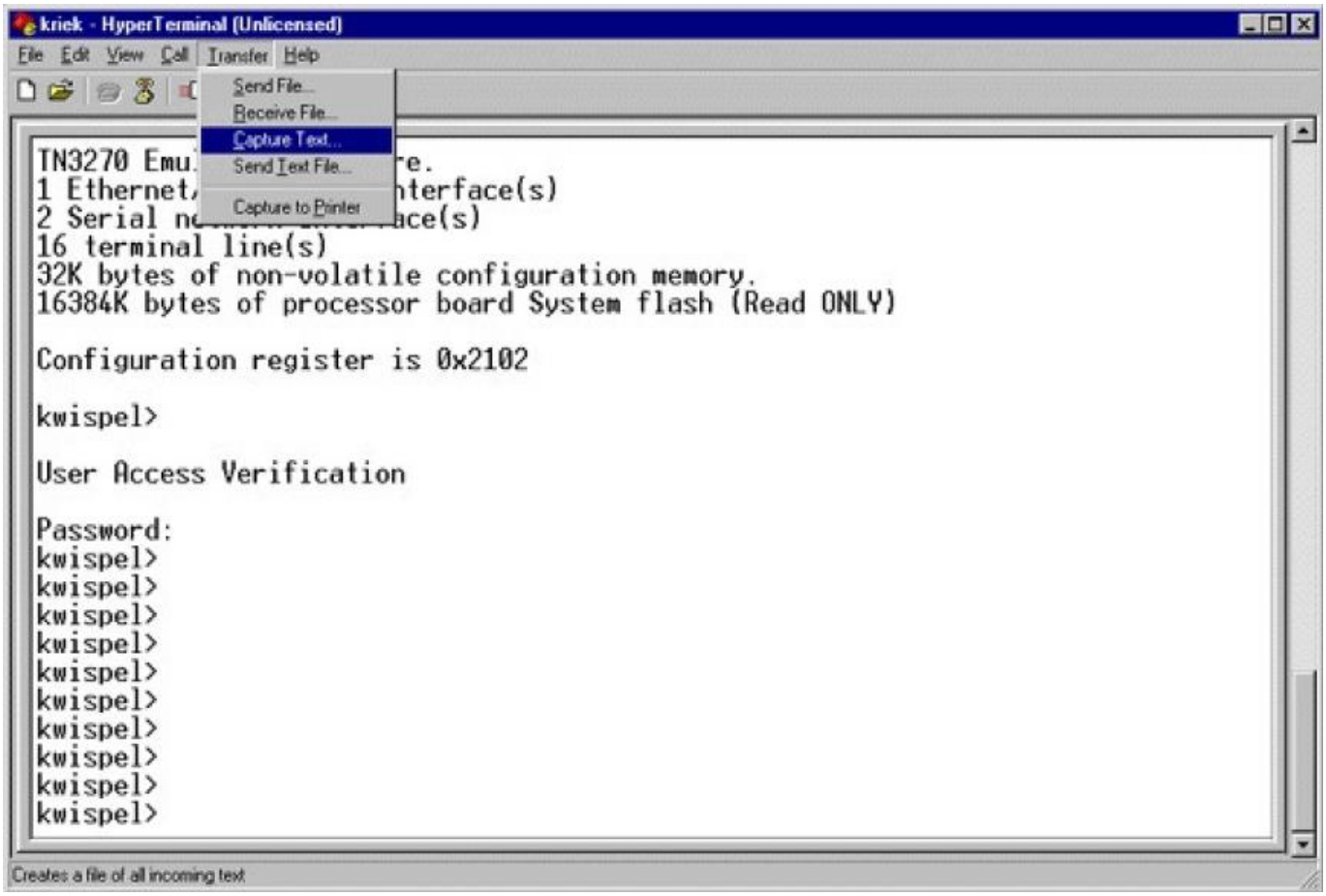
التحليل الجنائي الرقمي للمُوجّه router:

أثناء عملية التحليل الجنائي للشبكة سوف نتعامل مع أجهزة **routers**.

المُوجه **router** يمكن أن يكون عرضة للعديد من الهجمات ومنها تزوير جدول التوجيه **routing tabe poisoning** والذي يسمح للمهاجم بالوصول لكامل البيانات في الشبكة الهدف.

في الجرائم المعلوماتية التي تتم عبر الشبكة فإن البيانات التي يرسلها المهاجم سوف تمر من خلال أجهزة **routers** ومن المهم عدم إيقاف تشغيل المُوجه قبل أو أثناء عملية التحليل الجنائي الرقمي للحفاظ على الدليل الرقمي داخله.

يمكننا استخدام أداة للاتصال والتفاعل مع المُوجه عن بعد مثل الأداة **Hyper Terminal**



بعض التعليمات المفيدة في عملية التحليل الجنائي الرقمي للمُوجّه:

- **show version**: هذه التعليمة تعرض معلومات عن إصدار المُوجه ونظام التشغيل الخاص به ومعلومات أخرى.
- **show running-config**: تعرض الإعدادات الحالية للمُوجه.
- **showstartup-config**: تعرض الإعدادات عند إقلاع المُوجه.

إذا وجدنا اختلاف بين الإعدادات الحالية والإعدادات عند إقلاع المُوجه فهذا يشير إلى أن المهاجم قام بتغير إعدادات المُوجه.

- **show ip route**: تعرض جدول التوجيه، التلاعب في جدول التوجيه هو السبب الرئيسي الذي يدفع أي مهاجم لاستهداف المُوجه.

- show clock detail
- show version
- show running-config
- show startup-config
- show reload
- show ip route
- show ip arp
- show users
- show logging
- show ip interface
- show interfaces
- show tcp brief all
- show ip sockets
- show ip nat translations verbose
- show ip cache flow
- show ip cef
- show snmp user
- show snmp group
- show tech-support

التحليل الجنائي الرقمي للجدار الناري:

الجدار الناري **Firewall** عبارة عن جهاز أو برنامج يتم وضعه بين أجهزة الشبكة والوسط الخارجي ويتم إعداده بمجموعة من القواعد للسماح لاتصالات معينة ومنع اتصالات أخرى.

عملية التصفية يمكن أن تتم بالاعتماد على حجم البيانات أو بحسب البرتوكول المستخدم في عملية الاتصال أو بحسب عنوان **IP address** وأمور ومعايير أخرى.

خلال عملية التحليل الجنائي الرقمي يجب أن نقوم بفحص السجل الخاص بالجدار الناري، العديد من الهجمات تظهر وبشكل واضح من خلال هذا السجل مثل إغراق الشبكة بحزم البيانات وذلك من نفس عنوان **IP** أو هجوم تخمين كلمة السر باستخدام تقنية القوة الغاشمة **brute force**

إذا كان سجل الجدار الناري يحوي على نفس حزم بيانات تمر عبر عدد من المنافذ **ports** بالترتيب فهذا يعني أن شخص ما يقوم بعملية فحص المنافذ المفتوحة.

إذا كان سجل الجدار الناري يحوي على حزم بيانات قادمة من نفس عنوان **IP** ولها قيم **TTL (Time To Live)** مختلفة فهذا يعني أن شخص ما يقوم بعملية **firewalking** المهاجم يقوم بإرسال حزم بيانات من مسافات مختلفة ليرى الإجابات القادمة من الشبكة الهدف.

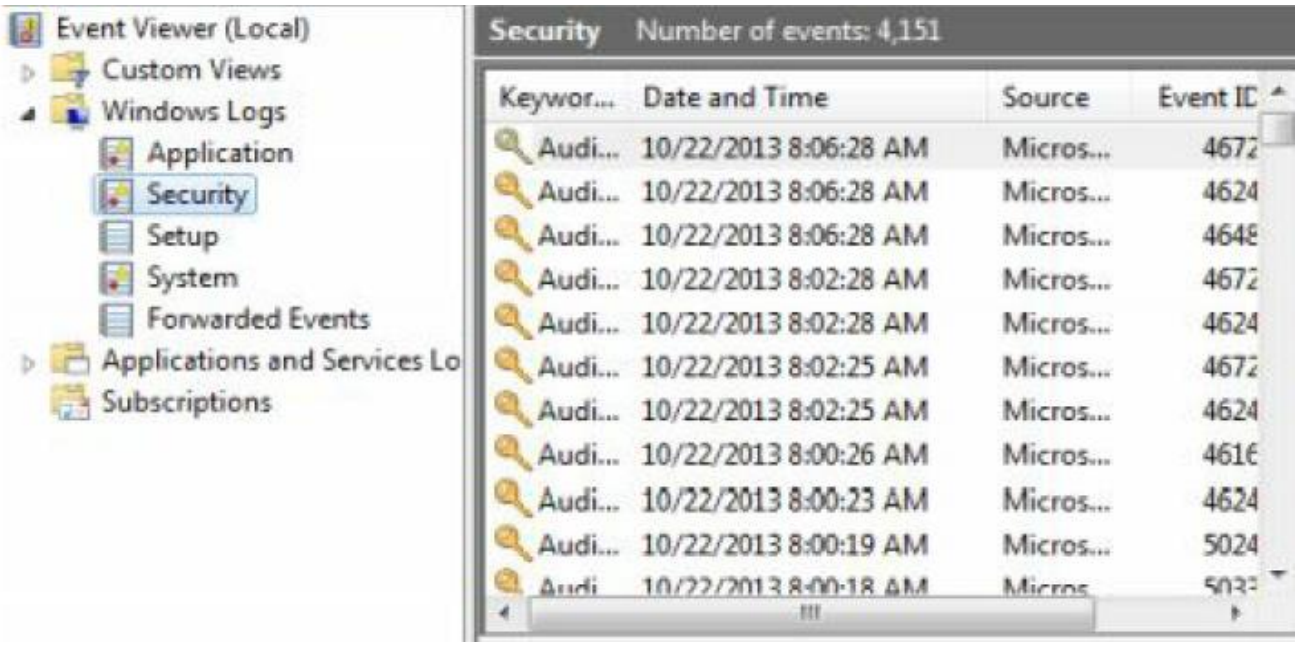
يوجد العديد من التقنيات المستخدمة للقيام بعملية فحص واستطلاع الشبكة وهذا الأمر يختلف بحسب خبرة المهاجم.

السجلات في نظام windows:

في **windows 7/8 and windows server 2008/2012** يمكننا الوصول للسجلات من خلال فتح لوحة التحكم ومن ثم اختيار **Administrative Tools** ومن ثم اختيار **Event Viewer** وسوف نجد السجلات التالية:

- **Security log**: وهو أهم سجل يجب فحصه خلال عملية التحليل الجنائي الرقمي ويحوي على معلومات عن عمليات تسجيل الدخول للنظام.

- **Application log**: العديد من البرامج والتطبيقات تقوم بتسجيل الأخطاء في هذا السجل.
- **System log**: يحوي على الأحداث الخاصة بعمليات النظام وهو غير مهم جداً في عملية التحليل الجنائي الرقمي.
- **ForwardedEvent log**: يستخدم لتسجيل الأحداث الخاصة من الأجهزة البعيدة.
- **Application and Services log**: يحوي على معلومات الأحداث المتعلقة بتطبيقات أو الأحداث التي يمكن أن تؤثر على النظام.

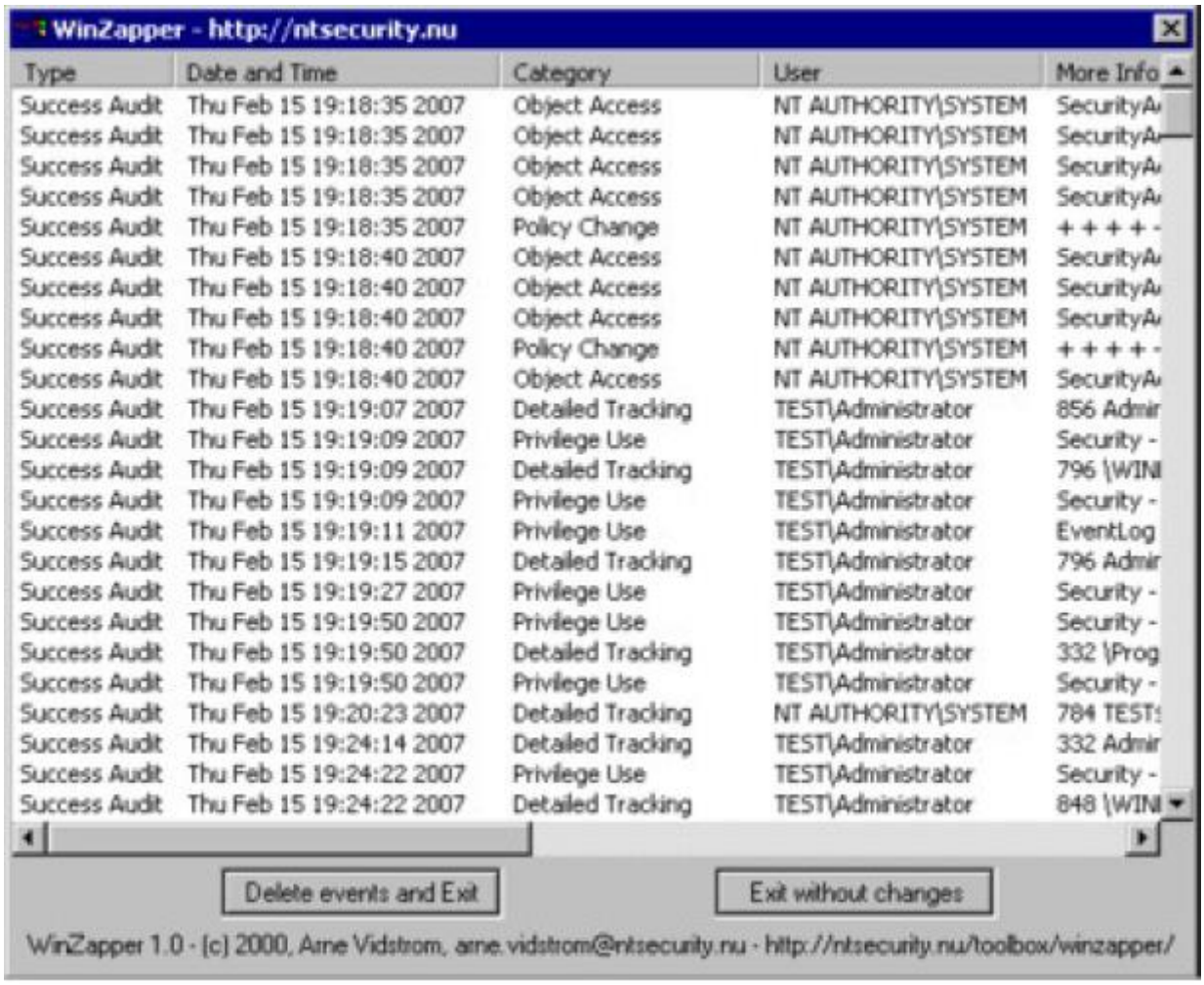


من الممكن أن يقوم المهاجم بحذف هذه السجلات.

في جلسة **meterpreter** فعالة لها أعلى مستوى صلاحيات مع النظام الهدف يمكن استخدام التعليمة التالية لحذف هذه السجلات

```
meterpreter > clearev
[*] Wiping 1587 records from Application...
[*] Wiping 5140 records from System...
[*] Wiping 4151 records from Security...
```

كما يوجد العديد من الأدوات التي تسمح للمهاجم بالقيام بهذه المهمة مثل الأداة **WinZapper** كما توجد أداوت أخرى تسمح للمهاجم بإيقاف عملية المراقبة والتسجيل بشكل مؤقت لحين انتهاء الهجوم مثل الأداة **auditpol.exe**



السجلات في نظام linux:

مكان وجود السجلات يمكن أن يختلف بحسب التوزيعة المستخدمة وبحسب الخدمات التي تعمل على النظام وبشكل عام السجلات في **linux** تكون في الأماكن التالية:

- **/var/log/faillog**: هذا السجل يحوي على محاولات تسجيل الدخول الفاشلة وهو مفيد جداً في عملية التحليل الجنائي الرقمي.
- **/var/log/kern.log**: يحوي على رسائل خاصة بنواة نظام التشغيل وهو غير مفيد في عملية التحليل الجنائي الرقمي.
- **/var/log/lpr.log**: يحوي على كل عمليات الطباعة التي تمت باستخدام هذا النظام.
- **/var/log/mail.***: يحوي على سجلات البريد الالكتروني وهو مفيد جداً في عملية التحقيق الجنائي الرقمي.
- **/var/log/mysql.***: يحوي على النشاطات المتعلقة بمُخدم قواعد البيانات **MySQL** وهو مفيد في عملية التحقيق الجنائي الرقمي.
- **/var/log/apache2/***: إذا كان النظام يستخدم **Apache** كمُخدّم ويب فهذا السجل يحوي على كل النشاطات المتعلقة بمُخدّم الويب وهو مفيد جداً لاكتشاف محاولات الاختراق.
- **/var/log/lighttpd/***: إذا كان النظام يستخدم **Lighttpd** كمُخدّم ويب فهذا السجل يحوي على كل النشاطات المتعلقة بمُخدم الويب وهو مفيد جداً لاكتشاف محاولات الاختراق.
- **/var/log/apport.log**: هذا السجل يحوي على معلومات متعلقة بإنهيار التطبيقات وفي بعض الأحيان يمكن أن نكشف من خلاله أدلة عن وجود فايروسات أو برمجيات تجسس.
- **/var/log/user.log**: يحوي على كل نشاطات المستخدم وهو مهم جداً في عملية التحقيق الجنائي الرقمي

التحليل الجنائي الرقمي للويب

محتوى هذا الفصل:

- ثغرة **SQL Injection**
- ثغرة **(XSS) Cross-Site Scripting**
- ثغرات المصادقة وإدارة الجلسة.
- ثغرة تجاوز المسار ورفع الملفات.
- التحليل الجنائي الرقمي للبريد الالكتروني.
- التحليل الجنائي الرقمي لقواعد البيانات.

مقدمة:

العديد من الجرائم المعلوماتية تتم من خلال اختراق مُخدّمات ومواقع الويب وهذه الهجمات هي الأكثر انتشاراً في الفترة الحالية.

الهجوم على موقع الويب يمكن أن يتم من خلال إحدى الطرق التالية:

- **استهداف المُخدم:** المُخدّم هو جهاز بمواصفات عالية يقوم باستضافة موقع أو عدد من مواقع الويب، المهاجم يحاول استهداف المُخدّم من خلال البحث عن ثغرات محتملة في نظام التشغيل الخاص بالمُخدّم أو ثغرات في البرامج التي تعمل على المُخدّم ومحاولة استغلالها ومن ثم الوصول إلى الملفات الخاصة بالموقع والتعديل عليها أو تخريبها.
- **استهداف موقع الويب:** مواقع الويب يمكن أن تحوي على ثغرات برمجية والتي يمكن للمهاجم استغلالها وتعديل أو تخريب محتوى الموقع وأشهر هذه الثغرات هي **SQL injection and XSS**
- **استهداف المستخدم:** ويتم ذلك باستخدام الهندسة الاجتماعية كمحاولة لخداع مدير الموقع أو مستخدمي الموقع من أجل الحصول على معلومات تسجيل الدخول الخاصة بهم.

ثغرات SQL injection:

SQL injection هي أقدم ثغرات مواقع الويب ومازالت منتشرة حتى الآن وتعتبر من أكبر المخاطر على مواقع الويب.

SQL injection قديم جداً ومدمر جداً وعملية تصليحه سهلة جداً.

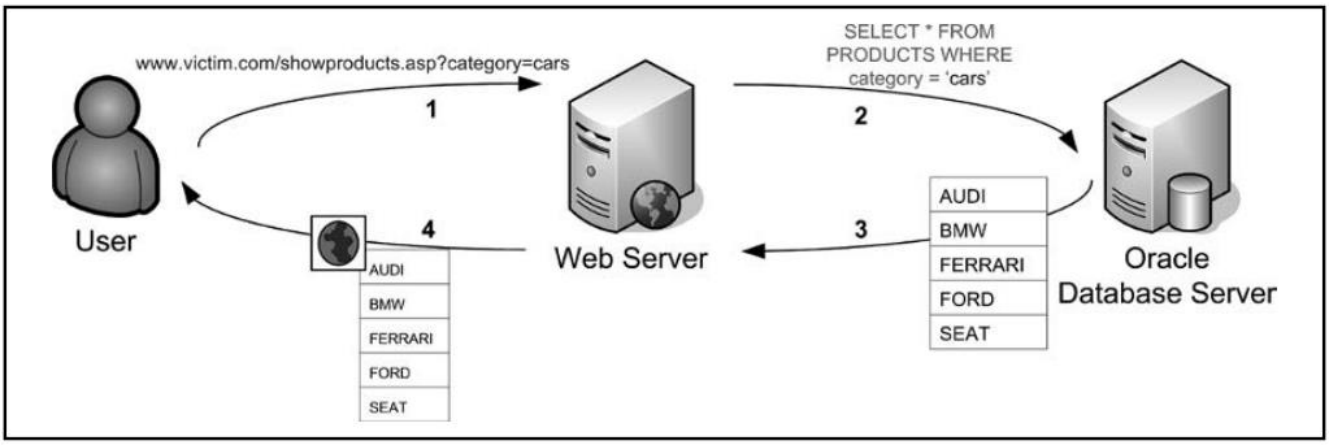
أظهرت بعض الدراسات الحديثة أن **SQL injection** مازالت موجودة في **30%** من مواقع الويب الحالية.

ثغرات SQL injection تحدث لسببين:

- ضعف في عملية تنقيح دخل المستخدم (المبرمج لم يقم بعملية تصفية لمتغير الدخل).
- البيانات والتحكم مدمجان في نفس قناة النقل.

الضعف في عملية تنقيح دخل المستخدم تسمح للمهاجم بالقفز من الجزء الخاص بالبيانات (السلسة النصية الموجودة بين إشارات تنصيص مفردة) إلى حقن تعليمات تحكم (مثل **SELECT, UNION, AND, OR**)

يجب أن تفهم كيف تتم عملية تدفق المعلومات في بنية مؤلفة من ثلاث صفوف هي المستخدم مُخدّم الويب ومُخدّم قاعدة البيانات كما في الشكل التالي:

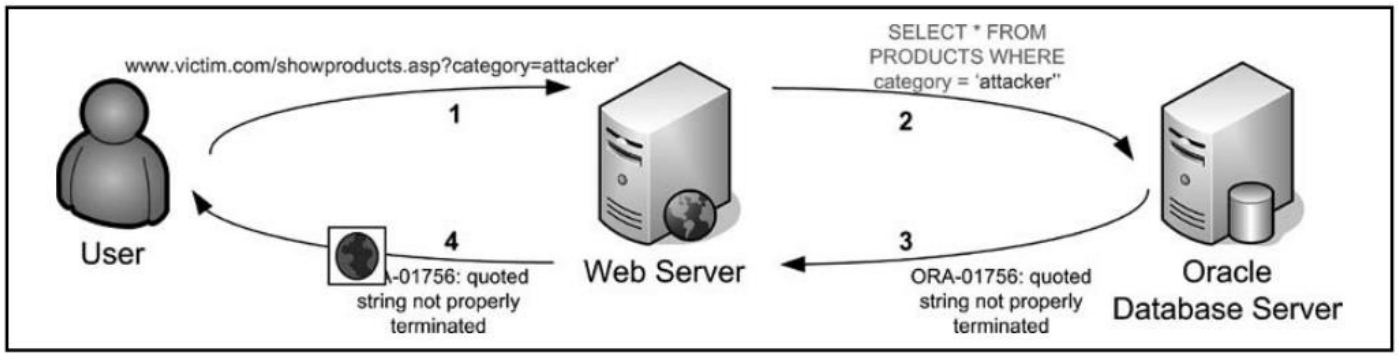


1. المستخدم يرسل طلب إلى مُخدّم الويب.
2. مُخدّم الويب يقوم بتضمين طلب المستخدم ضمن عبارة **SQL** ويرسلها كطلب (استعلام) إلى مُخدّم قاعدة البيانات
3. يقوم مخدّم قاعدة البيانات بتنفيذ طلب **SQL** بدون أن يعرف منطق التطبيق، فقط يقوم بتنفيذ الطلب ويعيد النتيجة إلى مخدّم الويب.
4. يقوم مخدّم الويب بإنشاء صفحة **HTML** بشكل ديناميكي بالاعتماد على الإجابة القادمة إليه من مخدّم قاعدة البيانات ويرسلها إلى المستخدم.

كما ترى فإن مخدّم الويب ومخدّم قاعدة البيانات منفصلان، مخدّم الويب فقط يقوم بإنشاء طلب **SQL** ويترجم النتيجة ويعرضها للمستخدم أما مخدّم قاعدة البيانات فهو يستقبل طلب **SQL** ويعيد النتيجة إلى مخدّم الويب وهذا مهم جدا من أجل استغلال ثغرات **SQL injection** لأننا نستطيع التلاعب بعبارة **SQL** وجعل مخدّم قاعدة البيانات يعيد بيانات مهمة مثل أسماء المستخدمين وكلمات السر.

من المهم أن تكون مدركاً لرسائل الخطأ المختلفة الصادة عن مخدّمات قواعد البيانات والتي ستحصل عليها من مخدّم الويب عندما تقوم باختبار ثغرة **SQL injection**

الشكل التالي يظهر كيف يحدث خطأ **SQL injection** وكيف يتعامل مُخدّم الويب معه.



1. المستخدم يرسل طلب لمحاولة معرفة إذا كانت ثغرة **SQL injection** موجودة في هذا التطبيق، في هذه الحالة المستخدم يرسل القيمة أو الاسم مضافاً إليه علامة تنصيص مفردة.
2. سيقوم مخدّم الويب بتضمين بيانات المستخدم ضمن طلب **SQL** إلى مخدّم قاعدة البيانات، في هذا المثال فإن عبارة **SQL** التي سينشئها مخدّم الويب سوف تحتوي على دخل المستخدم وعلامة التنصيص المفردة المضافة من قبل المستخدم بالإضافة إلى علامة تنصيص مفردة أخرى يقوم التطبيق بإضافتها.
3. مُخدّم قاعدة البيانات يستقبل طلب **SQL** غير سليم ويعيد رسالة خطأ إلى مُخدّم الويب.

