أكاديمية التعلم
Academy Of Learning

مقدمة في الأدلة الجنائية الرقمية

الفهرس

الفصل الأول

العلوم الجنائية المتعلقة بالحاسب الآلي

الفصل الثاني

أساسيات التحليل الرقمي

- الهدف من التحليل الجنائي الرقمي
- خطوات التحليل الجنائي الرقمي
  - الوصول للموقع
  - الحصول على الأدلة الرقمية
  - تحديد مكان الأدلة الرقمية
  - حماية الأدلة الرقمية
  - نقل الأدلة الرقمية
  - تخزين الأدلة الرقمية
  - إجراء التحقيق
  - إعداد التقارير
  - الاستجابة و تجهيز الأدوات

الفصل الثالث

عملية الفحص و الحصول على الأدلة الجنائية الرقمية

- الوصول للموقع
- أماكن وجود الدليل الرقمي
- التحليل الجنائي الرقمي في الحاسب
- استخراج المعلومات الذاتية لملف الويندوز Metadata
- أدوات و تقنيات الجرائم الرقمية
- النموذج المرجعي
- تحليل السجل في ويندوز (عملي)
- تحديد حادثة التحليل المباشر في النوافذ(عملي)
- فحص القرص الصلب و استعادة الملفات المحذوفة في ويندوز (عملي)
- الحصول على البيانات في النوافذ (عملي)
- كيف يتم المحافظة على الدليل في الجرائم الرقمية

- مشاريع المعمل (عملي)

الفصل الرابع
المحكمة الرقمية

- مفهوم المحكمة الرقمية و القاضي الرقمي
- أدوات الجريمة في المحكمة الرقمية
- المواد الرقمية
- التوقيع الالكتروني بالمحكمة
- الإثبات في الجرائم الرقمية
- تحديد هوية الشخص رقميا (عملي)
- مستقبل المحكمة الرقمية

الفصل الأول

العلوم الجنائية المتعلقة بالحاسب الآلي

تعريف العلوم الجنائية المتعلقة بالحاسب الآلي

هي فرع من فروع العلوم الجنائية الرقمية، تتعلق العلوم الجنائية المتعلقة بالحاسب الآلي و بالأدلة المستخلصة من الحاسب الآلي ووسائط التخزين الرقمية، الهدف هو فحص الوسائل الرقمية للتحديد والتعريف identifying والحفاظ preserving و استرجاع واسترداد recovering وتحليل analyzing وإظهار حقائق وآراء حول البيانات الرقمية .digital information

مفهوم التحقيق الجنائي الرقمي

هو دراسة الحقائق الجنائية الرقمية للتحقق من وجود جريمة الكترونية وإثبات ذنب المجرم، التحقيق الجنائي الرقمي يمكن أن يشتمل البحث و المقابلة والاستجواب وجمع الأدلة وحفظها وعدة أساليب مختلفة للتحقيق.

وهو عمليَّة التحقيق في الجرائم المرتكبة بِاستخدام أي نوع من أجهزة الحوسبة والهدف من ذلك هو تفسير وإثبات أصل الأدّلة الرقميَّة وأهميتها وتحليل الأدلة وصلاحيتها وموثوقيتها وصلتها بالقضية وإبلاغ بالأدّلة ذات الصلة بالقضية .

فقد أصبح التحقيق الجنائي الرقمي الآن مطلب أساسي لأي جهة لتدريب موظفيها المختصين لأساليب التحقيق الجنائي خاصة مع إرتفاع الجرائم الإلكترونية. فهو يستخدم في متابعة الحالات مثل سرقة الملكية الفكرية و التجسس الصناعي و التجاري و منازعات العمل و تحقيقات الاحتيال و التزوير.

أهداف التحقيق الجنائي الرقمي

هناك العديد من الأهداف من التحقيق الجنائي الرقمي وهي:

1- اِستعادة البيانات و المواد ذات الصلة وتقديمها كدليل.

2- معرفة دوافع الجريمة.

3- معرفة هويّة الجاني.

4- رسم مسرح الجريمة.

5- الحصول على البيانات لِاستخراج الأدّلة والتحقُّق منها.

6-التعرُّف على الأدّلة.

7- إنتاج تقرير جنائي حاسوبي.

8-حفظ الأدِّلة.

معمل و أدوات التحقيق الجنائي الرقمي

معمل التحليل الجنائي الرقمي هو المكان الذي يتم نقل الأدلة من مسرح الجريمة إليه ليتم عمل نسخ منها و تحليليها و حفظها أما الأدوات فهى عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد علي واجهة رسومية يستخدم في تحليل أجهزة الحاسب والهواتف الذكية و المعدات اللازمة لحفظ و تأمين الأدلة.

أولا" :معمل التحقيق الجنائي :

أحيانا يتطلب نوع من التحقيقات نقل الأدلة إلى معمل جنائي رقمي للمساعدة على إنتاج عمل يتطلب جودة عالية و استخدام أحدث التقنيات و يختلف المعمل الجنائي الرقمي الحكومي عن المعمل الجنائي الرقمي الخاص الذي يختلف تجهيزه حسب الميزانية المتاحة .

التجهيزات :

يجب تجهيزه بكامل المعدات اللازمة للقيام بالعمل المطلوب :

1-الحماية المادية

معدات لإغلاق الباب تلقائيا بإستخدام بطاقات يتم من خلالها تسجيل كامل المعلومات

أو ببصمة اليد أو بصمة العين للفتح ، يكون لها مدخل واحد للمعمل أفضل حتى يمكن التركيز عايه بشكل كامل و مزود المبنى بالسياج أو الجدران المحمية المزودة بالكاميرات و أنظمة الإنذار.

تكون محمية من الغبار أو الرطوبة الزائدة أو الحرارة للحفاظ على البيئة التي تتواجد فيها الأدلة

2- البرامج

يجب أن يحتوي الجهاز المخصص لتحليل البيانات على برامج تحليل البيانات فقط و لابد أن تكون البرامج أصلية مأخوذة من المصدر مباشرتا حتى تعتمد من المحكمة .

كما يجب أن يتواجد على أجهزة الحاسب أنواع مختلفة من أنظمة التشغيل ويندوز و لينكس و العديد من البرامج التي تفتح أنواع كثيرة من الملفات بصيغ متعددة و إصدارات مختلفة و يتواجد برامج التحليل الجنائي الرقمي بمختلف أنواعها

3- المعدات

- طقم كامل يمكن شراؤه يحتوي على العديد من الأدوات و الأسلاكو الموصلات

- أجهزة مختلفة لكل غرض كجهاز مخصص فقط للتحاليل

- جهاز مخصص لحيازة الأدلة

-أجهزة منع الكتابة

- أقراص مختلفة

ملاحظات :

- يتم توثيق الإعدادات الخاصة بكل جهاز
- عند البدء بأي عمل لابد من إلغاء أي بيانات قد تُركت على هذه الأجهزة

المعمل الجنائي الرقمي المتنقل

يكون عبارة عن حقيبة بها معدات لهذا الغرض و تراعي المعايير .

جميع الإجراءات والخطوات المتبعة في معامل الأدلة الرقمية هدفها الرئيسي هو المحافظة على عجلة ملكية الدليل أو ما يسمى بالـ Chain of Custody والتي من خلالها يتم توثيق كل إجراء تم القيام به للحصول على الدليل.

-لحماية الأدلة

يتم وضع الأدلة في صندوق محمي و مؤمن ، و التأكد من إغلاق الصندوق بطريقة تجعل الأدلة محمية و يصعب التغيير أو التعديل عليها.

-يتم استخدام أدوات التحقيق الجنائي الرقمي لجمع الأدلة وحفظها وتحليلها، ويتم استنساخ الأدلة الرقمية أكثر من مرة لتبدأ الخطوة الأخيرة وهي تحليل الأدلة لاستخراج تسلسل الجريمة الإلكترونية للوصول الي مرتكبها ومقاضاته.

وقد يتم تقسيم الأدوات التي يتم استخدامها في التحقيق الجنائي إلى أقسام عديدة منها التي يتم استخدامها في:

-تحليل الشبكات

-تحليل قواعد البيانات

-تحليل الملفات

-تحليل الأقراص الصلبة

-تحليل الهواتف المحمولة

- تحليل البريد الاكتروني

وغيرها الكثير حيث يتم تطوير تلك الأدوات باستمرار وتوجد بعض الأدوات مثل :

Autopsy -1

هو عبارة عن برنامج للتحقيق الجنائي الرقمي مفتوح المصدر يعتمد علي واجهة رسومية يستخدم في تحليل أجهزة الكمبيوتر والهواتف الذكية ويوجد به العديد من المميزات منها:

-استخراج اي أنشطة تمت علي متصفحات الويب.

-تحليل البريد الإلكتروني.

-تحليل وسائط الميديا واستخراج المواقع الجغرافية ونوع الكاميرا.

-تحليل وفحص أنواع الملفات.

-استخراج البيانات من هواتف الأندرويد :

سجل المكالمات – جهات الاتصال – رسائل الـSMS.

- استعادة الملفات من بطاقات الذاكرة.Memory Card

Oxygen Forensic Detective-2

هي عبارة عن أداة برمجية عالية ومتعددة الوظائف يتم استخدامها في تحقيقات التحليل الجنائي الرقمي ، مصممة خصيصاً لاستخراج الأدلة والبيانات من مصادر رقمية متعددة وفك تشفيرها وتحليلها ويمكن استخدامها في:

- جمع بيانات المستخدم من علي أجهزة الكمبيوتر سواء كانت تعمل بنظام Window أو Linuxأو MacOS مع فك تشفيرها وفحصها.

-البحث عن كلمات المرور وفك تشفيرها سواء لحسابات مستخدمين أو نقاط اتصال الـ Wifi التي تم استخدامها.

-فك تشفير بيانات الاعتماد من iOS keychain و.Android KeyStore

-استخراج البيانات من الهواتف منها تفاصيل الجهاز من نوعه وطرازه وبيانات شريحة الهاتف بالاضافة إلى سجلات الهاتف والرسالة والارقام المسجلة مع تجاوز قفل الشاشة.

-تحليل ملفات الـ CDR المستلمة من مزودي خدمة الهاتف.

-اخد نسخ احتياطية مع امكانية استعادة البيانات المحذوفة.

-استخراج البيانات من الأجهزة التي تدعم انترنت الأشياء والساعات الذكية.

- استخراج البيانات من الطائرات بدون طيار من تاريخ بداية الرحلة وخط السير.

Kit Forensic-3

أداة قوية قادرة علي استعادة كلمات المرور لأكثر من 340 نوع من أنواع الملفات يتضمن ذلك MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notesكما انها قادرة أيضا علي التعامل مع محافظ العملات المشفرة و Apple iTunes Backup و Mac OS X Keychain و BitLocker والمزيد.

الأداة قوية للتحقيق في الجرائم الإلكترونية الخطيرة حيت يتم استخدامها من قبل الـ FPI و الـ Europol وتأتي بعدة إصدارات ، احدها مجاني للاستخدامات المحدودة.

Cellebrite UFED (Universal Forensics Extraction Device) -4

عندما يتم فحص هاتف محمول اثناء التحقيق الجنائي فإن كلمات المرور وطبقات التشفير والملفات المحذوفة تمثل تحدي للمحقق الجنائي في عملية جمع الأدلة يأتي برنامج UFED لمساعدة المحققين الجنائيين في كسر الحواجز للوصول للأدلة الرقمية ، فبإمكان البرنامج تجاوز كلمات المرور وكسر الحماية وفك الـ PIN Code واستخراج الملفات وبيانات بطاقة الـ SIM ، حيث يدعم البرنامج أكثر من 30 الف جهاز بأنظمة IOS و Andorid وغيرها ، ويأتي Cellebrite UFED بعدة منصات.

Xplico -5

وفي تحليل البريد الإلكتروني تأتي أداة Xplico مفتوحة المصدر التي تستخدم عدة لغات برمجية منها (C و Python و PHP و JS) فهي قادرة على تحليل حركة المرور في بروتوكولات POP و SMTP و IMAP واستخراج محتويات البريد الإلكتروني و تأتي البيانات المستخرجة بواسطة الأداة علي هيئة واجهة ويب تمتلك قاعدة البيانات الخاصة بها التي يمكن تحديدها من بين SQLite أو MySQL أو PostgresSQL كما يمكن استخدام الأداة لتحليل البيانات علي الشبكات السحابية.

FTK Imager -6

عبارة عن جموعة أدوات جنائية رقمية تم تطويرها بواسطةAccess Data والتي يمكن استخدامها للحصول على الأدلة ونسخها وتحليلها أيضاً يمكنه إنشاء نسخ من البيانات دون إجراء تغييرات على الدليل الأصلي

ExifTool-7

هو برنامج مجاني ومفتوح المصدر للتعامل مع بيانات الصور الرقمية يمكن استخدام ExifTool لقراءة وكتابة عناصر EXIF و IPTC و XMP وغيرها من العلامات والمعلومات المتعلقة بالصور

الرقمية وتستخدم هذه الأداة بشكل شائع في مجال تحليل بيانات الصور ومعرفة التفاصيل والخصائص المختلفة المتعلقة بالصور ومعرفة مكان وزمن التقاط الصور إن توفرت.

