جمهورية العراق
وزارة التربية
المديرية العامة للتعليم المهني

# التحقيق الجنائي الرقمي

# فرع الحاسوب وتقنية المعلومات

## اختصاص الامن السيبراني

### الصف الثالث

### تأليف

د. بشار مكي نعمـــة
د. عامرعبد المجيد عبد الرحمن
د. مروة مشتاق طالب
م.م فرهـــاد حسيـــن شاه مـراد

الطبعة الاولى
2026م – 1448هـ

# المصمم الطباعي

هيثم حمزة عبد



# بسم الله الرحمن الرحيم

## المقدمة

يشهد العالم اليوم تطورًا متسارعًا في تقنيات الحاسوب والاتصالات الرقمية، رافقه توسّع كبير في استعمال الأنظمة الإلكترونية في مختلف مجالات الحياة، الأمر الذي أدى إلى ظهور أنماط جديدة من الجرائم تعتمد في تنفيذها على الوسائل الرقمية وشبكات الإنترنت. ومع هذا التحول، ظهرت الحاجة إلى تخصصات علمية قادرة على مواجهة هذه التحديات التقنية، وكان من اكثرها **تخصصاً التحقيق الجنائي الرقمي** الذي يُعد أحد المرتكزات الأساسية في منظومة **الأمن السيبراني** الحديثة.

وانطلاقًا من هذا الواقع، جاء اعتماد **كتاب التحقيق الجنائي الرقمي للصف الثالث لقسم الأمن السيبراني ضمن فرع الحاسوب وتقنية المعلومات** ليكون مرجعًا علميًا وتطبيقيًا يواكب متطلبات العصر، ويسهم في إعداد طلبة يمتلكون المعرفة والمهارة اللازمة لفهم الجرائم الإلكترونية، وتحليلها، والكشف عن أدلتها الرقمية على وفق الأسس العلمية والقانونية المعتمدة. ويهدف هذا الكتاب إلى بناء قاعدة معرفية متينة لدى الطالب، تجمع بين الجانب النظري والتطبيق العملي، وتُنمّي قدرته على التفكير التحليلي والتقني في مجال التحقيقات الرقمية.

يتناول الكتاب المفاهيم الأساسية للتحقيق الجنائي الرقمي، ونشأته وتطوره، وأهميته في مكافحة الجرائم الإلكترونية، مع تسليط الضوء على مبادئه والتحديات القانونية والأخلاقية المرتبطة به. كما يعرّف الطالب بالأدوات والتقنيات المستعملة في التحقيقات الرقمية، وطرائق استرجاع البيانات وتحليل السجلات ودراسة البرمجيات الضارة لتتبع الأنشطة المشبوهة.

ويركز الكتاب على إجراءات جمع الأدلة الرقمية وتحليلها وتوثيقها، مع التأكيد على الحفاظ على سلامتها، إضافة إلى استعراض أنواع الجرائم الإلكترونية ودور التحقيق الجنائي الرقمي في مكافحتها. ويختتم بعرض آفاق التحقيق الرقمي المستقبلية، ودور التقنيات الحديثة والتشريعات في تطوير هذا المجال، بهدف إعداد جيل مؤهل يسهم في تعزيز الأمن السيبراني.

**وقد حرص المؤلفون** على إعداد هذا الكتاب بأسلوب علمي مبسّط يجمع بين الجانب النظري والتطبيقي، مع مراعاة تسلسل المفاهيم ومواكبة التطورات الحديثة في مجال التحقيق الجنائي الرقمي.

**المؤلفين**

# الفصل الاول
# اساسيات التحقيق الجنائي الرقمي

## (1-1) تعريف التحقيق الجنائي الرقمي

أصبح التحقيق الجنائي الرقمي موضوعًا مهمًا في صلب الأبحاث القانونية المعاصرة، وذلك لما يتميز به من طبيعة مختلفة عن نظيره التقليدي، لاسيما في طرق جمع الأدلة الرقمية وتحليلها. فقد أدى التزايد في التقنيات الحديثة المعتمدة على الحاسوب إلى جعل الأدلة الرقمية عنصراً شبه أساسي في أي تحقيق جنائي معاصر، إذ بات من النادر أن يخلو التحقيق من جمع معلومات وبيانات رقمية من الحواسيب، الأجهزة النقالة، أو وسائط التخزين المختلفة. وتُعد الخطوة الحاسمة في أي تحليل للتحقيق الجنائي الرقمي هي التعامل مع الدليل المعلوماتي والذي يشمل جمع البيانات الرقمية، مروراً بعملية التحقق من مصداقيتها، وصولًا إلى كيفية توظيفها لإضفاء قيمة حقيقية على التحقيق. إن هذه الأدلة تساهم مباشرةً في دعم عملية اتخاذ القرار عبر الإجابة عن تساؤلات جوهرية مثل: ماذا حدث؟ ومن الفاعل؟ ومتى وقع الحدث؟ وأين؟.

وعليه، يُعرَّف التحقيق الجنائي الرقمي باعتباره العلم الذي يُعنى باستخراج البيانات الرقمية من مختلف الأجهزة الإلكترونية وتحليلها بحيث تكون هذه البيانات موثوقة وقابلة للاعتماد عليها أمام المحكمة لإقناع القاضي بالحجة القانونية. ويُعد هذا المجال بمثابة علم لتحديد المواقع والأحداث عبر تتبع مصادر البيانات الرقمية وفحصها وفق معايير علمية وقانونية معتمدة.

ويمتاز التحقيق الجنائي الرقمي عن التحقيقات التقليدية بتركيزه على البيانات مثل محتويات الذاكرة أو سجلات النظام المؤقتة، والتي قد تختفي بمجرد إيقاف تشغيل الجهاز، مما يستلزم سرعة في التعامل وتقنيات خاصة لحفظها. وقد شهد هذا المجال تطورا ملحوظا خلال العقود الأخيرة، فبعد أن كان يُمارس بشكل يعتمد على خبرة فردية محدودة، أصبح اليوم علماً منهجياً يُبنى على أسس علمية ومعايير معتمدة ، ويركز على قواعد الإثبات ومعدلات الخطأ المقبولة، مما منحه طابعًا أكاديميا ليكون مجالا بحثيا مستقلاً.

يمكن العثور على الأدلة الرقمية في طيف واسع من الوسائط، تشمل: الأقراص الصلبة للحواسيب، الهواتف المحمولة، الكاميرات الرقمية، الأقراص المدمجة (CDs)، الأقراص البصرية (DVDs) بالإضافة إلى شبكات الحاسوب والإنترنت. وتُفسَّر هذه الأدلة عادةً من قبل الخبراء المتخصصين الذين يمتلكون القدرة على تحويل البيانات التقنية المجردة إلى أدلة قانونية قابلة للاستخدام في الإجراءات القضائية.

## (2-1) تاريخ التحقيق الرقمي وتطوره

وبعد توضيح مفهوم التحقيق الجنائي الرقمي وخصائصه الأساسية، يصبح من الضروري التطرق إلى الخلفية التاريخية لتطور هذا المجال. ففهم نشأة التحقيق الرقمي ومراحل تطوره يوفر منظورا أعمق يساعد على إدراك كيفية تحوله من ممارسة بسيطة في بدايات استخدام الحواسيب إلى علم مستقل له مناهجه ومعاييره المعتمدة عالميا. ومن هنا سنعرض بإيجاز المراحل التاريخية التي مرّ بها التحقيق الجنائي الرقمي والتطورات التي أسهمت في ترسيخ مكانته ضمن العلوم الجنائية الحديثة.

### (1-2-1) المرحلة التمهيدية (قبل العام 1985م)

تُعد المدة السابقة لعام 1985 مرحلة تمهيدية في تاريخ التحقيق الجنائي الرقمي، إذ لم يكن المصطلح قد ظهر بعد، وكانت الحواسيب مقتصرة على المؤسسات الحكومية والجامعات والشركات الكبرى، وتُستخدم أساسًا في معالجة البيانات ضمن بنى تحتية ضخمة وكوادر متخصصة. ويعد الكاتب (دون باركر) اول من تطرق إلى إمكانية توظيف المعلومات الرقمية كأدلة جنائية، وهو ما شكل بداية الوعي القانوني بأهمية البيانات الرقمية في كتابه الجريمة بالحاسوب (1976). وفي تلك الفترة أنشأت جهات مثل وزارة الدفاع الامريكية فرقاً صغيرة غير رسمية من محققين تلقوا تدريبًا أوليًا على الحواسيب المركزية، وكانوا يتعاونون مع مديري الأنظمة لاستخراج البيانات وسجلات الدخول. يتبين ان هذه الفترة تمثلت بجهود فردية وعشوائية في غياب مؤسسات أو أدوات مخصصة، حيث اعتمدت التحقيقات على أدوات أنظمة التشغيل والأساليب العلمية التقليدية.

### (2-2-1) مرحلة التأسيس المبكر (1985-1995)

في هذه المرحلة بدأ التحقيق الجنائي الرقمي يتبلور تدريجيا مع ظهور الحاسوب الشخصي IBM PC، حيث تم تأسيس الجمعية الدولية لمحققي الكمبيوتر الجنائي، كما استضاف مكتب التحقيقات الفيدرالي (FBI) عام 1993 أول مؤتمر دولي للأدلة الحاسوبية بمشاركة ممثلين من 26 دولة، ما مهد لتأسيس المنظمة الدولية للأدلة الحاسوبية عام 1995 لتنسيق الجهود عالميًا. وقد ركزت الجهود في تلك الفترة على استعادة البيانات من الحواسيب المنفصلة في ظل ارتفاع تكلفة التخزين واعتياد المستخدمين على حذف البيانات وإعادة تهيئة الوسائط. كما ظهرت أنماط جديدة من الجرائم مثل الاختراق عبر الاتصال الهاتفي والاحتيال على شبكات الهاتف. ورغم ضعف الدعم المؤسسي وغياب المختبرات المتخصصة، فقد أسهمت هذه المبادرات الفردية والمنظمات المهنية الناشئة في إرساء الأسس الأولى لهذا المجال.

### (3-2-1) مرحلة النمو و التوسع (1995-2005)

شهدت هذه المرحلة نقلة نوعية في النمو المؤسسي والتقني للتحقيق الجنائي الرقمي، حيث أصبحت الحواسيب والهواتف المحمولة والإنترنت جزءا لا يتجزأ من الحياة اليومية، وهو ما انعكس على طبيعة

الجرائم والأدلة الرقمية. تميزت هذه الفترة بانتقال الممارسات من جهود فردية إلى عمل منظم تقوده الوكالات الحكومية والمنظمات المهنية، مع ظهور تخصصات فرعية جديدة مثل تحليل الأجهزة المحمولة والوسائط المتعددة مما رسخ الاعتراف بالأدلة الرقمية كفرع معتمد من العلوم الجنائية. أما على مستوى الأدوات، فقد تطورت من تطبيقات الأوامر البسيطة إلى برامج متكاملة بواجهات رسومية مثل EnCase وFTK، إلى جانب مساهمات المجتمعات مفتوحة المصدر مثل Autopsy. وبذلك اصبحت هذه الحقبة مرحلة انتقالية نحو التخصص والاعتماد الرسمي في مجال التحقيق الجنائي الرقمي.

### (1-2-4) مرحلة التطور (2005 – الوقت الحالي)

تميزت هذه المرحلة بتوسع غير مسبوق في حجم الأدلة الرقمية وتنوعها، حيث اعترفت المحاكم بالمعلومات الرقمية كأدلة رسمية. كما أصبح التحقيق الرقمي مسارا مهنيا معتمدًا و مدعوم ببرامج أكاديمية وشهادات متخصصة. كما تطورت طبيعة المواد فأصبح كل جهاز تقريبا يحتوي على وسائط تخزين رقمية، مع انتشار الشبكات السلكية واللاسلكية، وظهور خدمات الإنترنت والبرمجيات السحابية. وبدأت منصات التواصل الاجتماعي مثل فيسبوك وتويتر في التأثير على طرق جمع الأدلة الرقمية، فيما أصبح البريد الإلكتروني مصدر رئيسي للمعلومات القضائية.

أما على مستوى الأدوات، فقد انتقلت ادوات التحقيق مثل EnCase وFTK إلى بيئة المؤسسات والشبكات، وأصبحت تُستخدم في الأمن المؤسسي وعمليات الاكتشاف الإلكتروني. كما جرى تكييفها للعمل في بيئات المختبرات الافتراضية (مثل VMware) وشبكات التخزين (SANs). وقد أتاح استخدام الشبكات عالية السرعة دعم مراجعة الأدلة عن بُعد من قبل المحققين والمدعين. وقد تطورت أدوات التحقيق الجنائي الرقمي لتصبح أسرع وأكثر دقة بفضل الأتمتة، مما سهّل التعامل مع كميات كبيرة من البيانات وتحديد الأدلة المهمة بسرعة. كما بدأ الاهتمام بالاعتماد الرسمي ووضع معايير للجودة لضمان موثوقية النتائج أمام المحاكم، وبرزت الحاجة إلى معايير دولية موحدة للتعاون بين الدول في مواجهة الجرائم الرقمية العابرة للحدود.

## (1-3) أهمية التحقيق الجنائي في مكافحة الجرائم الالكترونية

بسبب الطفرة الكبيرة في استخدام تقنيات المعلومات والاتصالات وما نتج عنها من أنماط جديدة للجرائم الإلكترونية. فقد باتت الأجهزة الرقمية وشبكات الإنترنت من الأدوات الأساسية في الحياة اليومية، لكنها في الوقت ذاته شكلت بيئة خصبة لجرائم الكترونية وبالتالي لم يعد بالإمكان الاعتماد على الوسائل التقليدية وحدها، بل برزت الحاجة إلى التحقيق الجنائي الرقمي كوسيلة علمية لكشف هذه الجرائم والتعامل مع آثارها. تكمن أهمية التحقيق الرقمي كالتالي:

1. **التعامل مع الجرائم الالكترونية الحديثة**: أدى التطور المتسارع في التكنولوجيا إلى ظهور أنماط جديدة من الجرائم، مثل سرقة الهوية التي تستغل البيانات الشخصية بطرق غير قانونية، والمطاردة الإلكترونية التي تهدد الأفراد عبر الرسائل أو المنصات الرقمية، إضافة إلى برمجيات الفدية (Ransomware) التي تشفر بيانات الضحايا مقابل دفع مبالغ مالية. هذه الجرائم يصعب كشفها بالطرق التقليدية لأنها تعتمد على تقنيات التخفي والاختراق، وهو ما يجعل التحقيق الجنائي الرقمي الوسيلة الأساسية لمواجهتها وتوثيقها بشكل قانوني.

2. **استخدام الأدلة الرقمية كجزء أساسي في التحقيقات:** ، لم يعد بالإمكان الاستغناء عن الأدلة الرقمية اذ أصبحت جزء لا يتجزأ من التحقيقات الجنائية . فالمعلومات المخزنة في الحواسيب والهواتف الذكية ووسائط التخزين تمثل مصدر غني بالدلائل التي يمكن أن تربط المشتبه بهم بالجرائم. هذه البيانات الرقمية توفر قيمة عالية في عملية الإثبات أمام القضاء، لكونها قادرة على توضيح الأنشطة الإلكترونية التي قام بها الجاني، وبالتالي تعزيز قوة الأدلة في القضايا الجنائية.

3. **تتبع الأنشطة الالكترونية:** يعتمد التحقيق الجنائي الرقمي على سجلات الدخول والمعاملات الرقمية التي تعد من أهم مصادر الأدلة. هذه السجلات تمكّن المحققين من إعادة بناء مسار الأحداث الرقمية من خلال تتبع العمليات التي قام بها المستخدم على الأنظمة المختلفة. فهي تكشف محاولات الدخول غير المشروع، وتوضح هوية المشتبه بهم، وتسهم في تحديد التوقيتات الدقيقة للأحداث. ومن خلال هذه العملية المنهجية، يصبح بالإمكان ربط النشاطات الإلكترونية مباشرة بالأشخاص المتورطين في الجريمة.

4. **القيمة القضائية للأدلة الالكترونية:** تُعد الأدلة الرقمية ذات أهمية بالغة في الإجراءات القضائية، لكن قبولها أمام المحاكم يتطلب الالتزام الصارم بمعايير علمية دقيقة ، وهذا القبول مرتبط بجمع الأدلة بطرق سليمة وحفظها وفق ضوابط تضمن سلامة سلسلة الحيازة (Chain of Custody)، مما يضفي عليها الموثوقية اللازمة للاستخدام القانوني.

## (4-1) المبادئ الأساسية للتحقيق الجنائي الرقمي

إن تناول المبادئ الأساسية للتحقيق الجنائي الرقمي يقتضي عرضها ضمن إطار منهجي منظم يبين أبعادها الرئيسة. لذا جرى تقسيمها إلى ثلاثة محاور أساسية تتضمن الفروع التي توضح مجالات التخصص، ومصادر الأدلة الرقمية التي تحدّد أماكن الحصول عليها، والإجراءات القياسية التي تضمن جمعها وتحليلها وتقديمها وفق معايير علمية وقانونية كما سيتم توضيحه في الفقرات التالية:

### (1-4-1) فروع التحقيق الجنائي الرقمي

تُعَد فروع التحقيق الجنائي الرقمي أحد المرتكزات الرئيسة لفهم هذا المجال، إذ يوضح كل فرع منها جانب محدد من عملية التعامل مع الأدلة الرقمية و تعكس طبيعة العمل الميداني ويبين كيفية التعامل مع كل نوع من البيانات. وفيما يلي أبرز هذه الفروع:

**أولا: التحقيق في الشبكات (Network Forensics)**

يعنى بمراقبة وتحليل حركة مرور الشبكات لاكتشاف محاولات التسلل أو جمع الأدلة القانونية. بخلاف غيره من الفروع، يتعامل هذا المجال مع بيانات متطايرة وسريعة الزوال، مما يتطلب تقنيات استباقية لاعتراض حزم البيانات وحفظها للتحليل لاحقًا. يُستخدم هذا الفرع لتحديد كيفية وقوع الاختراق، ورصد الأطراف المسؤولة عنه، وضمان تتبع سلسلة الأدلة بدقة لتقديمها أمام القضاء.