4. يستقبل مُخدّم الويب رسالة الخطأ من مُخدّم قاعدة البيانات ويرسلها كإجابة على شكل **HTML** إلى المستخدم.

المثال السابق يشرح سيناريو الطلب من المستخدم الذي يحرض رسالة خطأ في قاعدة البيانات بالاعتماد على رماز التطبيق فإنه سيتم إعادة النتيجة في الخطوة الرابعة بإحدى هذه الطرق:

1. **SQL error** يعرض على متصفح المستخدم.
2. **SQL error** يخفى في مصدر صفحة الويب لأغراض تصليح الأخطاء.
3. إعادة التوجيه إلى صفحة أخرى.
4. **HTTP error code 500** (خطأ داخلي بالمُخدّم)

   أو **HTTP redirection code 302**
5. التطبيق يتعامل مع الخطأ بشكل فوري ويظهر أنه لا يوجد نتيجة أو يظهر صفحة خطأ عام.

SQL من أجل الاختراق:

المهاجم يستطيع خلق دخل خبيث ويدخله في صندوق البحث لاستغلال ثغرة **SQL injection** مع المحافظة على كتابة الدخل بين علامات التنصيص لكي لا تظهر رسالة خطأ

مثال كلاسيكي على هذا الاستغلال هو إدخال التالي إلى صندوق البحث

```
Jameel' OR 1=1#
```

هذا الدخل سيبني عبارة **SQL** التالية وإرسالها إلى المترجم ليقوم بتنفيذها

```
SELECT * FROM users WHERE UserName='jameel' OR 1=1'#
```

اشارة # هي **inline comment** تجعل المترجم يتجاهل كل شيء بعدها

نتيجة عبارة **SQL** لهذا الرماز المحقون هي:

```
SELECT * FROM users WHERE UserName='jameel' OR 1=1
```

لاحظ كيف أصبح الدخل (**jameel**) بين علامتي التنصيص فالعلامة الاولى تكون مكتوبة مسبقاً من قبل المبرمج والعلامة الثانية قمنا نحن بإدخالها بعد الدخل

اشارة التنصيص (') التي يتم إضافتها إلى نهاية دخل المستخدم من قبل التطبيق سيتم تجاهلها بسبب وجود # التي هي **inline comment**

لن يتم عرض اسم المستخدم **jameel** فقط بل سيتم عرض كل المستخدمين الموجودين لأن **1=1** دائماً محققة

يمكنك أيضاً حقن سلسة نصية وترك علامة التنصيص معلقة كالتالي

```
jameel' OR 'a'='a
```

نحن نعلم بالضبط أين ستضاف علامة التنصيص (') وبالتالي النتيجة ستكون عبارة **SQL** صحيحة وستصبح كالتالي:

```
SELECT * FROM users WHERE UserName='jameel' OR 'a'='a'
```

هجوم SQL injection:

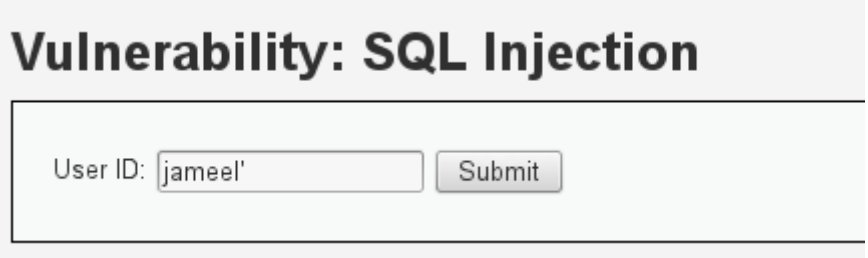
يجب أن تكون قد فهمت أساسيات **SQL injection** ، في هذا المثال سوف استخدم بيئة **DVWA** (موقع ويب تجريبي يحوي على ثغرات) لمحاولة استخراج اسم المستخدم وهاش كلمة السر الخاص بمدير الموقع:

إيجاد ثغرة SQL injection:

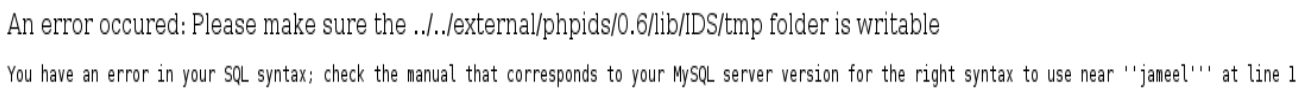
منذ **10-15** سنة ماضية عندما تم استغلال **SQL injection** لأول مرة كان إيجاد الثغرة أمر سهل جداً ويتم من خلال وضع إشارة تنصيص واحدة (') داخل صندوق البحث ومشاهدة رد فعل الموقع.

إشارة التنصيص المفردة ستؤدي إلى خلل في صيغة التعليمة والموقع سوف يرد برسالة خطأ. يمكننا محاولة معرفة إذا كان **DVWA** يحوي على ثغرة **SQL injection** من خلال استخدام نفس الطريقة أي ادخال اشارة تنصيص مفردة (') في **User ID textbox**

أو بدل ذلك سوف نقوم بإدخال سلسة نصية مع إشارة تنصيص مفردة كالدخل التالي:



هذا الدخل سيؤدي إلى ظهور خطأ **SQL** التالي:



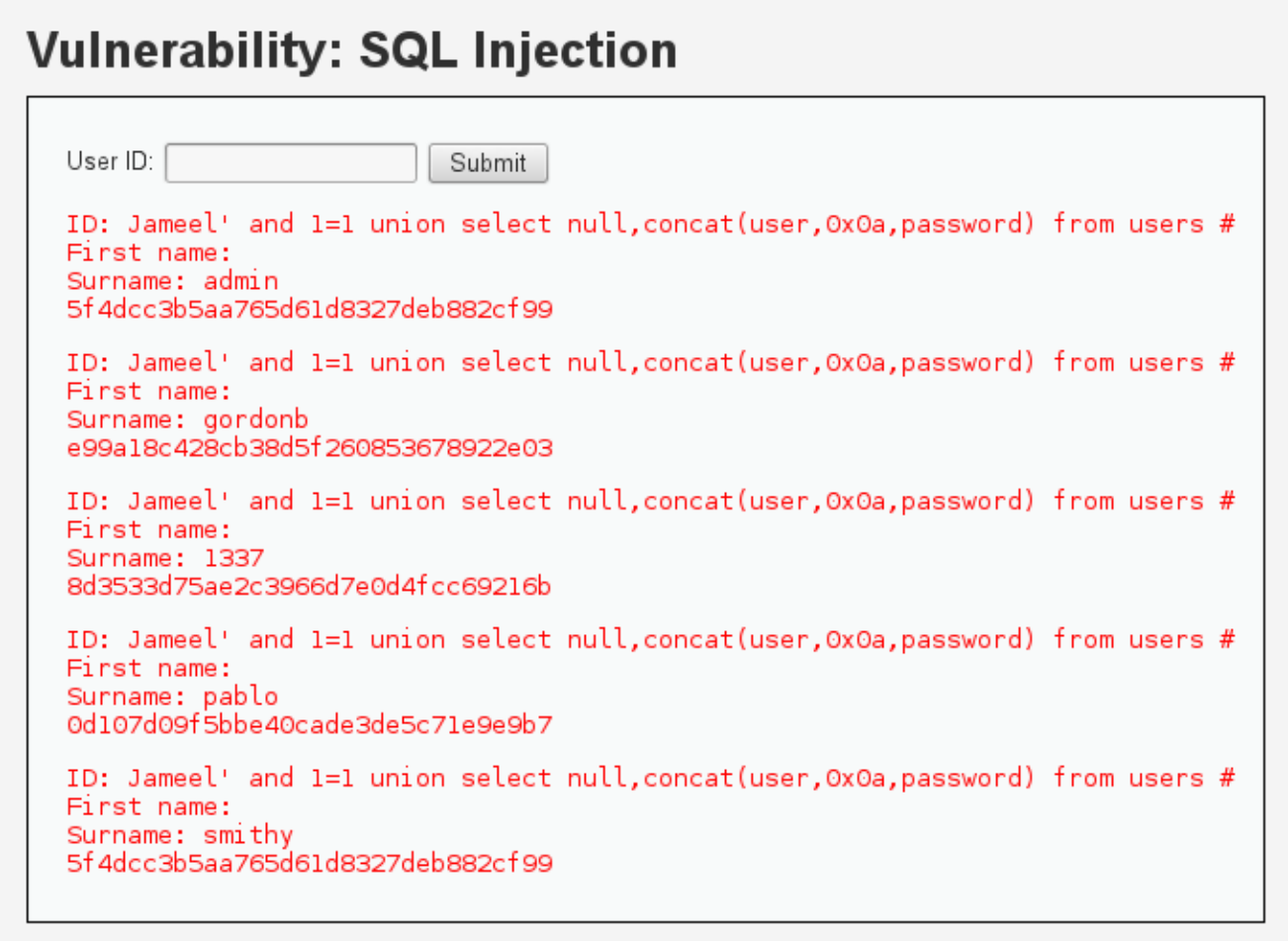
في هذا الموقع كل دخل المستخدم يكون مغلف بين مجموعتين من إشارات التنصيص المفردة (ليست إشارة تنصيص مزدوجة)

لعرض محتوى العامودين **user and password** من جدول قاعدة البيانات ندخل العبارة التالية:

Jameel' and 1=1 union select null,concat(user,0x0a,password) from users#

النتائج التي سوف تظهر هي القيم التي يسعى أي هاكر للحصول عليها.

سوف نحصل على اسم وكلمة السر لك مستخدم في قاعدة البيانات كما يظهر في الشكل التالي:



طبعاً كلمات السر لن تظهر كنص صريح، سوف تكون على شكل **hash** ومن السهل جداً كسر هذا النوع من الهاش وهو بالتحديد من نوع **MD5 hash** لأنه عبارة عن **32** رقم سته عشري.

لمعرفة نوع الهاش يمكننا استخدام أداة **Hash-ID** وهي تساعد على معرفة نوع الهاش الذي يكون أكبر من **50** حرف أو رقم وهذه الأداة موجودة بشكل تلقائي بنظام **Kali**.

يمكننا أن نستخدم أداة مثل **John the Ripper (JtR)** أو للاختصار فقط **John** لكسر الهاش والحصول على كلمة بشكل نص صريح.

استخدام هذه الأداة سهل جداً، فقط نحتاج إلى نسخ ولصق الأسماء وكلمات السر إلى ملف نصي وتقديمه للأداة ثم انتظار اظهار النص الصريح لكلمة السر لكل مستخدم.

العملية السابقة هي شرح بسيط لاستغلال ثغرة حقن تعليمات قواعد البيانات **SQL injection** بشكل يدوي كما يوجد العديد من الأدوات التي يمكن أن تقوم باستغلال هذه الثغرة وبشكل أتوماتيكي.

الأمر المهم في عملية التحليل الجنائي الرقمي هو البحث في سجلات قواعد البيانات وسجلات مُخدّم الويب وسجلات أجهزة الحماية عن دليل رقمي لاستغلال ثغرة **SQL injection**

الدليل الرقمي يمكن أن يكون كالعبارة التالية **'or '1'='1**

ثغرة Cross-Site Scripting (XSS):

هي ثغرة منتشرة جداً في مواقع الويب، عندما تقوم بزيارة موقع ويب فإن متصفحك يطور علاقة موثوقة مع موقع الويب، متصفحك يفترض أن هذه العلاقة موثوقة لأنه يقوم بالطلب من موقع الويب ويجب عليه أن يثق بأي إجابة تعود إليه من هذا الموقع.

هذه العلاقة الموثوق بها تسمح للصور والمستندات و الرمازات البرمجية **scripts** من موقع الويب بالظهور على متصفحك.

هذه العلاقة لا تكون آمنة عندما يكون الموقع مصاب بثغرة **XSS**

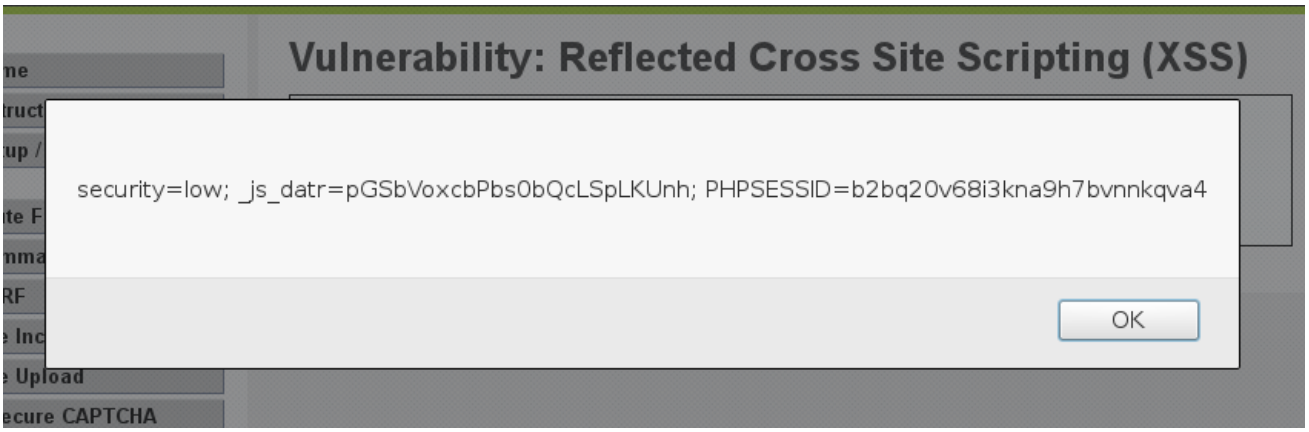
إذا كان الموقع مصاب بثغرة **XSS** فإن المهاجم يستطيع خلق طلب لعنوان **URL** يحوي على رماز برمجي **script** خبيث ويقوم بتمرير عنوان **URL** إلى المستخدم الهدف، إذا قام الهدف بالضغط على هذا الرابط فإن الطلب الخبيث سوف يرسل إلى موقع الويب، الموقع سوف يقوم بالرد من خلال إرسال إجابة إلى المستخدم تحوي على رماز برمجي خبيث، هذا الرماز يتولد في المُخدّم ويرسل إلى متصفح الهدف ويتم تنفيذه في المتصفح.

أشهر طريقة لاستغلال هذه الثغرة هي سرقة مُعرف الجلسة **cookie** الخاصة بمدير الموقع ومن ثم إعادة استخدامه من خلال حقنه في المتصفح والدخول إلى حساب المدير من دون معرفة كلمة السر الخاصة به كما في المثال التالي:

المهاجم يستخدم الطريقة **document.cookie** في هجوم **XSS** من أجل عرض مُعرف الجلسة **cookie** الخاص بالهدف.

وذلك باستخدام الصيغة التالية:

```
<script>alert(document.cookie)</script>
```



الآن يمكنه وبسهولة حقن مُعرف الجلسة (**cookie**) في المتصفح الخاص به والدخول إلى حساب الهدف بدون معرفة كلمة السر الخاصة به.

من خلال سجلات مُخدّم الويب وسجلات أجهزة الحماية يمكننا رؤية كل التعليمات أو الرمازات البرمجية الخبيثة التي تم تنفيذها والتي يمكن أن تعتبر دليل رقمي يثبت حدوث الهجوم.

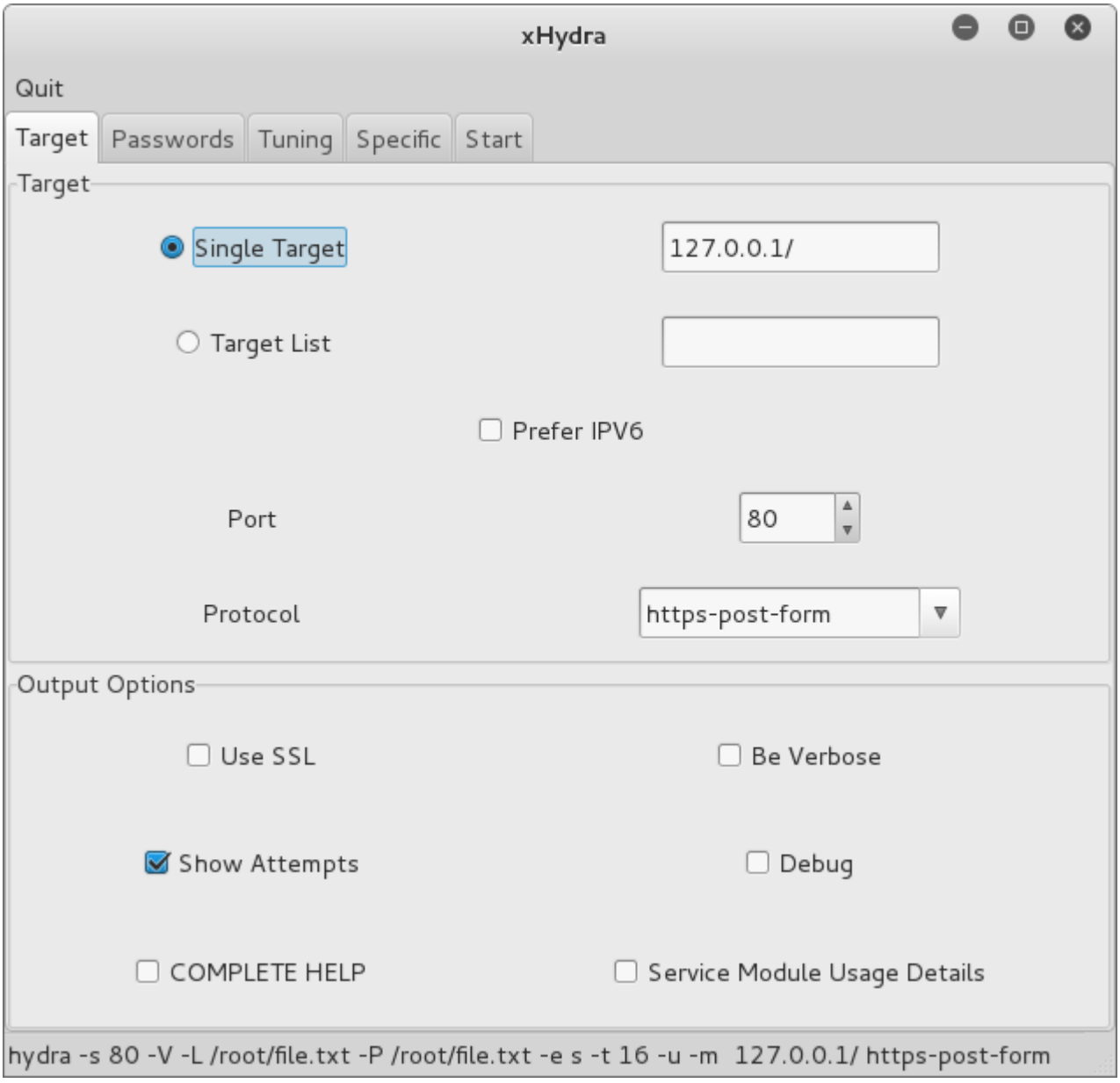
ثغرات المصادقة وإدارة الجلسة:

عملية المصادقة تسمح لنا بتسجيل الدخول إلى موقع الويب بينما إدارة الجلسة تتبع الطلبات والإجابات التي تتم خلال عملية التصفح.

عملية المصادقة **authentication** وعملية إدارة الجلسة لم تؤخذان بعين الاعتبار عندما تم إيجاد بروتوكول **HTTP** ، لسوء الحظ فإن المصادقة وإدارة الجلسة تحوي على ثغرات كثيرة في العديد من مواقع الويب.

.هجوم المصادقة الأكثر شيوعاً يتم من خلال أدوات تسمح بتخمين كلمة السر باستخدام القوة الغاشمة **brute force** للتخمين على معلومات تسجيل الدخول مثل الأداة **xHydra**

(موجودة بشكل تلقائي في **Kali**) ولها واجهة رسومية بسيطة ومن السهل التعامل معها



لا يوجد الكثير من السرية في هذا النوع من الهجوم ولكنه ناجح جداً لأن معظم المستخدمين مازالوا يستخدمون كلمات سر ضعيفة.

مهاجمة إدارة الجلسة يمكن فقط من خلال إحدى الطريقتين:

1. مهاجمة آلية توليد مُعرف الجلسة.
2. مهاجمة آلية استخدام مُعرف الجلسة وآلية تسليمها من قبل موقع الويب.

مهاجمة آلية توليد مُعرف الجلسة صعب جداً لأن آلية توليد إدارة الجلسة تكون متضمنة داخل مُخدّم الويب الذي يقوم بخلق مُعرف الجلسة ومن الصعب جداً تخمينها.

الهجوم الأكثر شيوعاً يتم من خلال اختبار كيفية استخدام مُعرف الجلسة من قبل الموقع وهذا النوع من الهجوم لا يتطلب منك فهم عملية توليدها بل يركز على الوصول إليها وطريقة استخدامها.

المهاجم يقوم بسرقة مُعرف الجلسة وإعادة استخدامها

الأداة **Firesheep** وهي عبارة عن إضافة **add-on** خاصة بالإصدارات القديمة من المتصفح **Firefox** تسمح للمهاجم بإلتقاط حزم البيانات اللاسلكية والحصول على مُعرف الجلسة الخاصة بالفيس بوك ومن ثم يقوم المهاجم بحقن المُعرف في متصفحه ويمكنه الدخول إلى حساب الضحية بدون معرفة كلمة السر وهذه الطريقة يمكن أن تعمل مع مواقع التواصل الاجتماعي الأخرى.

ثغرة تجاوز المسار Directory Traversal :

تتم عملية تخصيص المساحات التخزينية للمواقع الالكترونية ضمن المُخدّم المضيف أثناء إعداد وتشغيل مُخدّم الويب، يعمل كل موقع ضمن المساحة المخصصة له والتي تحوي الرمّازات الخاصة بالموقع والصور والملفات بالإضافة الى قواعد البيانات وملفات الموقع الأخرى، تحدث ثغرة تجاوز المسار عندما يتم إعداد مُخدّم الويب بحيث يسمح للمستخدم (المهاجم) بالتنقل بين مجلدات الموقع الالكتروني.

يجب ضبط إعدادات المواقع الالكترونية بحيث لا تتمكن من محاولة الوصول إلى موارد أو بيانات خارج حدود المساحة التخزينية المخصصة لكل موقع وذلك لأن هذه الموارد والبيانات ستكون حتماً مخصصة لمواقع أخرى.

إذا استطاع المهاجم الوصول إلى خارج حدود المساحة المخصصة للموقع والوصول إلى المصادر الأخرى على مُخدّم الويب فهذا يسمى هجوم تجاوز المسار.

ثغرة رفع الملفات File Inclusion:

في حال وجود هذه الثغرة فإن المهاجم يستطيع رفع **shell** عبارة رماز برمجي صغير يمكن رفعه إلى مُخدّم الويب من خلال موقع مصاب بهذه الثغرة وهو يؤمن للمهاجم وصول لمُخدّم الويب ويسمح له بتنفيذ التعليمات عن بعد.

يجب أن يكون الرماز مكتوب بلغة يدعمها مُخدّم الويب (**php or asp**)

إذا كان المُخدّم الهدف يدعم **PHP** فيجب استخدام رماز مكتوب بهذه اللغة.

وهي تسمح للمهاجم القيام ومن عن بعد بالأمور التالية:

- التنقل بين المجلدات.
- تعديل الملفات.
- تحميل أو رفع ملفات.
- حذف الملفات.
- تنفيذ تعليمات في نظام التشغيل.
- الاتصال بقاعدة البيانات.
- كشف معلومات عن بنية الشبكة.

يمكن رفع **shell** إلى المواقع المصابة بثغرة **RFI – Remote File Inclusion**

يوجد العديد من **shells** والتي تؤمن واجهة للتحكم بالمُخدّم الهدف مثل: **China Chopper, WSO, C99 and B374K**

في عملية التحليل الجنائي الرقمي يجب أن نقوم بفحص ملفات الموقع باستخدام مضاد فيروسات لإكتشاف وجود هذه الملفات كما يجب فحص ملفات الموقع بشكل يدوي وفتح وفحص أي ملف نشتبه به و له اللاحقة الاسمية "**.php**"

المهاجم يمكن أن يقوم بتغير الاسم كمحاولة لعدم إثارة شك مدير الموقع.

الإعداد الخاطئ للحماية:

هذه الثغرة تصنف بشكل خاص للتعامل مع الحماية (الضعف في الحماية) وهي متعلقة بنظام التشغيل ومُخدّم الويب ونظام إدارة قاعدة البيانات، هذه المخاطر تصبح أكثر صعوبة عندما لا تؤمن الحماية منع الوصول الغير مسموح به للموقع.

أمثلة على هذه الثغرة التي يمكن أن تكون في مُخدّم الويب:

- البرامج الغير ضرورية.
- تفعيل الخدمات الغير ضرورية.
- سياسات الحساب الغير محمية.
- رسائل الخطأ المفصلة.