8- Magnet RAM captures

يسجل Magnet RAM صورة عن ذاكرة الكمبيوتر المشتبه به والمعد لعملية التحقيق الجنائي يسمح للمحققين باستعادة وتحليل العناصر القيمة الموجودة في الذاكرة.

9-X-Ways Forensics

إحدى الأدوات القوية للتحقيقات الرقمية وتتميز بواجهة مستخدم سهلة الاستخدام تتيح أداء مهام التحقيق بشكل فعال.

10-SIFT Workstation

هي توزيعة خاصة بالتحقيقات الجنائية الرقمية مبنية هذه التوزيعة علىUbuntu ، تعتبر واحدة من أفضل أدوات التحليل الجنائي الرقمي التي تتوفر لفحص الأدلة الجنائية والاستجابة للحوادث وتحتوي على العديد من البرامج والأدوات المناسبة من أجل سير عملية التحقيق بشكل صحيح.

11- Volatility Framework

تساعدك على اختبار حالة وقت تشغيل النظام بإستخدام البيانات الموجودة في ذاكرة الوصول العشوائي وأبرز البرامج التي تم تشغيلها وفي حال وجود برامج ضارة كانت تعمل بالخلفية فيمكن العثور عليها عن طريق هذه الاداة.

خطوات عملية التحقيق الجنائي الرقمي

حيث يبدأ التحقيق بتلقي بلاغات عن جريمة الكترونية فيبدأ الاستجابة للحادث بالذهاب لموقع الحادثة و معاينة مسرح الجريمة لإثبات وجود جريمة أم مجرد بلاغ كاذب وجمع أكبر عدد من الأدلة الرقمية من خلال البحث والفحص وحفظ الأدلة التي تم العثور عليها من خلال البحث وعزلها لتجنب تلفها و توثيقها ليتم استخدامها قانونيا .

عملية التحقيق الجنائي الرقمي تتكون من ست خطوات أساسية:

1- Preservation :

الأدلة محفوظة على نفس الحالة التي وجدت بها

2- Acquisition :

الحصول على تلك الأدلة

3- Analysis:

تحليل تلك الأدلة و معرفة نوع المعلومات التي تم الحصول عليها

4- Discovery :

عزل البيانات و اكتشاف ما يكون متعلق بالقضية

:Documentation -5

التوثيق

Presentation -6

العرض

تلقي الإخبارات والبلاغات والشكاوى

عند تلقي جهة التحقيق معلومات بالإبلاغ عن الجرائم الإلكترونية عليه فهم الجوانب التقنية التي يتطرق اليها المبلغ والاستيضاح عن كل الجوانب الفنية ذات العلاقة بالجريمة المبلغ عنها التي ربما يغفل المبلغ عن شرحها.

2- وضع خطة عمل التحقيق

يتم وضع خطة حسب نوع القضية و البحث عن كيفية جمع الأدلة الرقمية وكيفية نقلها والحفاظ عليها وثم كيفية تحليلها حيث يبدأ المحقق عمله عند جمع الاستدلالات المتعلقة بالجريمة الإلكترونية بوضع خطة عمل، على ضوء المعلومات المتوفرة وتحديد فريق العمل الفني اللازم بالمساعدة وذلك من خلال.

1- التخطيط للتحقيق:

وضع خطة عمل مناسبة لاتبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات للتصدي للجريمة.

2-إجراءات التحقيق

أساليب المواجهة والاستجواب مع عرض الحالة ودراستها.

3- تجميع المعلومات وتحليلها.

4- أساليب المعمل الجنائي.

دور المحقق

هو فقط جمع الأدلة و استخراج الحقائق و يجب أن يتحلى بالأخلاقيات المهنية و يعمل على تقديم الحقائق فقط و ليس إدانة أي شخص .

تشكيل فريق التحقيق

فريق الاستجابة للحادث يتكون هذا الفريق من متخصصين ذو مهارات عالية في مجال التحقيق الجنائي الرقمي .

العمل في التحقيق في الجرائم الإلكترونية أصعب من أن يتولاه شخص واحد بمفرده، حتى لو كانت المضبوطات هي مجرد جهاز حاسب واحد فيفضل تعاون أكثر من شخص في إنجاز مهمة التحقيق والعثور على الأدلة، ومن الأهمية أن يكون لدى فريق التحقيق جهاز حاسب أو محمول مثبت به بطاقة شبكة ليتمكنوا من أخذ نسخة احتياطية من محتويات الأجهزة التي يعثروا عليها في مسرح الجريمة.

تشكيل فريق من مجموعة متنوعة من المتخصصين في مهمة واحدة هو الأفضل ويندرج هذا الفريق تحت ثلاث مجموعات رئيسية هي:

1-مجموعة مهمتها تنفيذ القانون وتشمل:

أ- قائد الفريق:

الذي يشترط به خبرة طويلة في مجال التحقيق ولديه خبرة ومعرفة بطبيعة جرائم الحاسب والانترنت ويتولى السيطرة الكاملة على مسرح الجريمة ويوزع المهام على الفريق والإشراف بعملهم.

ب-محقق جنائي:

شخص أو أكثر بحسب ظروف الجريمة لديه خبرة بوسائل وأساليب التحقيق واجراءاته وملم بطبيعة جرائم الحاسب والانترنت.

ج -خبراء ضبط وتحريز الأدلة الإلكترونية.

د-خبراء التصوير والبصمات والرسم التخطيطي.

2-متخصصين في التدقيق والمراجعات الحسابية.

3- متخصصين في معالجة البيانات الكترونياً.

الوسائل المساعدة التي يستخدمها المحقق

للقيام بالتحقيق في جريمة ما فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني، ذلك ان هذه الجرائم لها طابعها الخاص المميز، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة بهدف الوصول إلى الجاني، وتوجد عدة وسائل تساعد على تلك اهمها:

أولاً: الوسائل المادية:

هي وسائل يمكن استخدامها إجراءات وأساليب التحقيق المختلفة للمساعدة في ضبط مرتكب الجريمة وتحديد شخصيته ويستخدم بها أدوات فنية يستعمل بها نظم معلومات وبيانات الكترونية تتناسب وطبيعة الجرائم المستحدثة واهمها:

1-عناوين MAC, IP والبريد الإلكتروني، وبرامج المحادثة:

عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر الشبكة المعلوماتية وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة وهو يوجد بكل جهاز مرتبط بالشبكة العالمية للمعلومات

وعند وجود أي مشكلة أو أي اعمال تخريبية فالعمل الأول هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال التخريبية، ويمكن لمزود خدمة الشبكة العالمية للمعلومات ان تراقبه ايضاً إذا توافرت لديها أجهزة وبرامج خاصة لذلك.

2-البروكسي Proxy:

يكون عمله كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لادارة الشبكة، وضمان الامن وتوفير خدمات الذاكرة الجاهزة Cache Memory وتقوم الفكرة في البروكسي على تلقيها مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ثم يقوم بإعادة ارسالها إلى المستخدم بدون الحاجة إلى ارسال الطلب إلى الشبكة العالمية ، وفيما اذا لم يتم تنزيلها من قبل فيتم ارسال الطلب إلى الشبكة العالمية، وفي هذه الاخيرة يعمل البروكسي كمزود خدمة ويستخدم احد عناوين IP. ومن أهم مزايا مزود البروكسي انه يمكن للذاكرة Cache الاحتفاظ بتلك العمليات التي تمت عليها مما يجعل دوره

قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

3-برامج التتبع:

هذه البرامج يتم التعرف من خلالها على محاولات الاختراق ومن قام بها التي تتم وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، وتحمل اسم الحدث وتاريخ حدوثه وعنوانه IP التي تمت من خلال عمليات الاختراق، وكذلك اسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى.

4- نظام كشف الاختراق Intrusion Detection System

وهو يرمز له الاختصار بالأحرف IDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الألي أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد امن الحاسوب أو الشبكة. ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في أجهزة الحاسوبية واطلق عليها أصحاب الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاختراق في سجلات حاسوبية خاصة مما يمكن معه تقديم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

5- نظام جرة العسل Honey Pot:

نظام مصمم خصيصاً لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أي بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعاً خاطئاً بسهولة اختراق هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الهجوم على أي جهاز آخر في الشبكة، في

الوقت الذي يتم جمع اكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاختراق، وتحليلها وبالتالي اتخاذ وقائي فعال وهذه المعلومات التي تم جمعها تقيد في تحليل أبعاد الجريمة في حال وقوعها ومد فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.

6- أدوات تدقيق ومراجعة العمليات الحاسوبية Auditing Tools:

إن عمل هذه الأدوات مراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها logs والكثير من هذه الأدوات تأتي مصممة في أنظمة التشغيل المختلفة، وبعضه الأخر منها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعداها للعمل، وهنا ما يقوم به مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يستطيع ان يقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وتساعد في كشف أسلوب الجريمة وشخصية مرتكبها، والمثال عليها أداة Event Viewer لبيئة النوافذ.

7- أدوات الضبط:

إن جهاز التحقيق وجمع الاستدلالات تحتاج لضبط ماديات الجريمة واثبات وقوعها والمحافظة على الأدلة لتقديم الجاني للنيابة العامة، لذا فإن هناك أدوات تساعد في ضبط الجريمة الإلكترونية، كبرامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي، والتسجيل وغيرها من الأدوات مثل IDS, MNM4, Content Management

8- الوسائل التي تساعد على التحقيق:

يمكن من خلال هذه الوسائل (البرامج) استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب، وبرامج نسخ البيانات، وبرامج الكتابة على القرص الصلب المرتكبة والبرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني إلى حذفها نهائياً من الحاسب الألي وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة.

9- أدوات فحص ومراقبة الشبكات:

هي أدوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها، ومنها:

1- أداة ARP:

ووظيفتها تحديد مكان الحاسب الألي فيزيائياً على الشبكة التي تحتفظ بجميع كروت الشبكة.

2-برنامج Visual Route:

وهو برامج تلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين البيانات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو أسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

3-أداة التتبع Tracer:

ترسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها الوقت والفترات التي قضاها، وتسمح كذلك برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الخيار Time to live (TTL) التي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات. ويتم بذلك تحديد وبشكل

دقيق المسار الذي تسلكه الرزمة. وهذه الاداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن ايضاً من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.

4-أداة التفحص New Stat:

هي أداة لفحص حالة الاتصال الحالي للبروتوكول TCP/IP وتقوم بالعديد من المهام لعرض جميع الاتصالات الحالية، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه.

10- الاستعانة بالذكاء الاصطناعي:

أثبت مدى نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، ويتم ذلك من خلال حصر الحقائق والاحتمالات تمهيداً لاستنتاج النتائج النهائية بناء على تعاملات حسابية يتم تحليلها وفق البرامج المخصصة لهذا الغرض.

ثانياً: الوسائل الإجرائية:

هي الإجراءات التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها وتتمثل في:

1- اقتفاء الأثر:

يحرص المجرم الإلكتروني على عدم تقصي أثره ومتابعته أثناء ارتكابه للجريمة، فكثير من الوثائق تنشر في المواقع الخاصة بالمخترقين تحمل العديد من النصائح مثل نصيحة قم بمسح اثارك

Cover Your Track ، إذا لم يقم المخترق بمسح أثاره فسيتم القبض عليه وإن كانت عملية الاختراق تمت بشكل سليم ويمكن تقصي الأثر بطرق عدة سواء عن طريق البريد الإلكتروني أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

2-الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:

يجب على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، وكذلك يجب عليه الاطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات للمستفيدين، واجراءات امن العاملين واسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام، بالاضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها والاستفادة من التقارير التي تنتهجها نظم أمن البيانات وتقارير جدران الحماية.

معوقات التحقيق الجنائي الرقمي

تثير الجريمة الرقمية نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها وقد يكون مصدر صعوبة الدليل في أن أجهزة الحاسب الآلي، وحسب نظمها، لا يمكن فيها أن تتبع الطريق العكسي لما يخرج منها، الدليل المتحصل من الوسائل الرقمية يتخذ أيضا طبيعة الكترونية بحيث تصعب على المحقق إلا بإتباع إجراءات معينه يكون الغالب منها ذو طبيعة فنية.

زيادة استخدام أجهزة الحاسب الآلي الشخصية و استخدام الإنترنت على نطاق واسع و سهولة توفر أدوات الاختراق و عدم وجود أدلة مادية كافية مما يجعل الملاحقة القضائية صعبة.

بالإضافة للحجم الكبير من مساحة التخزين التي تستخدمها المنظمات التجارية في الوقت الحاليو امتناع ضحايا الجرائم الاكترونية عن الإبلاغ عن الجريمة الالكترونية

يمكن تصنيف المعوقات لنوعين :

أولا :معوقات تتعلق بصعوبة استخلاص الأدلة الجنائية الرقمية مثل :

1- الطبيعة الغير مرئية للدليل الجنائي الرقمي

فهو مختلف عن الأدلة الناتجة عن الجرائم التقليدية ، فعدم رؤيته يُشكل العديد من الصعوبات خلال جمعه و تحليله مما يتطلب توفر محققين على دراية كافية و مهارات فنية علمية في التعامل مع هذا النوع من الأدلة.