**ثانيا: التحقيق في الأقراص (Disk Forensics)**

يركز على استخراج البيانات من وسائط التخزين مثل الأقراص الصلبة، وحدات USB، الأقراص الضوئية، وبطاقات الذاكرة. يشمل هذا الفرع عدة مراحل:

1. التعرف على وسائط التخزين المضبوطة في مسرح الجريمة.
2. الاستحواذ على نسخة طبق الأصل باستخدام أدوات التصوير الجنائي (Bit-stream).
3. التحقق من مطابقة النسخة مع الأصل عبر خوارزميات الهاش.
4. الحفظ الآمن للأدلة الأصلية وإنشاء نسخ إضافية للتعامل معها.
5. التحليل للبحث في الملفات المحذوفة، والسجلات، والكوكيز، وسجل التصفح.
6. إعداد التقرير الذي يوضح النتائج بشكل مبسط ودقيق قابل للفهم من غير المتخصصين.

**ثالثاً: التحقيق في الأجهزة المحمولة (Mobile Device Forensics)**

يتضمن التحقيق في الأجهزة المحمولة استعادة الأدلة الرقمية من الهواتف النقالة في ظل ظروف جنائية سليمة باستخدام أساليب معتمدة. يشمل التحقيق في الأجهزة المحمولة تحليل كل من شرائح SIM وذاكرة الهاتف، حيث يتطلب كل منهما إجراءات مختلفة. وعلى عكس التحقيقات الجنائية للحواسيب، يتعامل التحقيق في الهواتف المحمولة مع أنظمة اتصال مدمجة (مثل GSM) وآليات تخزين خاصة. غالبا ما تركز التحقيقات على البيانات البسيطة مثل سجلات المكالمات ووسائل الاتصال بدلاً من الاستعادة المتعمقة للبيانات المحذوفة.

**رابعاً: التحقيق في قواعد البيانات (Database Forensics)**

يقصد به فحص قواعد البيانات وما يرتبط بها من بيانات وصفية (Metadata) و يهدف إلى التحقق من الطوابع الزمنية وتاريخ التعديلات على الجداول، وتحديد المعاملات التي قد تدل على أنشطة غير قانونية

مثل الاحتيال. كما يهتم بسلامة السجلات وأصالتها، ويُعد أداة مهمة لضمان الشفافية ومساءلة مستخدمي قواعد البيانات.

**خامساً: التحقيق في الطابعات والماسحات الضوئية (Printer and Scanner Forensics)**

يُستخدم لتحديد الطابعات أو الماسحات الرقمية التي استُعملت في إنتاج وثائق مزورة أو مواد مطبوعة مرتبطة بأنشطة إجرامية أو إرهابية. يعتمد هذا التحقيق على الخصائص المميزة لكل جهاز مما يتيح ربط الوثيقة المطبوعة بجهاز معين، وهو أمر بالغ الأهمية في تتبع عمليات التزوير.

**سادساً: التحقيق في الذاكرة (Memory Forensics)**

يتعامل مع البيانات المخزنة في ذاكرة الحاسوب (RAM). هذا النوع من التحقيق يكشف عن أنشطة خفية لا تُسجل على الأقراص، مثل البرامج الضارة التي تعمل بصورة مؤقتة. لذا يُعتبر أداة مهمة لفهم الهجمات السيبرانية والتعامل مع التهديدات التي لا تترك أثرا دائم.

### (2-4-1) مصادر الأدلة الرقمية

الأدلة الرقمية يمكن أن تنشأ من مجموعة متنوعة من المصادر، كل منها يوفر معلومات بالغة الأهمية يمكن أن تُفيد في التحقيقات والملاحقات القضائية. وفيما يلي أهم هذه المصادر:

**أ. أنظمة الحاسوب (Computer Systems)**

يمكن أن تُشكل أنظمة الحاسوب ومكوناتها مصدر رئيسي للأدلة الرقمية. ومن أبرز هذه العناصر:

1. المكونات المادية (Hardware)
2. المكونات البرمجية (Software)
3. البريد الإلكتروني والمرفقات
4. قواعد البيانات
5. سجل التصفح ويشمل المواقع التي تم زيارتها من قبل المستخدم.
6. سجلات النظام و المحادثات
7. الوثائق والصور.
8. البيانات المخزنة على الأجهزة الخارجية مثل الأقراص الصلبة الخارجية ووسائط USB.
9. معلومات التعريف وتشمل البيانات الوصفية (Metadata) والمعرّفات المرتبطة بالنظام.

**ب. الأجهزة المحمولة (Portable Devices)**

الأجهزة المحمولة باليد تمثل أيضا مصادر مهمة للأدلة الرقمية حيث قد تحتوي هذه الأجهزة على تطبيقات برمجية، وثائق، رسائل بريد إلكتروني، تاريخ تصفح الإنترنت، سجلات محادثة، قوائم

الأصدقاء، صور، ملفات وسائط، قواعد بيانات، وسجلات مالية تشكل أدلة مهمة في التحقيق. ومن هذه الأجهزة:

1. الهواتف المحمولة والذكية (Mobile Phones and Smartphones) بما تحويه من سجلات مكالمات، رسائل نصية، وبيانات تطبيقات.
2. المساعدات الرقمية الشخصية (PDAs) كأحد أشكال الحواسيب المحمولة المبكرة.
3. أجهزة الوسائط الرقمية مثل مشغلات MP3 والفيديو المحمولة.
4. أجهزة تحديد المواقع (GPS Receivers) التي تخزن بيانات المواقع.
5. الكاميرات الرقمية (Digital Cameras) التي تحفظ الصور والفيديوهات.

**جـ. وسائط التخزين (Storage Devices)**

تخزن وسائط التخزين كميات ضخمة من المعلومات التي قد تكون أساسية في التحقيقات، مثل:

1. الأقراص الصلبة والأقراص الخارجية
2. الوسائط القابلة للإزالة (Removable Media) مثل الأقراص المدمجة (CDs)، أقراص الفيديو الرقمية (DVDs)
3. وحدات التخزين المحمولة وبطاقات الذاكرة المستخدمة في الكاميرات والهواتف الذكية.

**د. الأجهزة الطرفية (Peripheral Devices)**

تعزز الأجهزة الطرفية من وظائف الحاسوب، ويمكن أن تشكل مصدر مهم للأدلة. ومن أمثلتها:

1. الطابعات والماسحات الضوئية (Printers and Scanners) التي تخزن معلومات عن المستندات المطبوعة أو الممسوحة أو المرسلة بالفاكس.
2. أجهزة الفاكس (Fax Machines) التي تنقل المستندات إلكترونيًا.
3. وحدات التخزين الخارجية.
4. لوحات المفاتيح والفأرة التي قد تحتوي على أدلة فيزيائية مثل بصمات الأصابع أو الحمض النووي DNA.
5. المعلومات المخزنة في هذه الأجهزة مثل أرقام الهواتف والفاكسات أو المستندات المطبوعة والممسوحة التي من الممكن أن تكون بالغة الأهمية في التحقيق.

**هـ. الشبكات الحاسوبية (Computer Networks)**

تربط الشبكات الحاسوبية عدة أنظمة وأجهزة وهي تمثل بيئة غنية بالأدلة. ومن عناصرها:

1. الحواسيب المربوطة بالشبكة.

2. الأجهزة الطرفية المرتبطة.
3. أجهزة توجيه البيانات (Routers Switches Hubs).
4. المعلومات الشبكية (Network Information): مثل البرمجيات، المستندات، الصور، رسائل البريد الإلكتروني، المرفقات، قواعد البيانات، البيانات المالية، سجل التصفح، سجلات الدخول، سجلات الأحداث، سجلات المحادثة وغيرها من المعلومات الخاصة بالشبكات.
5. معلومات التعريف (Identifying Information) مثل عناوين IP، عناوين الشبكة المحلية LAN، عناوين MAC، وعناوين NIC المرتبطة بالأجهزة.

### (1-4-3) الإجراءات القياسية للتحقيق الجنائي الرقمي

أنّ مصادر الأدلة الرقمية التي تم ذكرها في الفقرة السابقة تحدد (أين) يمكن العثور على الدليل الرقمي وبالتالي يبرز محور اخر يوضّح (كيف) تُدار عملية التعامل مع هذا الدليل ضمن مسار منظم يضمن سلامته وقابليته للاعتماد القانوني. لذلك تعد الإجراءات القياسية للتحقيق الجنائي الرقمي بمثابة الإطار المنهجي الذي يربط بين تنوع المصادر الرقمية من جهة وبين متطلبات التوثيق والتحقق من جهة أخرى، بما يضمن أن يُنجزالتحقيق وفق ضوابط فنية وقانونية. ووفقاً للمعهد الوطني للمعايير والتكنولوجيا (NIST)، تُدار عملية التحقيق الرقمي ضمن أربع مراحل مترابطة تمثل دورة العمل الأساسية للتحقيق، وهي: الجمع (Collection) والفحص (Examination) والتحليل (Analysis) والتقرير (Reporting)؛ وتهدف هذه المراحل إلى ضبط انتقال الدليل من لحظة تحديده واستلامه إلى لحظة عرض النتائج، مع المحافظة على توثيق الإجراءات وتقليل احتمالات الخطأ أو الطعن في موثوقية الدليل. وسيتم تفصيل آليات التنفيذ والتقنيات والأدوات العملية المرتبطة بهذه المراحل بصورة مفصلة في الفصل الثالث.

## (1-5) التحديات القانونية والأخلاقية في التحقيقات الرقمية

التعامل مع الأدلة الرقمية يثير مجموعة من التحديات القانونية والأخلاقية التي يجب أخذها بعين الاعتبار. فالأدلة الرقمية لا تُقبل في المحكمة إلا إذا جُمعت وحُفظت وفق معايير صارمة، كما أنّ المحققين مطالبون بالالتزام بمواثيق النزاهة واحترام خصوصية الأفراد. و بالتالي يمكن تلخيص التحديات القانونية في التحقيقات الرقمية بالتالي:

1. **السلامة الجنائية:** ويقصد به بقاء الدليل كاملًا دون تعديل نتيجة الفحص أو النقل. ويتحقق ذلك عبر العمل على نسخة طبق الأصل بدلاً من الأصل، مع توثيق أي تغيير يطرأ، والالتزام بالقوانين وعدم القيام بأعمال تتجاوز خبرة المحقق.

2. **اصالة الأدلة الرقمية:** من أبرز التحديات القانونية التي تواجه التحقيقات الرقمية مسألة إثبات الأصالة والسلامة للأدلة. فالمحكمة لا تكتفي بمجرد تقديم ملف أو بيانات، بل تشترط أن يكون الدليل حقيقيا وأن يظل دون تغيير منذ لحظة جمعه وحتى عرضه. ولضمان ذلك يُستخدم ما يُعرف بـ البصمة الرقمية (Hash Value) عبر خوارزميات مثل MD5 أو SHA، التي تولد قيمة فريدة تمثل محتوى الملف، فإذا أعيد حسابها لاحقًا وظهرت مطابقة فهذا دليل على عدم تغيير البيانات.

3. سلسلة الحيازة (Chain of Custody): وهي من أهم الجوانب للحفاظ على أصالة الأدلة الرقمية وسلامتها، وتعتبر سجل رسمي يوثق جميع المراحل التي مرّ بها الدليل الرقمي منذ لحظة جمعه من مسرح الجريمة الرقمية، مروراً بعمليات الفحص والتحليل، وحتى تقديمه إلى الجهة القضائية المختصة. وتُستخدم هذه السلسلة لإثبات انتقال ملكية الدليل الرقمي بين الجهات المختلفة، كما تُعد مرجع للتحقق من سلامة الأدلة عند عرضها في المحكمة. وفي حال غياب سلسلة الحيازة، يمكن الادعاء بأن الأدلة قد تم العبث بها أو تغييرها أو التعامل معها بصورة غير صحيحة. ويمكن القول ان الهدف الأساسي من سلسلة الحيازة هو ضمان عدم التلاعب بالدليل الرقمي وإثبات أن الدليل بقي محفوظاً بشكل قانوني طوال فترة التحقيق.

ويجب أن تتضمن سلسلة الحيازة المعلومات التالية:

1. وصف الدليل الرقمي نوع الجهاز، السعة التخزينية، الرقم التسلسلي إن وجد.
2. مكان وتاريخ جمع الدليل مع تسجيل الوقت بدقة.
3. اسم الشخص الذي قام بجمع الدليل وتوقيعه الرسمي.
4. الأدوات المستخدمة في الجمع مثل أدوات حجب الكتابة أو برامج النسخ الجنائي.
5. سجل انتقال الدليل أي انتقال الدليل من شخص إلى آخر، مع ذكر السبب.
6. تاريخ ووقت كل عملية فحص أو تحليل مع اسم المحلل الرقمي.
7. حالة الدليل هل هو مغلق، مختوم، أو مفتوح للفحص.

مثال توضيحي

عند ضبط قرص صلب من جهاز مشتبه به:

- يتم تسجيل وقت الضبط.
- يوضع القرص داخل حقيبة مخصصة ويُغلق بختم رسمي.
- يُسجَّل اسم الشخص الذي استلمه وعند نقله إلى المختبر، يتم تسجيل وقت الاستلام واسم المستلم.

أي نقص في هذه البيانات قد يؤدي إلى رفض الدليل قانونياً.

اما بالنسبة للتحديات الأخلاقية فيمكن تلخيصها كالتالي:

1. احترام خصوصية الأفراد وعدم فحص البيانات غير المرتبطة بالقضية.
2. الالتزام بالنزاهة وتجنب تضارب المصالح أثناء التحقيق.
3. المحافظة على سرية المعلومات الحساسة التي يتم جمعها.
4. تقديم الشهادة الفنية أمام المحكمة بصدق وحيادية.
5. إثبات العلاقة السببية بين النشاط الرقمي وصاحبه قبل توجيه الاتهام.

رقم التمرين: 1 الزمن المخصص: 3 ساعات
اسم التمرين: فحص وتحليل عينات مشبوهة باستخدام VirusTotal
مكان التنفيذ: مختبر الحاسوب

**اولاً: الاهداف التعليمية**

بعد إتمام هذا التمرين، سيتمكن الطالب من:

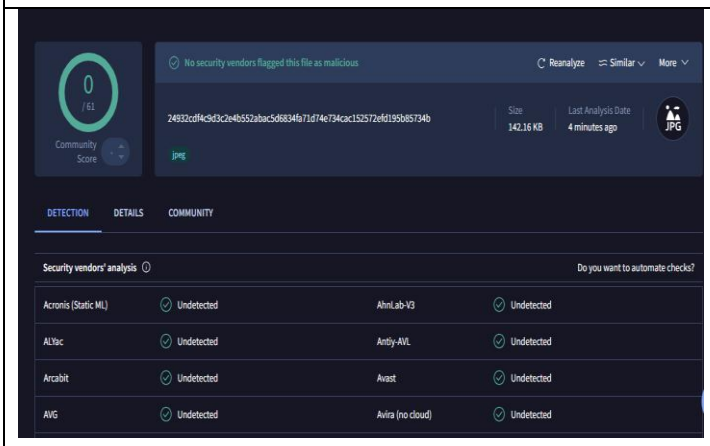
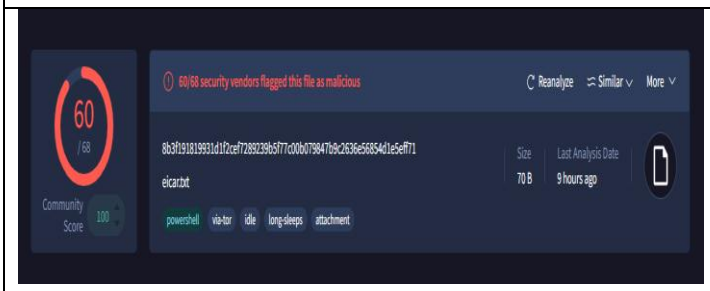
- استخدام موقع VirusTotal وقراءة تقرير الفحص (نسبة الكشف، أسماء المحركات، الهاش).
- تفسير معنى نتائج الفحص واتخاذ حكم أولي (آمن / مريب) استنادًا إلى نسبة الكشف وسلوكيات التقرير
- اقتراح خطوات استجابة أولية عند اكتشاف سلوك شبكي مريب (عزل جهاز، جمع الأدلة، حظر اتصالات مشبوهة)

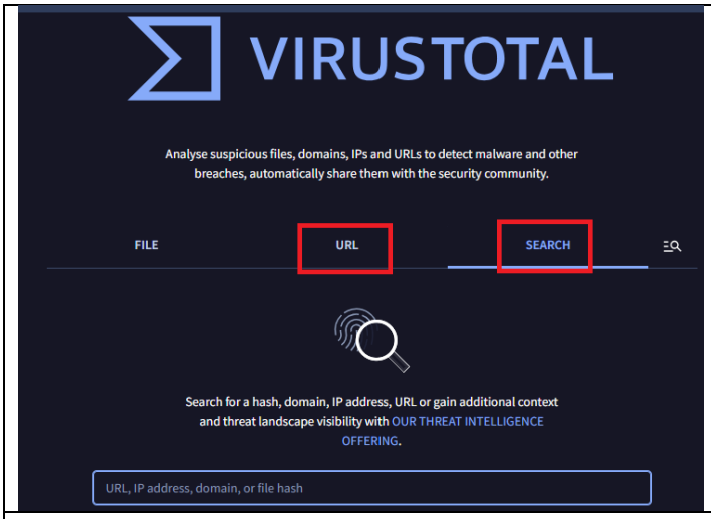
**ثانياً: التسهيلات التعليمية**

- اجهزة حاسوب مع نظام تشغيل Windows 10/11.
- اتصال بالإنترنت.