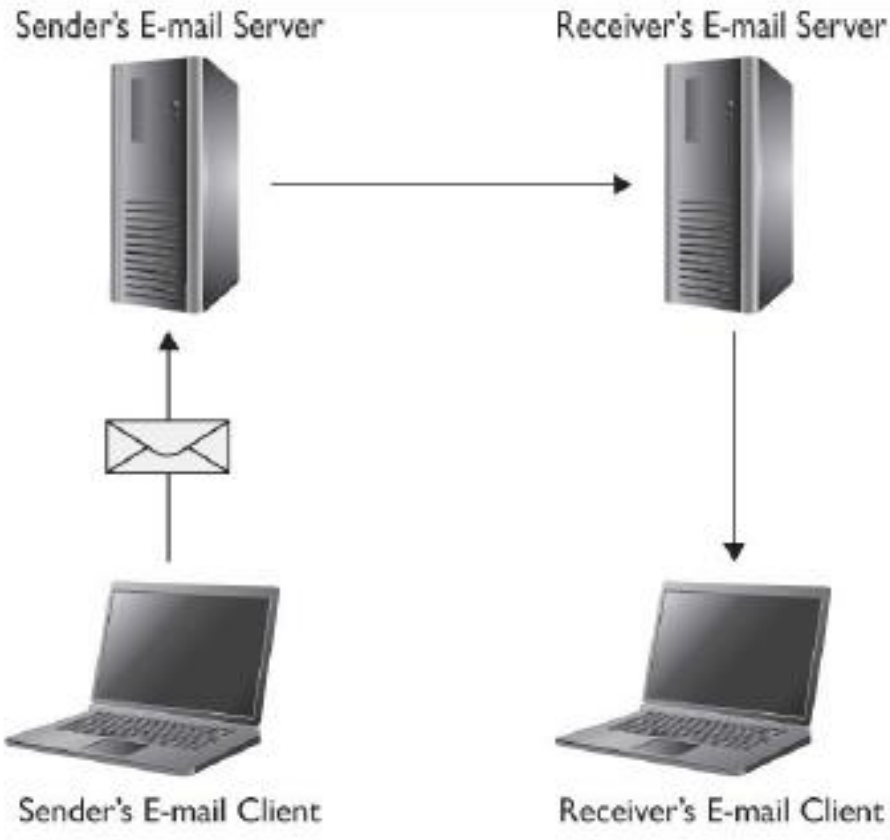
الحماية الفعالة تتطلب إعدادات محمية تُعرف وتُنفذ على الموقع وعلى إطار العمل وعلى مُخدّم الويب وعلى مُخدّم قاعدة البيانات وعلى نظام التشغيل، كل هذه الإعدادات يجب أن تُعرف وتنفذ بدل من إعدادات الحماية الافتراضية، وهذا يتضمن كل البرامج التي تتعامل مع البيانات ومكتبات الرماز البرمجي الذي يستخدمه التطبيق، بالإضافة إلى تطبيق سياسية صارمة تحدد الأشخاص المسموح لهم بالوصول إلى المُخدّم أو إدارة موقع الويب.

التحليل الجنائي الرقمي للبريد الالكتروني:

وهو مهم جداً في عملية التحليل الجنائي الرقمي، العديد من الجرائم المعلوماتية تتم عبر البريد الالكتروني مثل البريد الواغل **spam** أو رسائل التصيد **phishing** أو الرسائل المزورة.

قبل البدء بعملية التحليل الجنائي الرقمي للبريد الالكتروني من المهم أن نفهم الطريقة التي يتم من خلالها إرسال واستقبال رسائل البريد الالكتروني.

المرسل يقوم بكتابة الرسالة باستخدام برنامج مثل **Outlook** أو من خلال موقع مخدّم البريد الالكتروني، الرسالة سوف ترسل إلى مُخدّم الإرسال **sender's email server** والذي سوف يقوم بدوره بإرسال هذه الرسالة إلى مُخدّم الاستقبال **recipient's email server** وعندما يقوم الشخص المستقبل بتسجيل الدخول إلى نظام البريد الالكتروني سوف يقوم باسترداد الرسالة من المُخدّم.



الدليل الرقمي يمكن أن يوجد في أي من الأماكن السابقة، يمكن أن يكون في جهاز المرسل أو في جهاز المستقبل أو يمكن أن يكون في مُخدّم الإرسال أو مُخدّم الاستقبال.

عند إجراء عملية التحليل الجنائي الرقمي للبريد الالكتروني يجب أن نطلب سجلات الرسائل من الشركة المزودة للإنترنت **ISP (Internet Service Provider)**

التحليل الجنائي الرقمي للبريد الالكتروني مهم جداً، لأن الاتصال باستخدام رسائل البريد الالكتروني يمكن أن يستخدم في الجرائم العادية (الغير معلوماتية) أيضاً.

من الممكن أن يقوم المرسل أو المستقبل بحذف الرسائل ولكن من الممكن أن نجد نسخة احتياطية **backup** في المُخدّم عن الوسائط التي تم إرسالها أو استقبالها.

برتوكولات البريد الالكتروني:

أول برتوكول لنظام البريد الالكتروني هو **SMTP (Simple Mail Transfer Protocol)** والذي يعمل باستخدام المنفذ **port 25**

يوجد نسخة من هذا البرتوكول تستخدم التشفير **SSL or TLS** من أجل الحماية وتعمل باستخدام المنفذ **port 465**

في السنوات الماضية تم تطوير البرتوكول **POP3** للبرتوكول **IMAP (Internet Message Access Protocol)** والذي يعمل على **port 143**

أحد ميزات **IMAP** عن **POP3** هو السماح للمستخدم بتحميل ترويسة الرسالة فقط إلى جهازه ومن ثم يمكنه تحميل الرسالة بشكل كامل وهذه العملية مفيدة عند فتح الرسائل الالكترونية من أجهزة الموبايل الحديثة.

Spoofed Email:

هذه العملية تتم من خلال إرسال رسالة عبر البريد الالكتروني لتبدو على أنها قادمة من شخص أخر أو من مكان أخر.

هذه العملية تتم باستخدام برنامج معين يسمح بتغيير عنوان **IP address** وأول جهاز يقوم باستقبال الرسالة المزورة يقوم بتسجيل عنوان **IP** الحقيقي

للمرسل (لأن ترويسة الرسالة تحوي على كل من العنوان الأصلي والعنوان المزور) إلا إذا كان المجرم ذكي لدرجة أنه قد قام أيضاً بتغير عنوان **IP** الأصلي الخاص به.

يوجد العديد من المواقع التي تسمح بإرسال رسائل بريد الالكتروني وتسمح للمستخدم بتحديد وتغير عنوان المرسل ومنها:

- http://sendanonymousemail.net/
- http://theanonymousemail.com/
- http://send-email.org/

ترويسة الرسالة الالكترونية Email header:

ترويسة الرسالة تحوي على معلومات مهمة عن هوية المرسل ووجهة الرسالة.

يوجد معيار محدد لرسائل وترويسات الرسائل الالكترونية وهذا يسمح لنا بإرسال الرسالة من برنامج **Outlook** في نظام **windows** واستقبال وقراءة الرسالة من حساب **Hotmail** من جهاز موبايل يعمل بنظام التشغيل **Android** (المبني باستخدام نظام **linux**)

كل برامج البريد الالكتروني تستخدم نفس النمط المعياري بغض النظر عن نظام التشغيل المستخدم.

عند تقديم رسالة الكترونية على أنها دليل رقمي يجب أن يتضمن الدليل نص الرسالة والمرفقات (إن وجدت) وترويسة الرسالة.

الترويسة تحوي على معلومات عن الرحلة التي مرت بها الرسالة عبر الشبكة ومعلومات إذا تم مرور الرسالة عبر واحد أو أكثر من مُخدّمات البريد الالكتروني، كل مُخدّم يقوم بتسجيل معلوماته الخاصة في ترويسة الرسالة.

يمكننا فحص عنوان **IP address** الموجود في ترويسة الرسالة كمحاولة لتحديد هوية أو مكان المرسل.

المعيار المعتمد في الرسائل الالكترونية هو **RFC 2822** والذي يوصي بالأمور التالية:

- ترويسة الرسالة يجب أن تحوي على الأقل على الحقلين التاليين:
  - **From**: عنوان المرسل وبشكل اختياري اسم المرسل.
  - **Data**: وقت وتاريخ كتابة الرسالة.
- ترويسة الرسالة يجب أن تحوي على الحقول التالية:
  - **Message-ID**: عبارة عن رقم معرف الرسالة الالكترونية وهو رقم فريد لا يمكن أن يتكرر لرسالتين مختلفتين ويتميز بتنسيق خاص.
  - **In-Reply-To**:يحوي على **Message-ID** للرسالة التي تم الرد عليها.

المعيار **RFC 3864** يصف حقل ترويسة الرسالة والتي يجب أن تحوي على الأمور التالية:

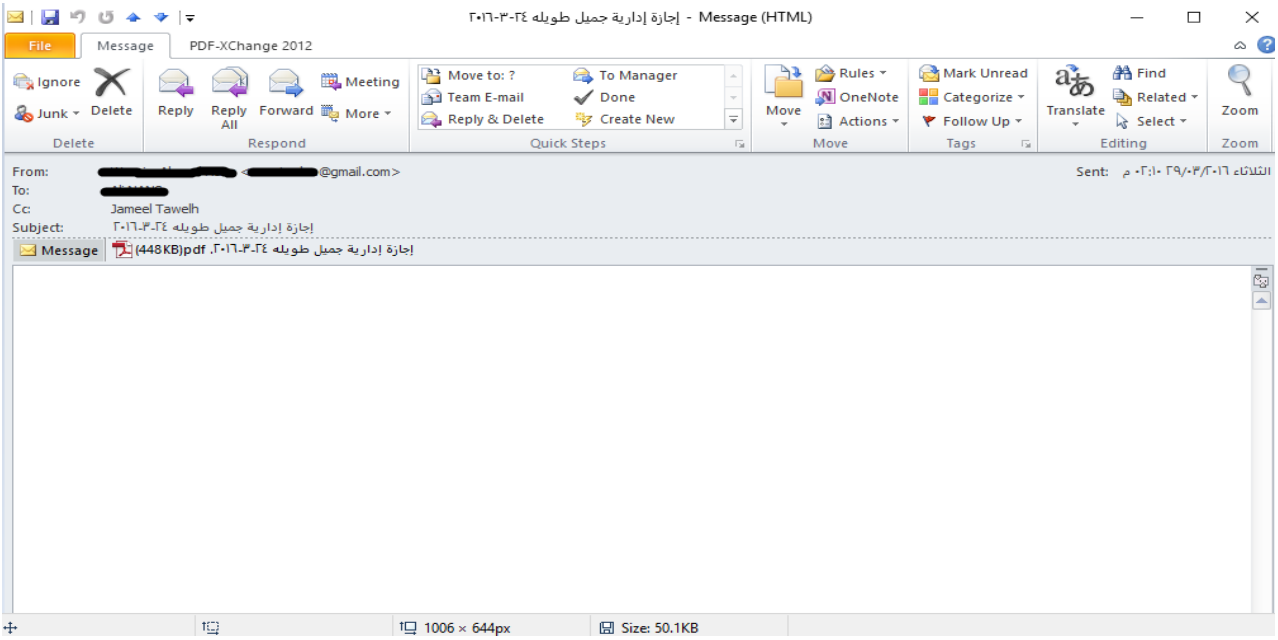
- **To**: إلى عنوان معين.
- **Subject**: عنوان الرسالة.

- **Cc**: **(Carbon copy)** إرسال نسخة إلى عناوين أخرى.
- **Bcc**: **(Blind carbon copy)** العناوين التي يتم إضافتها إلى قائمة التسليم والتي لا نريد أن تظهر لباقي المستلمين.
- **Content-Type**: معلومات عن كيفية عرض الرسالة.
- **Precedence**: الأولوية ويمكن أن يكون **junk** للإشارة إلى أنه ذو أولوية ضعيفة.
- **References**: يحوي على **Message-ID** للرسالة التي تم الرد عليها.
- **Reply-To**: العنوان الذي يجب استخدام للرد على الرسالة.
- **Sender**: معلومات عن المرسل.

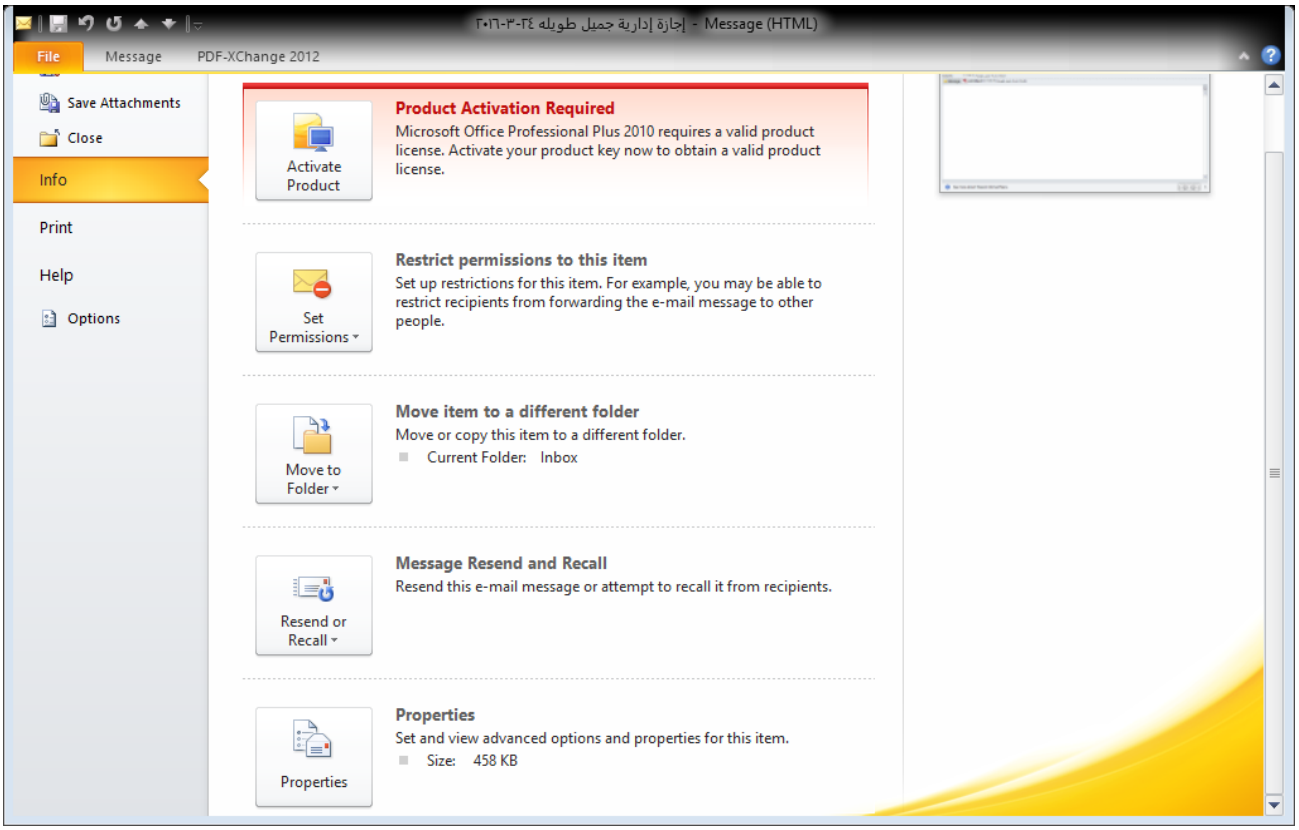
الترويسة يجب أن يتم قرأتها من الأسفل إلى الأعلى بسبب الترتيب الزمني الخاص بها وهي تحوي على عنوان **IP** الخاص بالمرسل.

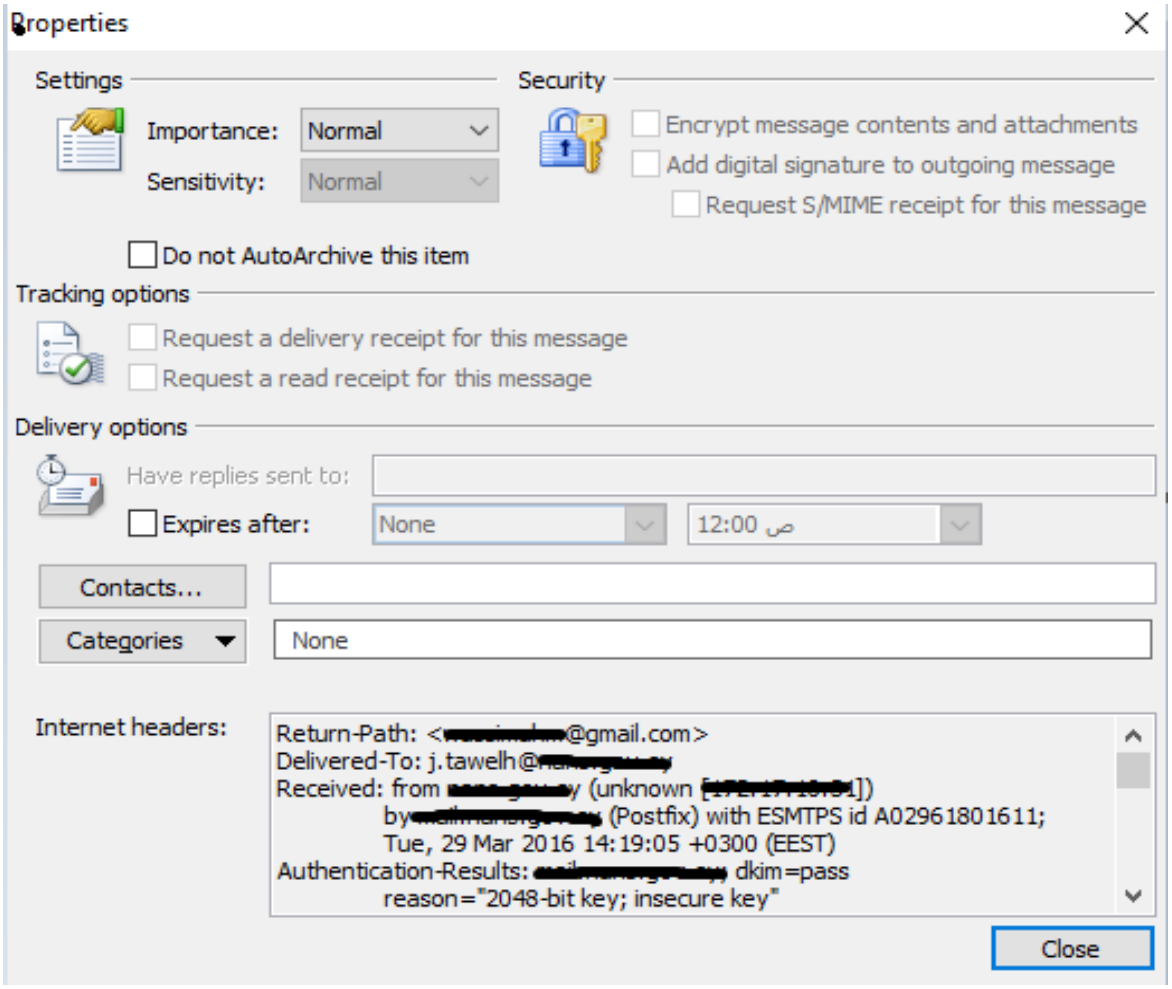
الحصول على ترويسة الرسالة في Outlook:

نختار الرسالة المطلوبة



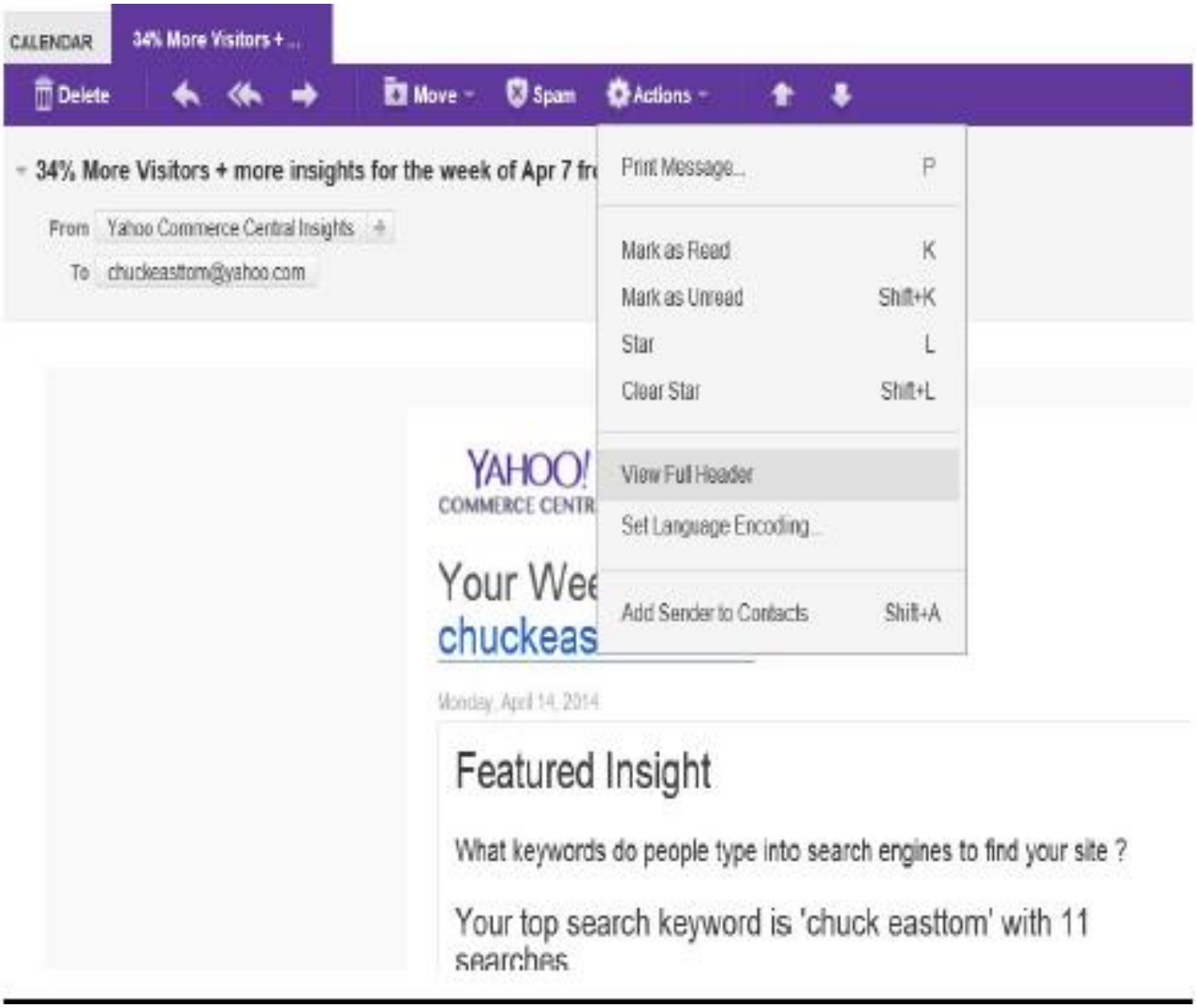
نختار **File** ومن ثم **Properties**




Properties
Settings
Importance: Normal
Sensitivity: Normal
Security
Encrypt message contents and attachments
Add digital signature to outgoing message
Request S/MIME receipt for this message
Do not AutoArchive this item
Tracking options
Request a delivery receipt for this message
Request a read receipt for this message
Delivery options
Have replies sent to:
Expires after: None 12:00 ص
Contacts...
Categories
None
Internet headers:
Return-Path: <[redacted]@gmail.com>
Delivered-To: j.tawelh@[redacted]
Received: from [redacted] (unknown [redacted])
by [redacted] (Postfix) with ESMTPS id A02961801611;
Tue, 29 Mar 2016 14:19:05 +0300 (EEST)
Authentication-Results: [redacted] dkim=pass
reason="2048-bit key; insecure key"
Close

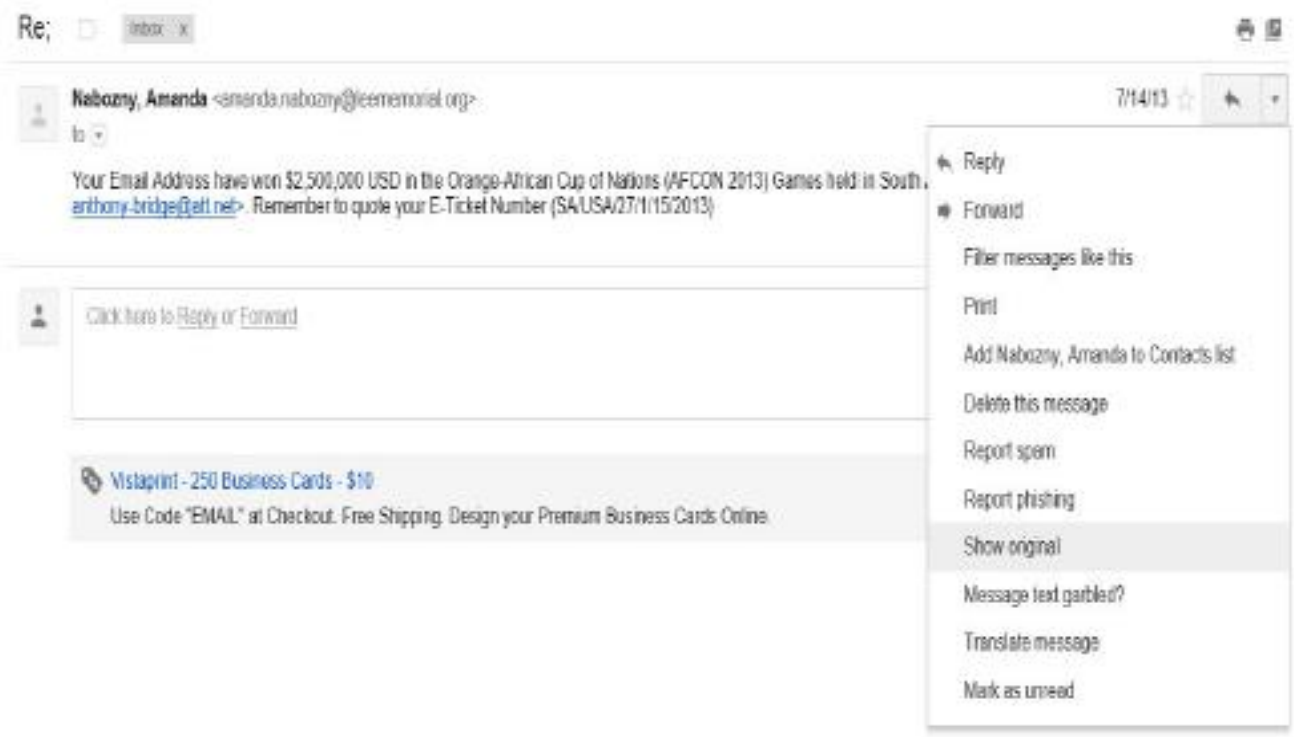
الحصول على ترويسة الرسالة في Yahoo:

بعد فتح الرسالة المطلوبة نختار **Actions** ومن ثم **Full Headers** كما في الشكل التالي:



الحصول على ترويسة الرسالة في Gmail:

بعد فتح الرسالة المطلوبة، نضغط بالزر الأيمن على الرسالة ونختار **Show Original** كما في الشكل التالي:



ملفات البريد الالكتروني:

عندما يتم استخدام برنامج لتصفح البريد الالكتروني فإن الرسائل سيتم حفظها في الجهاز المحلي.