2- سهولة تدمير و محو الدليل الجنائي الرقمي

مرتكبي الجرائم الالكترونية يتميزون بالذكاء و الاتقان الفني للجرائم التي يقومون بها و يحرصون على مسح دليل إدانتهم عن طريق إعدادت غير مرئية في أنظمة الحاسب.

3- إعاقة الوصول إلى الدليل الجنائي الرقمي

يلجأ مرتكبي الجرائم الالكترونية دائما لابتكار أحدث الوسائل و الأساليب لعرقلة جمع أدلة الإدانة باستخدام تقنية التشفير أو فرض تدابير أمنية لمنع عملية التفتيش و الاطلاع على الأدلة و ذلك باستخدام كلمات سر أو إخفاء هويتهم و خاصتا عند استخدام شبكة الانترنت باستخدام برامج و تطبيقات تعمل على محو هويتهم في شبكة الانترنت.

4- ضخامة البيانات المطلوب فحصها

من أكبر المعوقات التي تواجه المحققين في مجال الحاسب و ملحقاته و يجب أن يتوافر فيه المعرفة بمكان و كيفية جمع المعلومات و البيانات التي يمكن أن تفيد في استخلاص الدليل الجنائي الرقمي .

ثانيا" : المعوقات المتعلقة بجهات التحقيق

الصعوبات تتعلق بجهة التحقيق، منها نقص المعرفة الفنية لدى سلطات التحقيق، ولدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة الالكترونية عن طريق الحاسب الآلي وكيفية التعامل معها

حيث يتطلب استخلاص الأدلة الجنائية الرقمية و فحصها إلى مهارات و خبرات خاصة في مجال الحاسب الآلي بالإضافة إلى أساسيات و أصول التحقيق الجنائي الرقمي الفني المطبقة في مجال الجرائم التقليدية لذا فنقص خبرة المحققين و عدم متابعتهم للمستجدات في الأساليب و التقنيات المستعملة في ارتكاب الجرائم الالكترونية يشكل عائق كبير في جمع الأدلة الجنائية الرقمية و تحليها .

و لتجاوز هذه المعوقات يجب تخصيص وحدات خاصة لديها الإلمام الكافي بتقنيات الحاسب الآلي و تدريبهم على أحدث المستجدات في هذا المجال.

الدليل الجنائي الرقمي

المقصود بالدليل الرقمي

هو الدليل المسجل على وسائط غير ورقية والذي يمكن رؤيته عن طريق العرض على شاشة عرض جهاز الكمبيوتر الـ Monitor أو سماعه ويمكن نقله.

الدليل الرقمي Digital Evidence قد يكون صورة رقمية Image أو مطبوعة من اصل رقمي أو يكون متناً Text لموضوع أو رسالة Message أو غيرها

أماكن وجود الدليل الرقمي

- بالنسبة للدليل الرقميّ فهو يختلف بِاختلاف الجريمة والهدف منها فالدليل الرقميّ في قضية الفدية ليس مثل قضيّة اِختراق شبكة مؤسسة ما. فهو يكون في أحد الأمور التاليَّة:
- الأقراص الصلبة.
- سجلات النظام.
- أدوات التخزين.
- البريد الإلكتروني.
- المحادثات.
- الهواتف.
- قواعد البيانات.

تصنيف الدليل الرقمي

1- الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي و تشمل الحاسب الآلي و ملحقاته

2- الأدلة الرقمية الخاصة بشبكة الانترنت كالبريد الالكتروني و غرف المحادثة

3- الأدلة الرقمية الخاصة ببروتوكولات نقل و تبادل المعلومات بين الأجهزة المتصلة بشبكة الانترنت مثل بروتوكول TCP/IP، Cookies .

4- السجلات المحفوظة في الحاسب و تشمل الوثائق المكتوبة و المحفوظة مثل البريد الالكتروني و ملفات معالجة الكلمات.

5- السجلات التي تم إنشاؤها بواسطة الحاسب و تعد مخرجات أصلية بالحاسب مثل سجلات الهاتف و فواتير أجهزة السحب الآلي للنقود.

6- السجلات المختلطة التي جزء منها تم حفظه بالإدخال و جزء أخر تم إنشاؤه عن طريق الحاسب الآلي .

معايير الإثبات للديل الرقمي في الإثبات الجنائي الرقمي

-أن تتم عملية الجمع أو الحصول على أو استخراج أو استنباط الادلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات أو أنظمة المعلومات والبرامج، أو الدعامات الإلكترونية وغيرها. ومنها على الأخص تقنيةDigital Images Hash ، Write Blocker، وغيرها من التقنيات المماثلة.

-أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المصرح لهم التعامل في هذه النوعية من الأدلة، أو الخبراء المُتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يُبين في محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخة مُماثلة مطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني ومع ضمان استمرار الأصل دون إجراء أي تعديل به.

-في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الاجهزة محل الفحص لأي سبب يتم فحص الأصل ويثب ذلك كله في محضر الضبط أو تقرير الفحص والتحليل.

-أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته.

واذ كان من الثوابت فى الأحكام الجنائية هو مبدأ القناعة الوجدانية للقاضي الجنائي وسلطته التقديرية في قبول الأدلة أو استبعادها تبعًا لما يطمئن اليه؛ الا ان تخلف اى من ضوابط الدليل الرقمي المشار اليها تفقده الحجة فى الاثبات الجنائى ، ولا يمكن التعويل عليه كدليل عند الحكم فى الدعوى.

مشروعية الدليل الرقمي

في مقبوليته يشترط أن يتم الحصول عليه بطريقة مشروعة موافقة للقانون و عليه فإن استخدام وسائل غير مشروعة للحصول على الأدلة الرقمية يترتب عليها بطلان الإجراءات و عدم صلاحيتها لأن تكون أدلة إدانة مثل استخدام الإكراه المادي أو المعنوي.

الفصل الثاني

أساسيات التحليل الجنائي الرقمي

- الهدف من التحليل الجنائي الرقمي
- خطوات التحليل الجنائي الرقمي
  - الوصول للموقع
  - الحصول على الأدلة الرقمية
  - تحديد مكان الأدلة الرقمية
  - حماية الأدلة الرقمية
  - نقل الأدلة الرقمية
  - تخزين الأدلة الرقمية
  - إجراء التحقيق
  - إعداد التقارير
  - الاستجابة و تجهيز الأدوات

أساسيات التحليل الرقمي

الهدف من التحليل الجنائي الرقمي

هو دراسة وتحليل الأدلة الرقمية والمحافظة على تسلسل حجز الأدلة.

يتم استخدام التحليل الجنائي الرقمي للتحقيق في أي جريمة تحتوي على استخدام الأجهزة الإلكترونية ، سواء تم استخدام هذه الأجهزة لارتكاب جريمة أو كهدف لها. للتصدي للجرائم الالكترونية التي ترتكب بإستخدام الأجهزة الحاسوبية أو الشبكة أو التي تقع على المنظمات المعلوماتية عن طريق:

1-معاينة مسرح الجريمة

2-استعادة ملفات جهاز الحاسب و كل المواد المرتبطة بالتحقيق و تحليلها و حفظها حفظا يساعد جهات التحقيق على تقديمها بصفتها دليل في المحكمة القانونية

3-استخلاص البيانات و نسخها بما يضمن استرجاع الملفات المحذوفة لضمان عدم تلف الأدلة الرقمية المستخلصة

4- حفظ كل الأدلة بنسخ عديدة في أماكن سرية

5-إنتاج تقرير جنائي حاسوبي و تقديمه بكل إجراءاته منذ البداية إلى النهاية

خطوات التحليل الجنائي الرقمي

1- الوصول للموقع

عند الوصول لمكان الجريمة يجب على المحقق القيام بعملية توثيق دقيقة لكل الأحداث و العمليات الجارية و الأشخاص الموجودين في مكان الجريمة و ما هي الأجهزة المتصلة بالجهاز المشبوه و الاتصالات الحالية بالشبكة و نوع الحاسب و نوع نظام التشـــــغيل .

2- الحصول على الأدلة الرقمية

للحصول على الأدلة الرقمية يتم القيام بعملية الفحص من خلال الفحص البصري لتحديد حالة الجهاز الهدف و مكان وجوده و البيئة المحيطة به ثم القيام بنسخ الملفات قبل بدء الفحص و القيام بعمل صورة طبق الأصل ليتم العمل عليها ، غير مســموح بالعمل على النسخ الأصلية للملفات. ثم يتم فحص القرص الصلب و الذاكرة للحصول على الدليل

3- تحديد مكان الأدلة الرقمية

عند الانتهاء من عملية الفحص يتم تحديد المكان أو الملف الذي يحتوي على الدليل الجنائي الرقمي و توثيقه .

قد يكون الدليل في قواعد البيانات مثل Oracle ، SQL Server ، جهاز الحاسب هو تاريخ تصفح الانترنت أو الملفات المحذوفة أو مفاتيح سجلات النظام في نظام ويندوز أو السجلات Logs ، الشبكة : البيانات عبر الشبكة و التي يمكن تحليلها بإستخدام برنامج مثل Wireshark ، جهاز الموبايل (سجل المكالمات و الرسائل)

كما يجب بعملية مراقبة و إلتقاط كل البيانات التي تم تسجيلها على الذاكرة RAM و إنشاء صورة طبق الاصل عن هذه البيانات .

4- حماية الأدلة الرقمية

بعد الحصول على الأدلة يجب على المحقق المحافظة على سلامتها حتى لايتم التعديل عليها أو تخريبها و عمل صورة طبق الأصل منها عن طريق أدوات التحليل الجنائي الرقمي. و منع الحقول الكهربية الساكنة لأنها تخرب الدليل الرقمي و ذلك بإستخدام حقيبة خاصة .

5- نقل الأدلة الرقمية

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

إذا كان الدليل الرقمي في ملقم Server يتضمن عدد من مواقع الويب فمن الصعب قطع هذا الجهاز عن الشبكة في حال توافر ملقم احتياطي Backup Server يتم إيصاله على الشبكة لحين إنشاء صورة طبق الأصل للملقم المصاب و إذا لم يتوافر ملقم احتياطي Backup Server يتم

قطع اتصال الملقم عن الشبكة بشكل مؤقت للقيام بإنشاء صورة طبق الأصل و من ثم إعادته للعمل .

وفي بعض الحالات يصعب الوصول إلى الجهاز المصاب لأسباب معينة فيتم جمع الأدلة الرقمية عن بُعد و ذلك من خلال إنشاء صورة طبق الأصل للجهاز المصاب عبر الشبكة

6- تخزين الأدلة الرقمية

يجب أن يتم تخزين الأدلة في بيئة أمنة لا يمكن الوصول إليها من قبل أشخاص غير مصرح لهم و من المهم أن تكون معزولة عن الحقول الكهرومغناطيسية و محمية من الحرائق و بعيدة عن أنابيب المياه و أن يكون المكان مغلق و يمنع أي شخص غير مصرح له من الاقتراب من هذا المكان كما يجب أن يكون مراقب بشكل كامل.

كما يجب على المحقق أن يقوم بتوثيق الطريقة التي قام باستخدامها لنقل الدليل الرقمي إلى مختبر التحليل الجنائي الرقمي الخاص به و توثيق كل أداة قام بإستخدامها و كل عملية فحص قام بها .

7- إجراء التحقيق

وهي الإجراءات التي يتم تنفيذها عند ثبوت ووقوع الجريمة وتحديد شخصية مرتكبيها بعد العمل على إدارة عمليات المعاينة لمسرح الجريمة وتوجيه الفريق في التحقيق و توزيع المهام والأعمال المطلوبة منهم والتأكد من اتباع الجميع الإجراءات الصحيحة لضمان نجاح العمليات و التحاور والتشاور مع خبراء أجهزة الحاسب في فريق التحقيق خلال المراحل المختلفة كما يتم التحقق من النتائج بإعادة خطوات التحليل و جمع الأدلة بإستخدام أكثر من أداة مختلفة للتحقق من الأدلة التي تم الحصول عليها لتجاوز إحتمال وجود أي خطأ في الأدلة .

8- إعداد التقارير

التقرير النهائي يكون مدرج فيه كل شيء متعلق بالقضية و كل الملفات التي تم اكتشافها و تحليلها و ذكر طريقة اكتشاف الدليل الرقمي و الأدوات التي تم استخدامها في هذه العملية و تحديد معلومات الجهاز بشكل مفصل بإستخدام الأداة Encase التي تحتوي على نماذج جاهزة للتقارير ، كما تستخدم أيضا الأداة Access Data's Forensic Tool kit لإنتاج تقرير عن الواقعة .

9- الاستجابة و تجهيز الأدوات

الاستجابة هو ردت الفعل عن وقوع الحادثة المعلوماتية و تتضمن عملية الاستجابة الوصول لموقع الحادث و تصوير الأدلة و تأمين مسرح الجريمة و نقل الأدلة إلى مختبر (معمل) الجنائي الرقمي

بعد الانتهاء من تقارير المختبر الجنائي حول الأدلة الجنائية الرقمية التي تم تحريزها وفحصها والجوانب المتعلقة بها يتم الإقرار بوجود جريمة و مناقشة الشهود و استجواب المتهم وطرح الأسئلة عليه و تجهيز الأدوات لتقديم الأدلة للمحكمة الرقمية.