**ثالثاً: خطوات تنفيذ التمرين**

| | | |
|---|---|---|
| 1 | افتح الحاسوب ثم افتح المتصفح وانتقل إلى العنوان التالي: https://www.virustotal.com<br><br>عند فتح الصفحة ستظهر لك واجهة VirusTotal الرئيسية: تبويبات File / URL / Search وشريط رفع الملفات مثل الموضح في التمرين. |  |

| | | |
|---|---|---|
| 2 | من التبويب (File) قم بتحميل ملف في حاسوبك من خلال (Choose File) |  |
| 3 | اذا كان الملف أمن سوف يظهر من عبارة انه لم تُصنِّف أيّ من مزوِّدي برامج الحماية هذا الملف على أنّه خبيث |  |
| 4 | أ. من نفس التبويب قم بتحميل ملف يحتوي على معلومات مشبوهة (هذا الملف مُعدّ للأغراض التعليمية فقط ولا يحتوي على أي برمجيات ضارة فعلية)، ثم اضغط Enter<br>**ب.** لاحظ عزيزي الطالب أن 60 من أصل 68 برنامج حماية صنّف الملف كخبيث، وهذا يوضّح ان الملف غير أمن |  |

| | | |
|---|---|---|
| 5 | من خلال التبويب (URL) أو (Search) يمكن التحقق من روابط الويب والنطاقات (domains) وعناوين الـIP والهاش (hash) لاكتشاف البرمجيات الخبيثة والانتهاكات الأخرى. |  |
| | **المناقشة**<br>- ماذا تعني نتيجة الفحص (مثلاً 61/0 أو 68/60)؟<br>- متى يتم البحث عن الهاش (Hash) بدلاً من رفع الملف؟<br>- لو أظهر التقرير سلوكاً شبكياً مريباً: ما الخطوات العملية التي يجب اتباعها؟ | |
| | **نشاط**<br>سجّل دخولك إلى منصة (Threat Connect) وأنشئ حالة جديدة، (SHA256 أو نطاق أو IP أو URL) وشغّل عملية التحليل.<br>التقط لقطة شاشة للنتائج وأرفقها مع ملخّص يحدد إن كان المؤشر آمنًا أم مريبًا واذكر الإجراء العملي الأول المقترح. | |

**الأمن السيبراني لم يعد خيارًا، بل هو خط الدفاع الذي يحمي المجتمع،**

**والمرأة فيه ليست مشاركة فقط... بل صانعة أمانٍ وثقةٍ للمستقبل**

| **استمارة قائمة الفحص** | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: فحص وتحليل عينات مشبوهة باستخدام VirusTotal رقم التمرين:**1** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل وتشغيل الحاسوب والوصول الى المتصفح. | %10 | | |
| 2 | رفع الملف إلى VirusTotal | %10 | | |
| 3 | توثيق النتائج من خلال التقاط لقطات شاشة او حفظ رابط التقرير | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

رقم التمرين: 2 الزمن المخصص: 3 ساعات
اسم التمرين: تهيئة أداة Autopsy وإنشاء حالة تحقيق رقمية
مكان التنفيذ: مختبر الحاسوب

**اولاً: الاهداف التعليمية**

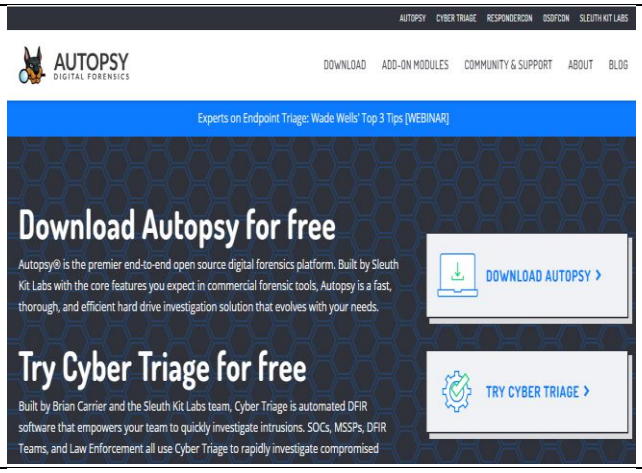
بعد إتمام هذا التمرين، سيتمكن الطالب من:

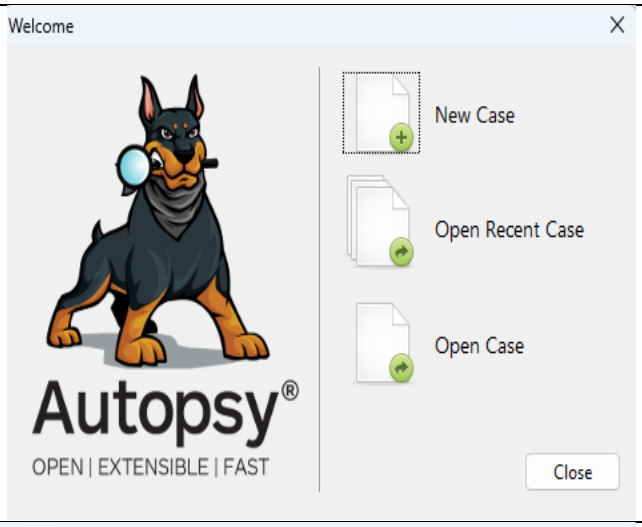
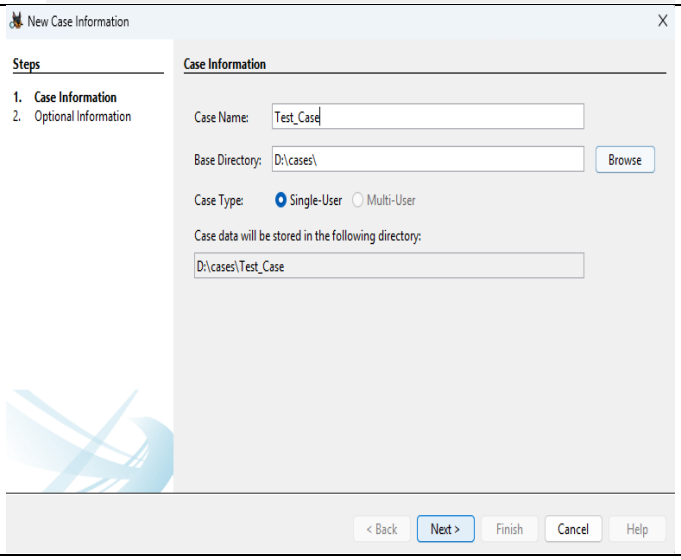
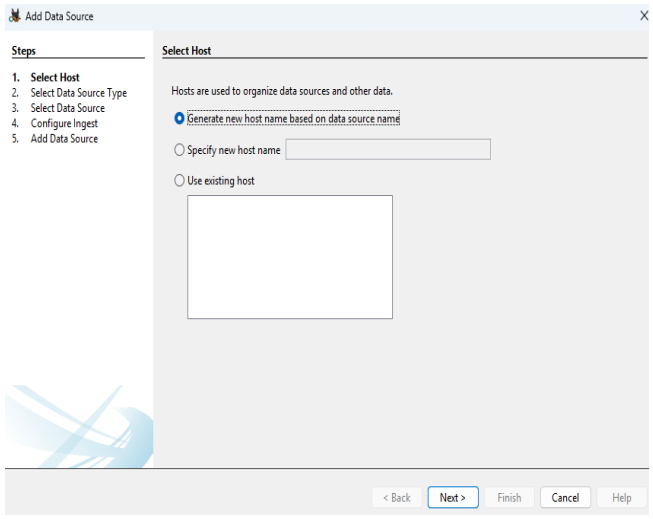
- تثبيت أداة Autopsy وتهيئتها لإنشاء حالة تحقيق رقمية جديدة.
- استكشاف واجهة البرنامج والتعرف على أقسامها ووظائفها الأساسية.
- تنفيذ فحص أولي بسيط وإنتاج تقرير مبدئي حول البيانات المضافة.

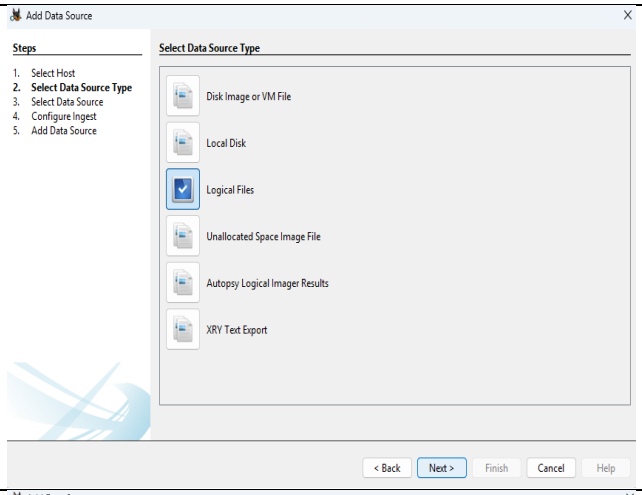
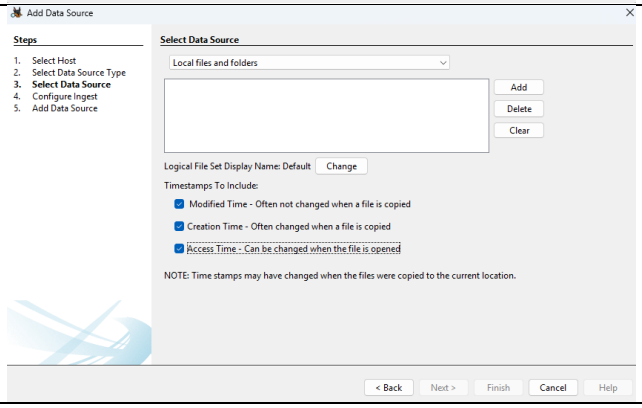
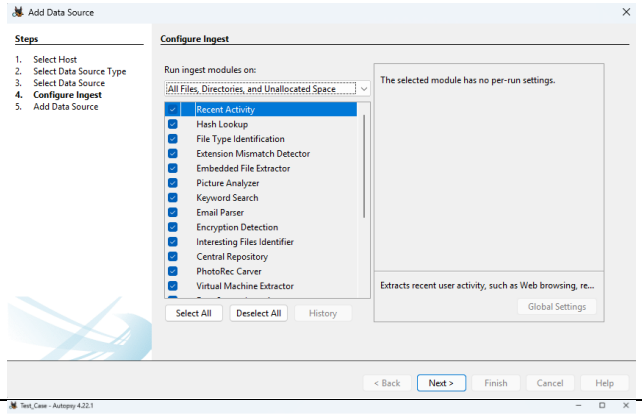
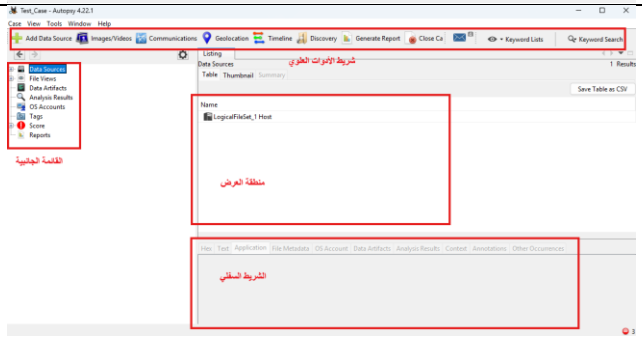
**ثانياً: التسهيلات التعليمية**

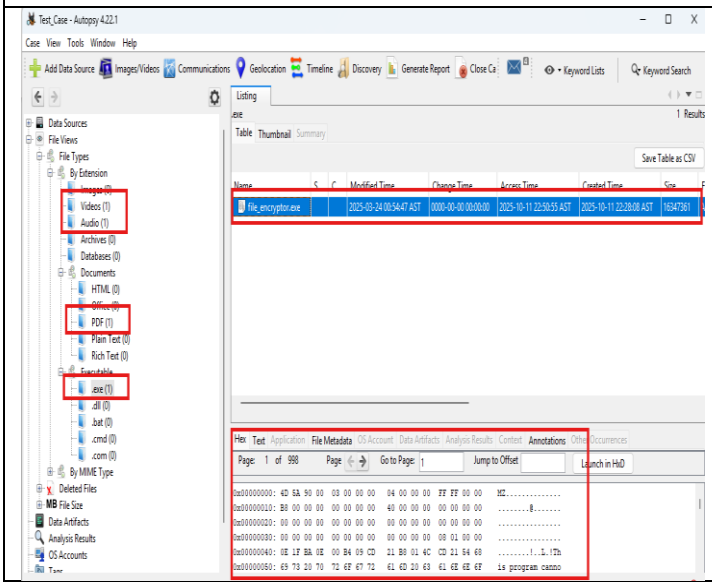
- جهاز كمبيوتر بنظام تشغيل Windows (لتثبيت Autopsy).
- اتصال بالإنترنت لتحميل البرنامج.
- ملفات بيانات تجريبية (نصوص أو صور) لاستخدامها كمصدر بيانات داخل التمرين.

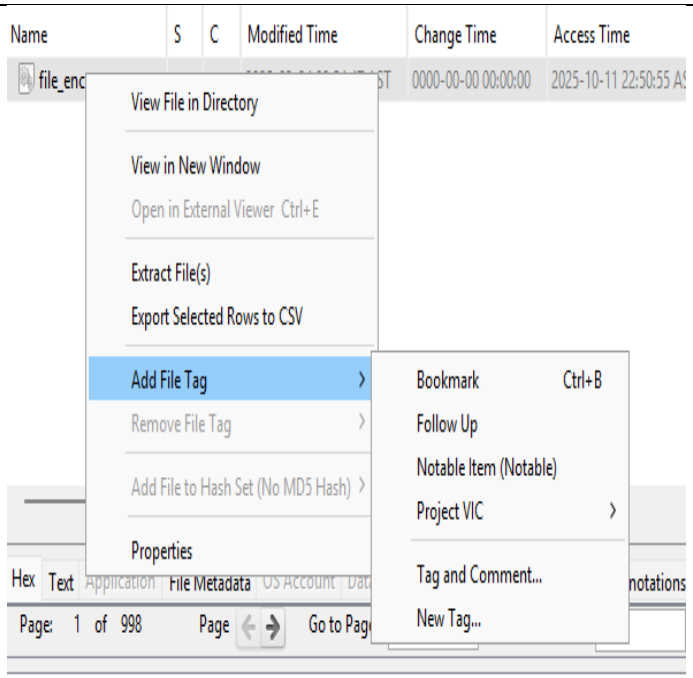
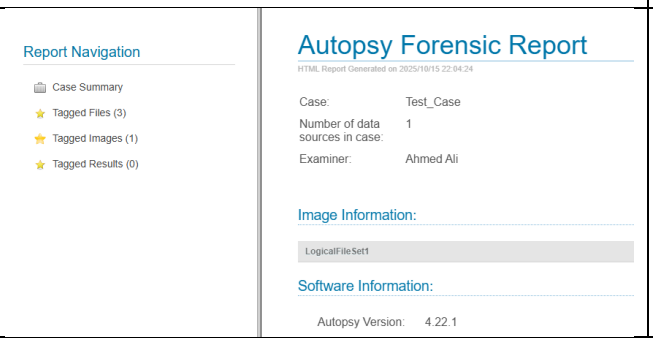
**ثالثاً: خطوات تنفيذ التمرين**

| | | |
|---|---|---|
| 1 | قم بتحميل البرنامج من الموقع الرسمي https://www.autopsy.com/<br><br>قم بالنقر على ( Free download) اي تحميل مجاني. |  |
| 2 | بعد النقر على ( download autopsy) اختر النسخة الخاصة بنظام الوندوز وقم بتحميلها ثم اتبع خطوات التثبيت. |  |

| | | |
|---|---|---|
| 3 | فتح Autopsy واختيار New Case لإنشاء مشروع جديد. |  |
| 4 | إدخال اسم المشروع (مثل: Test_Case) واختيار مجلد حفظه. |  |
| 5 | • تُستخدم نافذة Select Host لتحديد أو إنشاء اسم للمصدر الذي تُضاف منه البيانات داخل القضية مثل قرص صلب او جهاز محمول او غيرها.<br>• في الحالة الافتراضية يكون الخيار " Generate new host name based on data source name" مفعّلًا لإنشاء اسم مصدر جديد تلقائيًا، أما إذا وُجد مصدر سابق فيمكن اختيار "Use existing host" لإضافة البيانات إليه مباشرة، يُعد هذا ضروريًا عند وجود عدة أجهزة ضمن نفس التحقيق |  |

| | | |
|---|---|---|
| 6 | تُستخدم نافذة Select Data Source Type لتحديد نوع مصدر البيانات الذي يراد تحليله داخل أداة Autopsy.<br>فيها يختار المستخدم ما إذا كان يريد فحص صورة قرص ( Disk Image)، أو قرصًا فعليًا في الحاسوب (Local Disk)، أو ملفات منطقية (Logical Files) مثل مجلد يحتوي على ملفات نصية أو صور. |  |
| 7 | من تبويب (Logical Files) نختار الملفات أو المجلدات المراد تحليلها داخل البرنامج، وذلك عبر زر (Add) لإضافة البيانات. كما يمكن من (Timestamp) تحديد الاختيارات المدرجة معرفة وقت (الإنشاء، التعديل، الوصول) التي تساعد في تتبع نشاط الملفات أثناء التحقيق الرقمي. |  |
| 8 | تُستخدم نافذة ( Configure Ingest) لتحديد وحدات الفحص التي سيُشغّلها البرنامج لتحليل البيانات، مثل تتبع النشاط الأخير أو تحديد نوع الملفات. يُنصح بترك الإعدادات الافتراضية مفعّلة لإجراء فحص شامل واستخراج الأدلة تلقائيًا. |  |
| 9 | عند الانتهاء من الاعدادات السابقة سوف تظهر بيئة العمل الرئيسية التي تتكون من:<br>1. القائمة الجانبية: التي تحتوي على اقسام التحليل الأساسية مثل مصدر البيانات و استعراض الملفات و البيانات داخل المصدر وتحديد حالة البيانات (سيئة او مشتبه بها) من خلال الفحص المبدئي بالإضافة الى العديد من الخيارات التحليلية |  |