اللاحقة الاسمية لملفات رسائل البريد الالكتروني هي:

- **.pst (Outlook)**
- **.ost (Offline Outlook Storage)**
- **.mbx or .dbx (Outlook Express)**
- **.mbx (Eudora)**
- **.emi (common to several e-mail clients)**

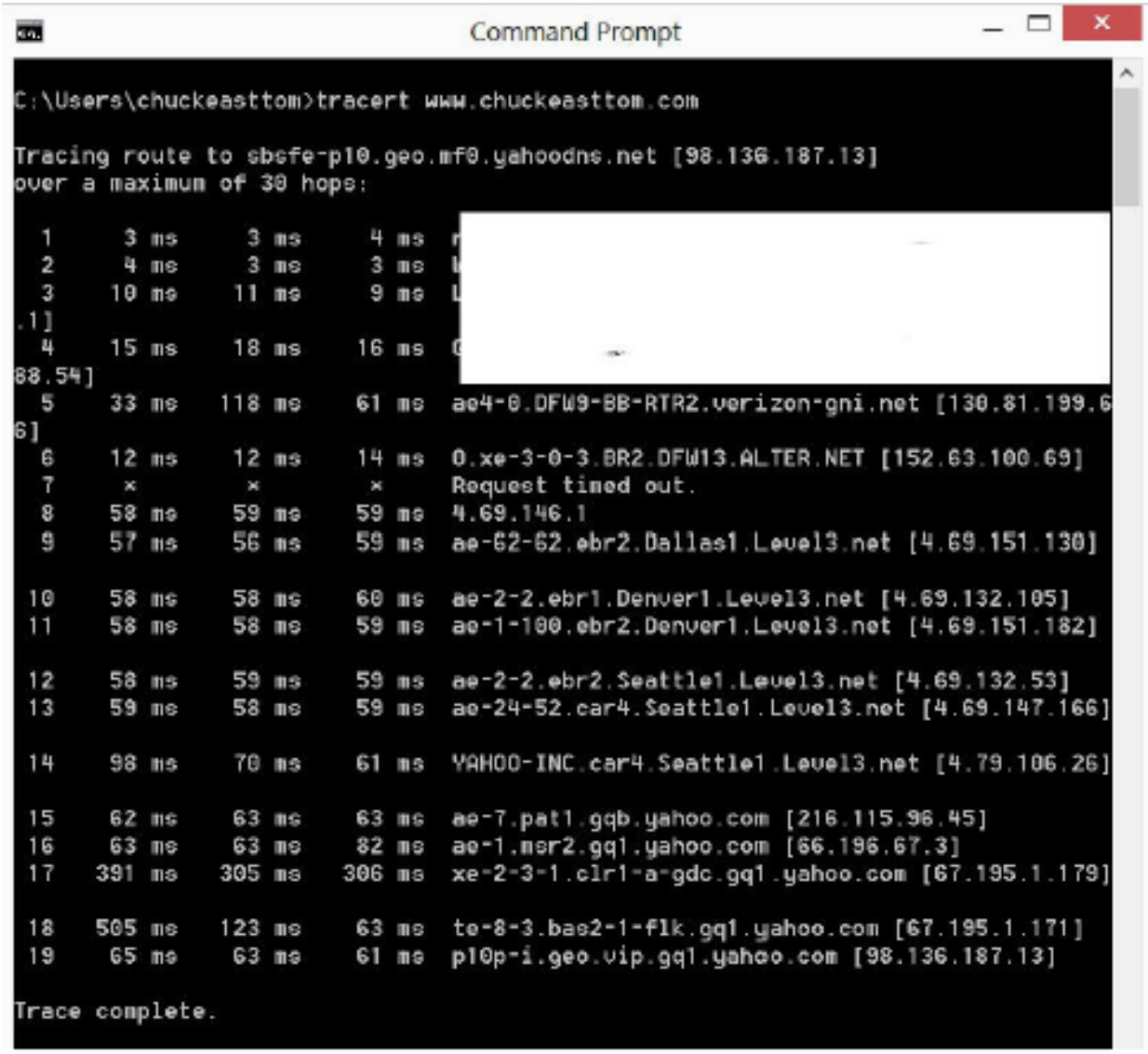
خلال عملية التحليل الجنائي الرقمي من المهم أن نقوم بالبحث في الجهاز المشتبه به عن الملفات ذات اللاحقة الاسمية السابقة.

برامج التحليل الجنائي الرقمي مثل **EnCase and FTK** يمكن أن تقوم بفحص رسائل البريد الالكتروني والبحث عن كلمات معينة داخل الرسائل.

تتبع رسائل البريد الالكتروني:

عملية تتبع الرسالة يتم من خلال فحص ترويسة الرسالة والبحث عن أي معلومات تشير إلى مرسل هذه الرسالة.

أول خطوة هي تحديد من أين تم إرسال هذه الرسالة وذلك من خلال تتبع عنوان **IP** الموجود في الترويسة ومن ثم القيام بتتبع مصدر هذه الرسالة ويمكن القيام بذلك من خلال التعليمة **tracet** في **windows** أو التعليمة **traceroute** في **linux** والتي يمكنها تتبع عنوان **IP** أو اسم موقع.



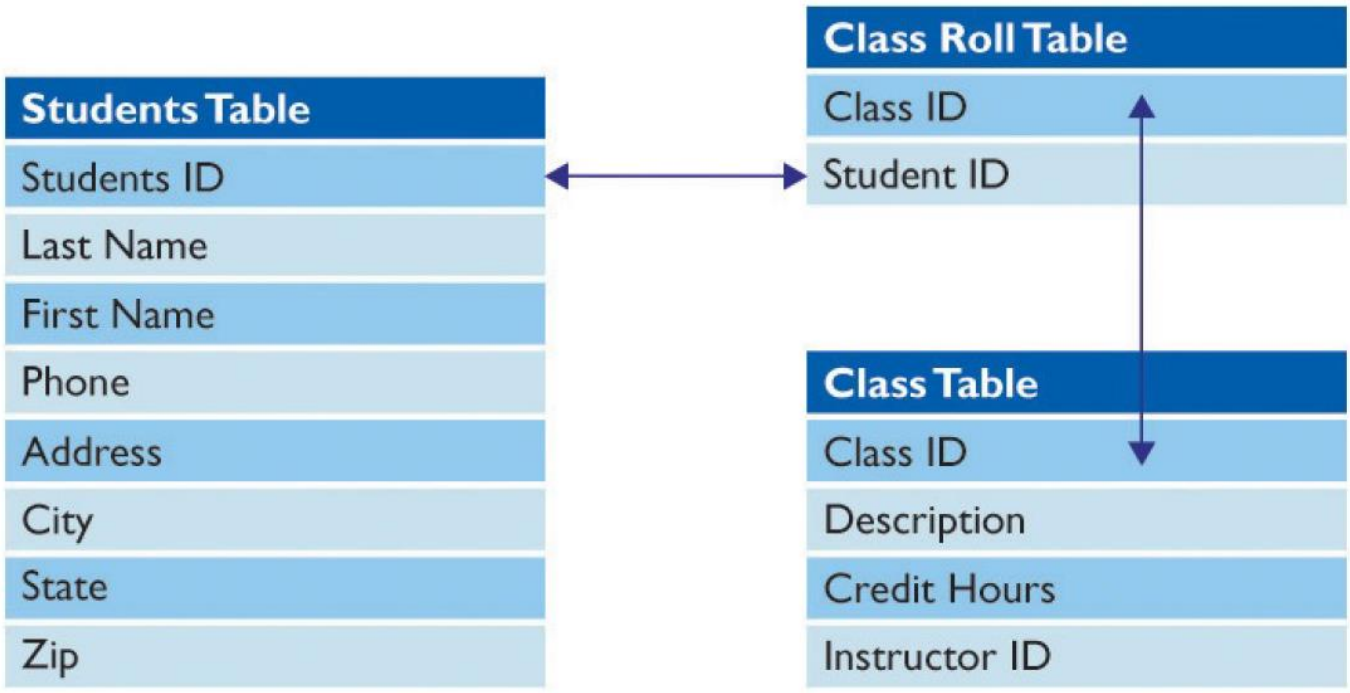
المجرم يمكن أن يقوم بحذف الرسائل، إذا استطعنا الوصول لمُخدّم البريد الالكتروني يمكننا رؤية محتوى الرسائل.

الأدوات **Forensic Toolkit an EnCase** يمكن أن تستخدم في عملية التحليل الجنائي الرقمي لمُخدّم البريد الالكتروني.

التحليل الجنائي الرقمي لقواعد البيانات:

التحليل الجنائي الرقمي لقواعد البيانات مهم جداً في الجرائم المعلوماتية.

قاعدة البيانات عبارة عن جداول تحوي أعمدة خاصة بالمعلومات المراد تخزينها، مثلاً ليكن لدينا قاعدة بيانات خاصة بالطلاب وهي عبارة عن جدول يحوي على عمود خاص بالاسم الأول وعمود خاص بالعنوان وعمود خاص برقم الهاتف.



يوجد العديد من أنظمة إدارة قواعد البيانات وأشهرها:

- **Microsoft SQL Server**
- **Oracle**
- **Microsoft Access**
- **MySQL**
- **PostGres**

قاعدة البيانات يتم حفظها عادةً في مُخدّم خاص بها وعملية الفحص والتحليل الجنائي الرقمي لهذا المُخدّم تتم بشكل مشابه لأي مُخدّم من خلال البحث في السجلات والبحث عن البرمجيات الخبيثة.

أفضل مكان للبحث عن الدليل الرقمي في قواعد البيانات هو سجل العمليات **transaction log** هذا السجل يحوي على كل عملية إدخال وكل عملية حذف أو اختيار أو تحديث لقاعدة البيانات وهو يؤمن صورة كاملة عن كل العمليات التي تمت في قاعدة البيانات.

من المهم أيضاً البحث عن حسابات المستخدمين في قاعدة البيانات، من الممكن إضافة مستخدم جديد من خلال حقن تعليمات **SQL injection**

النسخة الاحتياطية **backup** لقاعدة البيانات هي مكان مهم يجب فحصه خلال عملية التحليل الجنائي الرقمي.

تقوم أنظمة إدارة قواعد البيانات عادةً بعمليات النسخ الاحتياطي بشكل دوري وهذا يسمح للنظام بالعودة للعمليات في حال انهيار قاعدة البيانات، البحث في النسخ الاحتياطية يمكن أن يؤدي لكشف بعض المعلومات التي تم حذفها من قاعدة البيانات التي تعمل حالياً.

التحليل الجنائي الرقمي لأجهزة الموبايل

محتوى هذا الفصل:

- الشريحة **SIM**
- أنظمة تشغيل أجهزة الموبايل.
- أماكن وجود الدليل الرقمي في أجهزة الموبايل.
- خطوات التحليل الجنائي الرقمي لأجهزة الموبايل.
- أدوات التحليل الجنائي الرقمي لأجهزة الموبايل.

مقدمة:

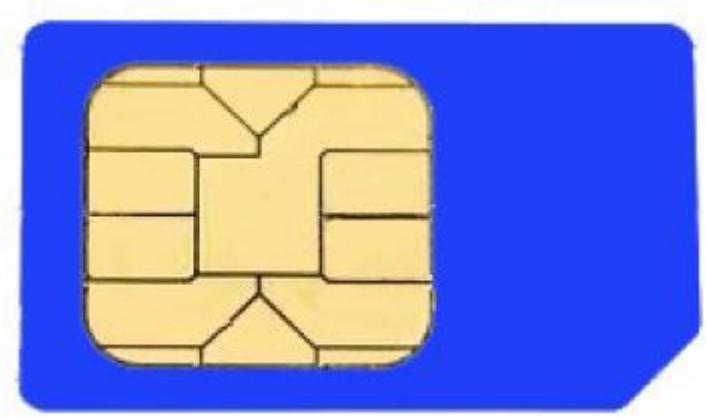
أجهزة الموبايل أصبحت موجودة في كل مكان وهي مستخدمة بشكل كبير في عمليات الاتصال وتصفح الانترنت وفي العديد من الجرائم المعلوماتية يمكن أن نجد الدليل الرقمي في جهاز الموبايل كما أن أجهزة الموبايل يمكن أن تحوي على أدلة للجرائم العادية (الغير معلوماتية) لذلك من المهم فهم طريقة عمل هذه الأجهزة وأنظمة التشغيل الخاصة.

الشريحة SIM:

SIM (Subscriber Identity Module)

شريحة **SIM** هي أهم جزء في أي جهاز موبايل، وهي التي تحدد الرقم الخاص بالمستخدم وتحوي أيضاً عن معلومات خاصة بالشبكة وتحوي أيضاً على كلمتين سر وهما:

1. **PIN (Personal Identification Number)**
2. **PUK (Personal Unblocking Code)**



بعض المصطات الأساسية:

- **IMSI (International Mobile Subscriber Identity)**: رقم الموبايل الخاص بالمستخدم.
- **ICCID (Integrated Circuit Card Identification)**: عبارة عن رقم خاص مطبوع على الشريحة.
- **IMEI (International Mobile Equipment Identy)**: رقم فريد يستخدم لتعريف أجهزة الموبايل ويكون مطبوع داخل الهاتف (مكان وجود البطارية) وباستخدام هذا الرقم يمكن مراقبة أو تتبع جهاز الموبايل.
- **PUK (Personal Unlock Number)**: يستخدم من أجل إعادة ضبط رمز **PIN** في حال نسيانه كما يستخدم عند إجراء عملية إعادة ضبط المصنع لجهاز الموبايل وإذا تم إدخال هذا الرمز عشر مرات بشكل غير صحيح فسوف يتم قفل الجهاز بشكل دائم.
- **PSTN (Public Switched Telephone Network)**: رقم الهاتف الثابت.
- **MSC (Mobile Switching Center)**: مركز التبديل في شبكات **GSM and 3G** ويتم من خلاله معالجة كل الاتصالات وهو المسؤول عن توجيه المكالمات بين المحطات.
- **Base Transceiver Station (BTS)**: جزء من شبكة الموبايل (الأبراج الموجودة في الشوارع) ومسؤولة عن الاتصال بين الأجهزة وبين مركز التبديل **MSC**

- **HLR (Home Location Register)**: مسجل الموقع الحالي ويحوي على جميع البيانات للمشتركين في المنطقة الحالية.
- **VLR (Visitor Location Register)**: مسجل موقع الزائر ويحوي على جميع البيانات للمشتركين الموجودين في منطقة مركز التبديل **MSC**
- **GSM (Global System Mobile)**: وتسمى أيضاً شبكة الجيل الثاني **2G**
- **EDGE (Enhanced Data Rates for GSM Evolution)**: وهي تطوير لشبكة الجيل الثاني وتسمى أيضاً **2.5 G**
- **UMTS (Universal Mobile Telecommunication System)**: وهي الجيل الثالث **3G**
- **LTE (Long Term Evolution)**: وهي الجيل الرابع **4G**

أنظمة التشغيل الخاصة بأجهزة الموبايل:

أنظمة تشغيل أجهزة الموبايل الحالية هي:

iOS:

وهو نظام التشغيل الخاص بأجهزة **iPhone, iPod and iPad** الخاصة بشركة **Apple** وهو مبني على نظام التشغيل **OS X for Macintosh**

نظام **iOS** مقسم إلى أربع طبقات، البرامج تتفاعل مع طبقة **Core Services** وهي الطبقة الثانية.

الطبقة الثالثة مسؤولة عن الموسيقى والفيديو أما الطبقة **Cocoa Touch layer** فهي مسؤولة عن الأوامر اللمسية من قبل المستخدم.

نظام التشغيل **iOS** يستخدم **HFS+ file system** التي تم إيجادها من قبل شركة **Apple** كبديل عن **HFS (Hierarchical File System)**

نظام التشغيل **iOS** قادر على استخدام **FAT32** عند الاتصال بنظام **windows** (عند عمل مزامنة لجهاز الموبايل مع جهاز الحاسب)

في نظام **iOS** يتم تقسيم البيانات إلى:

- **Calendar entries**
- **Contact entries**
- **Note entries**
- **iPod_control directory (this directory is hidden)**
- **iTunes configuration**
- **iTunes music**

دليل الهاتف والأسماء وبعض البيانات المخفية في مجلد **iPod_control** مهمة جداً في عملية التحليل الجنائي الرقمي.

المجلد **iPod_control\device\sysinfo** يحوي على المعلومات المهمة التالية:

- **iPod model number**
- **iPod serial number**

المصطلح **Jailbreaking** يشير إلى عملية تجاوز الحدود التي وضعتها الشركة المصنعة وهذا يسمح بتشغيل برامج ممنوعة وبصلاحيات عالية وهذا له أثر سلبي على حماية الهاتف وهو الأمر المشابه لعملية **rooting** في أجهزة **Android**

أجهزة **Apple** يمكن أن تعمل في نمط **recovery mode** والذي يمكن أن يستخدم من قبل المحقق الجنائي الرقمي.

هذا النمط يتجاوز نظام التشغيل ويقوم بالإقلاع بما يسمى **iBoot** وهذا يمنع أي عملية مزامنة مع الحاسب أو مع البرامج وذلك أثناء عملية إنشاء صورة طبق الأصل لمحتوى جهاز الهاتف.

Android:

وهو نظام التشغيل الأكثر استخداماً حول العالم وهو مبني بالاعتماد على نظام **linux** وهو مفتوح المصدر (يمكن رؤية الرماز البرمجي المصدري الخاص به).

يوجد عدة إصدارات من نظام **android** وآخرها:

- **V 4.1 – 4.2 Jelly Bean**
- **V 4.4 KitKat**
- **V 5.0 Lollipop**

كل الإصدارات مبنية على نظام **linux** ولكن كل إصدار يحوي على خصائص وتعديلات جديدة.

في نظام **android** يمكن للمستخدم تنزيل وتنصيب البرامج من أي متجر عبر الانترنت بعكس **iPhone** الذي يسمح فقط بنزيل وتنصيب البرامج من متجر **iTunes store** وهذا الأمر له إيجابيات وسلبيات عديدة وأحد اهم السلبيات هو انتشار البرمجيات الخبيثة الخاصة بأنظمة **android** بشكل أكبر من البرمجيات الخبيثة الخاصة بنظام **iOS** (**97%** من البرمجيات الخبيثة الخاصة بأجهزة الموبايل مصممة لتعمل على نظام **android**)

وهذا يزيد من أهمية عملية التحليل الجنائي الرقمي للأجهزة التي تعمل بأنظمة **android**.

تطبيقات الموبايل:

يمكننا الحصول على بعض الأدلة الرقمية من بعض التطبيقات التي تعمل في جهاز الموبايل مثل تطبيقات المحادثة وتطبيقات التواصل الاجتماعي

ومتصفحات الانترنت وبالتأكيد الصور ومقاطع الفيديو مهمة جداً في أي عملية تحليل جنائي رقمي.

يوجد بعض التطبيقات التي تسمح للمستخدم بأن يقوم بمسح محتوى الهاتف بشكل كامل ومن عن بعد، لذلك من الضروري وضع الهاتف في حقيبة أو علبة تمنع أي عمليات إرسال واستقبال تتم باستخدام الإشارات اللاسلكية لعزل الجهاز بشكل كامل عن الشبكة ويجب أن يكون مخبر التحليل الجنائي الرقمي محاط بقفص فارداي لمنع أي عمليات اتصال باستخدام الإشارات اللاسلكية.

أماكن وجود الدليل الرقمي:

أجهزة الموبايل يمكن أن تحوي على أدلة لكل من الجرائم المعلوماتية وغير المعلوماتية وهذه الأدلة يمكن أن توجد في الأماكن التالية:

- **سجلات الرسائل والمكالمات:** معرفة الجهات التي يتواصل معها المشتبه به هو أمر مهم في أي عملية تحليل جنائي.
- **الصور ومقاطع الفيديو:** الصور ومقاطع الفيديو يمكن أن تكون دليل رقمي ضد المتهم.
- **سجلات GPS:** (هذه الخدمة غير مدعومة في سوريا).
- **التطبيقات:** معرفة التطبيقات الموجودة في الجهاز هو أمر مهم في عملية التحليل الجنائي الرقمي، يجب إحصاء وتحليل كل السجلات الخاصة بتطبيقات المحادثة والتواصل الاجتماعي وتصفح الانترنت.

التحليل الجنائي الرقمي لأجهزة الموبايل:

خلال عملية التحليل الجنائي الرقمي يجب أن نقوم بتحديد الأمور التالية:

- معلومات عن نوع وحالة الجهاز.
- تاريخ المكالمات والرسائل.
- جمع الصور ومقاطع الفيديو.
- معلومات **GPS**
- معلومات عن اتصالات الشبكة.
- معلومات عن التطبيقات.
- سجلات المحادثة وتاريخ تصفح الانترنت.

المعلومات عن نوع الهاتف هي أول أمر يجب أن يقوم المحقق الجنائي الرقمي بتوثيقه في التقرير (رقم الهاتف ونوع الجهاز والرقم التسلسلي للجهاز ونوع وإصدار نظام التشغيل).

سجل المكالمات يجب أن يتم فحصه وبشكل دقيق وتحديد الجهات التي يقوم المتهم بالاتصال معهم بشكل دوري ومعرفة تاريخ ومدة كل مكالمة.

البحث في ذاكرة الجهاز وكرت الذاكرة عن الصور ومقاطع الفيديو أو أي ملفات أخرى يمكن أن تكون متعلقة بالجريمة وهذه الملفات قد تكون أدلة هامة في الجرائم المعلوماتية والغير معلوماتية.

فحص اتصالات الشبكة ومعرفة الشبكات اللاسلكية التي تم الاتصال بها هو أمر مهم جداً ومن خلال هذه الشبكات يمكن معرفة الأماكن التي تواجد فيها المتهم (وجد اسم شبكة يخص مقهى أو فندق معين)

بعض الجرائم المعلوماتية مثل إرسال البريد الواغل **spam** أو هجمات منع الخدمة أو حتى اختراق المواقع أو المنظومات المعلوماتية يمكن أن تتم باستخدام جهاز الموبايل.

التالي هو الخطوات المتبعة في عملية التحليل الجنائي الرقمي لأجهزة الموبايل:

1. عند وصل جهاز الموبايل بجهاز الحاسب يجب أن نتأكد من أن الهاتف لن يقوم بعملية المزامنة مع الحاسب (بعض الأجهزة مُعدة لتقوم بعملية المزامنة بشكل تلقائي)
2. نتبع نفس الخطوات المتبعة في عملية التحليل الجنائي الرقمي لجهاز الحاسب مع التركيز على عدم تخريب الدليل الرقمي وتوثيق كل العمليات.
3. خلق صورة طبق الأصل لكامل محتوى الهاتف.
4. وضع الهاتف في حقيبة أو علبة عازلة تمنع الإشارات اللاسلكية لضمان عزل الجهاز عن الشبكة أو عن أي اتصال مع الوسط الخارجي.

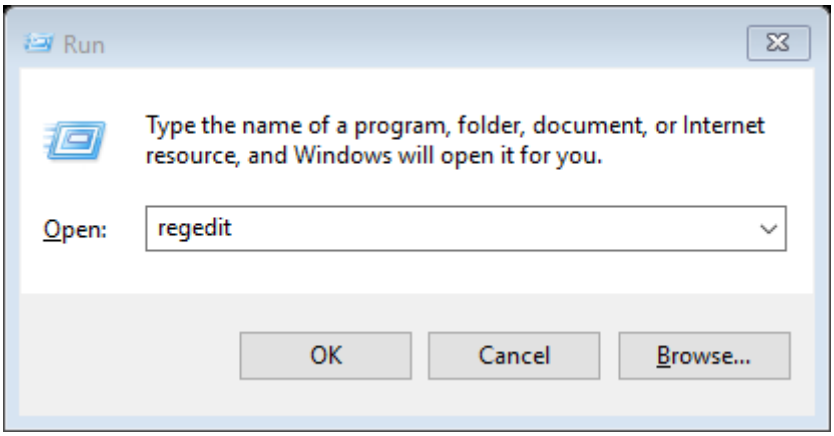
الأمر المهم عند القيام بهذه العملية هو التأكد من عدم كتابة أي بيانات على جهاز الموبايل، عند وصل جهاز الموبايل بجهاز الحاسب يجب أن نتأكد بأن الحاسب لن يقوم بكتابة أي بيانات على جهاز الموبايل.

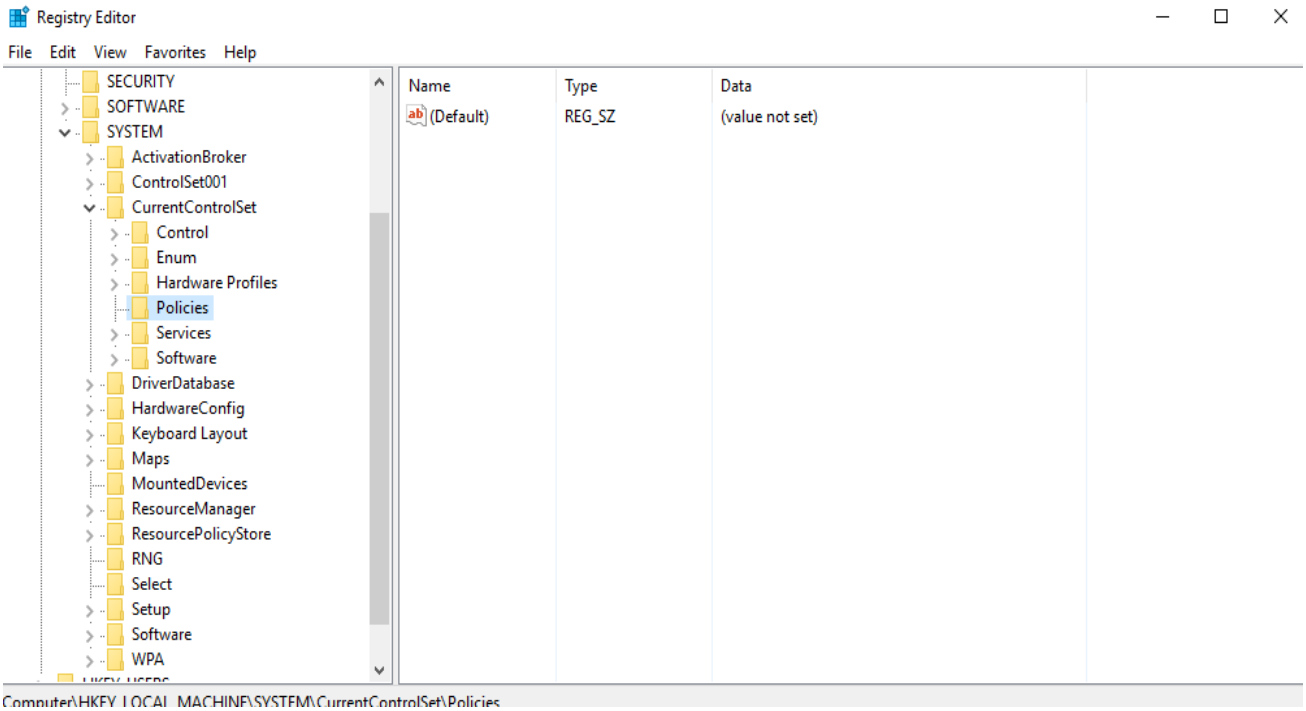
للتأكد من ذلك، إذا كنت تستخدم نظام **windows** يمكن تعديل **Windows registry** لمنع الحاسب من كتابة أي بيانات على جهاز الموبايل.