الدليل الرقمي و طريقة استخراجه يجب أن تكون متوافقة مع المعايير القضائية ليتم اعتماد هذا الدليل في المحكمة

أساس عملية الاستجواب تعتمد على الأدلة المكتشفة.

الفصل الثالث

عملية الفحص و الحصول على الأدلة الجنائية الرقمية

- الوصول للموقع
- أماكن وجود الدليل الرقمي
- التحليل الجنائي الرقمي في الحاسب
- استخراج المعلومات الذاتية لملف الويندوز Metadata
- أدوات و تقنيات الجرائم الرقمية
- النموذج المرجعي
- تحليل السجل في ويندوز (عملي)
- تحديد حادثة التحليل المباشر في النوافذ(عملي)
- فحص القرص الصلب و استعادة الملفات المحذوفة في ويندوز (عملي)
- الحصول على البيانات في النوافذ (عملي)
- كيف يتم المحافظة على الدليل في الجرائم الرقمية
- مشاريع المعمل (عملي)

عملية الفحص و الحصول على الأدلة الجنائية الرقمية

الوصول للموقع

عند وصول فريق العمل يجب إغلاق كل الأبواب و منع دخول أي أفراد غير مصرح لهم بالدخول لحين معاينة موقع الحادثة و فحص الموقع و تحديد العمليآت الحاليّة عن طريق أخذ لقطة لشاشة screen shotللعمليات الحالية التي تعمل على هذا الجهاز ،بالضغط علىTask Manager و تحديد اِتصالات الشبكة الحاليَّة ويمكن معرفة كل الاتصالات الحاليه و عدم إغلاق أي جهاز و تحديد هل تتم عملية الفحص في نفس المكان أم في معمل التحليل الجنائي الرقمي .

أماكن وجود الدليل الرقمي

غالبا ما توجد الأدلة الرقمية في الأقراص المرنة و الصلبة و أشرطة تخزين المعلومات و أجهزة المودم و أجهزة التصوير و مواقع الويب و البريد و يوجد كثير من البرامج التي تساعد المحلل الجنائي الرقمي منها :

1- برنامج إذن التفتيش Computer Scorch Warrant Program

هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة و تسجيل البيانات منها و يمكن لهذا البرنامج أن يصدر إيصالات بإستلام الأدلة و البحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل .

2-قرص بدء تشغيل جهاز الحاسب Bootable CD

هو قرص يمكن المحقق من تشغيل الجهاز إذا كان محمي بكلمة سر

3- برنامج معالجة الملفات مثل X tree Pro Gold

هو برنامج يُمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب و يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية كما يُمكن من البحث عن كلمات معينة أو أسماء ملفات

4- برامج كشف القرص View Disk

يُمكن من الحصول على محتويات الأقراص مهما كانت أساليب تهيئتها

5- برامج اتصالات مثل LANtastic

هو برنامج يستطيع ربط جهاز حاسب المحقق بجهاز المتهم لنقل منه المعلومات و حفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب

6- برنامج منع الكتابة على القرص الصلب Write Blocker

التحليل الجنائي الرقمي في الحاسب

هو عملية فحص الجهاز أو المنظومة المعلوماتية و تحليل العمليات و استرجاع البيانات و الملفات من أجل الحصول على دليل رقمي Digital evidence يستخدم في التحقيقات القانونية .

أي جمع الأدلة الرقمية وتحليلها، ودراسة حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات و للتصدي للجرائم الالكترونية المتطورة بأنماط ودرجات من التكنولوجيا تقتضي أن يتمكن المحقق من كشف غموضها والوصول إلى الحقيقة بالسرعة والدقة اللازمين.

استخراج المعلومات الذاتية لملف الويندوز Metadata

Metadata (البيانات الذاتية) هي بيانات رقمية تصف خصائص المصادر الرقمية المتاحة على شبكة الانترنت، أو هي جمل تصف مصادر المعلومات التي تُمكن من إيجاد واستخدام وحفظ تلك المصادر مثل تاريخ إنشاء الملف و تاريخ التعديل عليه و تاريخ أخر مرة تم فتح هذا الملف و هذه معلومات مفيدة في التحليل الجنائي الرقمي .

أما عملية استخراج المعلومات من مجموعة كبيرة من البيانات تسمى Data Carving و File Carving هو استخراج البيانات من القرص الصلب عندما يكون الملف المطلوب قد تم تخريبه.

البيانات الذاتية سلاح ذو حدين فسوف يحاول المجرم جاهدا إخفائها بإستخدام الأدوات:

- "METANULL" وهي أداة تستخدم لمحو البيانات الذاتية.

- "ExifTool" وهي أداة أيضا تصلح مع أنظمة تشغيل ويندوز وماك ولينكس

بينما سيحاول المحقق الحفاظ عليها كما هي وبالذات الوقت الذي تم إنشاء فيه الملف وتعديله.وبالذات الوقت الذي تم إنشاء فيه الملف وتعديله، يساعد الوقت معرفة التوقيت في عملية التحقيق عن الجريمة من حيث ماهي أخر الملفات التي قام الجاني بإنشائها أو تعديلها و في حال تم اختراق جهاز ما ويريد المحقق معرفة ماهي الملفات التي قام المخترق بإختراقها بها سواء من تعديل أو فتح لملف معين، لذلك أكثر ما يعرقل أي محقق جنائي هو عدم التمكن من حصول على بيانات التوقيت لأي دليل رقمي.

الأداة المستخدمة لاستعادة الملف هي : Caver Recovery

كما يوجد العديد من الأدوات التي تساعد في عملية تحليل المعلومات الذاتية و التي تُستخدم في عملية التحليل الجنائي الرقمي هي الأداة Sleuth Kit و هي تعمل من خلال سطر الأوامر كما يوجد أداة ذات واجهة رسومية مجانية هي Autopsy على الموقع

https://www.autopsy.com

أدوات و تقنيات الجرائم الرقمية

أدوات الجريمة الإلكترونية cybercrime tools هي الأدوات تستخدم في الجرائم الالكترونية ينتج عنها أضرار للضحية وفوائد يكتسبها المجرم الالكتروني، وغالبًا ما يكون الهدف من هذه الجرائم هو سرق معلومات أو مبالغ مالية، ومن أشهر أدوات الجرائم الالكترونية:

1- الطابعات الالكترونية.

2- تقنية الباركود الالكترونية.

3- البرامج الخبيثة والفيروسات.

4- وسيط الكتروني لا سلكي.

5- الكاميرات وخط يربطها بوسائل التجسس.

6- برامج خاصة بنسخ المعلومات على أجهزة الحواسيب.

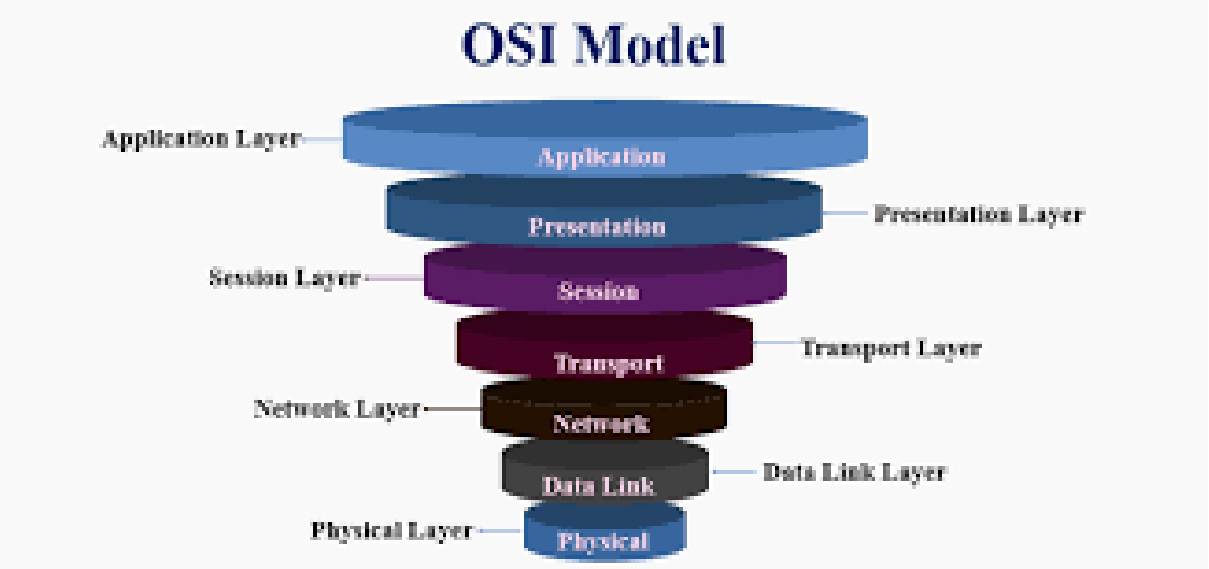
أما تقنيات الجرائم الإلكترونية هي مثل هجمات الحرمان من الخدمات و التصيد الاحتيالي و الهندسة الاجتماعية و البرامج المصمّمة لاستغلال أي أخطاء أو ثغرات أمنية في أجهزة الحاسب و الشبكات و برامج الفديةالتي تمنع صاحب الجهاز من الوصول إلى ملفّاته المخزّنة على محرّك الأقراص الصلبة، ويشترط المجرم على الضحيّة دفع مبلغ ماليّ كفدية لإتاحة استعادة ملفاته التي يحتاجها و برامج التجسس و برامج الفيروسات و البرمجيات الخبيثة و الاعلانات و غيرها .

النموذج المرجعي

هو تخطيط مفاهيمي يستخدم بشكل أساسي لوصف كيفية حدوث الاتصال بين الأجهزة، وتتمثل إحدى المزايا الرئيسية للنموذج المرجعي في أنّه يحدد معايير بناء مكونات الشبكة كما تحدد النماذج المرجعية الوظائف التي يجب إجراؤها في كل طبقة من طبقات النموذج وبالتالي فهي تعزز التوحيد القياسي.

في شبكات الحاسوب تعطي النماذج المرجعية إطاراً مفاهيمياً يوحد الاتصال بين الشبكات غير المتجانسة و يوجد نوعان :

أولاً: نموذج مرجعيOSI



هو نموذج تم تطويره بواسطة منظمة المعايير الدولية "ISO" وإنّه يعطي إطار عمل شبكي متعدد الطبقات يصور كيف يجب أن يتم الاتصال بين الأنظمة غير المتجانسة ولها سبع طبقات مترابطة.

تتكون بنية نموذج "OSI" من سبع طبقات وتحدد سبع طبقات أو مستويات في نظام اتصال كامل، وهذه الطبقات السبع مترابطة مع بعضها البعض.

الطبقات في نموذج"OSI"

1-الطبقة المادية.

2-طبقة ربط البيانات.

3-طبقة الشبكة.

4-طبقة النقل.

5-طبقة الجلسة.

6-طبقة العرض.

7-طبقة التطبيقات.

خصائص نموذجOSI

ينقسم نموذج "OSI" إلى طبقتين الطبقات العليا والطبقات السفلية، حيث ترتبط الطبقة العليا من نموذج "OSI" بشكل رئيسي بالمشكلات المرتبطة بالتطبيق ويتم تنفيذها فقط في البرنامج، وطبقة التطبيق هي الأقرب إلى المستعمل النهائي ويتفاعل كل من المستعمل النهائي وطبقة التطبيق مع تطبيقات البرامج، كما تشير الطبقة العلوية إلى الطبقة الموجودة فوق طبقة أخرى مباشرةً.

تتعامل الطبقة السفلى من نموذج "OSI" مع مشكلات نقل البيانات ويتم تنفيذ طبقة ربط البيانات والطبقة المادية في الأجهزة والبرامج، والطبقة المادية هي أدنى طبقة في نموذج "OSI" وهي الأقرب إلى الوسط المادي، والطبقة المادية مسؤولة بشكل أساسي عن وضع المعلومات على الوسط المادي.

ثانياً: نموذجTCP / IP

هي مجموعة بروتوكول"TCP / IP" ، ويشير "TCP" إلى بروتوكول التحكم في الإرسال بينما يرمز "IP" إلى بروتوكول الإنترنت، وإنّها مجموعة بروتوكولات للاتصال منظم في أربع طبقات ويمكن استخدامه للاتصال عبر الإنترنت وكذلك للشبكات الخاصة.

كما يُعد "TCP / IP" هو بروتوكول التحكم في الإرسال وبروتوكول الإنترنت والبروتوكولات هي مجموعة من القواعد التي تحكم كل اتصال ممكن عبر الإنترنت، كما تصف هذه البروتوكولات حركة البيانات بين أجهزة الكمبيوتر المضيفة أو الإنترنت وتقدم أنظمة تسمية وعنونة بسيطة.