| | | |
|---|---|---|
| | 2. شريط الأدوات العلوي: يضم خيارات سريعة مثل إضافة مصدر بيانات، عرض الصور والفيديو، إنشاء التقارير، الخط الزمني (Timeline)، وغيرها من أدوات الفحص.<br>3. منطقة العرض: تُعرض فيها تفاصيل القسم المحدد مثل الملفات، الأدلة، أو نتائج التحليل<br>4. الشريط السفلي: يحتوي على تبويبات فرعية مثل Hex، Text، Application، File Metadata لعرض تفاصيل الملف المختار بشكل دقيق. | |
| **10** | تُظهر هذه النافذة نتائج التحليل داخل برنامج Autopsy، حيث يمكن رؤية الملفات التي تم العثور عليها مثل ملفات الفيديو والصوت وملفات PDF والبرامج التنفيذية (.exe).<br>عند اختيار ملف معيّن، تظهر تفاصيله في الجدول مثل تاريخ الإنشاء والتعديل والحجم، أما في الأسفل فتُعرض محتويات الملف بالصيغة الثنائية (Hex) لمراجعة البيانات . |  |

| | | |
|---|---|---|
| 11 | تُظهر هذه النافذة عند النقر بالزر الأيمن على أحد الملفات المختارة، وتُستخدم لإضافة وسوم (Tags) أو ملاحظات على الملفات أثناء التحليل.<br>من خيار Add File Tag يمكن وضع علامة مثل Bookmark لحفظ الملف المهم، أو Follow Up لمراجعته لاحقًا، أو Notable Item لتمييزه كدليل مهم في التحقيق.<br>تساعد هذه الميزة في تنظيم الأدلة وتصنيفها ليسهل الرجوع إليها عند إعداد التقرير النهائي. |  |
| 12 | من خلال تبويب ( Generate Report) يمكن انشاء تقرير عن الدليل الرقمي يمكن استخدامه لاحقا كمرجع للقضية |  |
| 13 | المناقشة<br>• ما الفرق بين Case و Data Source في Autopsy؟<br>• ما المعلومات التي يمكن استخراجها من الملفات بعد الفحص؟<br>• كيف يساعد برنامج Autopsy في تنظيم الأدلة الرقمية داخل التحقيق؟<br>• ما أهمية الطوابع الزمنية (Timestamps) في التحقيق الرقمي؟<br>• متى نستخدم خيار Add File Tag، وما فائدته في إدارة الأدلة؟ | |
| 14 | نشاط<br>افتح برنامج EnCase وأنشئ قضية جديدة (Case) ثم أضف مصدر الأدلة (Evidence) وابدأ التحليل عبر تحديد ملف مشتبه وعرض خصائصه. التقط لقطة شاشة تُظهر نتائج التحليل داخل EnCase ثم أرفق اللقطة مع ملخص قصير يوضح إن كان الدليل طبيعيًا أم مريبًا ولماذا، مع ذكر الإجراء العملي الأول المقترح (عزل، حظر، تصعيد، أو توسيع الفحص). | |

| **استمارة قائمة الفحص** | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: : تهيئة أداة Autopsy وإنشاء حالة تحقيق رقمية | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | فتح البرنامج و إنشاء Case جديد وإضافة مصدر بيانات (Data Source) | %5 | | |
| 2 | تحديد نوع مصدر البيانات واختيار اعدادات الفحص لبدأ التحليل | %10 | | |
| 3 | تحليل الملفات واستعراض خصائصها وإضافة وسوم Tags | %15 | | |
| 4 | انشاء تقرير نهائي للقضية | %10 | | |
| 6 | المناقشة | %5 | | |
| 7 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## اسئلة الفصل الاول

س1: عرف ما يأتي:

التحقيق الجنائي الرقمي – سلسلة الحيازة – السلامة الجنائية – البصمة الرقمية

س2: وضح باختصار المراحل التاريخية لتطور التحقيق الجنائي الرقمي.

س3: وضح أهمية التحقيق الجنائي الرقمي في مكافحة الجرائم الالكترونية.

س4: ما المقصود بالتحقيق في الأقراص؟ و ما المراحل التي يتضمنها؟

س5: ما هي المعلومات التي يجب ان تتضمنها سلسلة الحيازة؟

س6: ما التحديات الأخلاقية في التحقيقات الرقمية؟

س7: املأ الفراغات التالية بما يناسبها:

1. يُعدّ الكاتب _____ أول من نبّه لإمكان استخدام المعلومات الرقمية كأدلة جنائية في كتابه الجريمة بالحاسوب.
2. لتحقق من مطابقة النسخة مع الأصل في التصوير الجنائي تُستخدم خوارزميات _____ و _____ لإنتاج قيمة الهاش.
3. في التحقيق بالأجهزة المحمولة، يُحلَّل كلٌّ من _____ و _____ بوصفهما مصدرين مهمَّين للأدلة.
4. تُسهم الأدلة الرقمية في دعم القرار عبر الإجابة عن أسئلة جوهرية مثل _____ و _____ و _____ و _____.
5. من أمثلة مصادر الأدلة الرقمية: _____، _____، _____، _____، و_____.

# الفصل الثاني
# ادوات وتقنيات التحقيق الجنائي الرقمي

## 1-2 الادوات البرمجية للتحقيق الرقمي

مع التقدم الكبير في مجال التكنولوجيا وانتشار استخدام الحواسيب والهواتف الذكية والإنترنت، ظهرت أنواع جديدة من الجرائم تُعرف بالجرائم الإلكترونية. هذه الجرائم لا تترك آثارًا ملموسة مثل الجرائم التقليدية، بل تكون أدلتها مخزنة داخل الأجهزة الرقمية. لذلك ظهر علم التحقيق الرقمي الذي يهتم بالبحث عن الأدلة الإلكترونية وتحليلها. ويعتمد هذا العلم بشكل أساسي على أدوات برمجية متخصصة تساعد في كشف الحقيقة بطريقة علمية وقانونية. وتُعد الأدوات البرمجية للتحقيق الرقمي من أهم الوسائل الحديثة في مكافحة الجرائم الإلكترونية.

**ويمكن تعريف الأدوات البرمجية للتحقيق الرقمي** على انها برامج حاسوبية لجمع الأدلة الرقمية، تحليلها، حفظها، والتأكد من سلامتها دون تغيير. ويستخدمها المحقق الرقمي للكشف عن المعلومات المخفية أو المحذوفة داخل الأجهزة الإلكترونية، وتكون على انواع:

**أ- أدوات جمع الأدلة الرقمية:** تُستخدم هذه الأدوات لأخذ **نسخة مطابقة للأصل** من البيانات الموجودة في الحاسوب أو الهاتف دون التأثير على الدليل الأصلي. ومن أمثلتها:

**FTK Imager:** برنامج مجاني يُستخدم في **التحقيق الجنائي الرقمي** لعرض وجمع الأدلة الرقمية دون التلاعب بها. يتيح للمحقق فحص الأقراص الصلبة وملفات الحاسوب وإنشاء نسخ رقمية(Images) للأدلة مع الحفاظ على سلامتها لاستخدامها في التحقيقات والقضايا القانونية.

**EnCase Imager:** برنامج يُستخدم في **التحقيق الجنائي الرقمي** لعمل نسخة رقمية مطابقة تمامًا لوسائط التخزين مثل الأقراص الصلبة والفلاشات. يَضمن البرنامج الحفاظ على سلامة الأدلة الرقمية دون تعديل عليها، مما يسمح باستخدامها بشكل قانوني في التحقيقات وتحليل البيانات لاحقًا.

**أهمية هذه الأدوات:**

- الحفاظ على الدليل الأصلي.
- ومنع التلاعب بالبيانات.
- قبولها كدليل في المحكمة.

**ب- أدوات تحليل الملفات والأقراص:** تُستخدم لفحص البيانات المخزنة داخل الأجهزة، مثل الملفات والصور والمستندات والملفات المحذوفة، ومن أشهر هذه الأدوات Autopsy، FTK. وتساعد هذه الأدوات في:

- استرجاع الملفات المحذوفة.
- معرفة تاريخ إنشاء الملفات وتعديلها.
- تحليل نظام الملفات.

**جـ- أدوات التحقيق في الهواتف الذكية:** تُستخدم لاستخراج البيانات من الهواتف المحمولة مثل:الرسائل النصية، الصور والفيديوهات، سجلات المكالمات، تطبيقات التواصل الاجتماعي ومن أمثلتها Cellebrite، Oxygen Forensic.

**د- أدوات تحليل الشبكات والإنترنت:** تُستخدم لمعرفة ما يحدث أثناء الاتصال بلشبكات والإنترنت، مثل المواقع التي تم الدخول إليها والبيانات المرسلة والمستلمة ومن أشهر هذه الأدوات Wireshark.

**هـ- أدوات تحليل البريد الإلكتروني:** تُستخدم لفحص رسائل البريد الإلكتروني ومعرفة المرسل الحقيقي ومكان الإرسال وهل الرسالة مزورة أم لا ومن أمثلتها MailXaminer.

**و- أدوات التحقق من سلامة الأدلة الرقمية:** تُستخدم للتأكد من أن الدليل الرقمي لم يتم تغييره أو العبث به، وذلك باستخدام رموز خاصة تُسمى (Hash). ومن أمثلتها SHA، MD5.

وبهذا تلعب الأدوات البرمجية للتحقيق الرقمي دورًا أساسيًا في كشف الجرائم الإلكترونية وتحليل الأدلة الرقمية، حيث تساعد المحققين على الوصول إلى الحقيقة بطريقة علمية وقانونية. **وتكمن أهميتها في النقاط الآتية:**

**1- الحفاظ على سلامة الأدلة الرقمية** :تضمن هذه الأدوات جمع الأدلة دون التلاعب بها أو تغيير محتواها، مما يحافظ على مصداقيتها عند استخدامها في التحقيقات والقضايا القانونية.

**2- استخراج البيانات المخفية أو المحذوفة** :تمكّن المحقق من استرجاع الملفات المحذوفة والبيانات المخفية التي قد تكون دليلاً مهمًا في كشف الجريمة.

**3- تسريع عملية التحقيق** :تساعد الأدوات البرمجية على فحص كميات كبيرة من البيانات بسرعة ودقة، مما يوفر الوقت والجهد مقارنة بالطرق التقليدية.

**4- تحليل الأجهزة ووسائط التخزين المختلفة** :تتيح فحص الحواسيب، الهواتف الذكية، الأقراص الصلبة، والفلاشات، مما يجعلها شاملة لمختلف مصادر الأدلة الرقمية.

**5- تقديم تقارير دقيقة ومنظمة** :تقوم هذه الأدوات بإعداد تقارير مفصلة وواضحة تُستخدم من قبل الجهات القضائية لفهم مجريات التحقيق بسهولة.

**6- دعم التحقيقات القانونية** :تساعد على تقديم الأدلة الرقمية بشكل قانوني معتمد، مما يعزز فرص إثبات الجريمة ومحاسبة الجناة.

وعند استخدام الأدوات البرمجية للتحقيق الرقمي يجب الالتزام بمجموعة من القواعد لضمان **سلامة الأدلة ومصداقية التحقيق**، ومن أهم هذه القواعد:

1- **عدم العمل على الدليل الأصلي** :العمل دائمًا على نسخة رقمية للحفاظ على سلامة الأدلة.

2- **توثيق جميع خطوات التحقيق** :تسجيل كل خطوة من جمع وتحليل الأدلة بالتفصيل.

3- **استخدام أدوات معتمدة وموثوقة** اختيار برامج معترف بها قانونيًا مثل FTK Imager وEnCase.

4- **الالتزام بالقوانين والأنظمة** :احترام حقوق الخصوصية والقوانين المحلية والدولية أثناء التحقيق.

5- **التحليل الدقيق والمنهجي** :فحص الأدلة بطريقة منظمة لتجنب الأخطاء وضمان مصداقية النتائج.

ان اتباع هذه القواعد يضمن أن يكون التحقيق الجنائي الرقمي **موثوقًا، قانونيًا، وفعالًا**، ويحمي الأدلة من أي تلاعب أو فقدان.

يتضح مما سبق أن الأدوات البرمجية للتحقيق الرقمي تلعب دورًا مهمًا وأساسيًا في كشف الجرائم الإلكترونية ومكافحتها في العصر الحديث. فهي تساعد على جمع وتحليل الأدلة الرقمية بطريقة علمية ودقيقة، مع الحفاظ على سلامة البيانات ومنع أي تلاعب فيها. هذا الأمر يجعل هذه الأدوات مقبولة قانونيًا كأدلة في المحاكم، مما يسهم في تحقيق العدالة وحماية المجتمع من الجرائم التقنية.

ومع التطور المستمر في التكنولوجيا وزيادة استخدام الأجهزة الرقمية والإنترنت، تزداد أهمية هذه الأدوات بشكل أكبر وأصبح الاعتماد عليها ضرورة لا غنى عنها. لذلك من المهم للمختصين في الأمن الرقمي تعلم كيفية استخدامها بكفاءة ومسؤولية. كما أن هذه الأدوات تساعد على فهم أساليب الجرائم الإلكترونية واكتشافها قبل وقوعها. وفي النهاية، يمكن القول إن التحقيق الرقمي ليس مجرد تقنية، بل هو علم قائم بذاته يجمع بين المعرفة التقنية والقانونية، ويعد من المجالات الحديثة والمهمة التي سيكون لها دور كبير في المستقبل في حماية المجتمع ومواجهة التحديات الرقمية الجديدة.

**كل جهاز متصل بالإنترنت يحتاج إلى أمن سيبراني، لأن الخطر اليوم لا يطرق الباب... بل يدخل عبر الشبكة**

رقم التمرين: 3 الزمن المخصص: 3 ساعات

**اسم التمرين:** استخدام اداة Autopsy لتحليل بيانات الاجهزة.

**مكان التنفيذ:** مختبر الحاسوب

## اولاً: الاهداف التعليمية:

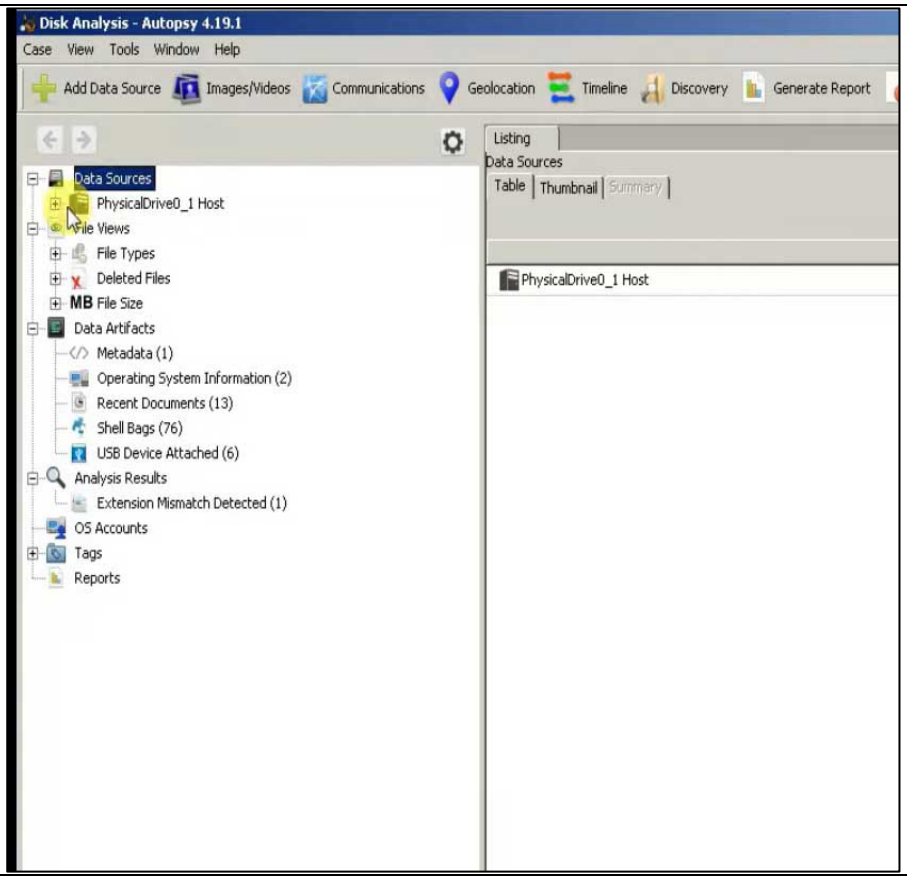
**بعد اتمام هذا التمرين، سيتمكن الطالب من:**