قبل وصل الموبايل بالحاسب يجب أن نقوم بتعديل مفتاح **Windows registry** التالي:

(HKEY_LOCAL_MACHINE\System\CurrentControlset\StorageDevice\Policies)

ليأخذ القيمة **0x00000001** ومن ثم إعادة تشغيل الحاسب، هذه العملية تمنع الحاسب من الكتابة على أي جهاز يتصل به.





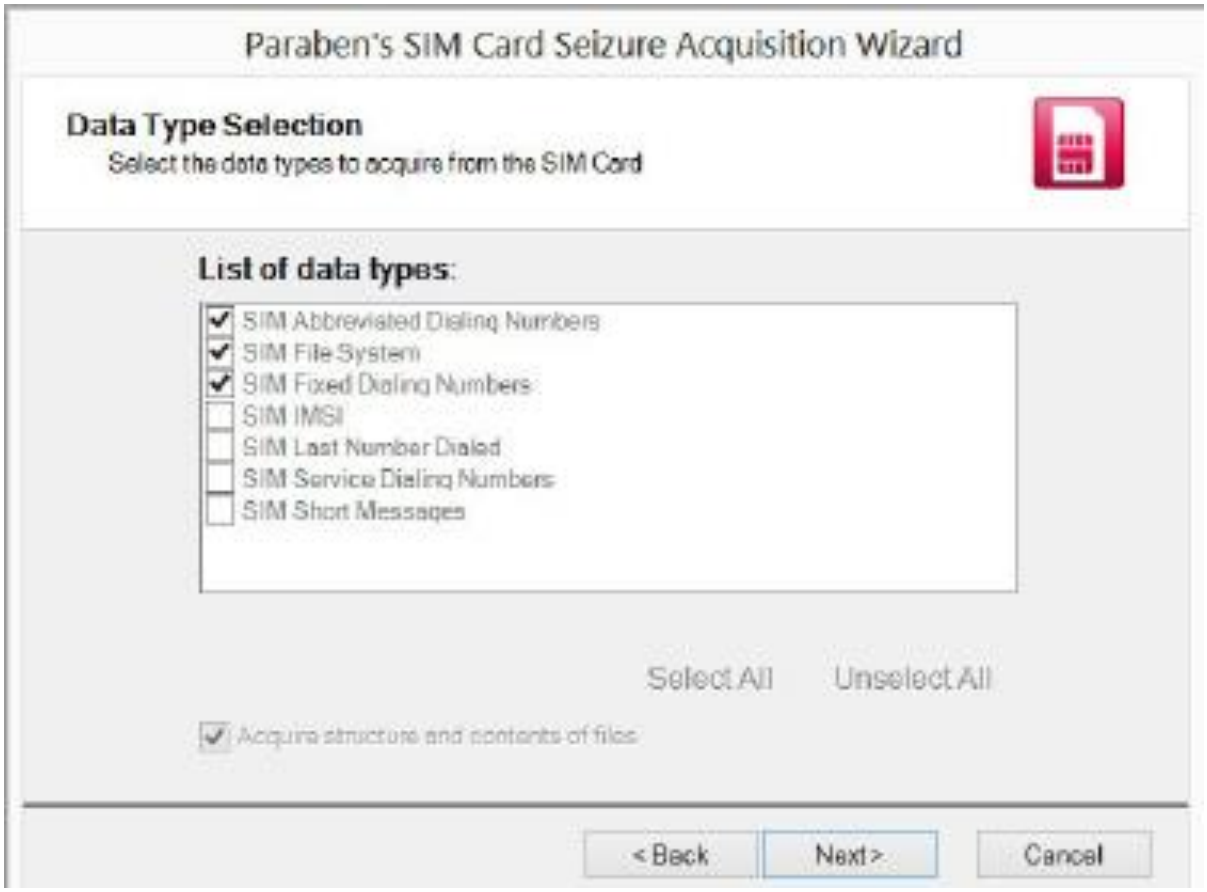
إنشاء صورة طبق الأصل لمحتوى جهاز الموبايل يمكن أن يتم من خلال نسخ كل الملفات في الموبايل إلى جهاز الحاسب ولكن عملية النسخ يجب أن تتم لكامل المحتوى ومن الملف الخارجي وهذا يسمح باستعادة الملفات أو إظهار الملفات المخفية لاحقاً أثناء عملية التحليل، كما يمكننا إنشاء نسخة مطابقة بنفس الطريقة المستخدمة في أجهزة الحاسب **bit-by-bit** ولكن يجب أن ندرك بأن الأجهزة التي تعمل بنظام **iOS** تقوم بعملية تشفير لكامل محتوى الجهاز كما أن الأجهزة التي تعمل بنظام **android** تؤمن آلية لتشفير كامل محتوى الجهاز وهذا يعني أننا لن نستطيع رؤية محتوى هذه البيانات لأنها ستكون مشفرة.

مؤخراً تمكنت **FBI** من كسر تشفير جهاز **iPhone** وبدون مساعدة شركة **Apple**

أدوات التحليل الجنائي الرقمي لأجهزة الموبايل:

Paraben:

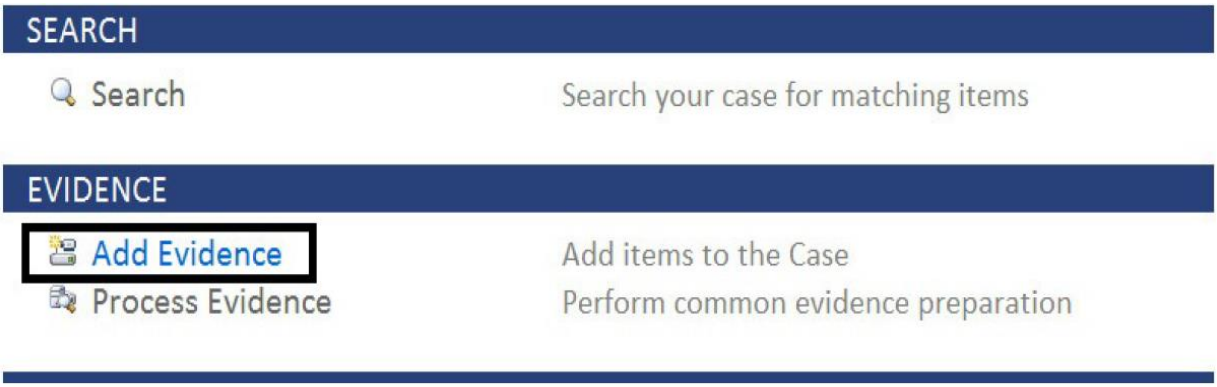
هذه الشركة تملك عدداً من أدوات التحليل الجنائي الرقمي ومنها أداة خاصة بالتحليل الجنائي الرقمي لشريحة **SIM** والتي تعمل بشكل تجريبي لمدة **30** يوم



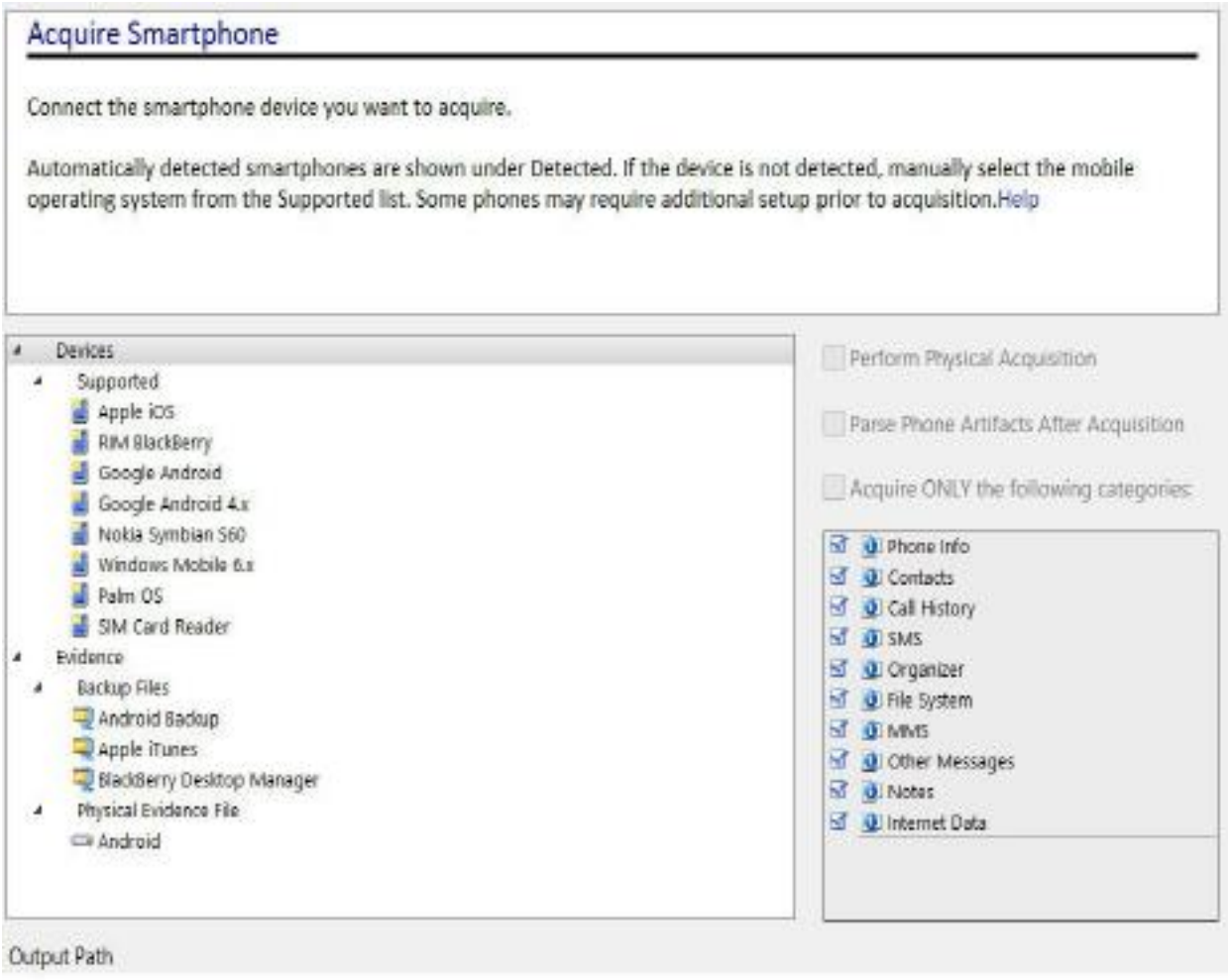
:EnCase

EnCase يحوي على أداة خاصة بأجهزة الموبايل.

في البداية يجب أن نفتح قضية جديدة ومن ثم نقوم بإضافة الدليل الرقمي **Evidence** كما في الشكل التالي:



ومن ثم نقوم بتحديد نوع الدليل **Acquire Smartphone**



DDR Phone from Data Recovery Software:

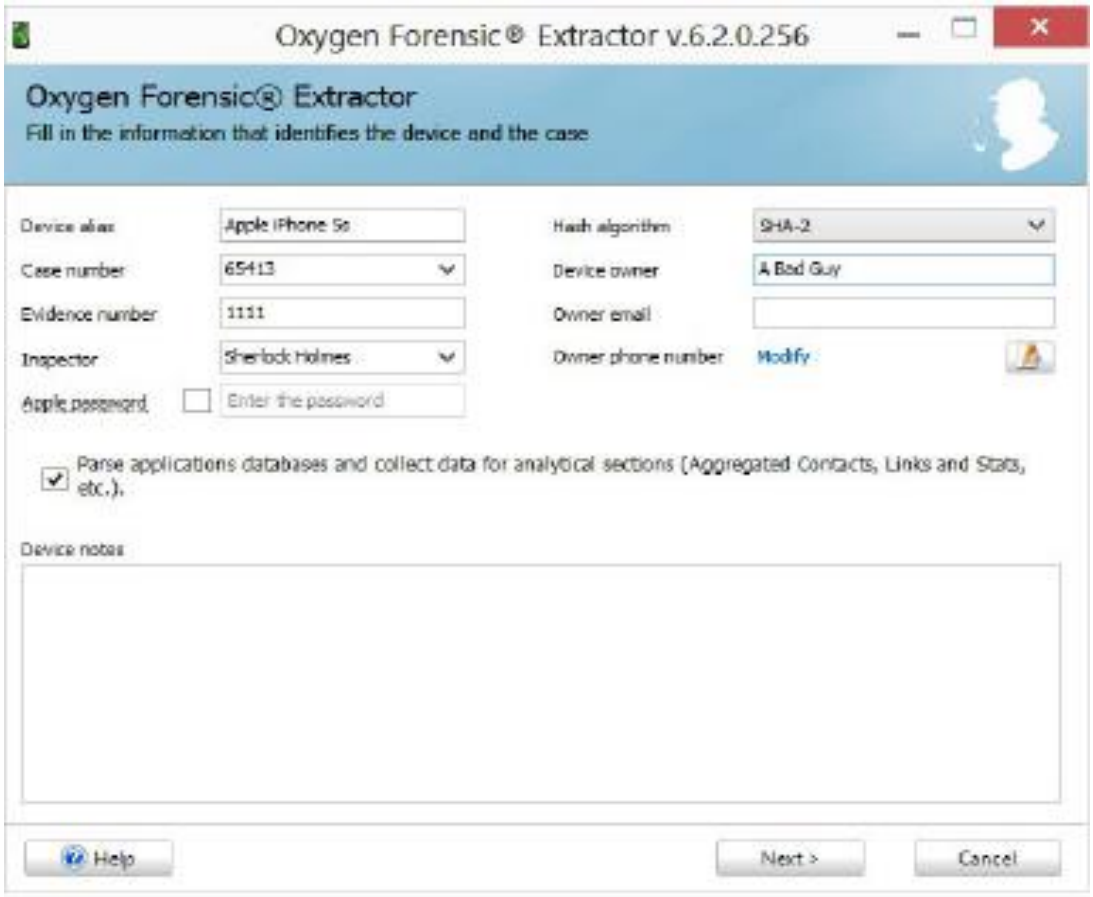
وهي أداة بسيطة وتسمح لنا بتحديد نوع البحث المطلوب لتقوم به ويمكن من خلالها البحث عن الصور أو مقاطع الفيديو أو أي ملفات أخرى في جهاز الموبايل.

Oxygen:

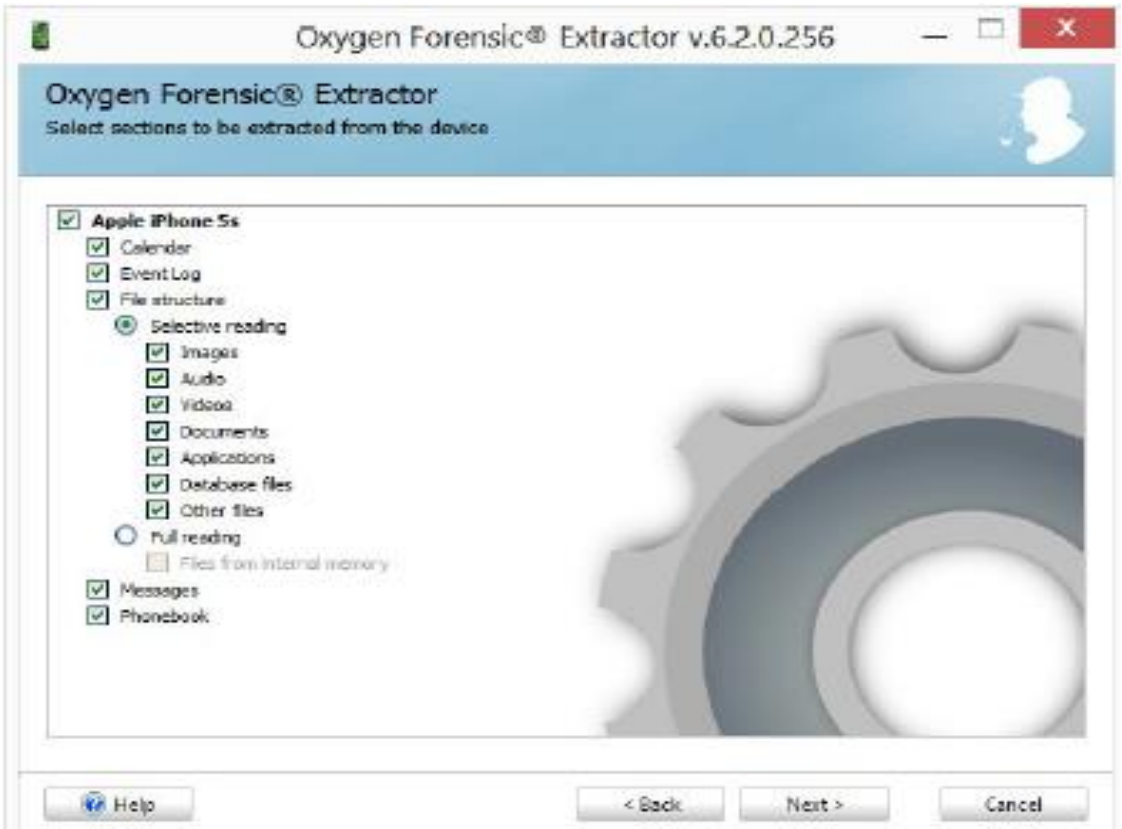
أداة للتحليل الجنائي الرقمي لأجهزة الموبايل ولها نسخة مجانية ولكنها محدودة الإمكانيات.

المثال التالي لاستخدام هذه الأداة للحصول على المعلومات الخاصة بجهاز من نوع **iPhone 5**

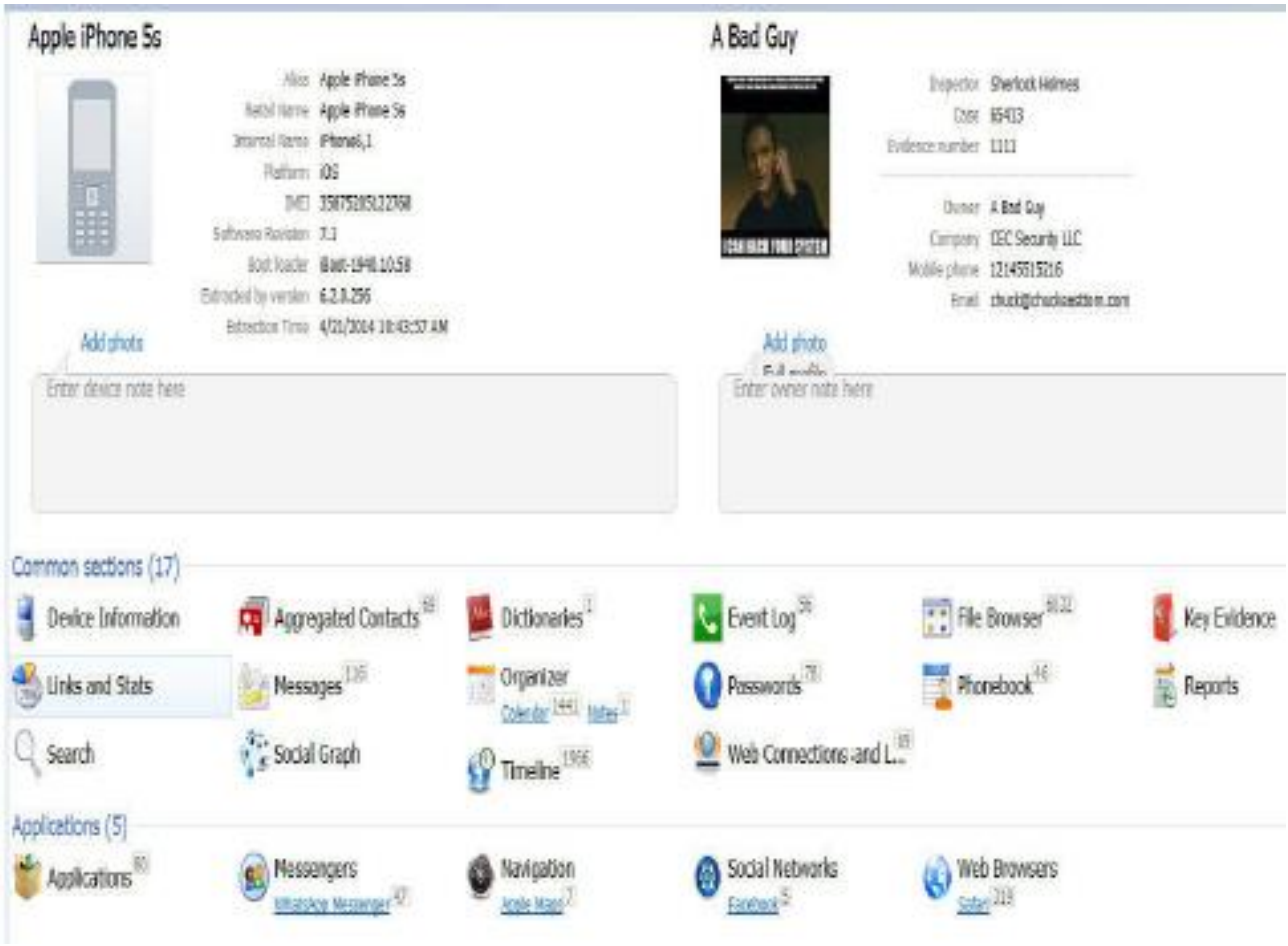
الخطوة التالية هي إدخال تفاصيل القضية (اسم المحقق ورقم القضية وأمور أخرى) بشكل افتراضي فإن هذه الأداة سوف تستخدم خوارزمية **SHA2** للقيام بحساب الهاش.



الخطوة التالية هي لتحديد المعلومات المراد استخراجها

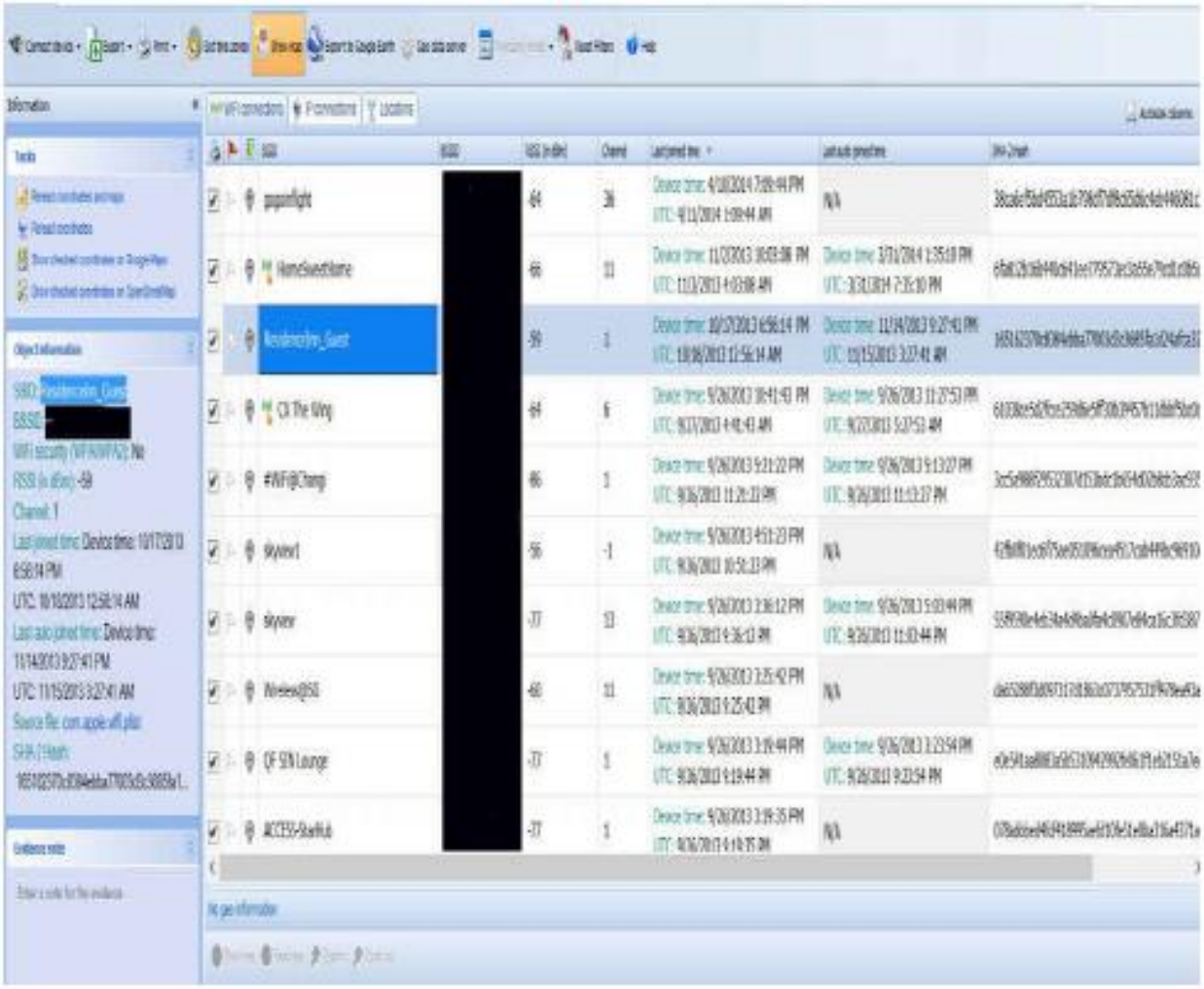


والنتيجة سوف تكون كما في الشكل التالي حيث يمكننا رؤية الرسائل والمكالمات وسجل تصفح الانترنت وأمور أخرى



هذه الأداة لها القدرة على استعادة الملفات المحذوفة كما يمكنها استعادة سجلات المكالمات والرسائل المحذوفة وهذا أمر مهم جداً في عملية التحليل الجنائي الرقمي.