الطبقات في نموذجTCP / IP

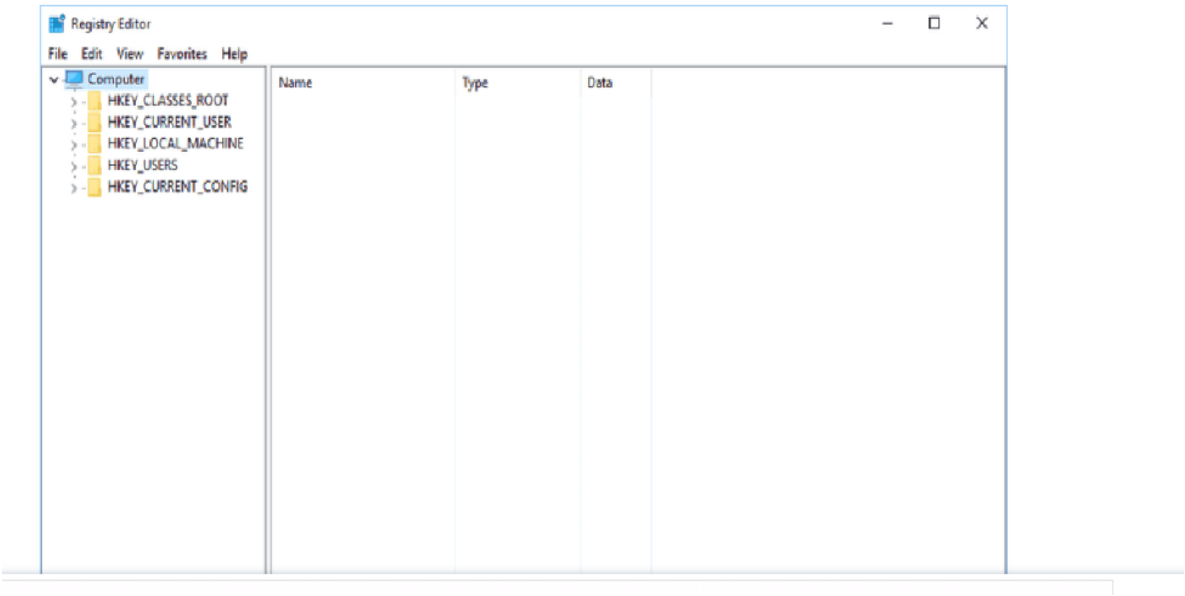
1- طبقة الربط.

2- طبقة الإنترنت.

3- طبقة النقل.

4- طبقة التطبيقات.

تحليل السجل في ويندوز (عملي)



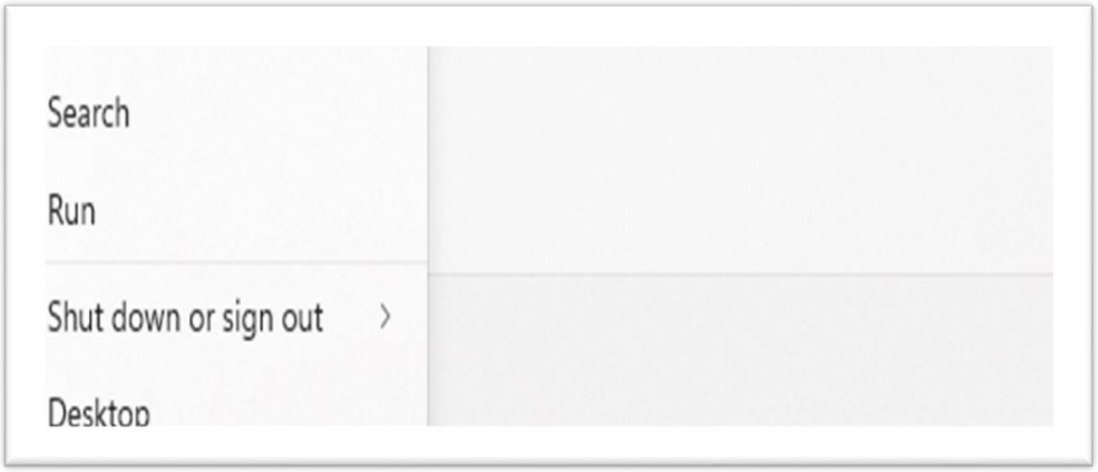
سجلات النظام Registry مسئولة عن كل شئ في نظام النوافذ Windows وهي تحوي على كل الإعدادات والملفات التي تم فتحها ومعلومات الشبكة والبرامج وأمور أخرى.

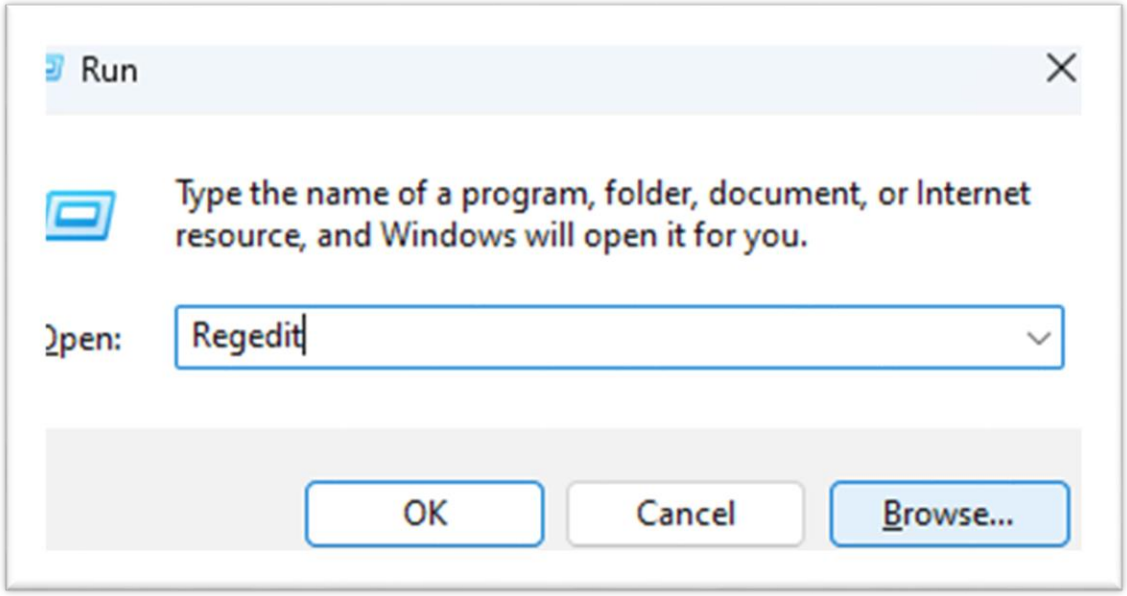
وهي مبنية بشكل هرمي ومكونة من خمس أفرع أساسية وتحوي على معلومات مهمة جداً في عملية التحليل الجنائي الرقمي.

شركة Microsoft عرفت سجلات النظام أنها :

قاعدة بيانات مركزية تستخدم من قبل أنظمة التشغيل الخاصة بشركة Microsoft ويتم فيها تخزين كل البيانات الضرورية لإعدادات النظام والمستخدمين والبرامج والأجهزة وهي تحوي على بيانات خاصة بكل مستخدم والبرامج التي قام بتثبيتها على النظام والملفات والمستندات التي قام بفتحها والأجهزة المتصلة والمنافذ ports المستخدمة في اتصالات الشبكة.

يمكن الوصول إلى سجلات النظام من خلال كتابة Regedit في حقل التشغيل Run





وهي مرتبة خمس قطاعات:

1-HKEY-CLASSES-Root (HKCR) :

يتم فيها تخزين معلومات عن قواعد drag and drop (سحب وتحريك الملفات) وعن اختصارات البرامج وعن الواجهة الخاصة بالمستخدم وأمور أخرى.

2- HKEY-CURRENT-USER (HKCU):

تحتوي على معلومات مهمة في التحقيق الجنائي الرقمي متضمنة بيانات عن المستخدمين وإعدادات سطح المكتب والملفات والمجلدات.

3- HKEY-LOCAL – Machine (HKLM) :

تحتوي على معلومات مهمة في التحقيق الجنائي الرقمي متضمنة بيانات عن كامل الجهاز بغض النظر عن المستخدمين.

4- Hkey-users (HKU) :

تحتوي ايضاً على معلومات مهمة في التحليل الجنائي الرقمي متضمنة بيانات عن المستخدمين والإعدادات الخاصة بكل مستخدم.

5- Hkey-Current-Config (HCU)

تحتوي على إعدادات النظام الحالية وهي مفيدة أيضاً في التحليل الجنائي الرقمي.

كل مفاتيح سجلات النظام registry keys تحتوي 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 تحديد أجهزة USB التي تم وصلها بالجهاز وذلك من خلال المفتاح التالي:

AutoStart Location/HKEY-Local – Machine/System/ControlSet/Enum/UBSTOR

هذا المفتاح يستخدم عادة من قبل البرمجيات الخبيثة Malware من أجل تثبيت عملية الاستغلال على الجهاز الهدف وهو يحتوي على البرامج المعدة لتبدأ العمل بشكل أتوماتيكي عن إقلاع النظام.

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

الملفات والمواقع حديثة الزيارة

المفتاح التالي يعرض المواقع التي تم زيارتها مؤخراً.

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

- **Raymondcc RecDeHexer**
- **OTConvertlt**
- **RegHexSee.**

البرامج الملغي تثبيتها:

قيمة هذا المفتاح مهمة جداً في عملية التحليل الجنائي الرقمي، المجرم يمكن ان يقوم بتثبيت برمجية معينة على الجهاز لأغراض معينة (خلق backdoor أو استعادة كلمات السر الحفوظة) ومن ثم يقوم بإلغاء تثبيت هذا البرنامج.

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

المفتاح التالي يعرض البرامج التي تم الغاء تثبيتها

HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall

ملاحظة :

الستيغنوغرافي Steganography

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

الأداة Invisible Secret:

من أكثر أدوات الستيغنوغرافي شهرة، من المهم للمحقق الجنائي الرقمي ان يكون على معرفة بهذه الأدوات وطرق استخدامها.

المثال التالي لإخفاء مستند نصي داخل صورة باستخدام هذه الأداة.

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

تحليل الملفات:

يوجد اكثر 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 الالوان الفريدة.

الستيغنوغرافي مهمة جداً في عمليات التحليل الجنائي الرقمي

التحليل الجنائي الرقمي للموجة Router

أثناء عملية التحليل الجنائي للشبكة يتم مع أجهزة Routers

الموجه router يمكن أن يكون عرضة للعديد من الهجمات ومنها تزوير جدول التوجيه Routing table 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 الموجه قبل أو أثناء عملية التحليل الجنائي الرقمي للحفاظ على الدليل الرقمي داخله.

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

بعض التعليمات المفيدة في عملية التحليل الجنائي الرقمي للموجة:

- Show Version :

هذه التعليمة تعرض معلومات عن إصدار الموجه ونظام التشغيل الخاص به ومعلومات أخرى.

- Show running-config :

تعرض الإعدادات الحالية للموجه.

- Showstartup-config :

تعرض الإعدادات عند إقلاع الموجه.

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

- Show ip route :

تعرض جدول التوجيه، التلاعب في جدول التوجيه هو السبب الرئيسي الذي يدفع أي مهاجم لاستهداف الموجه.

تحديد حادثة التحليل المباشر في النوافذ(عملي)

سجلات أحداث Windows هي واحدة من مصادر البيانات الأكثر شيوعًا لعوامل Log Analytics على الأجهزة الظاهرية لـ Windows نظرًا لأن العديد من التطبيقات توفّر التحرير إلى سجل أحداث Windowsيمكن تجميع الأحداث من سجلات قياسية مثل System و Applicationبالإضافة إلى تحديد أي سجلات مخصصة أنشأتها التطبيقات التي تحتاج إلى مراقبة

Event Viewer

هو أحد مكونات نظام التشغيل Microsoft Windows الذي يتيح للمسؤولين والمستخدمين عرض سجلات الأحداث على جهاز محلي أو بعيد.

يمكن للتطبيقات ومكونات نظام التشغيل استخدام خدمة السجل المركزي هذه للإبلاغ عن الأحداث التي حدثت ، مثل الفشل في بدء مكون أو إكمال إجراء ما

في windows server يمكن الوصول للسجلات من خلال:

1- فتح لوحة التحكم

2- اختيار Administrative Tools

3- اختيار Event Viewer

تظهر السجلات التالية:

- Security Log :

وهو أهم سجل يجب فحصه خلال عملية التحليل الجنائي الرقمي ويحتوي على معلومات عن عمليات تسجيل الدخول للنظام.

- Application log:

العديد من البرامج والتطبيقات تقوم بتسجيل الاخطاء في هذا السجل.

- System log:

يحتوي على الأحداث الخاصة بعمليات النظام وهو غير مهم جداً في عملية التحليل الجنائي الرقمي.

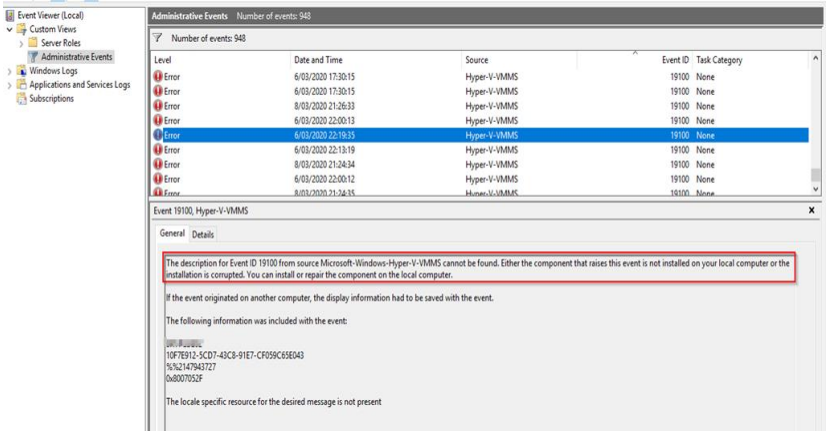
- Forwarded Event log :

يستخدم لتسجيل الأحداث الخاصة من الأجهزة البعيدة.