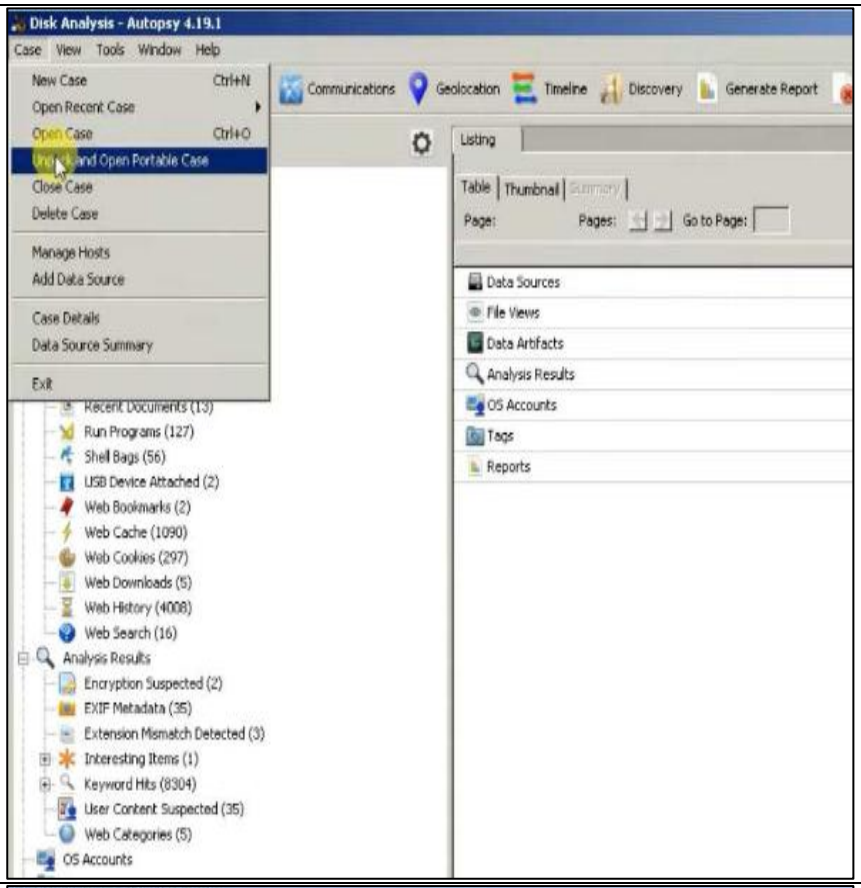
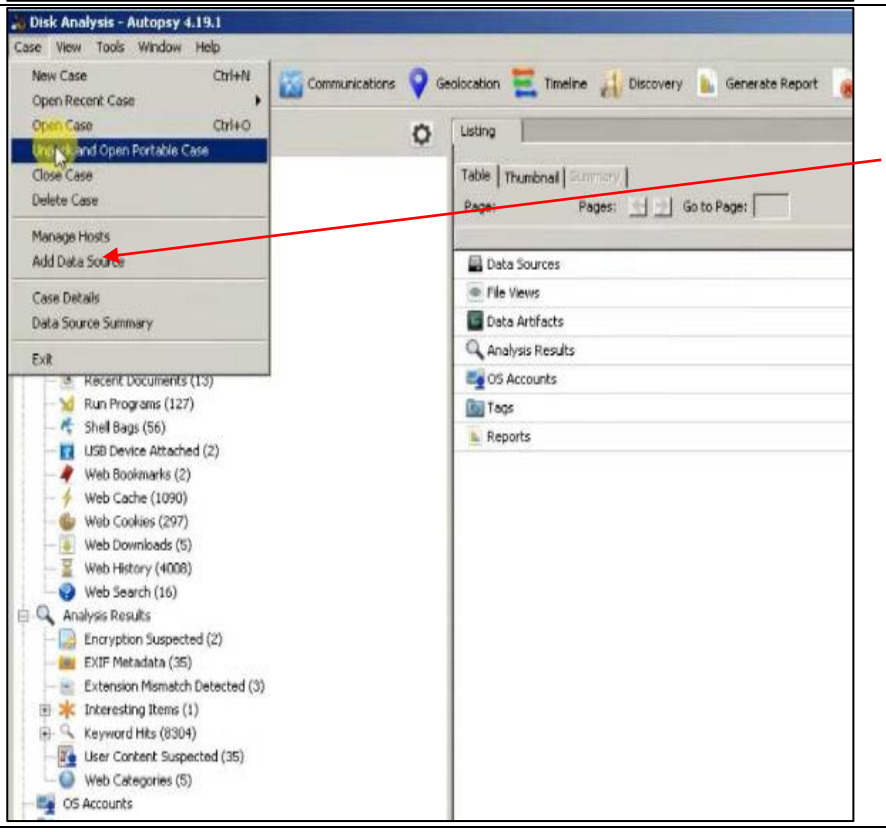
- التعرف على كيفية استخدام أداة Autopsy في التحقيق الرقمي، وفهم طريقة تحليل بيانات الأجهزة الإلكترونية واستخراج الأدلة الرقمية بطريقة صحيحة.

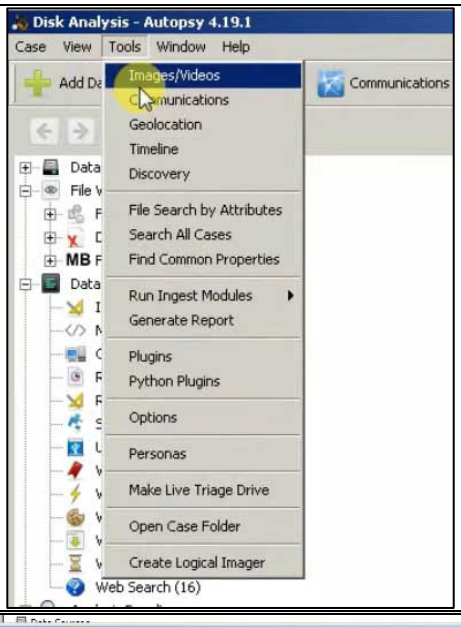
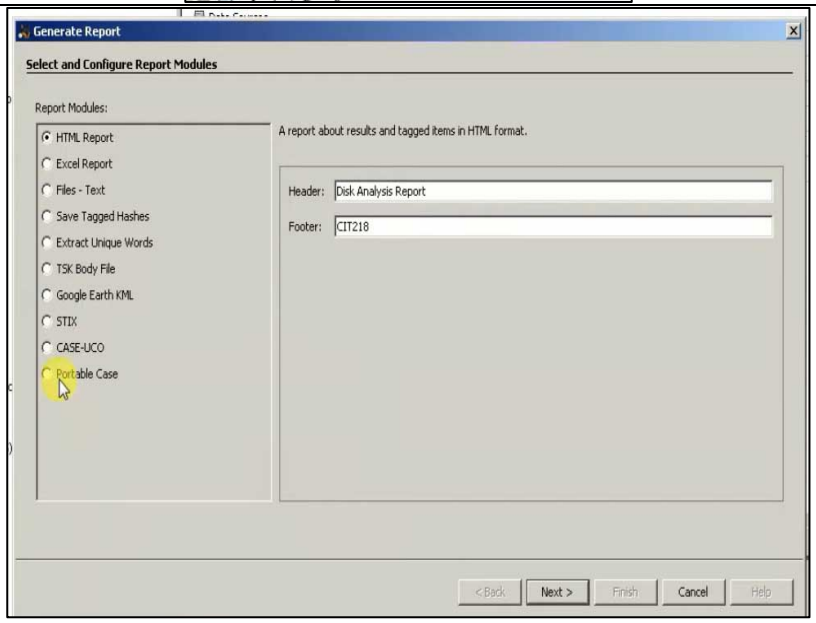
## ثانياً: التسهيلات العلمية:

- جهاز حاسوب.
- برنامج Autopsy مثبت على الجهاز وملف تجريبي (صورة أو مجلد يحتوي على

## ثالثاً: خطوات تنفيذ التمرين:

| | | |
|---|---|---|
| 1 | ارتداء بدلة العمل ثم: نقوم بفتح برنامج Autopsy على الحاسوب حيث تظهر الواجهة الرئيسية للبرنامج. |  |

| | | |
|---|---|---|
| 2 | نقوم بإنشاء قضية جديدة (New Case):<br>- نضغط على خيار **Create New Case.**<br>- نحدد اسم القضية ومكان حفظها على الجهاز.<br>- نضغط على **Next** للانتقال للخطوة التالية. |  |
| 3 | نقوم بإضافة مصدر البيانات: (Add Data Source) ونختار نوع البيانات (قرص، صورة قرص، أو مجلد) ثم نحدد موقع البيانات المراد تحليلها ونضغط على **Next**. |  |

| | | |
|---|---|---|
| 4 | نقـــوم بأختيـــار وحـدات التحليـل ونحـــدد وحـــدات التحليـل المطلوبـة مثل:<br>-اســـــــترجاع الملفات المحذوفة.<br>- تحليل الصور.<br>- تحليل التواريخ.<br>- نضـــغط علـــى **Finish** لبـدء التحليل. |  |
| 5 | نعـــرض نتـــائج التحليـل وننتظـر حتـــى ينتهـــي البرنـــامج مـــن التحليل ثم نقوم بمراجعـة الملفـات والمجلـــــــدات الظـاهرة ونلاحـظ الملفـات المحذوفـة أو المشـــــبوهة ونقوم بعمل تقرير نهائي عن ذلك. |  |
| 6 | نقوم بأستخراج الأدلة ونحدد الملف المطلوب ثم نقوم بحفظ نسخة منه في مجلد خاص بالأدلة وندوّن اسم الملف وتاريخه. |  |

| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: **استخدام اداة AutoPSY لتحليل بيانات الاجهزة.**<br>رقم التمرين:**3** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## 2-2 استرجاع الملفات المحذوفة

تُعد الحواسيب من أهم مصادر الأدلة الرقمية في التحقيقات الجنائية الحديثة، نظرًا لاعتماد الأفراد والمؤسسات عليها في تخزين ومعالجة المعلومات. ومع تزايد الجرائم الإلكترونية، أصبح حذف الملفات من أكثر الأساليب استخدامًا لإخفاء الأدلة الرقمية. غير أن عملية الحذف في أنظمة التشغيل لا تعني دائمًا زوال البيانات بشكل نهائي. وقد أتاح التطور في مجال الأدلة الرقمية الجنائية إمكانية استعادة هذه الملفات باستخدام أساليب وأدوات متخصصة. ويعتمد نجاح عملية الاستعادة بشكل أساسي على نوع وسيط التخزين المستخدم داخل الحاسوب، ولا سيما الأقراص الصلبة من نوع HDD وSSD .

وتُعرَّف استعادة الملفات المحذوفة في مجال الأدلة الرقمية الجنائية بأنها **عملية فنية وتقنية تهدف إلى إعادة الوصول إلى البيانات الرقمية التي تم حذفها أو فقدانها من وسائط التخزين الإلكترونية، باستخدام أدوات وأساليب متخصصة، مع الحفاظ على سلامة الدليل الرقمي ومنع التلاعب به.**

ولا تعني عملية الحذف في معظم أنظمة التشغيل إزالة البيانات فعليًا من وسيط التخزين، بل تعني غالبًا حذف المؤشر الذي يدل على موقع الملف داخل نظام الملفات، مما يسمح بإمكانية استعادته قبل أن يتم استبداله ببيانات جديدة. وتُعد هذه العملية من الركائز الأساسية في التحقيق الجنائي الرقمي لما لها من دور كبير في كشف الأدلة المخفية وربطها بالأحداث الجنائية.

اما بالنسبة لآلية حذف ملف معين من الذاكرة فتتم كالاتي:

يقوم نظام التشغيل بإزالة المرجع الخاص به من جدول نظام الملفات، بينما تبقى البيانات نفسها مخزنة فعليًا على القرص. وتُصنَّف هذه المساحة على أنها مساحة غير مخصصة قابلة لإعادة الاستخدام. ويستفيد المحقق الجنائي الرقمي من هذه الخاصية لإعادة قراءة البيانات المحذوفة قبل أن تتم الكتابة فوقها، وهو ما يشكّل الأساس العلمي لعملية الاستعادة، وبشكل عام يمكن تقسيم عملية الاستعادة حسب الجهاز الذي يتم حذف الملفات منه الى:

**اولاً: استعادة الملفات المحذوفة من الحاسوب:** يُعد الحاسوب المصدر الأهم للأدلة الرقمية، إذ يحتوي على مستندات نصية، صور، مقاطع فيديو، سجلات تصفح، وبرامج.

وتتم عملية الاستعادة الجنائية وفق مراحل منظمة تهدف إلى الحفاظ على سلامة الدليل، **وهذه المراحل هي :**

- فصل وسيط التخزين عن الجهاز الأصلي.
- إنشاء نسخة رقمية طبق الأصل(Forensic Image).
- تحليل نظام الملفات.

- البحث في المساحات غير المخصصة.
- استخراج الملفات المحذوفة وتوثيقها

**وتقسم الاقراص الصلبة في الحاسوب الى قسمين مهمين هما:**

**1- الأقراص الصلبة التقليدية (HDD):** تعتمد أقراص HDD على **التخزين المغناطيسي** باستخدام أقراص دوّارة وأذرع ميكانيكية للقراءة والكتابة، وآلية الحذف في هذه الاقراص تتم وفق التالي:

- لا يتم مسح البيانات فعليًا عند الحذف.
- تبقى البيانات محفوظة حتى تتم الكتابة فوقها.
- يمكن استرجاع الملفات كاملة أو جزئيًا.

وبالتالي فأن الأهمية الجنائية لاستعادة الملفات من هاردات HDD:

- ارتفاع نسبة نجاح الاسترجاع.
- سهولة تحليل المساحات غير المخصصة.
- إمكانية استعادة ملفات قديمة.

**2- اقراص الحالة الصلبة (SSD):** تعتمد أقراص SSD على **ذاكرة فلاش إلكترونية** دون أجزاء ميكانيكية، مما يجعلها أسرع في الأداء لكنها أكثر تعقيدًا في التحقيق الجنائي، وآلية الحذف في هذه الاقراص تتم وفق التالي:

- استخدام أمر **TRIM**.
- مسح البيانات المحذوفة فعليًا خلال وقت قصير.
- انخفاض كبير في فرص الاسترجاع.

**اما أسباب صعوبة استعادة البيانات من أقراص SSD فهي:**

1- أمرTRIM : يقوم نظام التشغيل بإرسال أمر TRIM إلى القرص لإعلامه بأن البيانات لم تعد مستخدمة، فيقوم القرص بمسحها نهائيًا، مما يمنع استعادتها لاحقًا.

2- تقنية Wear Leveling: تعمل هذه التقنية على توزيع البيانات على خلايا الذاكرة بشكل متساوٍ، مما يجعل تتبع موقع البيانات الأصلي أمرًا بالغ الصعوبة في التحقيق الجنائي.

3- المسح التلقائي للخلايا: تقوم أقراص SSD بمسح الخلايا غير المستخدمة تلقائيًا لتحسين الأداء، مما يؤدي إلى اختفاء بقايا الملفات بسرعة.

4- التشفير المدمج: العديد من أقراص SSD تحتوي على تشفير مدمج، يجعل البيانات غير قابلة للقراءة دون مفاتيح التشفير الأصلية.

5- سرعة إعادة استخدام المساحة: بسبب سرعة الكتابة العالية، يتم استبدال البيانات المحذوفة بسرعة كبيرة، مما يقلل زمن بقائها القابل للاسترجاع.

والجدول ادناه يتضمن عناصر مقارنة تؤثر على عملية حذف واستعادة البيانات بين اقراص HDD واقراص SSD داخل الحاسوب:

| عنصر المقارنة | HDD | SSD |
|---|---|---|
| نوع التخزين | مغناطيسي | ذاكرة فلاش |
| طريقة الحذف | حذف المؤشر فقط | حذف فعلي للبيانات |
| أمر TRIM | غير مستخدم | مستخدم |
| بقاء البيانات | طويل نسبيًا | قصير جدًا |
| نسبة الاسترجاع | مرتفعة | منخفضة |
| الصعوبة الجنائية | منخفضة | مرتفعة |

اما بالنسبة للعوامل المؤثرة على سرعة ونجاح استعادة البيانات فهي:

- نوع القرص الصلب المستخدم.
- الزمن المنقضي منذ الحذف.
- استخدام الحاسوب بعد الحذف.
- حجم الملف المحذوف.
- نوع نظام الملفات.
- كفاءة أداة التحقيق الجنائي.
- وجود تشفير أو حماية.
- سرعة المعالج الدقيق وحجم الذاكرة المؤقتة.

**ثانياً: استعادة الملفات المحذوفة من الهاتف المحمول:** تُعد الهواتف المحمولة من أكثر الأجهزة حساسية لاحتوائها على بيانات شخصية مهمة، مثل الرسائل النصية، المكالمات، الصور، مواقع GPS ، وسجلات التطبيقات، ان آليات الاستعادة تشمل:

**أ- النسخ الاحتياطي**

- Android: Google Drive

- iOS: iCloud
- تُعد النسخ الاحتياطية أول وأبسط طريقة لاسترجاع الملفات المحذوفة.

**ب- تحليل الذاكرة الداخلية**

- استخدام أدوات التحقيق الجنائي الرقمي المتخصصة (مثل Cellebrite ، Dr.Fone).
- استخراج البيانات المنطقية والفيزيائية

**وبالنسبة لتحديات استرجاع الملفات في الهواتف المحمولة فهي:**

- **تشفير البيانات** :غالبية الهواتف الحديثة مشفرة افتراضيًا، مما يصعب فك التشفير دون كلمات المرور أو المفاتيح.
- **حذف نهائي بواسطة TRIM أو Garbage Collection**: بعض الهواتف تستخدم هذه الآليات لمسح البيانات بشكل دائم.
- **القيود التقنية** :اختلاف أنظمة Android وiOS ، وجود صلاحيات مطلوبة للوصول الكامل للذاكرة.

**اما بالنسبة لمميزات عملية استرجاع الملفات المحذوفة في الهواتف المحمولة فهي:**

- إمكانية استرجاع بعض الملفات بسهولة من النسخ الاحتياطية
- أدوات متخصصة يمكنها استخراج البيانات المفقودة أحيانًا حتى بعد الحذف

**ثالثاً: استعادة الملفات المحذوفة من الذواكر الخارجية:** تشمل الذواكر الخارجية:

- **USB Flash Drives.**
- **كروت الذاكرة (SD Card).**
- **الأقراص الخارجية المحمولة**.