كما يمكن لهذه الأداة أن تقوم بعرض كل الشبكات اللاسلكية التي تم الاتصال بها وتاريخ أخر اتصال بكل شبكة



يقوم العديد من الأشخاص بعملية مزامنة بين الموبايل والحاسب أو عملية نسخ احتياطي لجهاز الموبايل على الحاسب، من المهم البحث في جهاز الحاسب الخاص بالمتهم عن أي ملفات خاصة بالنسخ الاحتياطي لأي جهاز موبايل.

تحليل البرمجيات الخبيثة

Malware Analysis

محتوى هذا الفصل:

- أنواع البرمجيات الخبيثة.
- الفيروسات.
- أحصنة طروادة.
- برمجيات التجسس.
- أدوات تحليل البرمجيات الخبيثة.

مقدمة:

Malware هي اختصار ل **malicious software** وتعني "برمجية خبيثة"

البرمجيات الخبيثة: هي برامج يتم تضمينها أو إدراجها في أنظمة الحاسب دون علم أو رضا المالك لأغراض تهدف إلى إلحاق الضرر بهذه الأنظمة، وتتعدد درجات الضرر بحسب درجة خطورة هذه البرمجيات كالوصول غير المشروع والتجسس وجمع المعلومات وعرقلة العمليات وتوفير الظروف للمهاجمين للقيام بعمليات اختراق أوسع، علماً بأن بعض أنواع البرمجيات الخبيثة يستطيع تكرار نفسه والانتشار بعدد من الطرق.

أنواع البرمجيات الخبيثة:

1- Keylogger مسجل ضربات المفاتيح:

وهو عبارة عن جهاز **hardware** أو برنامج **software** يقوم بمراقبة وتسجيل كل حرف يتم كتابته بواسطة لوحة المفاتيح كما يمكن أن يقوم أيضاً بالتقاط وتسجيل لقطات للشاشة.

2- Trojan Horse حصان طروادة (تروجان):

وهو أكثر أنواع البرمجيات الخبيثة انتشاراً وأكثرها خطورة.

للوهلة الأولى يبدو أنه برنامج شرعي وسليم ولكنه في الحقيقة يمنح المهاجم قدرة كاملة على الوصول والتحكم بجهاز الضحية.

3- RAT أداة الإدارة عن بعد:

وهي اختصار ل **Remote Administration Tool** وتعتبر من البرمجيات الخبيثة ذات الخطورة الشديدة فعندما يتم تنصيب هذه الأداة على جهاز الضحية فإن المهاجم يستطيع أن يقوم بكل شيء عن بعد، كتنصيب مسجل ضربات المفاتيح **Keylogger** أو إيقاف تشغيل الجهاز أو حذف الملفات.

4- Viruses الفيروسات:

وهي عبارة عن برامج يتم كتابتها وتطويرها من أجل إصابة أجهزة الحاسب وعندما تقوم بإصابة جهاز ما فهي تقوم بنسخ أو تكرار نفسها لتقوم بعدوى وإصابة أجهزة أخرى وهي تتكاثر وتنتشر بالاعتماد على ملفات أخرى.

5- Worms الديدان:

تشبه الفيروسات والفرق الوحيد بينهما هو أن الديدان تعتمد على نفسها للتكاثر وعدوى الأجهزة الأخرى وتتميز بسرعة الانتقال.

عندما تقوم الدودة **worm** بعدوى أو إصابة جهاز فهي تقوم بنسخ وتكرار نفسها وهي تنتقل بسرعة وتنتشر داخل الشبكة وتستهلك موارد الشبكة أثناء انتشارها.

الديدان تعتبر الخطر الرئيسي الذي يهدد الشبكات الكبيرة.

6- Adware برمجيات الإعلانات والتجسس:

Advertisement software

وتسمى أيضاً **Spyware** "برمجيات التجسس"

وهي مصممة لتقوم بجمع المعلومات وعرض الإعلانات على الجهاز المصاب بها، بعض هذه البرمجيات تحوي على فيروسات مؤذية وبرامج تجسس.

7- Ransomware برامج الفدية:

تقوم بتشفير الملفات الخاصة بالضحية وطلب مبلغ من المال (فدية) من أجل فك تشفير هذه الملفات.

8- RootKit:

مجموعة من الأدوات يقوم المهاجم بتنصيبها في الجهاز بعد النجاح في عملية الاستغلال من أجل تثبيت الاستغلال والمحافظة على الوصول والقيام بهجمات إضافية

الفيروسات:

الفيروس عبارة عن برنامج يقوم بالتكاثر وتكرير نفسه بشكل ذاتي ويقوم بنسخ وربط رمازه البرمجي مع رمازات برامج أخرى وهو يعمل بدون علم المستخدم ويلحق نفسه مع برامج أخرى أو ملفات أخرى أو مع ملفات إقلاع النظام.

الفيروسات تنتقل عادةً من خلال تحميل الملفات من مواقع غير موثوقة أو من خلال وسائط نقل البيانات (ذواكر **USB** أو الأقراص الليزرية) أو عبر مرفقات البريد الالكتروني أو عبر الأجهزة المتصلة بنفس الشبكة.

الفيروسات تقوم بمهاجمة النظام الهدف من خلال عدة طرق مختلفة حيث تقوم بإلحاق نفسها مع البرامج أو الملفات وتنتقل معها إلى برامج أخرى أو إلى أجهزة أخرى وذلك من خلال الاستفادة من بعض الأحداث.

أمثلة عملية لطرق انتشار الفيروسات:

- **مضاد الفيروسات المزور:** المهاجم يقوم بخداع الضحية عبر رسالة الكترونية مزورة تخبر المستخدم بأن جهازه مصاب بعدد من الفيروسات وتطلب منه تحميل برنامج مضاد الفيروسات المرفق وهو في الحقيقة عبارة عن فايروس.
- **تحميل البرامج من المواقع الغير موثوقة:** المستخدم يمكن أن يقوم بتحميل برامج مجانية من مواقع غير موثوقة تحوي على فايروسات.
- **مرفقات البريد الالكتروني:** المهاجم يمكن أن يقوم بخداع المستخدم عبر رسالة الكترونية ويطلب منه فتح المرفقات أو الضغط على رابط معين يؤدي لإصابة الجهاز بفايروس.
- **وسائط نقل الملفات:** الفايروسات يمكن أن تنتقل عبر وسائط نقل الملفات مثل ذواكر **USB** وأقراص **DVD**

أنواع الفيروسات:

لنتمكن من تحليل الفيروسات يجب أن نتعرف أولاً على أنواع هذه الفيروسات:

- **الفيروسات المدرعة:** من الصعب جداً تحليل هذا النوع من الفيروسات لأنها تكون مكتوبة بطريقة معينة تهدف إلى تشويش الرماز البرمجي المصدري الخاص بها.
- **الفيروسات المنتشرة:** تنتشر بشكل سريع جداً من خلال عدوى وإصابة ملفات أخرى وهذا يجعل من عملية حذف هذا الفايروس هو أمر صعب جداً وبعض أنواع هذه الفيروسات يمكن أن يعمل بعد فترة معينة من إصابته للجهاز الهدف.
- **فايروس الماكرو Macro:** في **Microsoft Office Word or Excel** فإن **macro** هو سلسلة من التعليمات والأوامر التي تساعد على القيام بعض المهمات بشكل اتوماتيكي.

تسمح لغة فيجوال بيسيك للتطبيقات (**VBA -Visual Basic for Applications**) بإنشاء برامج صغيرة ووحدات **Macro** يتم حفظها في مستندات وقوالب **Word or Excel** لأتمته المهام المستخدمة بشكل متكرر.

الماكرو هو سلسلة من الأوامر والإرشادات والتي يتم تجميعها كأمر واحد لإنجاز مهمة معينة بشكل تلقائي.

يمكن كتابة رماز ماكرو خبيث وجعله يعمل بشكل اتوماتكي عند فتح مستند **Word** لإصابة وعدوى جهاز الضحية.

- **الفيروسات متعددة الأجزاء:** يمكن أن تهاجم الجهاز بعدة طرق ولكنها عادةً تقوم بعدوى قطاع الإقلاع الخاص بالنظام وهي تعمل بمجرد إقلاع النظام كما يمكن أن تصيب ملف معين أو أن تصيب سجلات النظام **registry** الخاصة بنظام **windows**
- **الفيروسات متعددة الأشكال:** كما يشير الاسم فهذه الفيروسات يمكن أن تأخذ أشكال مختلفة كمحاولة لتجاوز تقنيات الحماية من قبل مضاد الفيروسات من خلال تشفير جزء من الرماز الخاص بالفايروس أو باستخدام طرق أخرى.

في السنوات السابقة كانت عملية كتابة الفيروسات تتم من قبل مبرمجين محترفين أما في الأيام الحالية فقد انتشرت العديد من الأدوات التي تسمح لأي شخص بخلق الفيروسات.

حصان طروادة Trojan Horse:

برمجية خبيثة تبدو للوهلة الأولى أنها برنامج أو ملف سليم (صورة أو ملف صوتي أو مقطع فيديو) وعند فتحه يقوم بتنصيب برمجية خبيثة على جهاز الضحية تمنح المهاجم سيطرة كاملة على الجهاز وبدون علم الضحية.

يعود سبب التسمية إلى الأسطورة اليونانية لحصار الإغريق لمدينة طروادة حيث قام الإغريقيون باستخدام حيلة من خلال صناعة حصان خشبي كبير وملئه بالمحاربين وتقديمه كهدية للطرواديين على أنه هدية سلام، قبل الطروايون الهدية واحتفلوا بفك الحصار عن مدينتهم وعندها خرج المحاربون الإغريق من

داخل الحصان وكان سكان طروادة في حالة سكر فقام المحاربون بفتح بوابات المدينة للسماح لبقية الجيش بدخولها وسقطت طروادة وحرقت وقتل رجالها.

وبشكل مشابه تطلق هذه التسمية على البرامج التي تبدو للوهلة الأولى أنها برامج سليمة ولكن في الحقيقة هي برامج خبيثة تسمح للمهاجم التحكم بجهاز الضحية واختراقه.

عند إصابة جهاز بهذا النوع من البرمجيات فإن المهاجم يصبح قادراً على سرقة أو حذف ملفات الضحية وتثبيت برامج أخرى مثل برنامج مسجل ضربات المفاتيح **keylogger** وسرقة المعلومات السرية كمعلومات تسجيل الدخول ومعلومات بطاقات الائتمان وتعطيل الجدران النارية ومضادات الفيروسات والاتصال مع جهاز الضحية والتحكم به بشكل كامل كما أن المهاجم يكون قادراً على استخدام جهاز الضحية في أعمال غير شرعية كالقيام بهجوم منع الخدمة الموزّع **Distributed Denial Of Service**

برمجيات التجسس Spyware or Adware:

وهي البرمجيات التي يتم تنصيبها في جهاز الحاسب بدون علم أو أذن المستخدم وتقوم بجمع معلومات عن المستخدمين ومراقبة تصرفاتهم على الشبكة من خلال تسجيل كل حرف يتم كتابته وتسجيل المواقع التي يتم زيارتها من أجل خلق الإعلانات الموجهة.

وتقوم بعرض النوافذ المنبثقة المزعجة أثناء تصفح الانترنت وتقلل من سرعة تصفح الانترنت وتقلل من أداء وسرعة الجهاز لأنها تستهلك موارد الشبكة وفي بعض الأحيان تجعل الجهاز المصاب بها أكثر عرضة للاختراق

ولأن هذا النوع من البرمجيات يتم تنصيبه في جهاز الضحية بدون علمه فمن الممكن أن تبقى في جهازه لفترة زمنية قبل أن يلاحظها أو يتمكن من اكتشافها و إزالتها.

تحليل البرمجيات الخبيثة Malware Analysis:

عملية تحليل البرمجية الخبيثة تتضمن دراسة وفهم كيفية عمل هذه البرمجية كمحاولة لكشف من قام بخلق هذه البرمجية أو كشف الهدف من نشرها واستخدامها.

عند تحليل برمجية خبيثة معينة إذا وجدنا أن هذه البرمجية تقوم بمحاولة اتصال عكسي مع عنوان IP معين، من خلال هذا العنوان يمكن أن نحدد هوية الشخص الذي قام بخلق أو استخدام هذه البرمجية.

عملية التحليل يمكن أن تصنف كالتالي:

- **Static Analysis:** عملية دراسة البرمجية بدون تنفيذها، محاولة ايجاد أكبر قدر من المعلومات بدون تنفيذ هذه البرمجية من خلال فحص الرماز البرمجي المصدري إذا أمكن ذلك.

- **Dynamic Analysis:** عملية دراسة البرمجية أثناء وبعد تنفيذها وتحليل التفاعل مع النظام والعمليات الخاصة التي قامت هذه البرمجية بخلقها أو الاعتماد عليها.

الأمر المهم الذي يجب أن يؤخذ بعين الاعتبار عن تحليل أي برمجية خبيثة هو استدعاء عمليات النظام، عندما تقوم البرمجية الخبيثة باستدعاء إحدى عمليات النظام يجب أن نعرف ماهي البارامترات التي تقوم البرمجية بتمريرها للتوابع الخاصة بعمليات النظام، هذه البارامترات يمكن أن تكشف معلومات مهمة جداً عن هذه البرمجية.

مراقبة مصادر النظام هو أمر مهم أيضاً وذلك لمعرفة مدى استهلاك البرمجية الخبيثة لمصادر النظام مثل الذاكرة **RAM** ولمعرفة ذلك يجب أن نقوم بإنشاء نسخة احتياطية لسجلات النظام **backup for registry** قبل تشغيل البرمجية الخبيثة ومن ثم استخدام أداة معينة لتقوم بالمقارنة واكتشاف التغيرات التي تمت بسبب تشغيل هذه البرمجية.

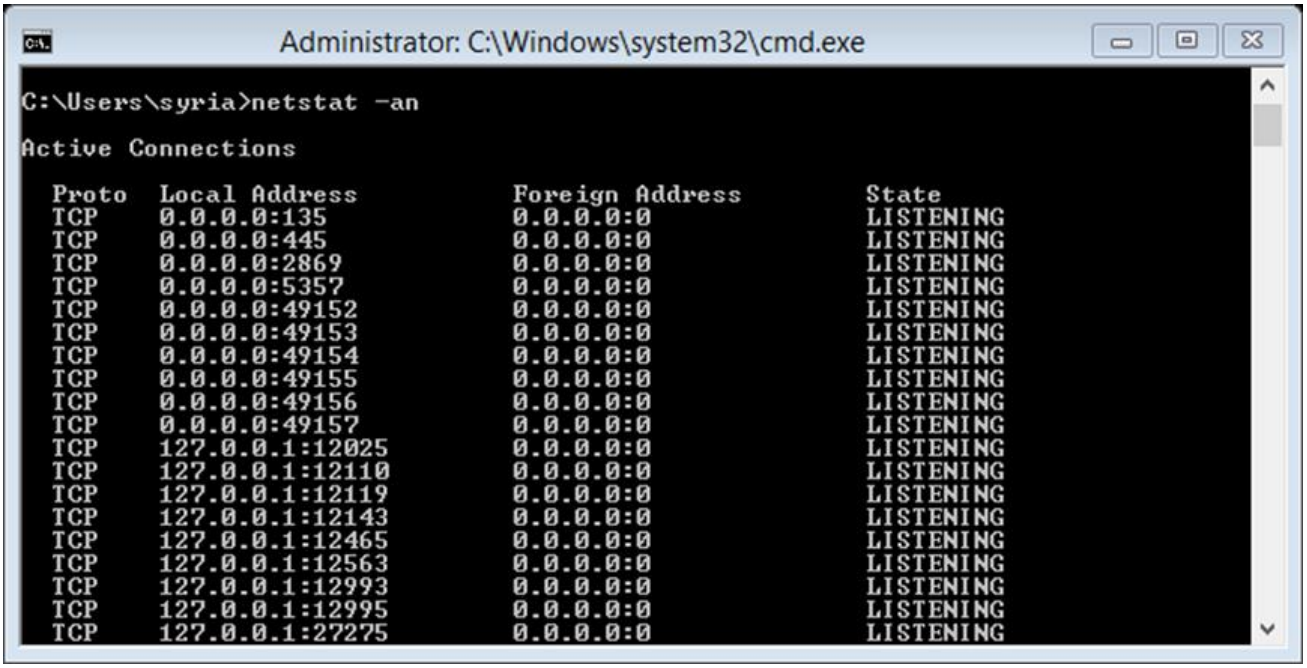
معرفة التغيرات التي تحدثها البرمجية الخبيثة في سجلات النظام **windows registry** مفيد جداً في عملية إزالة هذه البرمجية من النظام المصاب بها.

عملية تحليل البرمجية الخبيثة يجب أن تتم في بيئة تجريبية آمنة (تنفيذ البرمجية الخبيثة يجب أن يتم على **Virtual Machine**) معزولة بشكل كامل عن الشبكة.

أدوات تحليل البرمجيات الخبيثة:

يوجد العديد من الأدوات المفيدة في عملية تحليل البرمجيات الخبيثة.

يمكننا استخدام التعليمة **"netstat -an"** للبحث عن أي اتصالات مع عناوين **IP** غير معروفة

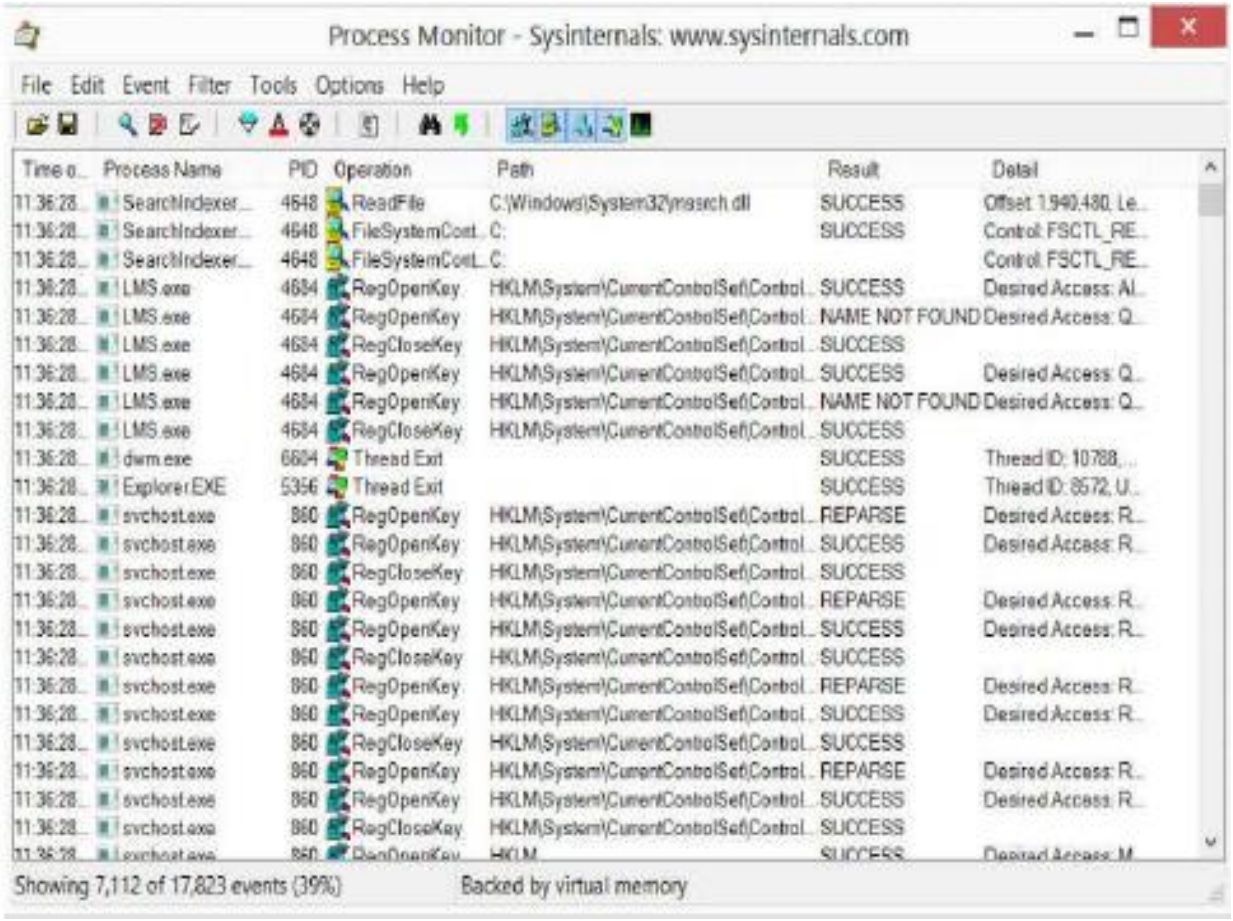


Windows Sysinternals هي مجموعة من الأدوات التي تعطينا صورة واضحة عن العمليات التي تتم على نظام **windows** بالوقت الحالي

بعض أدوات **Sysinternals** المستخدمة في تحليل البرمجيات الخبيثة هي:

Procmon:

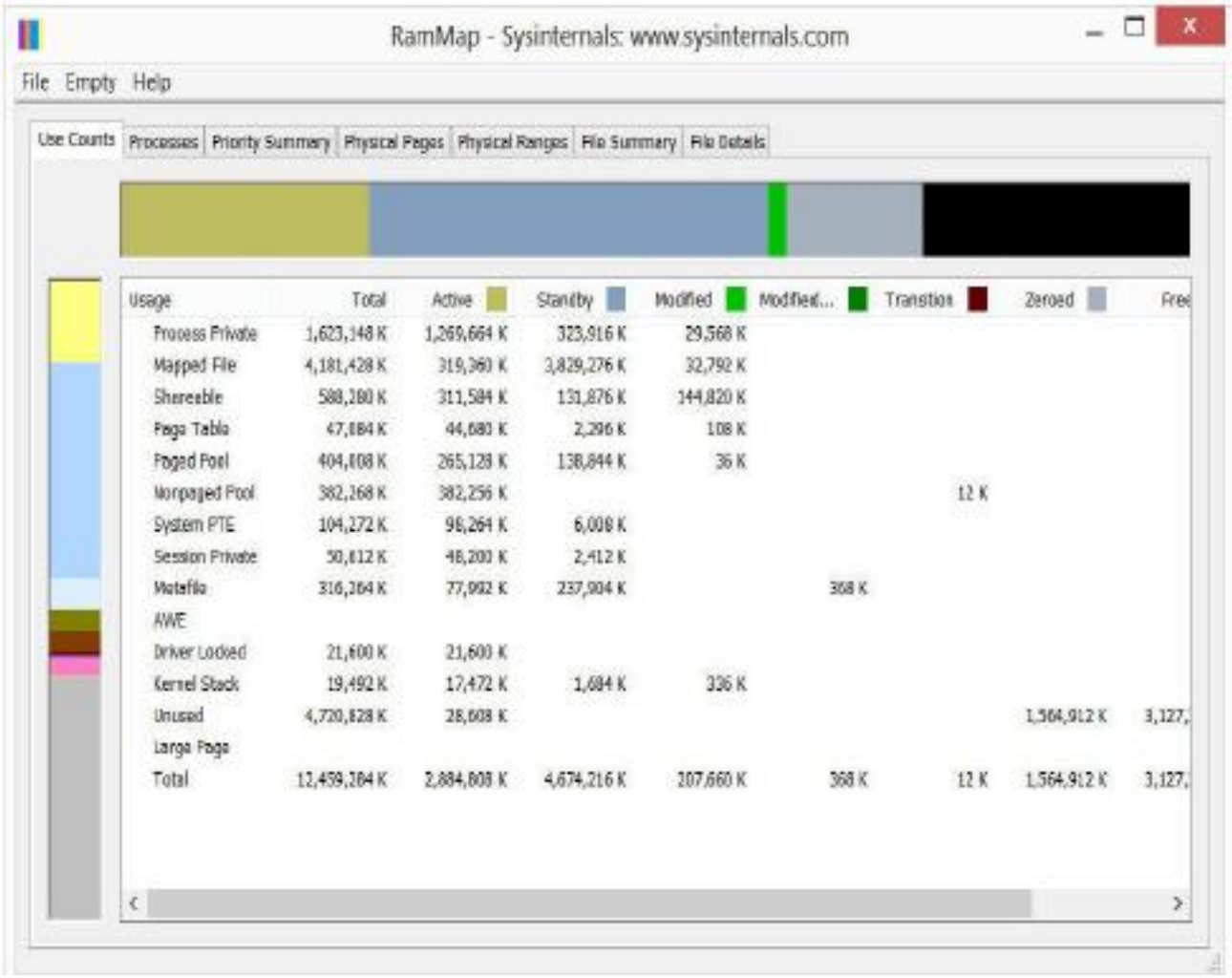
أداة ذات واجهة رسومية تقوم بعرض العمليات الحالية على النظام وتحدد رقم **ID** وزمن تنفيذ كل عملية وهذا يسمح لنا بمعرفة العمليات الخاصة بالبرمجية الخبيثة



:Rammap

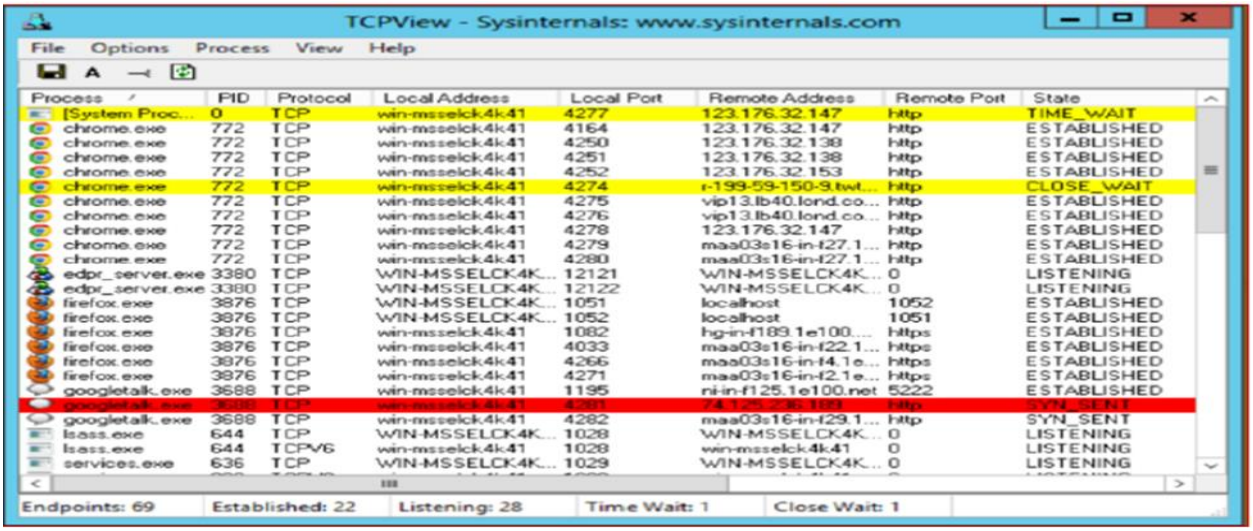
هذه الأداة تعرض معلومات مفصلة عن العمليات التي تحدث في الذاكرة وهذا يسمح لنا بمعرفة كمية الذاكرة المستخدمة من قبل كل برنامج.