- Application and Services log:

يحتوي على معلومات الأحداث المتعلقة بتطبيقات أو الأحداث التي يمكن أن تؤثر على النظام.

من الممكن ان يقوم المهاجم بحذف هذه السجلات.



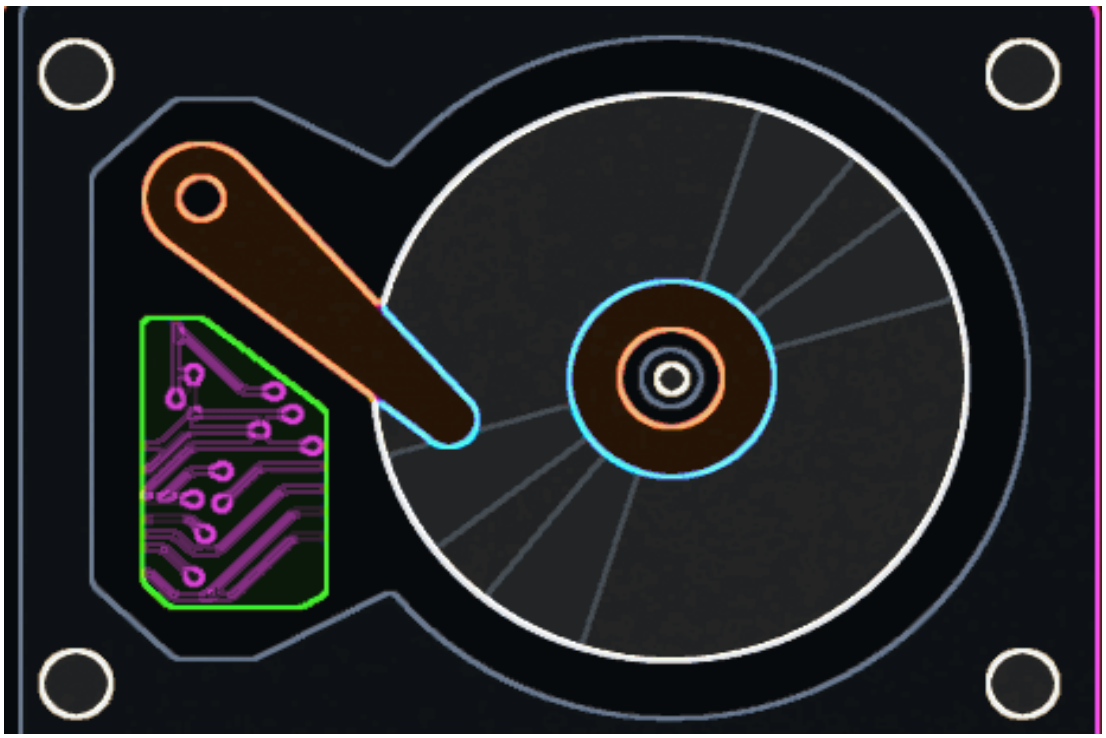
تحدث غالبية الاختراقات للبيانات الكبرى بسبب الموظفين الداخليين، فأصبحت مراقبة أنشطة الشبكات الداخلية المتطلب الأساسي للمؤسسات - الكبيرة أو الصغيرة. لتأمين شبكتها من التهديدات، كما

تحتاج المؤسسات إلى اتخاذ تدابير وقائية لضمان أمان الشبكات والبيانات وتعد مراقبة بيانات سجلات الأحداث أدق طريقة لاكتشاف وتعقب دخلاء الشبكات و التحليل المباشر لحادثة معينة مثل حالات تسجيل الدخول الفاشلة وحالات فشل تسجيل الدخول والمحاولات الفاشلة للوصول إلى الملفات المؤمّنة والتلاعب بسجلات الأمان وما إلى ذلك، مما يساعدك في الكشف عن الشخص الغير مصرح له الذي يحاول الدخول على نظام مثل الأداة EventLog Analyzer - أداة مراقبة سجلات الأحداث

فحص القرص الصلب و استعادة الملفات المحذوفة في ويندوز (عملي)

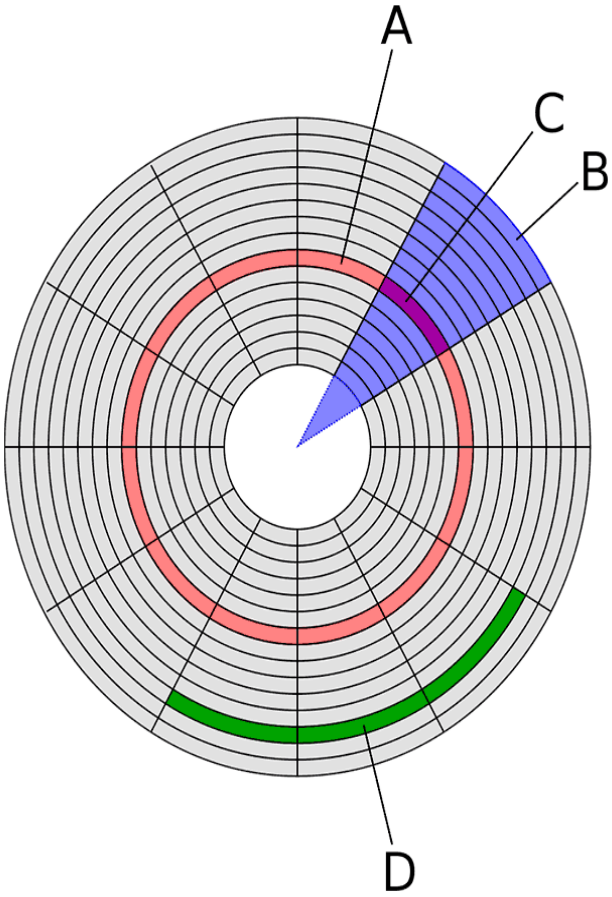
القرص الصلب كوسط تخزين هو المكان الرئيسي للبحث عن الدليل الرقمي، الخوادم (Servers) وأجهزة الحاسب المكتبية والمحمولة تملك أقراص صلبة لذلك من المهم فهم كيفية عمل هذه الأقراص.

حيث يتم تخزين البيانات على شكل إشارات مغناطيسية يفهمها الحاسب على إنها bits وتكون مرتبة ضمن قطاعات sectors وكتل clusters



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 والى طبقات القرص الصلب

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



A - مسار (Track)
B - قطاع (Sector)
C - كتلة (Block)
D - تجمع (Cluster)

يتم تنظيم الحبيبات على كل قرص ضمن دوائر متحدة المركز تسمى مسارات(Tracks) ، كما يقسم القرص إلى قطاعات .(Sectors) بمقاطعة قطاع مع مسار نحصل على الكتل(Blocks) ، وبجمع الكتل معاً يمكن صنع التجمعات (Clusters) المكونة من عدة كتل متجاورة.

البيانات تكون ضمن كتل clusters ويتم تسجيل البيانات عن طريق مغنطة المادة المكونة للطبقات لتمثل إما 1 or 0

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

ولكل قرص رأسا قراءة وكتابة موضوعتان فوقه وتحته. للتمكن من قراءة كامل محتوى القرص، يجب أن يدور القرص حول محوره من جهة، كما يجب أن تكون رؤوس القراءة والكتابة قابلة للحركة للانتقال من مسار إلى آخر.

في نهاية رأس القراءة يوجد مغناطيس صغير جداً، وعند القراءة ينجذب المغناطيس للقرص أو ينفر منه حسب اتجاه الحقل المغناطيسي لكل نقطة. وبناءً على هذه الحركة تتحول المعلومات المخزنة إلى إشارة كهربائية يتعامل معها الحاسوب.

بالنسبة للكتابة، يتم الاعتماد على الأثر المغناطيسي للتيار الكهربائي

بالنسبة للحذف فالأمر مختلف. حيث أن عملية الحذف لا تتضمن إزالة أو تغيير محتوى القطاعات، بل أنها تتم بمجرد إزالة سجل الملف المحذوف، حيث تبقى البيانات لكن يزال عنوانها. لهذا السبب تعد عملية الحذف أسرع بكثير من الكتابة، كما أن استعادة الملفات المحذوفة تبقى ممكنة كذلك.

تقسيمات القرص الصلب

جهاز الحاسب يمكنأن يحتوي على قرص صلب واحد أو اكثر والذي يمكن تقسيمه إلى أكثر من قرص.

يوجد أربع أنواع من التقسيمات:

1- Primary Partition :

هذا القسم الاساسي الخاص بنظام التشغيل والإقلاع، يجب أن يحتوي القرص الصلب ضمن الحاسب على قسم أساسي Primary partition واحد على الأقل من أجل اقلاع النظام ويمكن أن يحوي الجهاز على اكثر من قسم خاص بالاقلاع (في حال تثبيت نظامين windows and linux على نفس الجهاز).

2- Active Partition

وهو القسم الفعال المخصص ليكون القسم الأساسي للإقلاع الحالي (إذا كان الجهاز يحوي على قسمين أساسين لإقلاع احدهما خاص بـ Windows والاخر خاص بـ Linux عندما يتم الإقلاع من نظام Windows فيكون القسم الخاص به هو القسم الفعال.

3- Extended Partition

القسم الموسع ولايمكن ان يوجد أكثر من قسم واحد منه في القرص الصلب وهو القسم الذي يتم تقسيمه إلى الأقراص الفرعية الأخرى.

4- Logical Partition

القسم المنطقي وهو الأقراص الفرعية مثل C, D and E:

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

أ- Encrypted Partitions:

القسم المشفر، يوجد العديد من الأدوات التي تسمح بتشفير كامل القرص الصلب أو جزء منه مثل أداة TrueCrypt

ب- Hidden Partition :

القسم المخفي، عند تقسيم القرص الصلب إلى أقراص فرعية يمكن تعيين أقسام غير مرئية لبعض المستخدمين.

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

يوجد عدة طرق من أجل اكتشاف الاقسام المخفية ومنها مقارنة الحجم الكلي للقرص مع مجموع حجوم الأقراص الفرعية كما يمكن كشف الاقسام المخفية باستخدام أداة مثل

Raw Disk Viewer

جـ Unallocated Space

المساحة الغير مخصصة وهي المساحة من القرص الغير مخصصة لأي قرص فرعي وتسمى عادة بالمساحة الفارغة وهي مختلفة عن المساحة المخفية.

إيجاد البيانات:

عند طلب ملف تقوم رأس القراءة والكتابة بالتحرك حتى الوصول فوق المكان المخصص ومن ثم يدور القرص إلى أن يصل الرأس إلى القطاع المطلوب.

المصطلحات:

- Seek Time:

الزمن المطلوب لتحريك رأس القرص.

- Latency period:

فترة التأخير.

- Access time:

زمن الوصول ويساوي الزمن المطلوب لتحريك القرص مضافاً اليه زمن التأخير.

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

استعادة الملفات في ويندوز:

في بعض الحالات يقوم المتهم بتخريب القرص الصلب قبل أن يتمكن المحلل الجنائي من الحصول عليه ويجب عليه محاولة استعادة البيانات من القرص المخرب.

يوجد حالتين عند محاولة استعادة الملفات:

- الملفات تعرضت لضرر فيزيائي Physically damaged
- الملفات تعرضت لضرر منطقي Logical damage

الضرر الفيزيائي:

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

محاولة استعادة الملفات تتم بالخطوات التالية:

1- فك القرص الصلب من الجهاز توصيله بجهاز آخر كقرص صلب ثاني.

2- تقسيم إقلاع النظام إما من القرص الأساسي أو من قرص إقلاع اخر

3- تحديد فيما اذا تم اكتشاف القرص المصاب وتحديد إمكانية تعريف القرص المصاب، في حالة تم التعريف يتم القيام بنسخ الملفات وفي حال تم اكتشاف القرص ولا يمكن القراءة منه يتم استخدام أداة : DCFLdd (وهي نسخة مطورة من أداة dd) لمحاولة إنشاء صورة مطابقة لهذا القرص.

الضرر المنطقي:

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

معظم أنظمة التشغيل تؤمن أدوات اصلاح، نظام windows يحوي على أداة Chkdsk utility ونظام Linux يحوي على Fsck utility

كما يوجد العديد من الأدوات والبرامج الأخرى التي يمكنأن تقوم باصلاح الضرر المنطقي وتساعد على استعادة الملفات مثل:

- The Sleuth Kit.
- TestDisk

فحص ملف المبادلة 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 الجاني (المتهم) كان يعمل على مستند Word ولم يقم بحفظه فسوف يكون جزء من معلومات هذا المستند في ملفات المبادلة وهذه الملفات لايتم مسحها أثناء إيقاف تشغيل الجهاز وهي تعمل بنظام (الدور) لا يتم مسح البيانات إلى ان تبدأ الحاجة لاستخدام المساحة من قبل برنامج آخر.

ملفات التبادل (ترحيل الصفحات) تكون في Windows باسم Pagefile.sys ويجب على المحقق أن يفحص هذا الملف كمحاولة للحصول على معلومات مفيدة في عملية التحقيق.