وبالنسبة آليات الاستعادة من الذواكر الخارجية فهي:

- توصيل الذاكرة بالحاسوب
- استخدام برامج الاسترجاع الجنائي أو التجاري، مثل: Recuva، EaseUS Data Recovery.
- تحليل نظام الملفات: FAT32 ، exFAT، NTFS، وغيرها.
- البحث في المساحات غير المخصصة(Unallocated Space)
- استخراج الملفات وتوثيقها

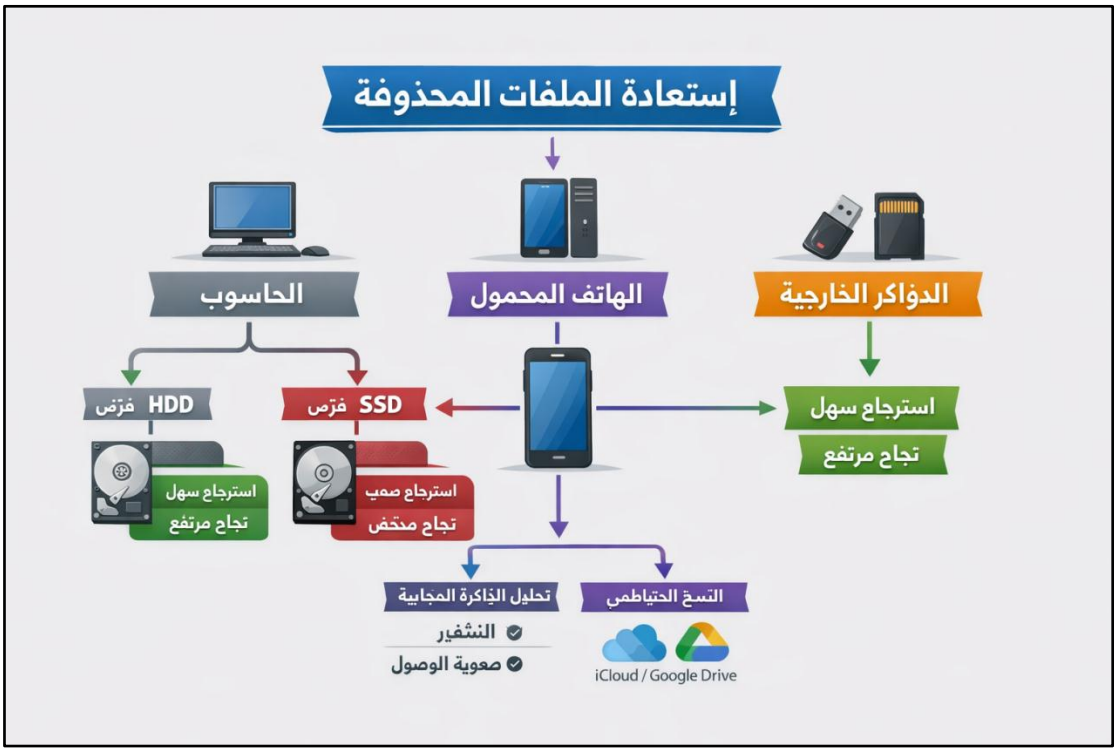
**وبالنسبة لتحديات استرجاع الملفات من الذواكر الخارجية فهي:**

- **التشفير** :بعض الكروت الخارجية الحديثة قد تكون مشفرة
- **استخدام متعدد** :إعادة الكتابة المتكررة تقلل فرص الاسترجاع
- **نوعية الذاكرة** :سرعة الكتابة وحجم الذاكرة تؤثر على استرجاع الملفات

**اما بالنسبة لمميزات عملية استرجاع الملفات المحذوفة من الذواكر الخارجية فهي:**

- سهولة التوصيل والفحص.
- نسبة استرجاع مرتفعة إذا لم تُستخدم الذاكرة بعد الحذف.

ان استعادة الملفات المحذوفة تُعد حجر الزاوية في مجال الأدلة الرقمية الجنائية، حيث يمكن أن تحتوي الملفات المحذوفة على معلومات حاسمة في كشف الجرائم. وقد أظهرت التجارب العملية أن نجاح الاسترجاع يعتمد على نوع الوسيط الرقمي، مع تفوق HDD والذواكر الخارجية في سهولة الاستعادة، بينما تمثل أقراص SSD والهواتف المحمولة تحديًا أكبر بسبب آليات الحذف والتشفير. ومن هنا تبرز أهمية **استخدام أدوات جنائية متقدمة وفهم خصائص كل وسيلة تخزين** لضمان استعادة الأدلة الرقمية بشكل صحيح، مما يعزز من القدرة على كشف الجرائم ودعم مسار العدالة.




الشكل (2-1) مخطط استعادة الملفات المحذوفة من وسائط التخزين المختلفة

يوضح الشكل اعلاه مخطط بصري للوسائط الرقمية المختلفة التي يمكن استعادة الملفات المحذوفة منها، مثل الحاسوب والهاتف المحمول والذواكر الخارجية.

في الحاسوب تم تقسيمه إلى نوعين من الأقراص: HDD وSSD ، حيث يبين المخطط أن استرجاع الملفات من HDD سهل ونسبة النجاح مرتفعة، بينما استرجاع الملفات من SSD صعب ونسبة النجاح منخفضة بسبب TRIM والتشفير وتقنيات توزيع البيانات.

أما الهاتف المحمول، فيوضح المخطط أن الاسترجاع يعتمد على النسخ الاحتياطية والتحليل المباشر للذاكرة، مع الإشارة إلى تحديات التشفير وصعوبة الوصول إلى البيانات.

وبالنسبة للذواكر الخارجية، يبين المخطط سهولة الاسترجاع وارتفاع نسبة النجاح إذا لم تُستخدم بعد الحذف.

يستخدم المخطط أسهمًا لتوضيح المسارات المختلفة لاسترجاع الملفات، مع رموز وصور للأجهزة لتسهيل الفهم البصري للطالب، يهدف المخطط إلى تقديم مقارنة واضحة بين وسائط التخزين المختلفة من حيث سهولة الاسترجاع والتحديات، مما يساعد المحقق الرقمي على فهم المخاطر والفرص أثناء التحقيق الجنائي.

**رقم التمرين: 4** **الزمن المخصص: 3 ساعات**

**اسم التمرين: توضيح كيفية استخدام FTK Imager لاسترجاع الملفات المحذوفة من القرص الصلب.**

**مكان التنفيذ: مختبر الحاسوب**

## اولاً: الاهداف التعليمية:

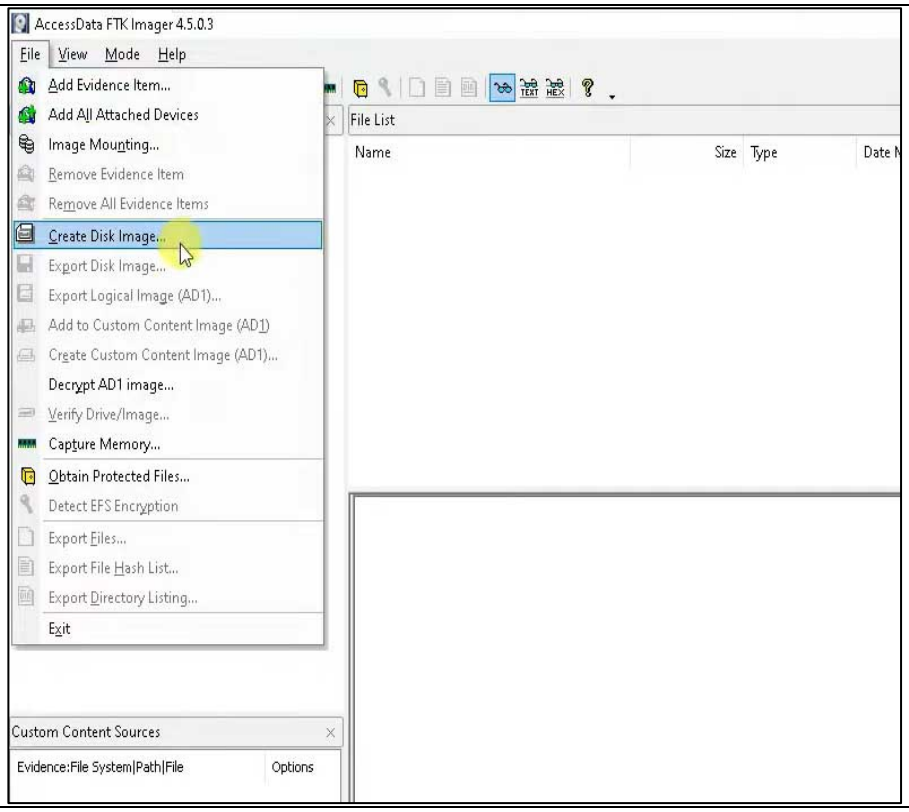
**بعد اتمام هذا التمرين، سيتمكن الطالب من:**

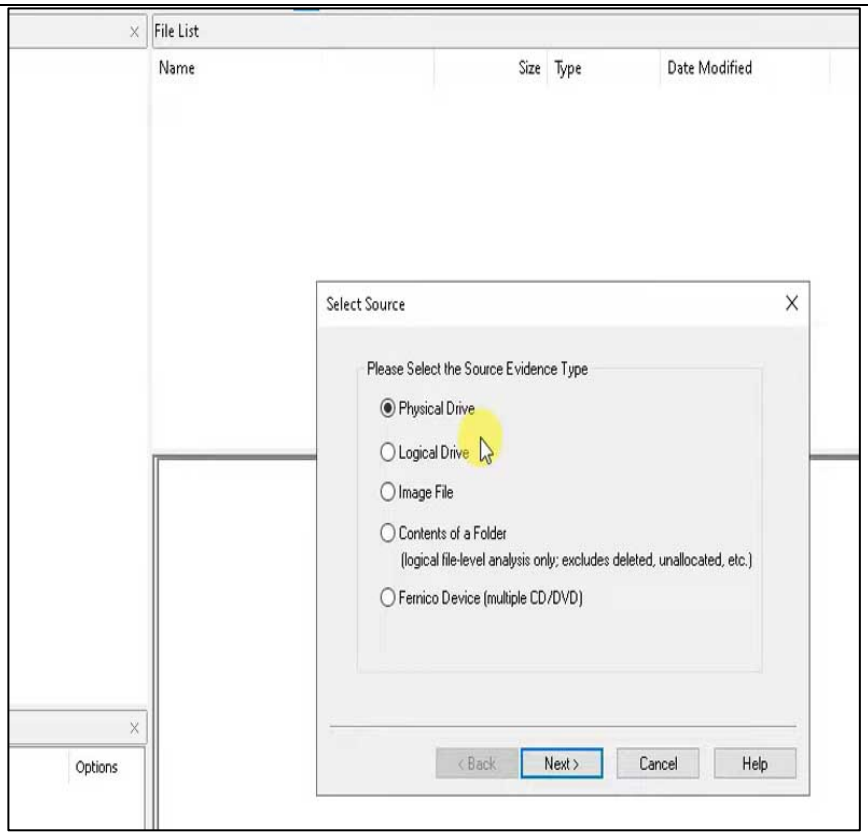
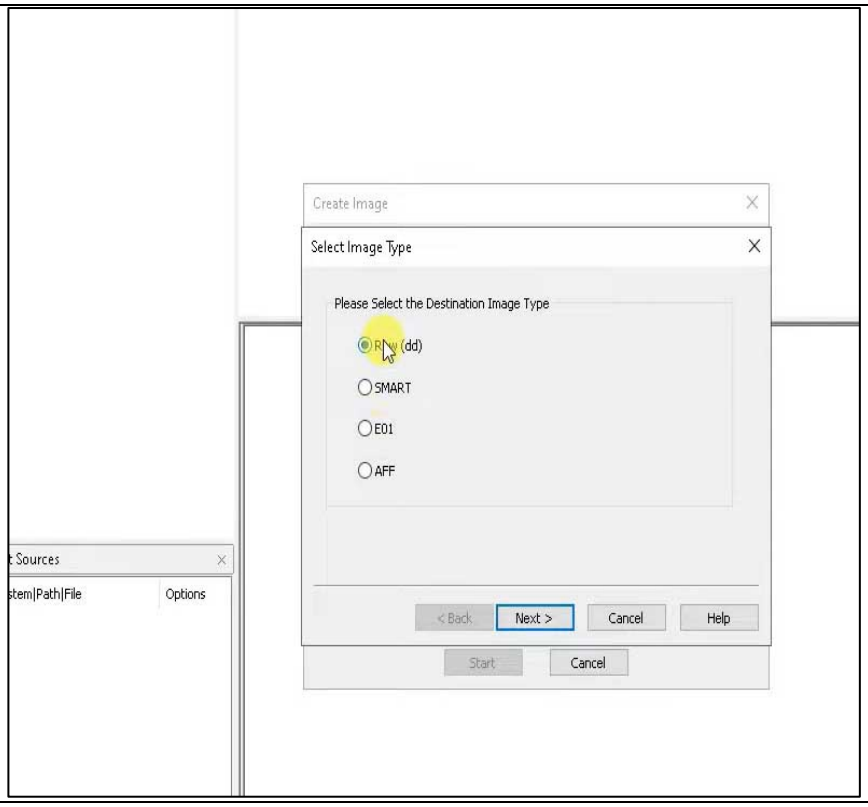
- **معرفة انشاء نسخة رقمية من القرص الصلب وفحص النسخة بأستخدام FTK Imager، تحديد الملفات المحذوفة واستخراجها وحفظها دون تغيير الادلة الاصلية.**

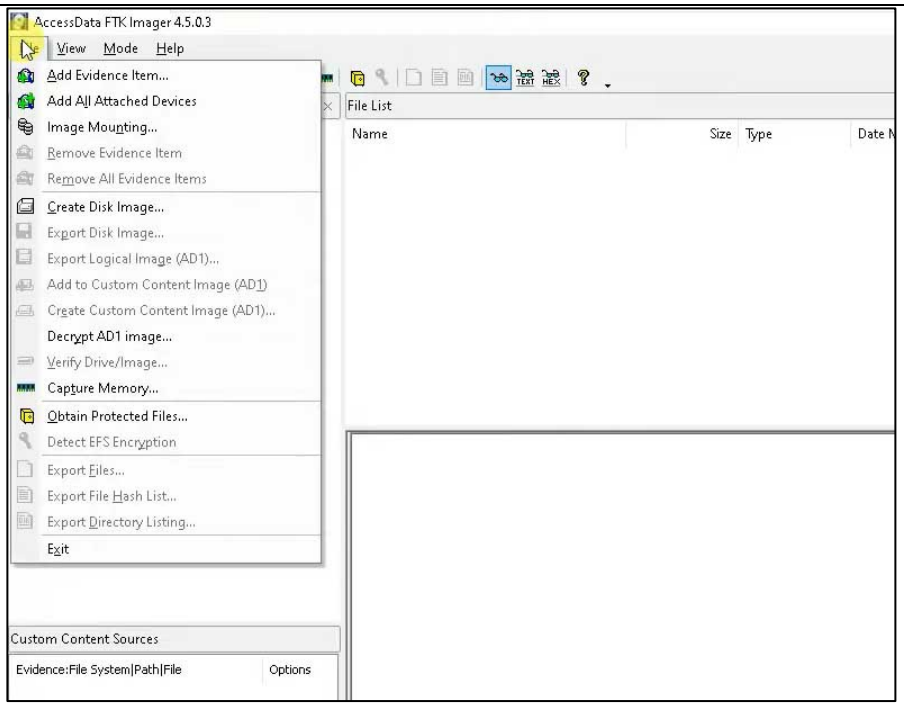
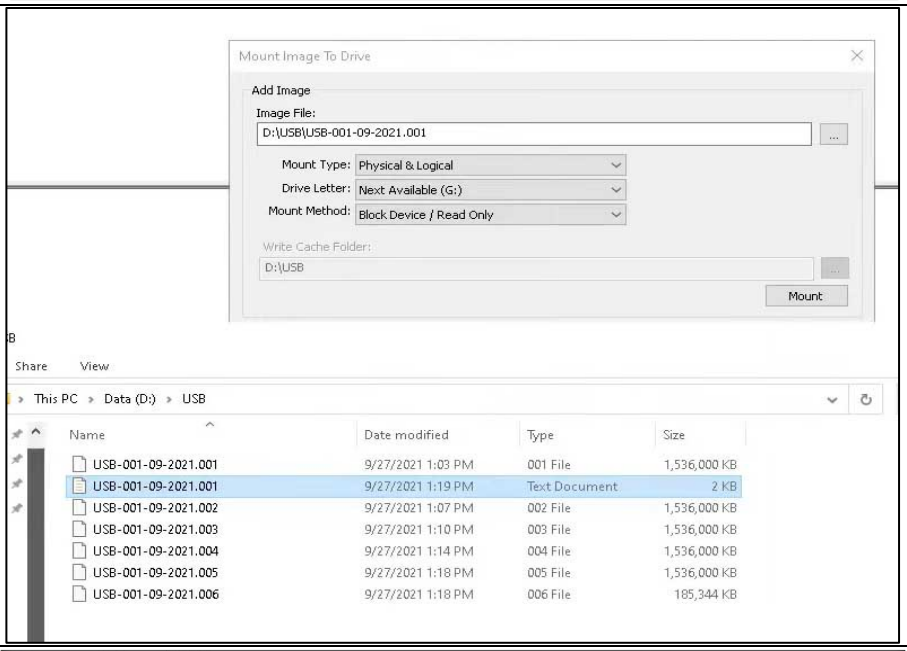
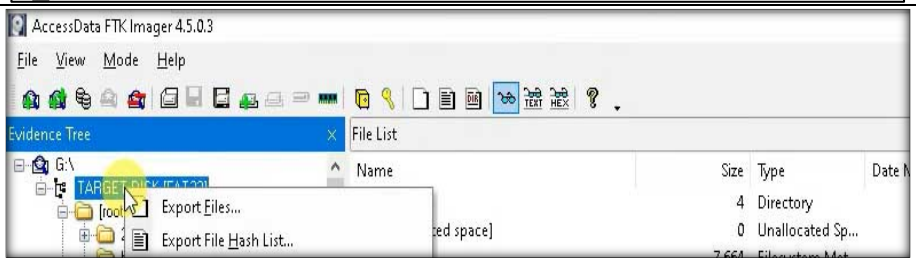
## ثانياً: التسهيلات العلمية:

- **جهاز حاسوب، برنامج FTK Imager.**
- **مجلد لحفظ النتائج.**

## ثالثاً: خطوات تنفيذ التمرين:

| | | |
|---|---|---|
| 1 | ارتداء بدلة العمل، وفتح نافذة البرنامج الرئيسة، واختيار File ثم اختيار Gredte Disk Image. |  |

| | | |
|---|---|---|
| 2 | ستظهر نافذة جديدة، اختر منها نوع المصدر حسب الذاكرة التي لديك :<br>- اذا كان القرص حقيقياً : Physical Drive<br>- اذا كان القرص منطقي او فلاش : Logical Drive<br>ثم نضغط التالي، سيظهر لك القرص حدده ثم اضغط : Finish. |  |
| 3 | نقوم بتحديد مكان حفظ النسخة بالضغط على: Add.<br>ثم اختر نوع الصورة RAW او غيرها بعدها ادخل المعلومات التالية:<br>- اسم المحقق.<br>- رقم القضية.<br>- الوصف.<br>ثم التالي ثم نختر مجلد الحفظ ونضغط : Finish.<br>ثم Start وننتظر. |  |

| | | |
|---|---|---|
| 4 | قم بفتح النسخة في البرنامج من خلال File ثم Add Evidence Item ثم اختر Image File ثم حدد ملف الـ Image الذي انشئته، ستظهر محتويات القرص داخل البرنامج. |  |
| 5 | قم بعرض الملفات المحذوفة من خلال الذهاب الى الملف الذي قمت بالخزن فيه ستلاحظ الملفات المحذوفة بلون باهت او تظهر بعلامة X. |  |
| 6 | نحدد الملف المحذوف ونضغط بزر الفارة الايمن ثم نختر Export Files ونحدد مجلد الحفظ ثم يتم استرجاع الملف. |  |

| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: **توضيح كيفية استخدام FTK Imager لاسترجاع الملفات المحذوفة من القرص الصلب.**<br>رقم التمرين:**4** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## 3-2 فحص سجلات النظام والتطبيقات

يُعدّ التحقيق الجنائي الرقمي أحد الفروع الحديثة في علوم الحاسوب، ويهتم بجمع الأدلة الرقمية وحفظها وتحليلها لاستخدامها في كشف الجرائم الإلكترونية وإثباتها قانونيًا. ومع التطوّر الكبير في استخدام الحواسيب والهواتف الذكية والإنترنت، أصبح من الضروري الاعتماد على مصادر موثوقة للمعلومات التقنية التي تساعد في تتبّع الأنشطة المشبوهة.