البرمجيات الخبيثة غالباً ما تستهلك كمية كبيرة من الذاكرة أكثر من البرامج العادية.



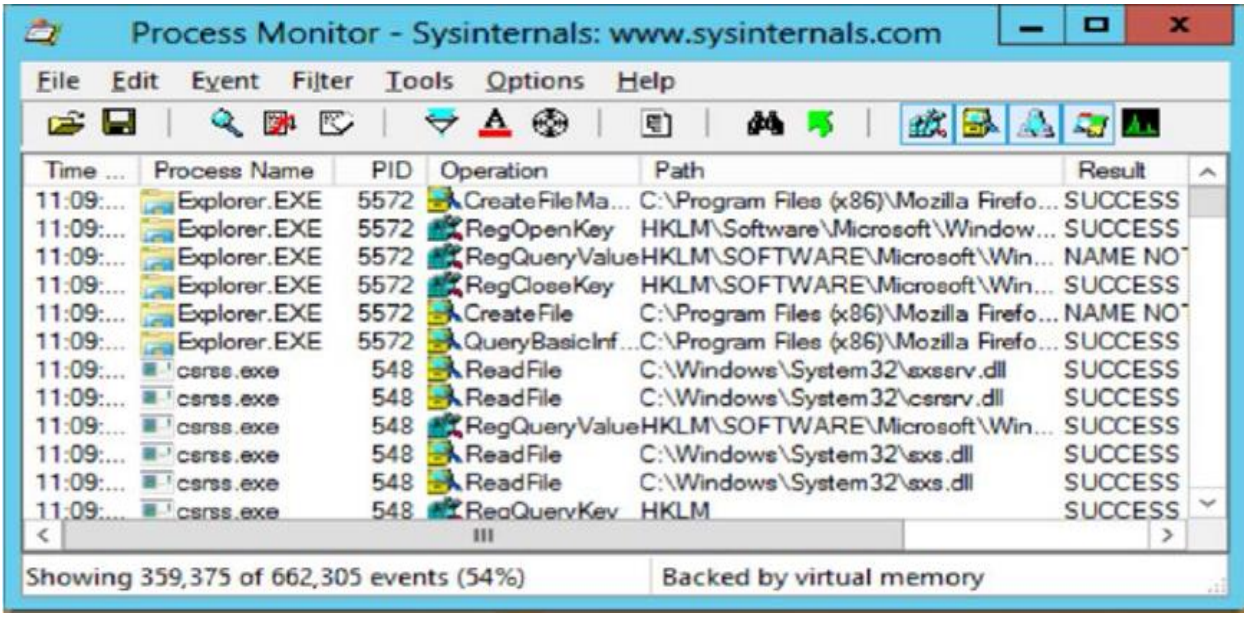
:TCPView

يتيح لنا رؤية جميع اتصالات بروتوكولات **TCP and UDP** ويعطي تقرير عن حالة الاتصال واسم العملية المرتبطة بها مع إمكانية إنهاء اتصال أي عملية نشك في طبيعة عملها.



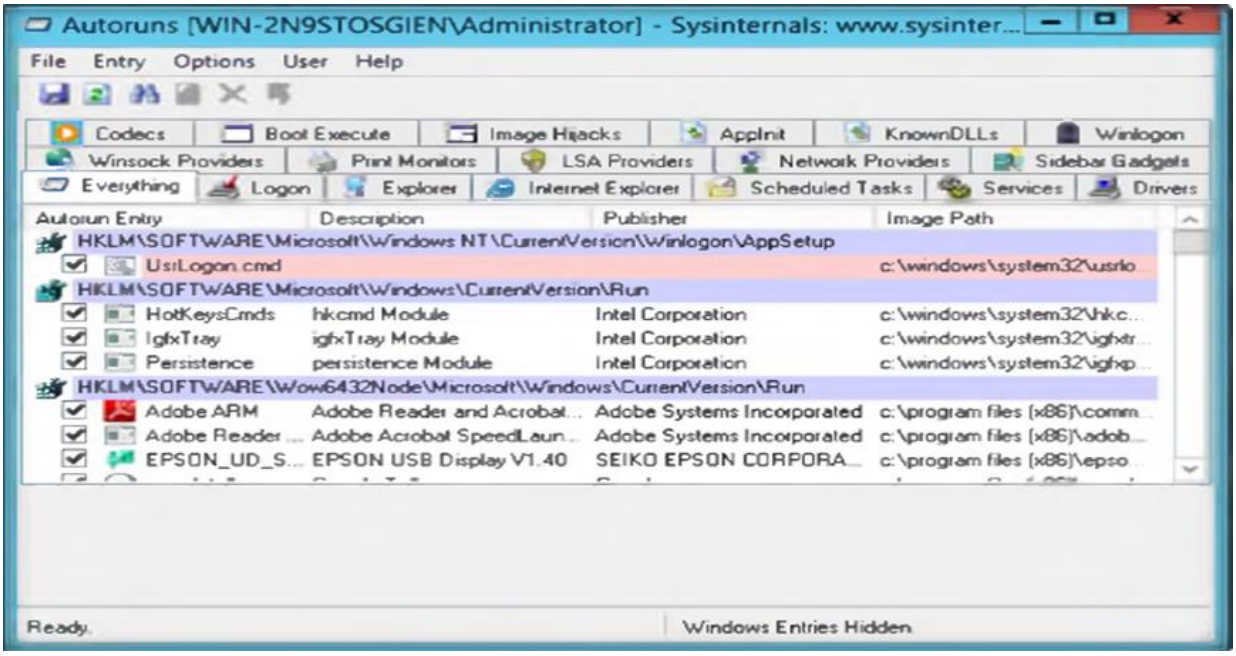
:Process Monitor

تظهر العمليات التي تعمل في الوقت الحالي وتفيد في كشف وتحليل سلوك البرمجيات الخبيثة وبرمجيات التجسس.



:AutoRun

مراقبة البرامج التي تبدأ العمل تلقائياً عند بدء تشغيل النظام



سجلات النظام

Windows Registry

محتوى هذا الفصل:

- سجلات النظام **Registry**
- الملفات والمواقع حديثة الزيارة.
- البرامج المُلغى تثبيتها.
- بطاقات الشبكة.
- الشبكات اللاسلكية وكلمات السر.

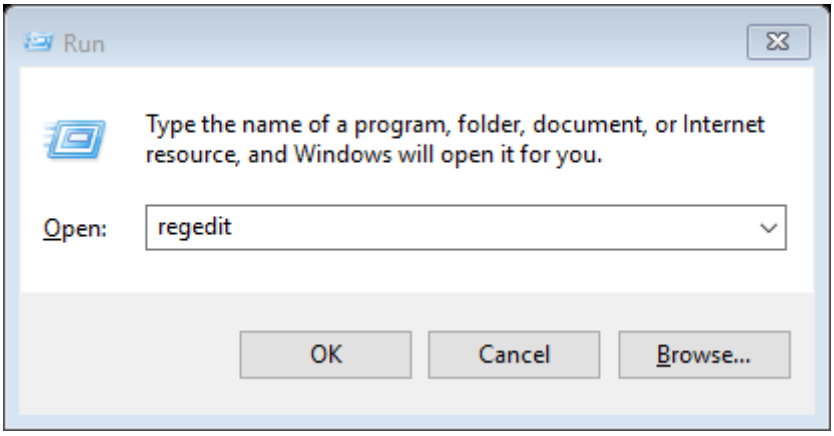
مقدمة:

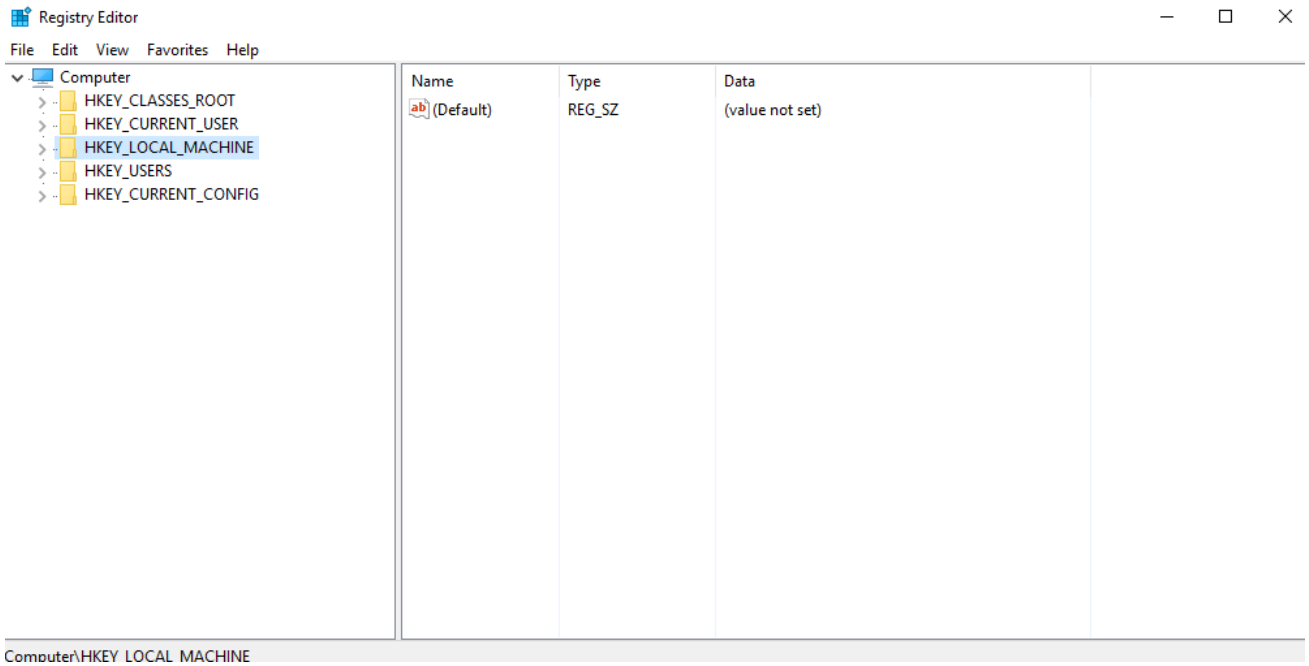
سجلات النظام **Registry** مسؤولة عن كل شيء في نظام **windows** وهي تحوي على كل الإعدادات والملفات التي تم فتحها ومعلومات الشبكة والبرامج وأمور أخرى.

وهي مبنية بشكل هرمي ومكونة من خمس أفرع أساسية و تحوي على معلومات مهمة جداً في عملية التحليل الجنائي الرقمي.

شركة Microsoft عرفت سجلات النظام كالتالي: قاعدة بيانات مركزية تستخدم من قبل أنظمة التشغيل الخاصة بشركة **Microsoft** ويتم فيها تخزين كل المعلومات الضرورية لإعدادات النظام والمستخدمين والبرامج والأجهزة وهي تحوي على معلومات خاصة بكل مستخدم والبرامج التي قام بتنصيبها على النظام والملفات والمستندات التي قام بفتحها والأجهزة المتصلة والمنافذ **ports** المستخدمة في اتصالات الشبكة.

يمكننا الوصول إلى سجلات النظام من خلال كتابة **regedit** في حقل التشغيل كما في الشكل التالي:

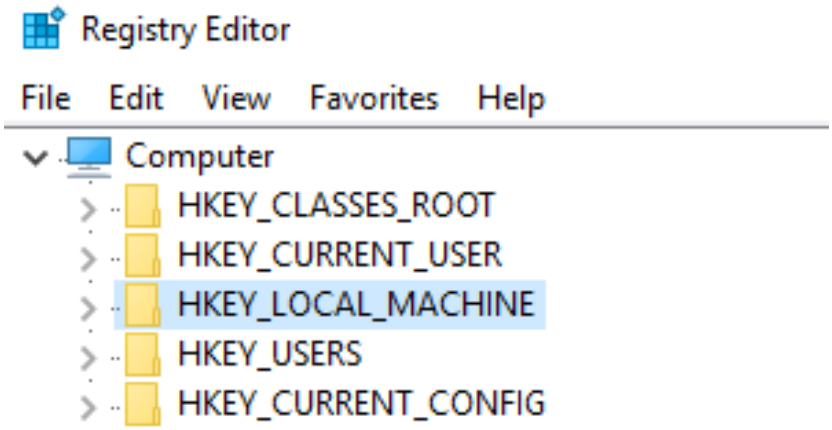




وهي مرتبة وفق خمس قطاعات:

- **HKEY_CLASSES_ROOT (HKCR)**: ويتم فيها تخزين معلومات عن قواعد **drag and drop** (سحب وتحريك الملفات) وعن اختصارات البرامج وعن الواجهة الخاصة بالمستخدم وأمور أخرى.
- **HKEY_CURRENT_USER (HKCU):** تحوي على معلومات مهمة جداً في التحقيق الجنائي الرقمي متضمنة معلومات عن المستخدمين وإعدادات سطح المكتب والملفات والمجلدات.
- **HKEY_LOCAL_MACHINE (HKLM)**: تحوي أيضاً على معلومات مهمة في التحقيق الجنائي الرقمي متضمنة معلومات عن كامل الجهاز بغض النظر عن المستخدمين.
- **HKEY_USERS (HKU):** وتحوي أيضاً على معلومات مهمة في التحليل الجنائي الرقمي متضمنة معلومات عن المستخدمين والإعدادات الخاصة بكل مستخدم.

- **HKEY_CURRENT_CONFIG (HCU):** تحوي على إعدادات النظام الحالية وهي مفيدة أيضاً في التحليل الجنائي الرقمي.

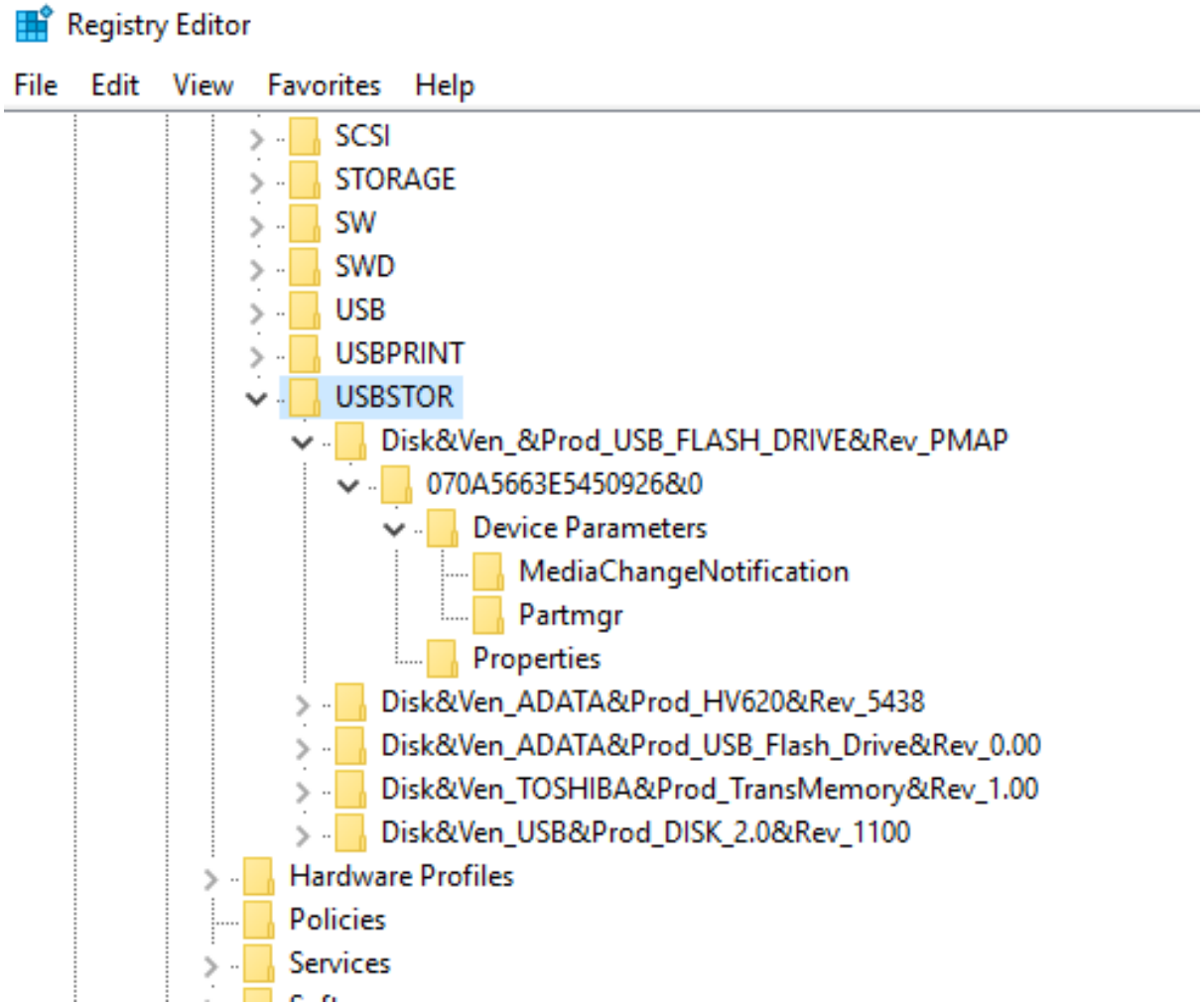


كل مفاتيح سجلات النظام **registry keys** تحوي على قيم مرتبطة بحالتها السابقة وهذه القيم تشير إلى أخر تغيير لقيم سجلات النظام.

معلومات عن منافذ USB:

عند القيام بعملية تحليل جنائي رقمي لسجلات النظام في نظام **windows** من المهم أن نحدد أجهزة **USB** التي تم وصلها بالجهاز وذلك من خلال المفتاح التالي:

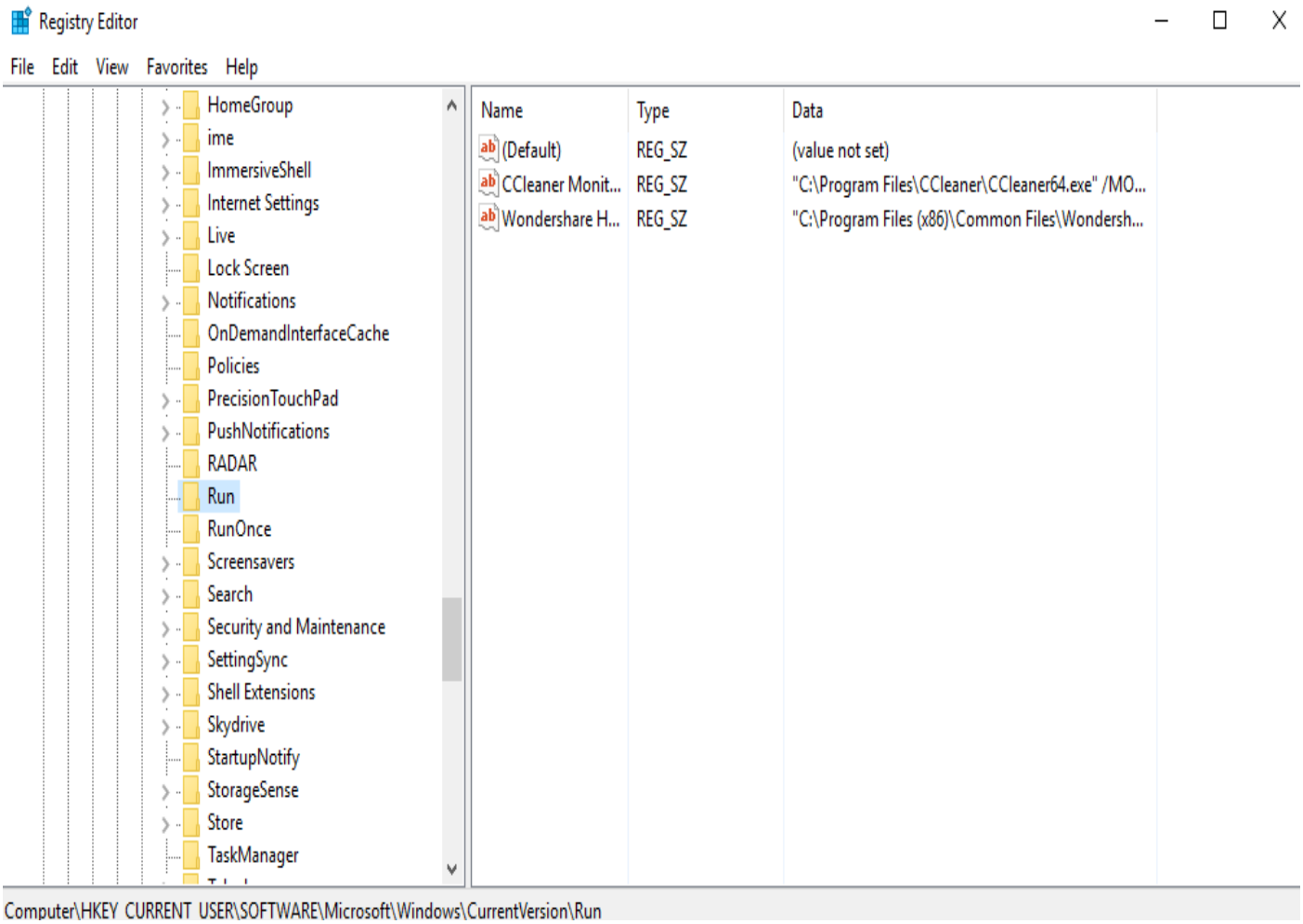
HKEY_LOCAL_MACHINE\System\ControlSet\Enum\UBSTOR



Autostart Location:

هذا المفتاح يستخدم عادةً من قبل البرمجيات الخبيثة **malware** من أجل تثبيت عملية الاستغلال على الجهاز الهدف وهو يحوي على البرامج المُعدة لتبدأ العمل بشكل اتوماتيكي عن إقلاع النظام

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

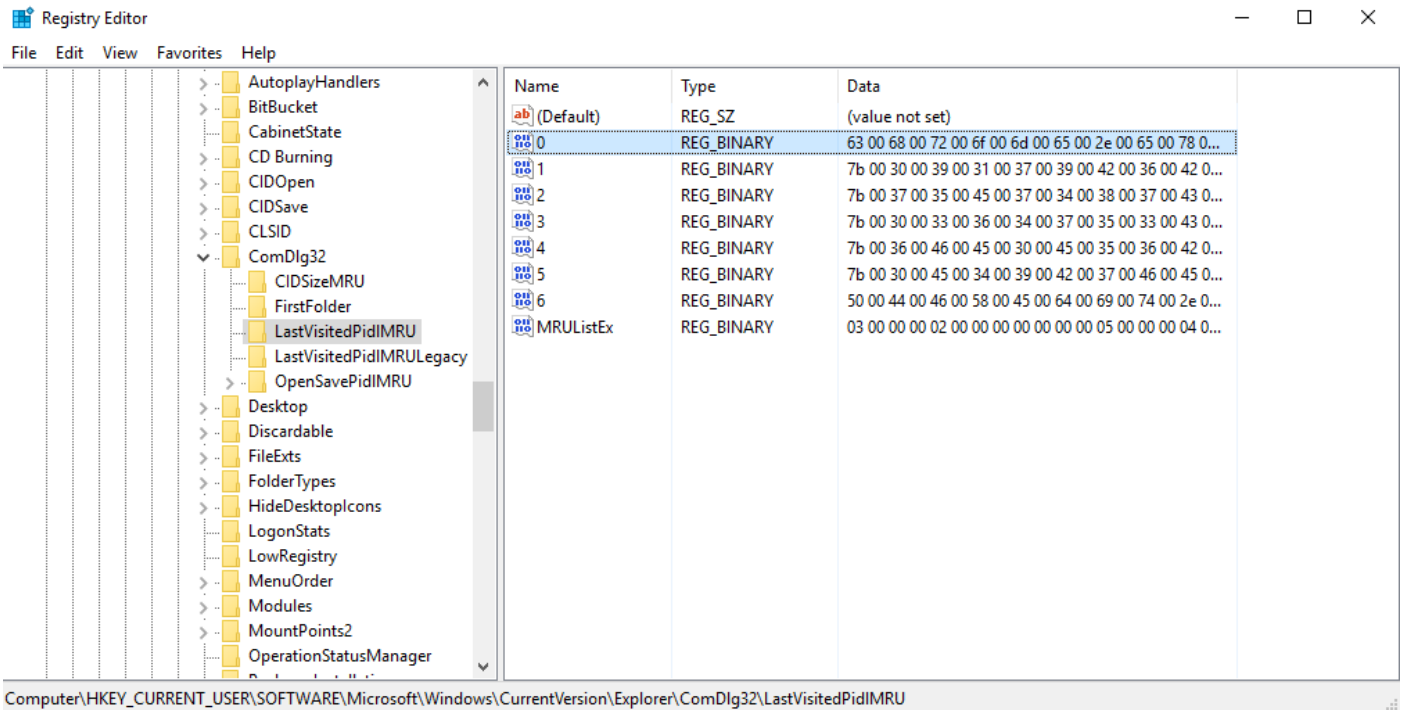


من خلال فحص قيمة هذا المفتاح يمكن أن نحدد البرمجيات الخبيثة التي تعمل بشكل تلقائي عند إقلاع النظام.