يمكن للمتهم أن يستخدم أداة معينة تمكنه من حذف هذا الملف

حذف الملفات لايقوم 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

طريقة استعادة الملفات

أنظمة التشغيل Windows تستخدم نوعين من نظام الملفات وهي:

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

النوع الأول: 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.

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 ان يتم استخدام المساحة المخصصة لهذا الملف من قبل ملف آخر وعندما يتم حفظ معلومات جديدة على القرص فمن الممكن ان يتم حفظها في الكتل الخاصة بالملف المحذوف ومن الممكن ألا يتم حفظها في هذه الكتل.

وممن 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.12

النوع الثاني: 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 ومعرفات 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 اليها اولاً على إنها محذوفة ليتم ارسالها إلى سلة المحذوفات وعندما نقوم بإفراغ سلة المحذوفات يتم الإشارة لهذه الكتل على إنها كتل متاحة وقابلة للاستخدام.

أداة استعادة الملفات المحذوفة DiskDigger

يوجد العديد من أدوات استعادة الملفات المحذوفة ومنها الأداة DiskDigger

يتم اختيار محرك القرص الصلب المطلوب استعادة الملفات منه . سوف يقوم بفحصه ويعرض قائمة من الملفات التي يمكن استرجاعها لاختيار الملفات المطلوبة .

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

كما يوجد أيضا **أداة استعادة الملفات المحذوفة Win Undelete**

الحصول على البيانات في النوافذ (عملي)

FTK Imagerهو برنامج استعراض البيانات وتصويرها، يعمل بنظام الويندوز، يمك;ن من خلاله الحصول على نماذج بصورة مناسبة قانونيّا، عبر توليد نسخ من محرّكات الأقراص دون إحداث تغييرات على الأصل. كما أنه يُمكن تشغيل التّطبيق من محرّك أقراص محمول.

فهو يستخدم لأغراض التحقيق الجنائي الرقمي و هو أول عمل يقوم به المحقق بعد حيازة الأدلة بعد تزصيل الدليل بجهاز منع الكتابة Write Blocker لمنع الكتابة و التعديل على القرص ثم يقوم بإستخدام FTK Imager لعمل نسخة كاملة للقرص و استعراض الملفات الموجودة داخل القرص في النوافذ بالإضافة لعمل نسخة من الذاكرة Ram

أولا للقيام بعمل نسخة كاملة من القرص

بعد تثبيت البرنامج أو العمل من محرّك أقراص محمول من واجهة البرنامج لعمل نسخة من القرص يتم اختيار :

File / Create disk Image

و إتباع مربعات الحوار حسب الاختيارات و الضغط على إنهاء

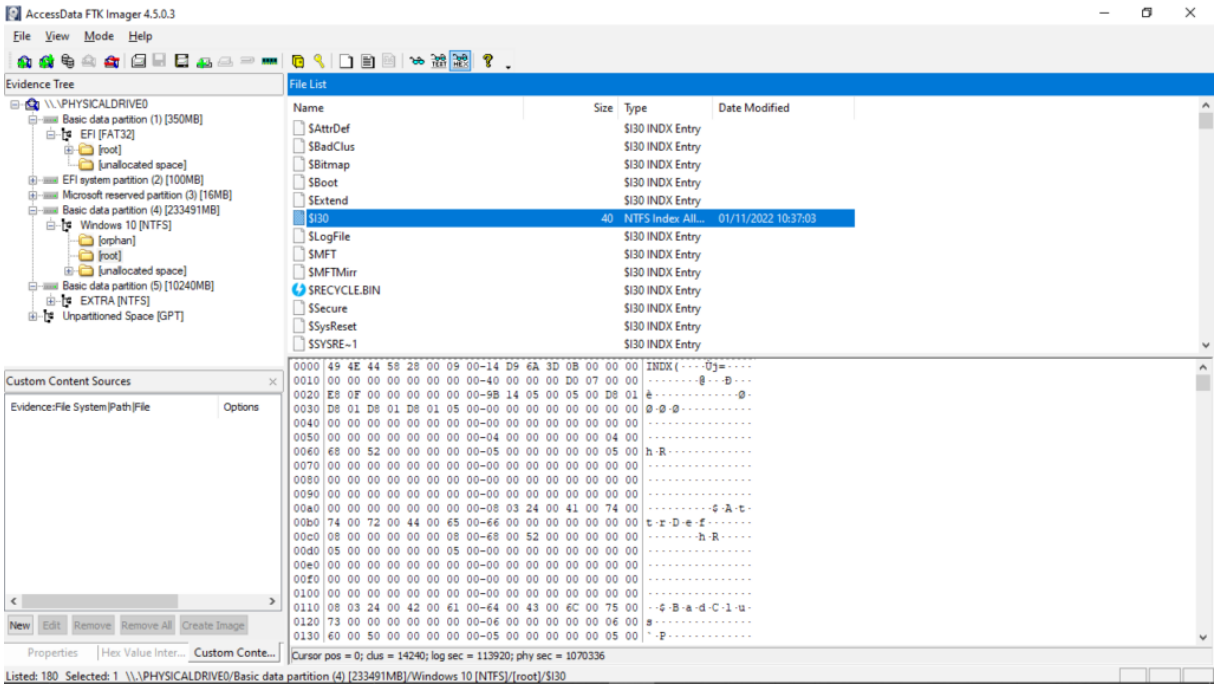
و عند الانتهاء من العملية النتيجة تواجد ملفين ، ملف بحجم القرص يظهر فيه تقرير بالعملية و بمعلومات عن الدليل و معلومات عن الهاش

كما يقوم أيضا بإستعراض الأدلة بإختيا الأمر

File/ Add Evidence Item

يتم إضافة النسخة المطلوب إضافتها

يتم رؤية القرص بالكامل و الملفات المحذوفة كما تظهر الملفات بال Hexa



يقوم المحقق بإستخدام هذه النسخة للتحقيق و تظل النسخة الموجود عليها الجريمة كما هي على الجهاز في مسرح الجريمة .

لعمل نسخة من الذاكرة الموجودة Ram في موقع الجريمة

نستخدم الأمر

File / Capture memory

حيث يتواجد في الذاكرة معلومات مهمة

يتم اختيار الموقع المطلوب حفظ المعلومات فيه

لمشاهدة محتويات الـ Ram يتم استخدام أمر

File/ Add Evidence Item

برنامج Encase

مصمم من قبل شركة Guidance Software و هو من أشهر برامج التحقيق الجنائي الرقمي و يُستخدم في حفظ الأدلة ، نسخ الأقراص ، تحليل الملفات ، إنشاء التقارير و التوثيقات ، إدارة القضايا ، فتح أغلب صيغ الملفات المعروفة و يتوفر في إصدارين Enterprise و Standard و كما يعمل في نظام التشغبل و يندوز و لينكس .

كيف يتم المحافظة على الدليل في الجرائم الرقمية

تعني المحافظة على الأدلة الرقمية في موقع الحادث، وعدم تعريضها للتغيير أو النقل أو المسح، ويتم ذلك باستخدام حقائب مخصصه تسمى Faraday bags ووظيفتها هي حماية الدليل او الجهاز الذي يتم نقله من فقدان البيانات أو محاوله اختراقة وتعديل المحتويات بل في بعض الحالات من الممكن الدخول عن بعد على الاجهزة المتنقلة ومسح محتوياتها. لذلك يعد استخدام الحقائب والحاويات الحافظة هو من اهم الاجراءات الضرورية للتعامل مع الادلة الرقمية. كما يجب التأكد من المحافظة على الاجهزة وحمايتها من انقطاع التيار الكهربائي في حاله انها وجدت على وضع التشغيل حيث أن الاغلاق قد يودي الى فقدان الأدلة او عدم القدرة على تشغيل الاجهزة مره اخرى

مشاريع المعمل (عملي)

1- استرجاع ملفات محذوفة

حذف ملفات من القرص الصلب ثم استرجاع الملفات المحذوفة منه بعد عمل تهيئة للقرص

2- الشبكات اللاسلكية:

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

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

3- 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 ما

المطلوب تحديد المفتاح

4- 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 ان تتم بالاعتماد على حجم البيانات أو بحسب البروتوكول المستخدم في عملية الاتصال أو بحسب عنوان IP address وأمور ومعايير أخرى.

خلال عملية التحليل الجنائي الرقمي يجب القيام 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.

المطلوب تحديد المفتاح و فحص السجل الخاص بالجدار الناري

5- التحليل الجنائي الرقمي لأجهزة الموبايل

يمكن أن تحتوي على أدلة لكل من الجرائم الاكترونية وغير الالكترونية وهذه الأدلة يمكن أن توجد في الاماكن التالية:

- **سجلات الرسائل والمكالمات:**

معرفة الجهات التي يتواصل معها المشتبه به هو أمر مهم في أي عملية تحليل جنائي رقمية.

- **الصور ومقاطع الفيديو:**

الصور ومقاطع الفيديو يمكن ان تكون دليل رقمي ضد المتهم.

- **سجلات GPS**

- **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 الإنترنت.

خلال عملية التحليل الجنائي الرقمي يجب القيام 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 الإنترنت.

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

سجل المكالمات يجب ان 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 ان تكون متعلقة بالجريمة وهذه الملفات قد تكون أدلة هامة في الجريمة .

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

الخطوات المتبعة في عملية التحليل الجنائي الرقمي لأجهزة الموبايل:

1-عند وصل جهاز الموبايل بجهاز الحاسب يجب التأكد من ان الهاتف لن يقوم بعملية المزامنة مع الحاسب .

2-تتبع نفس الخطوات المتبعة في عملية التحليل الجنائي الرقمي لجهاز الحاسب مع التركيز على عدم تخريب الدليل الرقمي وتوثيق كل العمليات.

3- نسخ 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.

المطلوب تطبيق

أدوات التحليل الجنائي الرقمي لأجهزة الموبايل:

- **Paraben**
- **EnCase**

الفصل الرابع

المحكمة الرقمية

- مفهوم المحكمة الرقمية و القاضي الرقمي
- أدوات الجريمة في المحكمة الرقمية
- المواد الرقمية
- التوقيع الالكتروني بالمحكمة
- الإثبات في الجرائم الرقمية
- تحديد هوية الشخص رقميا (عملي)
- مستقبل المحكمة الرقمية

المحكمة الرقمية

مفهوم المحكمة الرقمية و القاضي الرقمي

المحكمة الرقمية Digital Court:

تعني المحكمة التي تختص بالجرائم الرقمية Digital Crime، وذلك على غرار محاكم متخصصة معينة كمحكمة الأسرة ومحكمة الجنايات والمحاكم المدنية.

بصفة أساسية هي تتعامل مع جرائم الحاسب الألي سواء ما يقع به أو عليه، ثم تمتد إلى جرائم الشبكات ومنها الشبكة الدولية Web وأشهرها شبكة الإنترنت، كما تشمل جرائم الهواتف الجوالة أو المحمولة أو النقالة والمعروفة باسم الموبايلات.

كما تتعامل المحكمة مع جرائم أجهزة الصرف الألي Automatic Teller Machines (ATMs) وأجهزة قراءة البيانات والتي تسمى القارئات Readers ومخرجاتها.

المحكمة الرقمية تحتاج إلى إعداد مكاني يتطلب وجود جهاز حاسب آلي حديث لاستعراض ما هو مسجل على الأقراص Disks وعلى الأسطوانات CDs، وشاشة عرض متسعة توضع في مكان يشاهده كل من في القاعة بشكل واضح، ويمكن وضع اكثر من شاشة وتحتاج إلى سماعات تغطي كل القاعة. أما إذا كان المضبوط هو جهاز بمكوناته فيتطلب الأمر اختبار المحتويات وبحث ما هو مسجل وعلاقته بالواقعة.

حدود المحكمة الرقمية

المحكمة تكون داخلية في كل دولة، ويمكن ان تنشأ في العاصمة كبداية وان كانت الحاجة ملحة لأن تنشأ كدائرة في محاكم الاستئناف. وهذه المحكمة تتعامل مع الجريمة الرقمية التي هي عابرة للقارات، وتختلف قوانينها من دولة لأخرى وإن كان من الممكن أن يكون الأساس واحداً.

المتهم في المحكمة الرقمية

المجرم المعلوماتي هو المتهم أمام هذه المحكمة وهو الذي يسئ استعمال أجهزة الحاسب والشبكة الدولية والشبكات الأخرى بإحدى الطرف التي تعد جريمة يعاقب عليها القانون.

والمجرم المعلوماتي هو مجرم من نوع خاص، وهم من المبتكرين والمتجددين والمجددين للوسائل والطرق.

الدفاع الرقمي

يبدى دفاعه في المحكمة الرقمية من خلال استعراض القضية وصورها الرقمية خلال شاشة المحكمة من خلال دراسة خطوات الجريمة وتصور وقوعها وعلاقة المتهم بجهاز الحاسب المضبوط وتحديد مسئوليته عنه.

ويكون الوكيل مستوعباً للقوانين الخاصة بالجرائم الرقمية.

المُحضر الرقمي

هو الشخص الذي يرسل صور صحف الدعاوى والإعلانات وتحديد المواعيد والإخطارات عن طريق البريد الإلكتروني E-Mail أو ما يستجد مثل استخدام الموبايلات كوسيلة إرسال، ويعترف المرسل اليه ان الرسالة وصلته، أو الاستدعاء أو الأخطار ويقوم بالحضور في الميعاد المحدد وألا يماطل أو يدعي عدم العلم.