ومن أهم هذه المصادر سجلات النظام والتطبيقات (Logs)، إذ تقوم هذه السجلات بتوثيق الأحداث التي تحدث داخل الجهاز والبرامج بشكل تلقائي ومستمر، مما يجعلها مرجعًا أساسيًا للمحقق الرقمي في فهم ما جرى على النظام خلال فترة زمنية معيّنة.

وتعرف سجلات النظام والتطبيقات **بانها ملفات يتم إنشاؤها تلقائيًا بواسطة نظام التشغيل أو البرامج المثبّتة على الجهاز، بهدف تسجيل الأنشطة التي تتم داخل النظام أو التطبيق**. وتشمل هذه الأنشطة:

- تشغيل وإيقاف البرامج.
- تسجيل الدخول والخروج.
- محاولات الوصول غير المصرّح بها.
- الأخطاء والمشكلات التقنية.
- إعدادات وتغييرات النظام.

ويُطلق على هذه الملفات اسم Logs، وهي تُخزَّن غالبًا في مسارات معيّنة داخل نظام التشغيل، مثل برنامج Event Viewer في نظام Windows.

**ولفحص السجلات في التحقيق الجنائي الرقمي اهمية كبيرة تتمثل في:**

- تحديد المستخدمين الذين دخلوا النظام.
- معرفة توقيت كل عملية.
- اكتشاف محاولات الاختراق.
- تتبع الانشطة المشبوهة.
- اعادة بناء تسلسل الاحداث قبل وقوع الجريمة.

وبالتالي تصبح السجلات دليلاً تقنيًا موثوقًا أمام الجهات القضائية.

**اما بالنسبة لأنواع سجلات النظام والتطبيقات فهي:**

**1- سجلات نظام التشغيل (System Logs):** تسجل كل ما يتعلق بعمل النظام نفسه، مثل تشغيل الخدمات والتعريفات والأجهزة.

ففي نظام Windows تُصنّف إلى:

- System Log: تتعلق بمعلومات عن النظام.
- Application Log: تتعلق بمعلومات عن التطبيقات.
- Security Log: تتعلق بمعلومات خاصة بامن الحاسوب.

**2- سجلات الأمان (Security Logs):** تركز على الأنشطة الأمنية، مثل:

- تسجيل الدخول والخروج.
- المحاولات الفاشلة للوصول.
- تغيير الصلاحيات.
- إنشاء حسابات.

وهي الأهم في قضايا الاختراقات.

**3- سجلات التطبيقات (Application Logs):** وهي خاصة بكل برنامج، مثل:

- المتصفحات
- برامج البريد
- قواعد البيانات
- تسجل الأخطاء
- الملفات المفتوحة
- زمن الاستخدام

**4- سجلات الشبكة (Network Logs):** تسجل الاتصالات بين الأجهزة، وتفيد في تتبع الهجمات الإلكترونية.

**ومن أبرز الأدوات المستخدمة في فحص السجلات:**

أ- Event Viewer في Windows.

ب- برامج إدارة السجلات.

جـ - أنظمة SIEM.

د- أدوات الطب الشرعي الرقمي: وتساعد هذه الأدوات في:

- تصفية الأحداث.

- ترتيبها زمنيًا.
- البحث في ملايين السجلات بسرعة.

**اما بالنسبة لخطوات فحص السجلات جنائيًا فهي:**

**1- تأمين الدليل:** يتم إنشاء نسخة رقمية من الجهاز(حتى لا تتغير البيانات الأصلية).

**2- تحديد السجلات المهمة مثل:** Security، System، Application.

**3- تحليل الأحداث:** وفيها يتم البحث عن:

- تغييرات غير طبيعية.
- محاولات دخول مشبوهة.
- حذف او تعديل بعض البيانات.
- تشغيل برامج غير معروفة.

**4- إنشاء خط زمني:** وذلك بترتيب الأحداث حسب وقت حدوثها، مما يوضح تسلسل الوقائع بدقة.

**اما بالنسبة للتحديات التي تواجه المحققين فهي:**

- ضخامة حجم السجلات.
- حذف أو تعديل بعض البيانات.
- تعدد الأنظمة والتطبيقات.
- الحاجة إلى خبرة تقنية عالية.

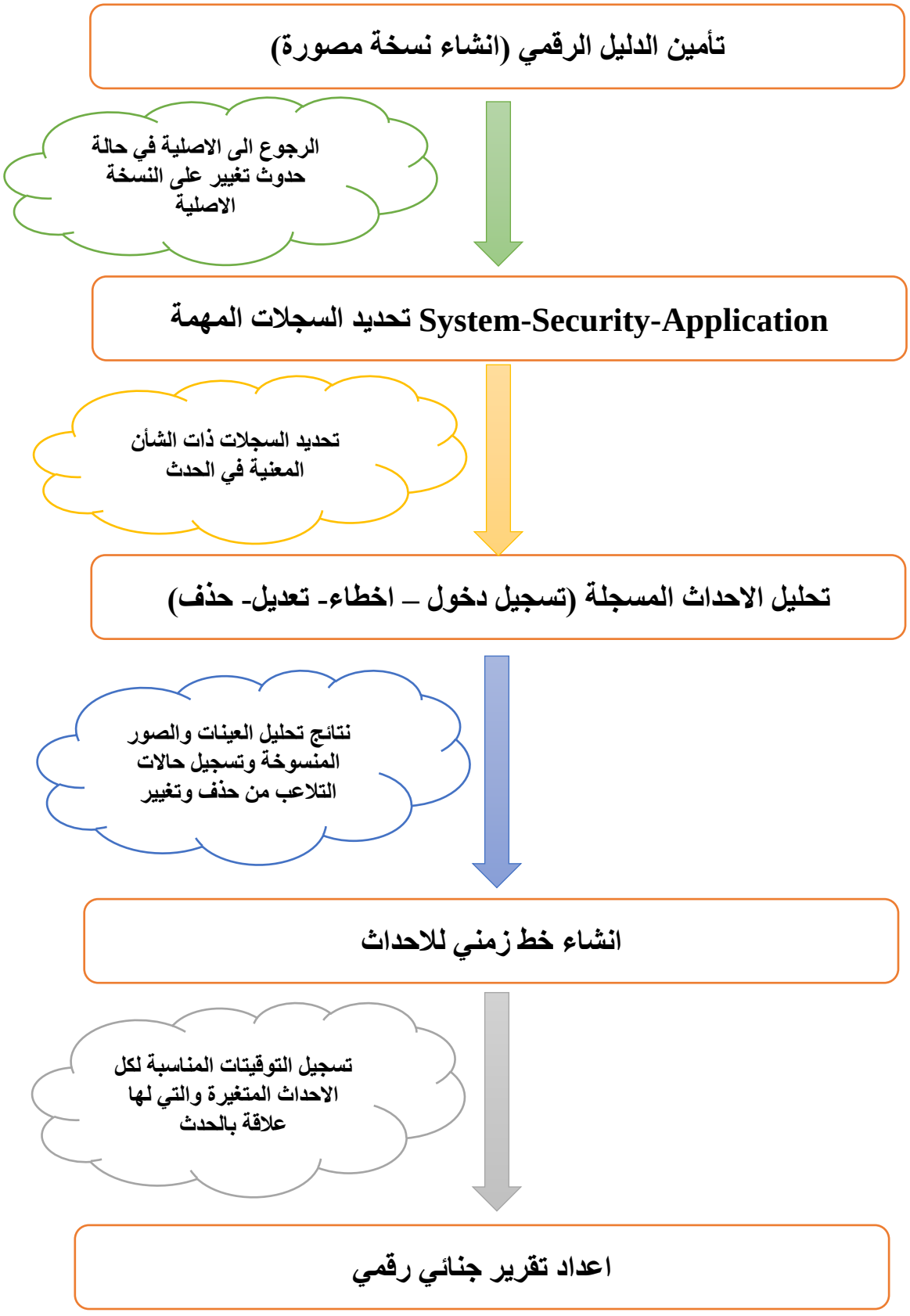
ومع ذلك، تبقى السجلات من أقوى الأدلة الرقمية، **وكمثال مبسّط عن السجلات:**

تم حذف ملفات مهمة من جهاز إداري، وبفحص سجلات الأمان ظهر أنّ:

المستخدم (A دخل الساعة 8:00) ثم قام بحذف ملفات الساعة 8:10 وبعدها أغلق الجهاز وهكذا يمكن إثبات الواقعة بدقة زمنية.

إنّ فحص سجلات النظام والتطبيقات يُعدّ ركيزة أساسية في التحقيق الجنائي الرقمي، لأنه يتيح إعادة بناء الأحداث التي وقعت داخل النظام بشكل موثّق ودقيق. ومن خلال تحليل هذه السجلات، يتمكّن المحققون من كشف الجرائم الرقمية، وتحديد المسؤولين عنها، وتقديم أدلة قانونية موثوقة أمام القضاء. ولذلك، فإن إتقان قراءة السجلات وتحليلها يمثل مهارة ضرورية لكل طالب في مجال التحقيقات الرقمية، ويساهم في حماية المؤسسات والمجتمع من الجرائم الإلكترونية المتزايدة.

والمخطط ادناه يمثل تسلسل العمليات التي يقوم بها المحقق الجنائي الرقمي:



رقم التمرين: 5 الزمن المخصص: 3 ساعات

**اسم التمرين:** تحليل سجلات نظام التشغيل (Windows Event Logs) وسجلات التطبيقات لتحديد النشاطات المشبوهة مثل محاولات الدخول غير المصرح بها.

**مكان التنفيذ:** مختبر الحاسوب

## اولاً: الاهداف التعليمية:

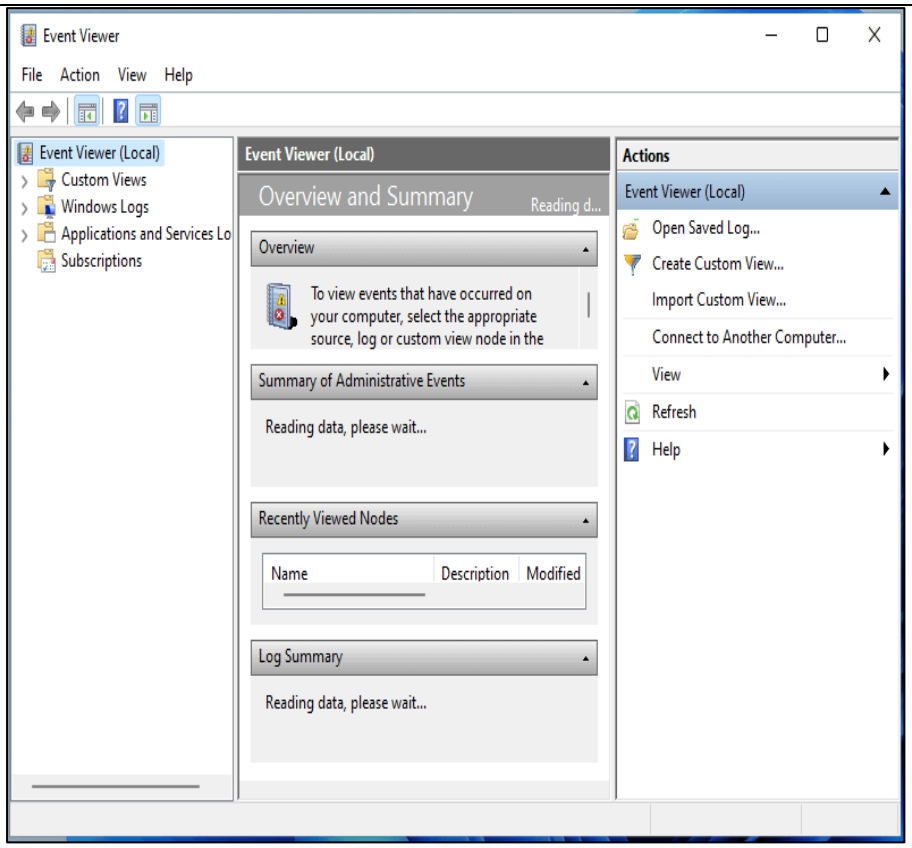
**بعد اتمام هذا التمرين، سيتمكن الطالب من:**

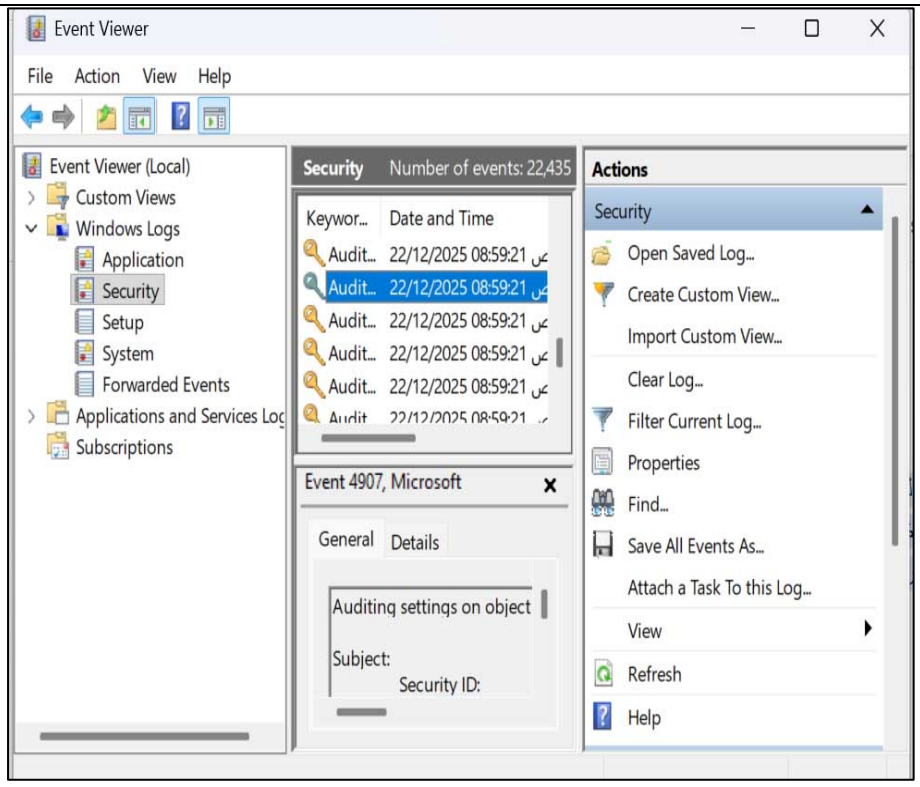
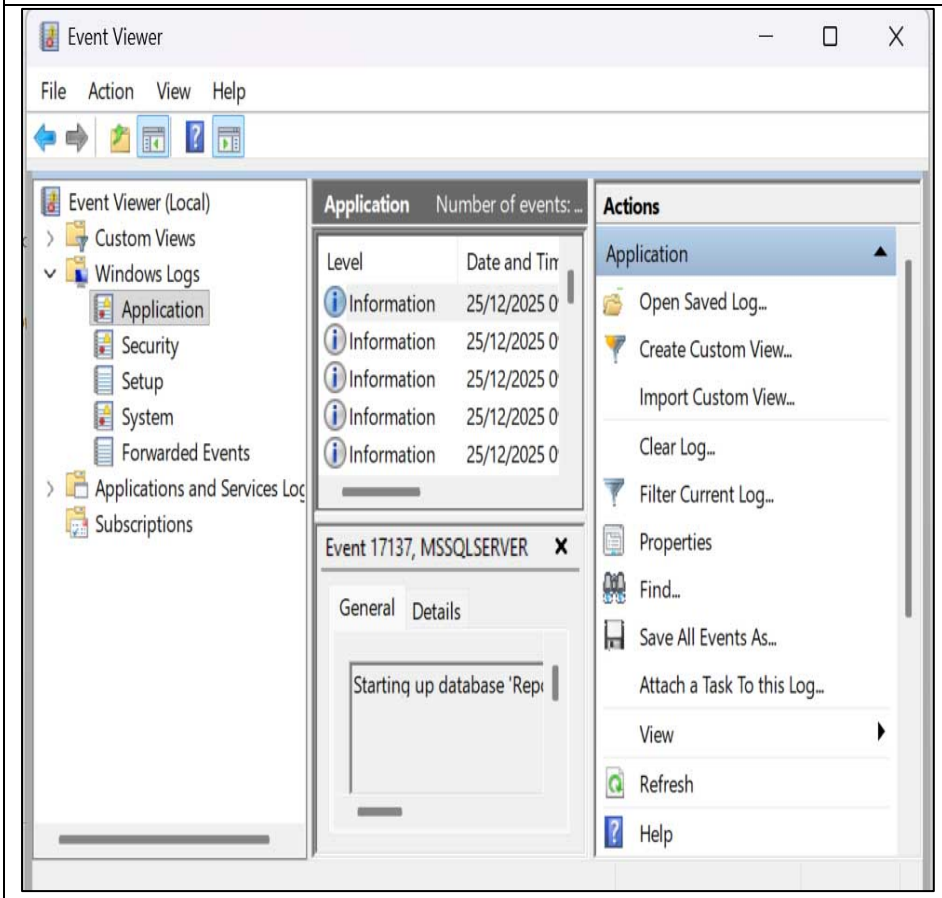
التعرف على سجلات أحداث نظام التشغيل.Windows Event Logs و اكتساب مهارة تحليل سجلات النظام وسجلات التطبيقات واكتشاف النشاطات المشبوهة مثل محاولات الدخول غير المصرّح بها وفهم دور السجلات الرقمية في التحقيق الجنائي الرقمي.