الملفات والمواقع حديثة الزيارة:

المفتاح التالي يعرض المواقع التي تم زيارتها مؤخراً

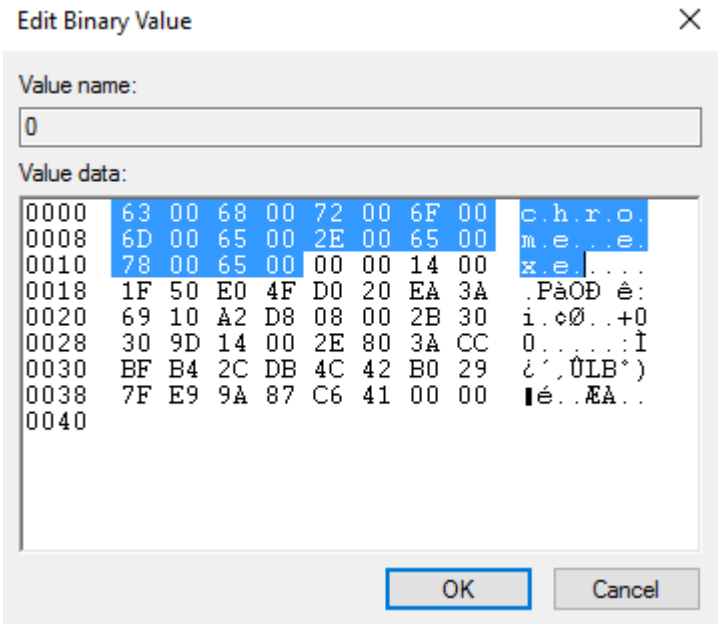
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU



البيانات يتم عرضها بشكل ستة عشري ولكن يمكننا رؤية ترجمة هذا النص باستخدام أدوات معينة مثل:

- **Raymondcc RecDeHexer**
- **OTConvertIt**
- **RegHexSee**

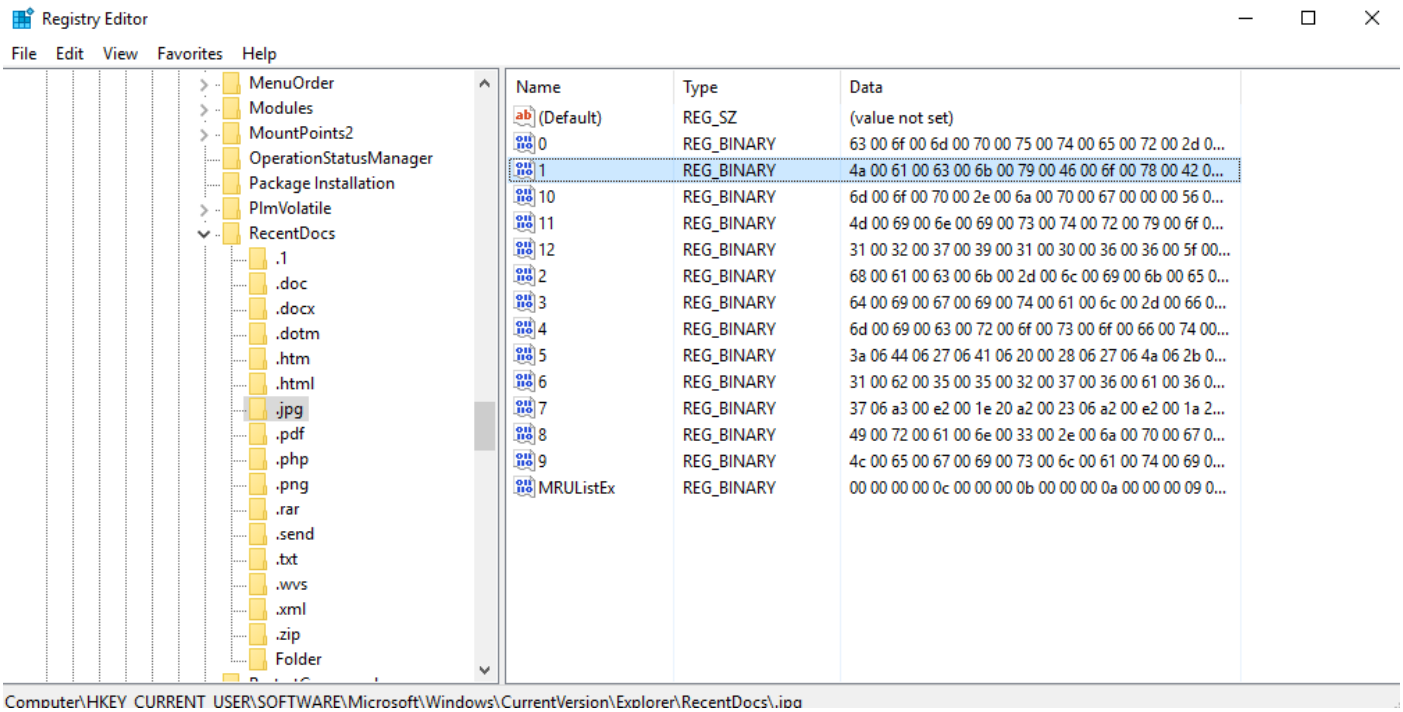
أو من خلال النقر المزدوج على الملف المطلوب وسوف تظهر النافذة التالية والتي من خلالها يمكن قراءة اسم البرنامج (في هذا المثال **chrome.exe**)

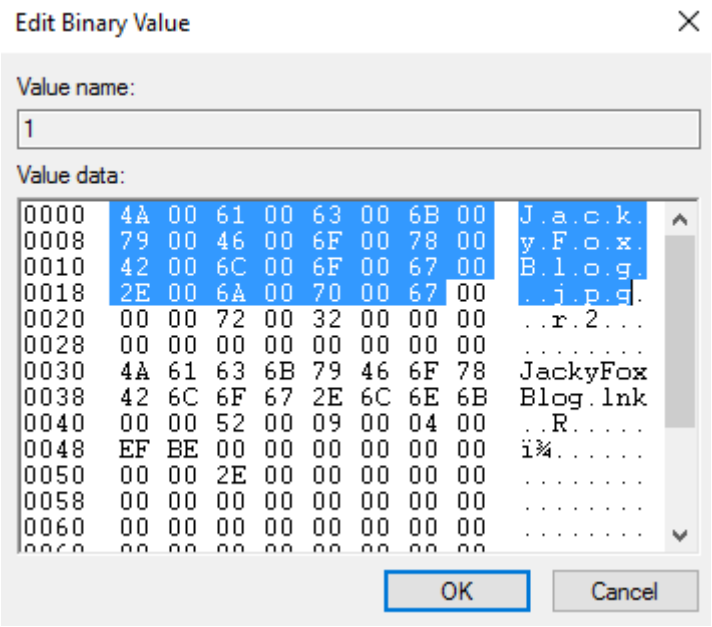


الملفات حديثة الزيارة يمكن إيجادها في المفتاح التالي:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.

ومن خلال هذا المفتاح يمكننا تحديد الملفات التي تم فتحها مؤخراً في هذا الجهاز





المثال السابق يظهر اسم لملف صورة **JackFoxBlog.jpg**

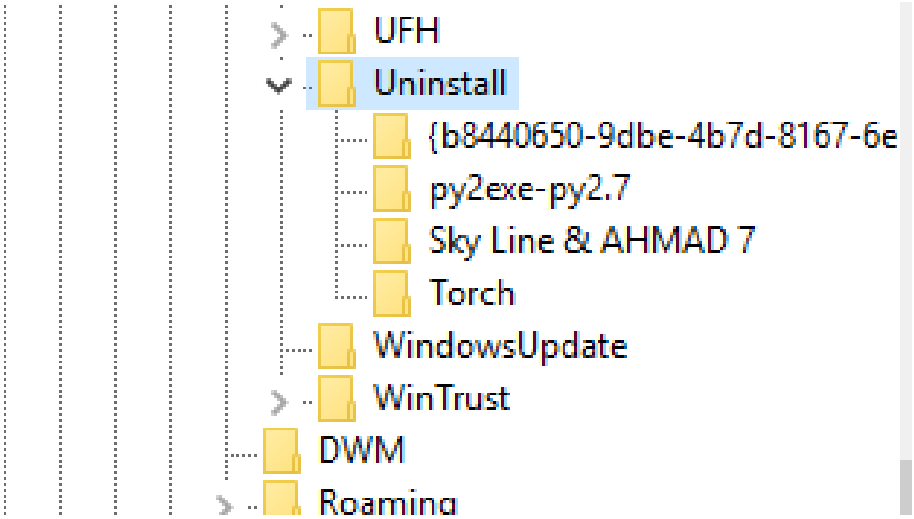
البرامج الملغى تثبيتها:

قيمة هذا المفتاح مهمة جداً في عملية التحليل الجنائي الرقمي، المجرم يمكن أن يقوم بتنصيب برمجية معينة على الجهاز لأغراض معينة (خلق **backdoor** أو استعادة كلمات السر المحفوظة) ومن ثم يقوم بإلغاء تنصيب هذا البرنامج.

كما يمكن أن يقوم المجرم بتنصيب برنامج لإخفاء البيانات (ستيغنوغرافي) ومن ثم يقوم بإلغاء تنصيب هذا البرنامج.

المفتاح التالي يعرض البرامج التي تم إلغاء تنصيبها

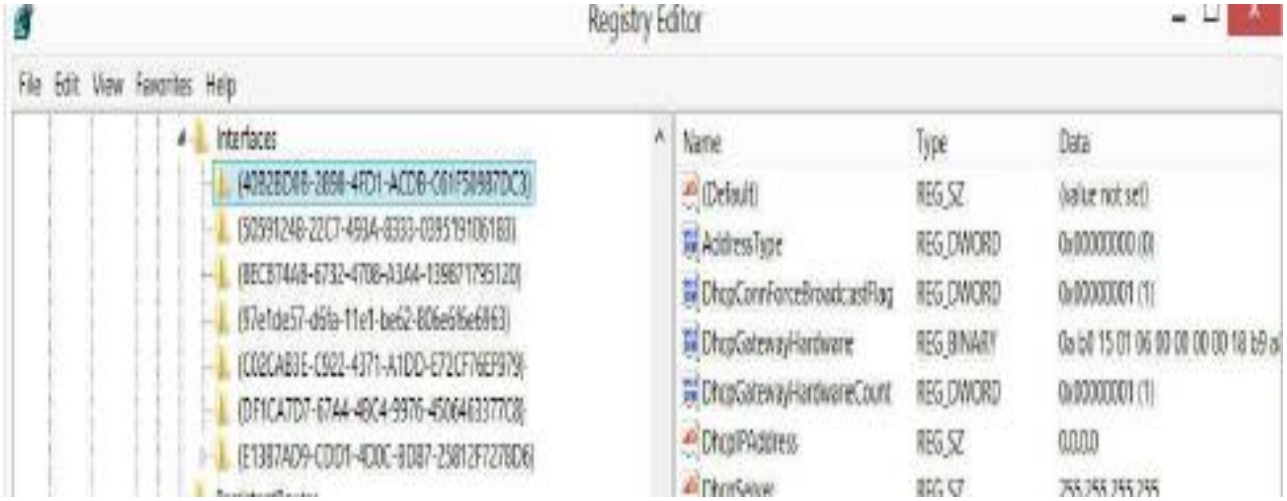
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall



بطاقات الشبكة:

المفتاح التالي يحوي على إعدادات بطاقات الشبكة

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID.

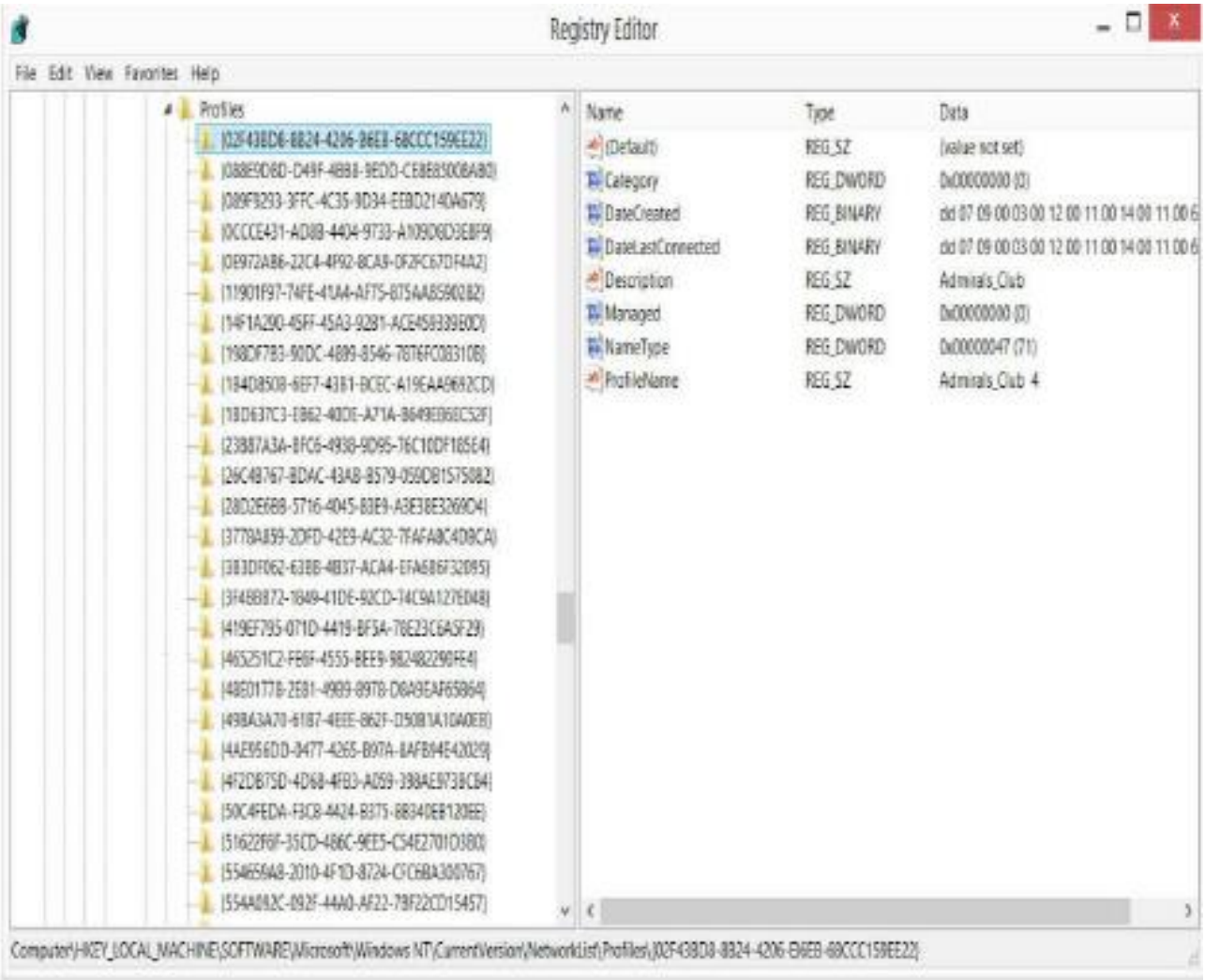


الشبكات اللاسلكية:

عند الاتصال بشبكة لاسلكية لأول مرة نقوم بإدخال كلمة السر الخاصة بالشبكة ولكن في المرات القادمة يمكننا الاتصال بدون إعادة كتابة كلمة السر مرة ثانية هذا يعني أن كلمة السر يتم حفظها في الجهاز في مكان معين وهذا المكان هو سجلات النظام.

المفتاح التالي يعرض معلومات عن الشبكات اللاسلكية التي تم الاتصال بها وكلمة السر الخاصة بكل شبكة.

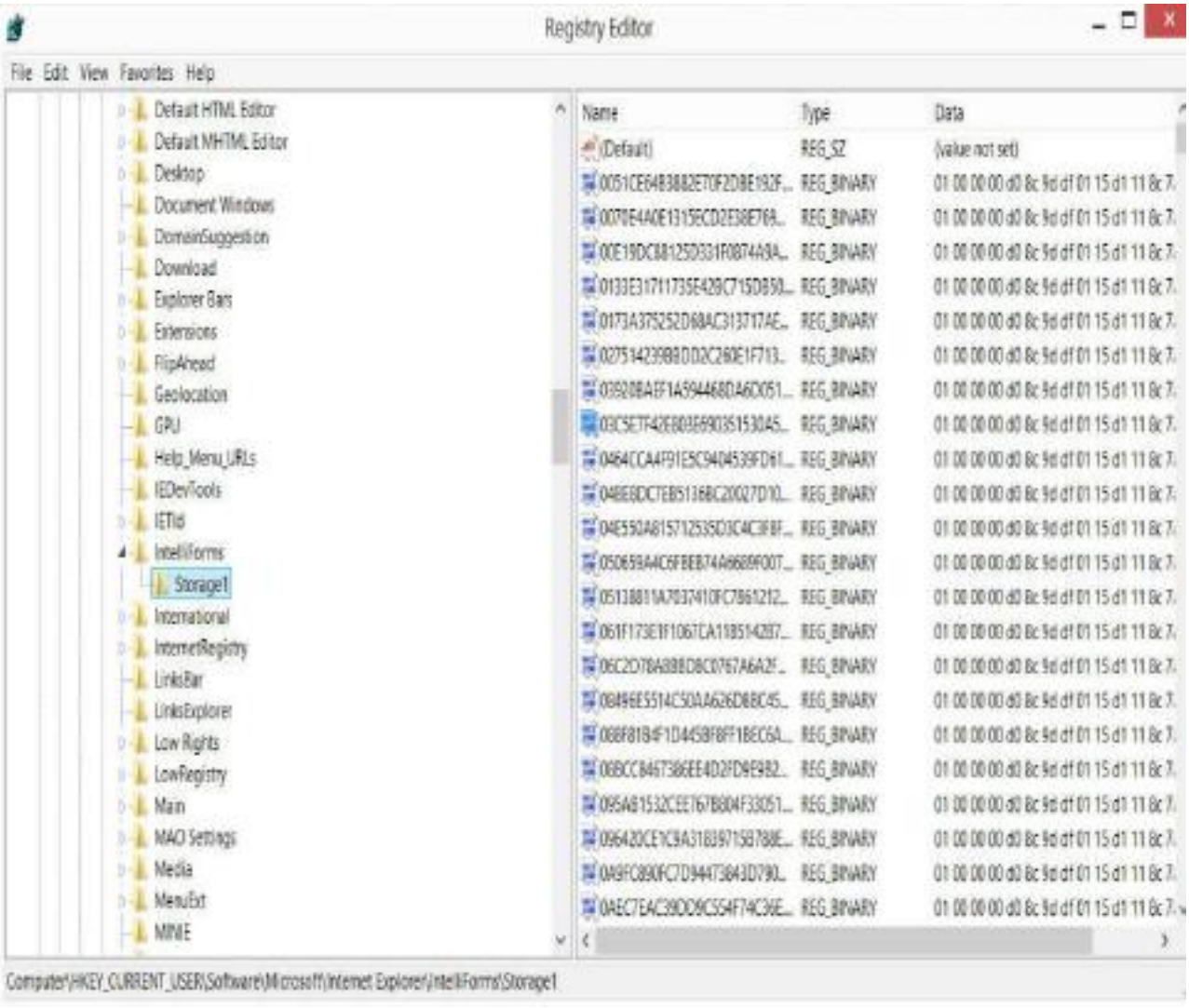
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\key.



كلمات السر المحفوظة:

إذا طلب المستخدم من المتصفح **Internet Explorer** القيام بتذكر كلمات السر لمواقع معينة فسوف يتم حفظ كلمات السر في سجلات النظام ضمن المفتاح التالي:

HKCU\Software\Microsoft\InternetExplorer\IntelliForms\SPW



كلمات السر تكون مشفرة أثناء عمل نظام التشغيل ولكن بعض الأدوات يمكنها القيام بعملية فك التشفير مثل أداة **Protected Storage PassView by NirSot** أو أدوات **Helix's incident response tools**

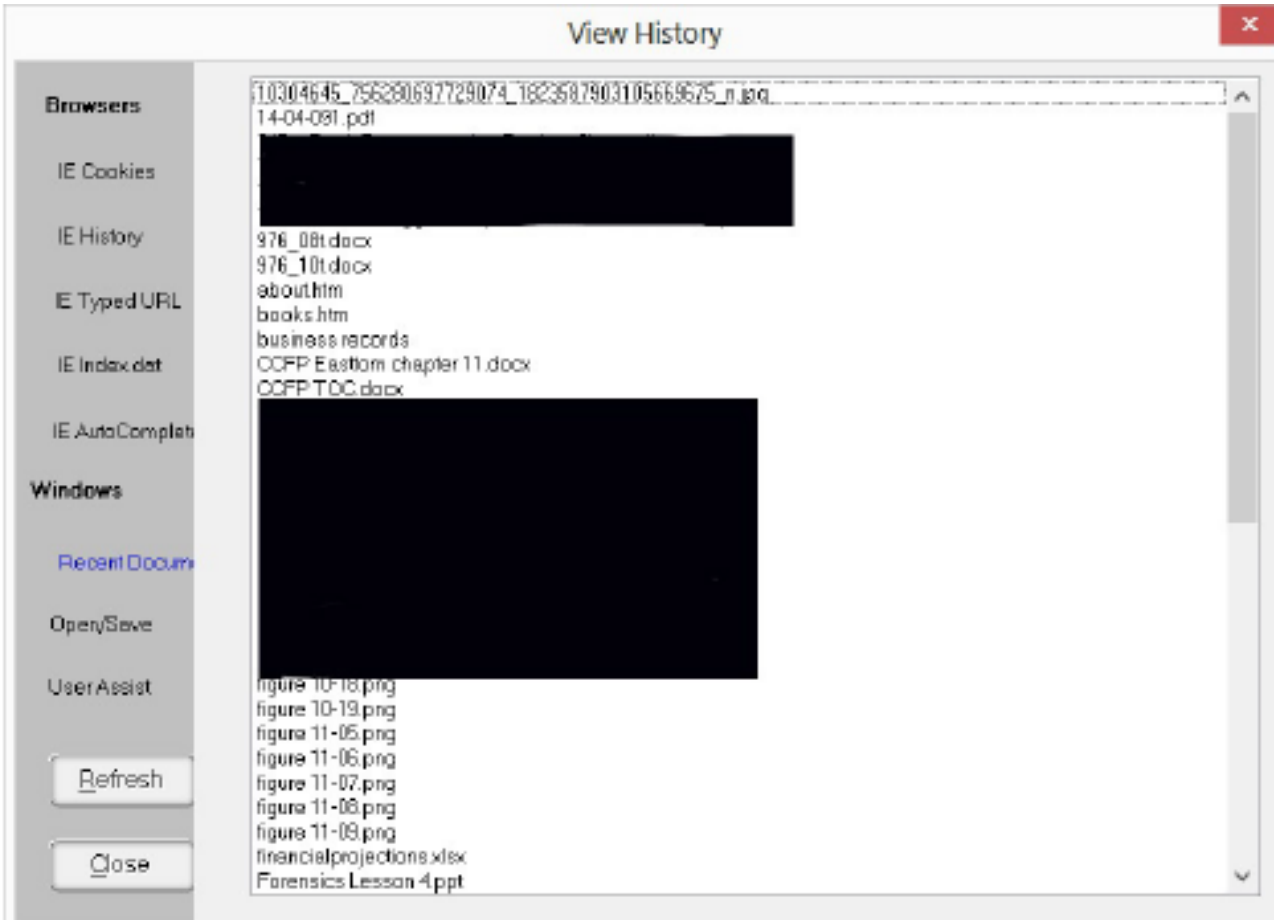
:Index.dat

هذا الملف مهم جداً في عملية التحليل الجنائي الرقمي فهو يحوي على كل عمل قام به المستخدم باستخدام متصفح الملفات أو متصفح الانترنت ويحوي على مُعرفات الجلسة **cookies** وصفحات الانترنت التي تم زيارتها وكل ملف تم فتحه.

يوجد العديد من الأدوات التي تسمح لنا برؤية محتوى هذا الملف ومنها:

- http://www.eusing.com/Window_Washer/Index_dat.htm
- http://www.acesoft.net/index.dat%20viewer/index.dat_viewer.htm
- http://download.cnet.com/Index-dat-Analyzer/3000-2144_4-10564321.html

المثال التالي يظهر استخدام أداة **Windows Washer**



برامج التحليل الجنائي الرقمي الغير مجانية يمكن أن تقوم بتحليل هذا الملف بشكل أكبر وتعرض معلومات بشكل أكثر.

التحليل الجنائي الرقمي علم واسع وهو في حالة تطور مستمر ولا يمكن الإحاطة بكل تفاصيله بكتاب واحد علماً بأن هذا الكتاب يحتوي على أساسيات التحليل الجنائي الرقمي وهو الجزء الأول من سلسلة كتب سيتم إصدارها مستقبلاً وذلك بهدف إغناء المحتوى العربي بهذا العلم المتقدم.