المحقق الرقمي

مرحلة التحقيق تكون في جهات الشرطة ثم تحول إلى المحكمة، أو قد تكون في جهات الشرطة ثم النيابة ثم المحكمة حسب نظام كل دولة. وهو الشخص الذي لديه معرفة علمية بالجريمة الرقمية وكيفية وقوعها وطريقة التحقيق الكاملة التي لاتترك ثغرة يمكن النفاذ منها أو نفيها.

وهو ايضاً الذي يستوعب ماهو مخبأ من ملفات وأماكن إخفائها وكيفية التشفير وكيفية فك الشفرات وكيفية التعامل مع المجرم المعلوماتي والاستفادة من الدليل الرقمي Digital Evidence وذلك بأقصى درجة ممكنة وبشكل سريع، ولديه الدراسات المسبقة لما هو متوقع الحدوث.

يضاف إلى ذلك استيعاب النيابة العامة للقوانين الخاصة بالجرائم الرقمية ومستجداتها ولتكييف القضية تكييفاً قانونياً.

كيفية الحصول على إذن الضبط

أن يتم رقمياً عن طريق الـ E-Mail أو الموبايل كوسائل سريعة، ولاتكون الأذون ورقية، وقد تستخدم الحكومة الإلكترونية من خلال مواقع التوثيق نقل هذه الأذون من السلطة المختصة لجهة الضبط.

القاضي الرقمي :

هو القاضي البشري، لكنه هو الذي يطبق القوانين الخاصة بمستجدات التعاملات الرقمية، والحكومة الإلكترونية، والتجارة الإلكترونية، والتوقيع الإلكتروني الرقمي، والمستندات الرقمية، وجرائم النصب الرقمية والسرقة والقتل بالوسائل الرقمي، والعملات المزيفة الرقمية، والكاميرات الرقمية، وتركيب الصور الرقمية، والشبكات ويعرف مفرداتها وثقافتها.

أدوات الجريمة في المحكمة الرقمية

أدوات الجريمة الرقمية هي: الحواسب الألية وملحقاتها، والشبكات الناتجة عن اتصالها ببعضها عبر الشبكة الداخلية الإنترنت أو عبر الشبكة الدولية الإنترنت.

المواد الرقمية

هي الرسائل المثبته على دعامات غير ورقية أو تلك المطبوعات عن أصول رقمية، وتشمل المتن والتوقيع أو التوقيعات ويلحق بها المصدر المرسلة منه.

أنماط الجرائم الرقمية المعرفة قانوناً

تتخذ الجرائم الرقمية أنماطاً شتى ولايمكن حصرها إذ إن الشبكة الدولية (الإنترنت) مفتوحة، فارتكاب الجريمة دولي وعابر للقارات ومفتوح لجميع العقول والأفكار، فهي جريمة متجددة الطرق ومتجددة الأدوات.

ومن أنماط الجريمة الرقمية المعرفة قانوناً الاخلال بأمن الحاسب في ذاته كاستعمال الجهاز دون موافقة من صاحبه، والدخول على البيانات المخزنة أو المحفوظة بدون موافقة المالك وإفشاء سر مؤتمن عليه الموظف عن طريق:

1- فتح كلمة السر أو الشفرة الخاصة بالتعريف أو أي معلومات سرية.

2- إتلاف الحاسب الألي أو جزء منه أو برامج أو بيانات أو يعدل أو يمحو برامج الحاسب أو البيانات.

3- إدخال حالة الغش بالجهاز أو أجزاء منه حالة الدخول اليه.

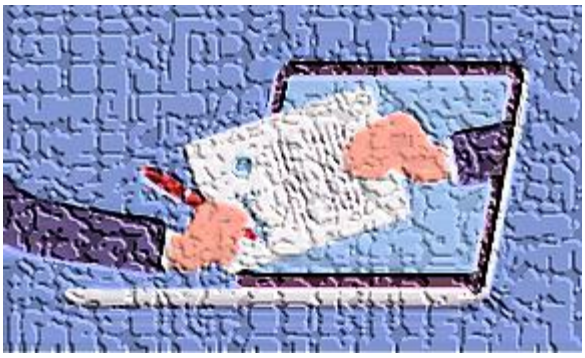
جرائم التزوير الرقمي

تمثل غالبية الجرائم الرقمية تزوير إذ أنها اذا وقعت بأي صورة فهي تتم عبر طرق غير مشروعة للبيانات والمستندات الرقمية والتوقيعات الرقمية والتي تعد طرقاً من طرق التزوير.

فالحذف والإضافة والتغيير هي الطرق المعتادة للتزوير، والتدمير والسرقة والاحتيال الرقمي هي من طرق التزوير أو ان ما يبدؤها هو استخدام مستندات رقمية.

يضاف إلى ذلك استخراج مستندات مسجلة بالحاسب تحمل توقيعاً عبارة عن صورة ويوضع مذيلاً لإيصال أمانة أو احد الشيكات وخاصة استخدام الطابعات الملونة ليتم التحجج بها على الغير دون وجه حق ودون ان تكون له صلة بهذا المستند أو التوقيع.

التوقيع الالكتروني بالمحكمة



تعريف التوقيع الإلكتروني هو ما يوضع على محرر الكتروني ويتخذ شكل حروف أو ارقام أو رموز أو اشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.

للتوقيع الإلكتروني أو الرقمي والمستندات الرقمية حجية في الإثبات كما هي حجيتها في الحالة الورقية، وقد نص على هذا القانون الخاص بالتوقيع الإلكتروني.

التوقيع الالكتروني هو محور التجارة الإلكترونية E-Commerce وبدونه لايتحقق الهدف منها، وله عدة أنواع واشكال مختلفة، ولايشترط أن يكون مذيلاً لنص إذ إنه قد يكون كلمة سر مشفرة.

التوقيعات الإلكترونية أو الرقمية تتخذ أشكالاً منها:

1–التوقيع الإجرائي:

يسمى هذا التوقيع بالتوقيع المكود أو المشفر، وهو عدة خطوات منطقية متتالية يمكن من خلالها التعريف بالشخص، ويحكمها مفتاحان احدهما يعرف بالمفتاح الشخصي أو السري Personal Identification Number (PIN) أو الـ Secrete Key ويمكن الوصول اليه من خلال مفتاح عام Public Key Infrastructure ومن امثلتها التوقيعات المستخدمة في بطاقات الائتمان Credit Cards والتي تستخدم في الصرف الالي من البنوك او الدفع خلال منافذ البيع من خلال قارئات Readers

2– التوقيعات البيومترية Biometric Signatures:

وهي تعرف بالتوقيعات القياسية وهي خاصية من خواص الإنسان مثل:

- قرنية العين.
- بصفة الإصبع
- بصمة الصوت
- بصمة الوجه
- بصمة الدم

3-التوقيعات البيولوجية Biological Signature

وهي خاصة بالشخص والتي توقع بخط اليد ويتم نقلها بإحدى وسائل النقل إلى جهاز الكمبيوتر لتسجل رقمياً باستخدام الوسائل الغالية:

- الفاكس (الناسوخ)

- الماسح الضوئي

- الادخال بالكاميرا الرقمية بقلم رقمي

- الادخال على سطح حساس

نتطرق لشرح نوعين من التوقيعات وهما: التوقيع ببصمة الدم، والتوقيع بالقلم الرقمي.

التوقيع ببصمة الدم:

حيث يتم تعريض اليد للجهاز للقارئ لكلمة السر Password فيفتح الجهاز لهذا الشخص ولايفتح لغيره، لأن للدم بصمة خاصة بكل شخص.

القلم الرقمي :

هو قلم يكتب به على ورق عادي في وجود كاميرا، فما يكتب يسجل على الشاشة في الحال بكل تفاصيله، فإن كان توقيعاً سجل توقيعاً كأنه بخط اليد وذات لون مداد القلم، والقلم هنا مزود برأس يمكن من إدخال صوت وصورة للشخص القائم بالكتابة.

تعد كلمات السر توقيعات رقمية إذ هي دالة على الشخص الذي يحتفظ بها فقط دون حالة الاختراق من الغرباء أو الافشاء من الأشخاص المؤتمنين عليها العاملين في الشركات والمؤسسات وغيرها.

الموقع الرقمي

الموقع الرقمي Signer هو الشخص الطبيعي أو الاعتباري الذي يتعامل بنفسه أو عن طريق غيره باستخدام التوقيع الإلكتروني من خلال مصدر توثيق.

حجية التوقيع الإلكتروني:

يجعل للمحرر الحامل له قيمة قانونية في الإثبات.

محاذير التوقيع الإلكتروني

يحيط بالتوقيع الإلكتروني أو الرقمي محاذير في التعامل إذ إنه عصب التجارة الإلكترونية ولذلك لابد أن يحاط بالموثوقية حتى لاتهتز الثقة فيه وحتى لايستغل في عمليات النصب ومن هذه المحاذير:

1- احتراز الموقع أن لايستغل توقيعه أو يستخدم بطرق غير مشروعة Abuse Methods

2-إخطار الشخص الذي علم باستغلال توقيعه الجهة أو الشركة التي يتعامل معها.

3-عند طلب شهادة من الموقع Signer تؤيد توقيعه فعليه ان يقدم ما يدل على تأكيد البيانات التي تدرج في الشهادة.

4-تحديث التوقيع الإلكتروني عبر منظومة حتى لايتم التوصل إلى المفتاح الخاص به بتقادم التكنولوجيا مع الزمن.

القانون النموذجي الخاص بالتوقيع الإلكتروني

هو القانون الذي يعرف بقانون اليونسترال أو الاونسترال Uncitral وهو اختصار للعبارة United Nations Commission on International Trade Law وهو الذي وضع بمعرفة لجنة مختصة بالأمم المتحدة.

الاعتماد فقط على التوقيع الإلكتروني الرقمي دون الاصول أو المراجع الورقية

من الخطورة بأن يتم الاعتماد كلية على الصور الرقمية والتي تعد وهمية Images والتي لابد وأن تكون لها أصول ورقية، حتى إن عملية التعامل بالتجارة الإلكترونية تتم على أساس إرسال فاكس ثم الرد بفاكس أو عبر البريد الإلكتروني للتأكيد على التعامل الرقمي.

أهمية مقدمي خدمة التوثيق للمستندات الرقمية

هم يضفون الثقة والشرعية في التعامل بالمستندات الرقمية والتوقيعات الرقمية والتجارة الإلكترونية والوثائق الحكومية الرقمية، ويقومون بحماية المعلومات الشخصية للمشتركين في الخدمة.

شروط الثقة في الشهادة الموثقة

- يجب أن تشمل الشهادة على البيانات محدد بها شخصية مقدمها والدولة التي أنشأتها.

- اسم الموقع الفعلي أو حتى المستعار لكي يمكن التحقق منه

- ان تكون للموقع Signer ميزة خاصة بالشهادة المعطاة له.

- المفتاح العام الذي يكون موصلاً للتوقيع الخاص والذي يكون تحت رقابة الموقع.

- تحديد قيمة الصفقات التي تستخدم الشهادة من أجلها.

- لابد من تحديد مدة صلاحية الشهادة من حيث بدايتها ونهايتها.

- تحديد المجال الذي تستخدم فيه الشهادة.

- الرقم الخاص بالشهادة.

الإثبات في الجرائم الرقمية

الجرائم الرقمية في ازدياد وذلك لتزايد أعداد المستخدمين للحاسبات الألية وللشبكة الدولية والشبكات الأخرى، لذا فإن عملية الإثبات في هذه الجرائم تشكل صعوبة حتى اذا تم ضبط الواقعة، فعملية إقامة الدليل هي من الصعوبة بمكان، فلو ان رسالة أرسلت من جهاز الموبايل تحتوي الفاظ سب و تهديد فليس بالضرورة ان يكون صاحب الجهاز هو الذي أرسلها، فقد تكون قد تمت في غيبته في وقت قصير.

تحديد هوية الشخص رقميا

من خلال ترميز الشخص وتشفيره بإعطائه رمزاً أو رقماً أو مجموعة من الرموز (حروف أو أرقام) وهي لاتمت إلى الشخص بصلة، وتقابل ما يعرف بتوقيع النموذج في المستندات الورقية والذي يحرر بخط اليد.

مستقبل المحكمة الرقمية

متوقع عند إنشاء المحكة أن تزداد أعدادها، وقد تكون في كل محكمة دائرة، لأن التوسع في الأجهزة الرقمية والبرامج يزداد يوماً بعد يوم.

المراجع

-1	WM. Arthur Conklin,Greg White ,2018,Principles of Computer Security, maps to Compatia Security + ,Comptia
-2	د.عدنان مصطفى البار،د.عيسى رفاعي السميري، 1440هـ ،أساسيات الأمن السيبراني،مكتبة الملك فهد الوطنية
-3	خالد عياد الحلبي ،2011م ، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت،دار الثقافة
-4	د.محمد رضوان هلال 1428 هـ ، دار العلوم للنشر
-5	Dr.Jeetendra Pande ,Dr.Ajay Prasad ,2016, Digital Forensics,Uttarakhand Open University