## ثانياً: التسهيلات العلمية:

- جهاز حاسوب يعمل بنظام Windows 10 أو Windows 11.

## ثالثاً: خطوات تنفيذ التمرين:

| | | |
|---|---|---|
| 1 | ارتداء بدلة العمل، ثم افتح سجلات الاحداث من خلال الضغط على: Start ثم نكتب: Event Viewer ثم نفتح الاداة. |  |

| | | |
|---|---|---|
| 2 | **قم بتحليل سجل الامان:**<br>**Security Log**<br>**من خلال الانتقال الى:**<br>**Windows Logs**<br>**ثم الى:**<br>**Security**<br>**ابحث عن محاولات الدخول الفاشلة :**<br>**Failed Logon**<br>**سجل عدد مرات الدخول الفاشلة والفترة الزمنية واسم المستخدم.** |  |
| 3 | انتقل الى سجل التطبيقات:<br>Application<br>وابحث عن اخطاء متكررة للتطبيقات او تطبيقات غير معروفة او رسائل تحذير، ثم دون اسم التطبيق ونوع الخطأ ووقت حدوثه.<br>قم بأعداد تقرير صغير يتضمن نوع السجل الذيتم تحليله، امثلة على نشاطات مشبوهة، والاستنتاج النهائي. |  |

| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: **تحليل سجلات نظام التشغيل (Windows Event Logs) وسجلات التطبيقات لتحديد النشاطات المشبوهة مثل محاولات الدخول غير المصرح بها.**<br>رقم التمرين:**5** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## 4-2 البرمجيات الضارة

مع التوسع الكبير في استخدام أنظمة الحاسوب وشبكات الإنترنت، أصبحت الجرائم الإلكترونية من أخطر التحديات التي تواجه الأفراد والمؤسسات. وتُعد **البرمجيات الضارة** من أبرز الوسائل المستخدمة في تنفيذ هذه الجرائم، لما تملكه من قدرة على اختراق الأنظمة، وسرقة البيانات، وتعطيل الخدمات. ومن هنا تبرز أهمية دراستها وتحليلها ضمن إطار **التحقيق الجنائي الرقمي**، بهدف كشف الهجمات الرقمية، وتحديد مصادرها، وجمع الأدلة الرقمية المرتبطة بها.

وتعرف البرمجيات الضارة (Malware) **على انها برامج أو شيفرات خبيثة يتم تصميمها بقصد إلحاق الضرر بالأنظمة الحاسوبية أو الوصول غير المصرّح به إلى البيانات والمعلومات، أو التجسس على المستخدمين، أو التحكم في الأنظمة دون علم أصحابها، وتشكل أداة رئيسية في ارتكاب الجرائم الإلكترونية.**

**وتكون على انواع هي:**

**1- الفيروسات (Viruses) :** الفيروسات هي برمجيات ضارة ترتبط بالملفات التنفيذية أو بقطاعات الإقلاع في نظام التشغيل، ولا تنشط إلا عند تشغيل الملف المصاب من قبل المستخدم.

تقوم الفيروسات بنسخ نفسها وإصابة ملفات أخرى داخل النظام، مما يؤدي إلى انتشارها تدريجيًا. وقد تتسبب في تلف الملفات أو حذفها أو تعديلها، إضافة إلى إبطاء أداء الجهاز أو تعطيله. وفي التحقيق الجنائي الرقمي، يتم اكتشاف الفيروسات من خلال تحليل الملفات المصابة، ودراسة سلوكها، ومقارنة تواقيعها الرقمية.

**2- الديدان (Worms):** الديدان هي برمجيات ضارة مستقلة قادرة على الانتشار الذاتي عبر الشبكات دون الحاجة إلى تدخل المستخدم.

تستغل الديدان الثغرات الأمنية في أنظمة التشغيل أو الخدمات الشبكية، وتنتشر بسرعة كبيرة بين الأجهزة المتصلة بالشبكة. وتكمن خطورتها في استنزاف موارد النظام والشبكة، وقد تؤدي إلى توقف الخدمات بالكامل. ويعتمد التحقيق الجنائي الرقمي على تحليل سجلات الشبكة وسجلات النظام لتتبع مسار انتشار الديدان وتحديد مصدرها.

3- **احصنة طروادة (Trojans):** أحصنة طروادة هي برمجيات خبيثة تتخفى على شكل برامج شرعية أو ملفات موثوقة، بهدف خداع المستخدم ودفعه إلى تثبيتها.

بعد التثبيت، تقوم بتنفيذ أنشطة خبيثة مثل فتح أبواب خلفية، أو تمكين المهاجم من التحكم بالجهاز عن بُعد، أو سرقة البيانات الحساسة. وفي التحقيق الجنائي الرقمي، يتم تحليل العمليات الجارية والاتصالات الشبكية المشبوهة لاكتشاف هذا النوع من البرمجيات.

**4- برامج التجسس (Spyware):** برامج التجسس هي برمجيات ضارة تهدف إلى مراقبة أنشطة المستخدم وجمع معلوماته الشخصية دون علمه أو موافقته.

تقوم هذه البرامج بجمع بيانات مثل كلمات المرور، وسجل التصفح، والمحادثات، والمعلومات الشخصية، وغالبًا ما تُثبت مع تطبيقات مجانية أو عبر مواقع مشبوهة. ويعتمد التحقيق الجنائي الرقمي على تحليل الذاكرة وسجلات النظام والمتصفحات للكشف عن هذا النوع من البرمجيات.

**5- برامج الفدية (Ransomware):** برامج الفدية هي برمجيات ضارة تقوم بتشفير ملفات المستخدم أو قفل النظام بالكامل، ثم تطلب دفع مبلغ مالي مقابل استعادة الوصول إلى البيانات.

تنتشر برامج الفدية عادة عبر مرفقات البريد الإلكتروني أو الروابط الخبيثة، وتُعد من أخطر التهديدات الرقمية في العصر الحديث. ويهتم التحقيق الجنائي الرقمي بتحليل آلية التشفير، ونقطة الإصابة، ومحاولة استعادة البيانات أو تتبع الجهة المهاجمة.

**6- برامج تسجيل ضغطات المفاتيح (Keyloggers):** برامج تسجيل ضغطات المفاتيح هي أدوات خبيثة تقوم بتسجيل كل ما يكتبه المستخدم على لوحة المفاتيح، تُستخدم هذه البرامج لسرقة أسماء المستخدمين وكلمات المرور والمعلومات الحساسة مثل البيانات المصرفية. وقد تكون هذه البرامج برمجية أو عتادية. ويعتمد التحقيق الجنائي الرقمي على تحليل العمليات الخفية والاتصالات الخارجية التي ترسل البيانات المسروقة.

**اما بالنسبة لدور التحقيق الجنائي الرقمي في مواجهة البرمجيات الضارة فهو:**

- اكتشاف وجود البرمجيات الضارة.
- تحليل سلوكها وآلية عملها.
- تحديد مصدر الهجوم ومساره.

- جمع الأدلة الرقمية وتوثيقها قانونيًا.
- دعم الإجراءات القانونية ومنع تكرار الهجمات.

## 5-2 مقارنة بين ادوات التحقيق الجنائي الرقمي التجارية والمفتوحة المصدر

تُعد أدوات التحقيق الجنائي الرقمي من العناصر الأساسية في عملية جمع وتحليل الأدلة الرقمية، إذ يعتمد عليها المحقق الرقمي لاستخراج البيانات وتحليلها وتوثيقها بطريقة علمية وقانونية. وتنقسم هذه الأدوات إلى نوعين رئيسيين هما **الأدوات التجارية** و**الأدوات مفتوحة المصدر**، ويختلف كل نوع من حيث الكلفة، والخصائص، ومستوى الدعم، والاستخدام العملي في بيئات التحقيق المختلفة.

**أولًا: أدوات التحقيق الجنائي الرقمي التجارية:** هي أدوات مدفوعة يتم تطويرها من قبل شركات متخصصة في أمن المعلومات والتحقيق الجنائي الرقمي، وتتميز بكونها حلولًا متكاملة وجاهزة للاستخدام المهني، ومن الامثلة المهمة على الأدوات التجارية **EnCase Forensic**، **FTK (Forensic Toolkit)**.

**وتمتاز بما يلي:**

- واجهات استخدام سهلة ومناسبة للمحققين المبتدئين.
- دعم فني وتحديثات منتظمة.
- توثيق رسمي وتقارير جاهزة للاستخدام القانوني.
- قبول واسع في المحاكم والجهات القضائية.

**اما عيوبها فهي:**

- ارتفاع الكلفة المادية.
- الاعتماد على الشركة المطوّرة.
- محدودية التعديل على وظائف الأداة.

**ثانيًا: أدوات التحقيق الجنائي الرقمي مفتوحة المصدر:** الأدوات مفتوحة المصدر هي أدوات مجانية أو منخفضة الكلفة، يكون كودها البرمجي متاحًا للمستخدمين، مما يسمح بتطويرها وتعديلها وفق الحاجة، ومن الأمثلة على الأدوات مفتوحة المصدر **Autopsy**، **The Sleuth Kit**.

**وتمتاز بما يلي:**

- مجانية أو منخفضة الكلفة.
- إمكانية تعديل الكود البرمجي.
- مناسبة للأغراض التعليمية والبحثية.

- مرونة عالية في التحليل المتقدم.

**اما عيوبها فهي:**

- تتطلب خبرة تقنية عالية.
- دعم فني محدود أو مجتمعي فقط.
- عدم توفر تقارير قانونية جاهزة في بعض الأدوات.

والجدول التالي يمثل مقارنة شاملة بين الأدوات التجارية والمفتوحة المصدر:

| جانب المقارنة | الأدوات التجارية | الأدوات مفتوحة المصدر |
|---|---|---|
| **الكلفة** | مرتفعة | منخفضة أو مجانية |
| **سهولة الاستخدام** | عالية | متوسطة إلى منخفضة |
| **الدعم الفني** | متوفر ورسمي | مجتمعي غالبًا |
| **المرونة والتخصيص** | محدودة | عالية |
| **القبول القانوني** | واسع | يعتمد على التوثيق |
| **الاستخدام التعليمي** | محدود | واسع |

**ويعتمد اختيار الأداة المناسبة في التحقيق الجنائي الرقمي على:**

- طبيعة القضية الرقمية.
- خبرة المحقق.
- الإمكانيات المالية.
- المتطلبات القانونية.
- البيئة التعليمية أو العملية.

وغالبًا ما يُفضّل الدمج بين الأدوات التجارية والمفتوحة المصدر للحصول على نتائج أكثر دقة وشمولية.

**رقم التمرين: 6** **الزمن المخصص: 3 ساعات**

**اسم التمرين: اجراء مقارنة بين أدوات التحليل الجنائي الرقمي التجارية ومفتوحة المصدر في استخراج البيانات من الملفات.**

**مكان التنفيذ: مختبر الحاسوب**

## اولاً: الاهداف التعليمية:

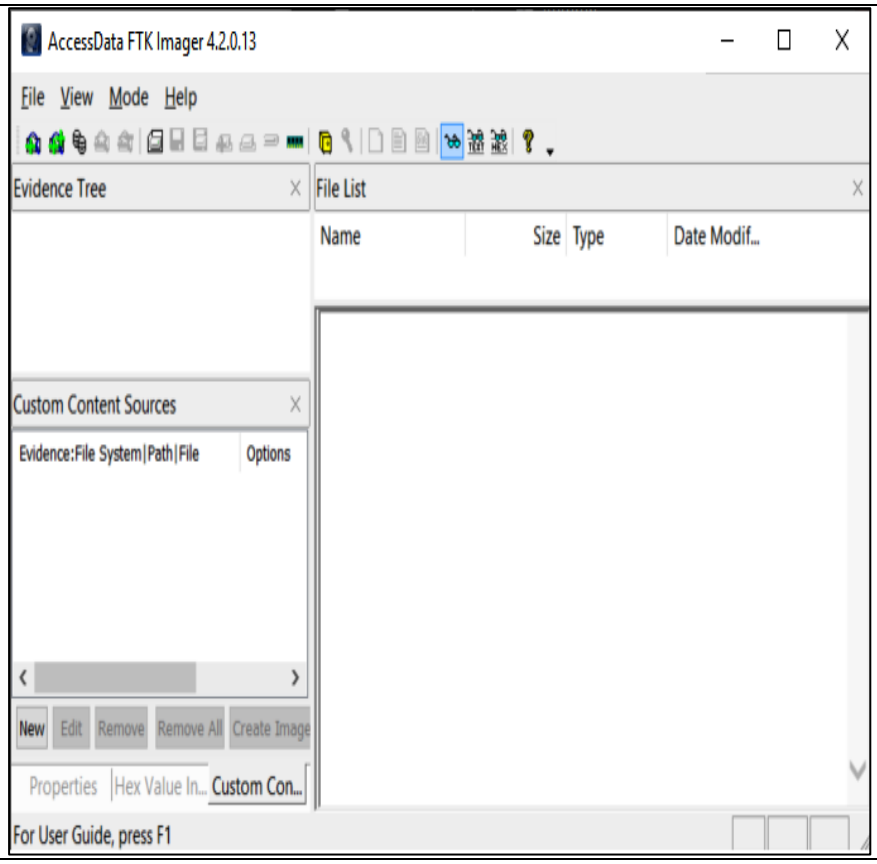
**بعد اتمام هذا التمرين، سيتمكن الطالب من:**

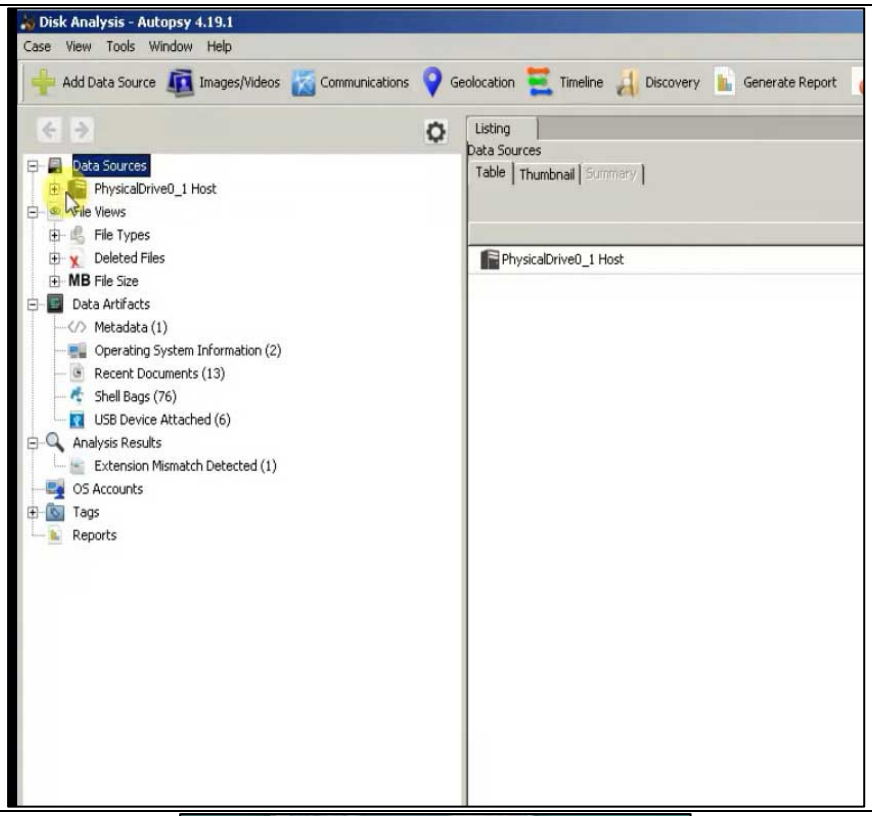
**التعرف على أدوات التحليل الجنائي الرقمي التجارية ومفتوحة المصدر، فهم آليات استخراج البيانات من الملفات باستخدام كل نوع من الأدوات، المقارنة بين كفاءة وسهولة استخدام الأدوات التجارية ومفتوحة المصدر، تنمية مهارات التحليل والتوثيق في التحقيق الجنائي الرقمي.**

## ثانياً: التسهيلات العلمية:

- **جهاز حاسوب يعمل بنظام Windows 10 أو Windows 11.**
- **داة تحليل جنائي رقمية تجارية FTK ومفتوحة المصدر Autopsy.**
- **مجلد ملفات يحتوي على ملفات موجودة وملفات محذوفة.**

## ثالثاً: خطوات تنفيذ التمرين:

| | | |
|---|---|---|
| **1** | ارتداء بدلة العمل، ثم افتح برنامج:<br>FTK<br>ثم استخرج الملفات المحذوفة ووثق النتائج. |  |

| | | |
|---|---|---|
| 2 | **قم بفتح البرنامج مفتوح المصدر:**<br>**Autopsy**<br>**ثم قم بتحميل الملفات واستخرج البيانات المحذوفة.** |  |
| 3 | قم بتسجيل النتائج من الخطوة الاولى والخطوة الثانية والفرق بينهما من حيث:<br>1- السرعة.<br>2- الدقة.<br>3- سهولة الاستخدام.<br>ثم قم بتدوين التالي:<br>- وصف الأدوات المستخدمة.<br>- آلية استخراج البيانات.<br>- نتائج المقارنة.<br>- الاستنتاج النهائي. | <br> |

**استمارة قائمة الفحص**

اسم الطالب: المرحلة: الثالثة

التخصص:

**اسم التمرين: اجراء مقارنة بين أدوات التحليل الجنائي الرقمي التجارية ومفتوحة المصدر في استخراج البيانات من الملفات.**

رقم التمرين:**6**

| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
|---|---|---|---|---|
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |

| اسم الفاحص: | التاريخ | التوقيع |
|---|---|---|
| | | |

## اسئلة الفصل الثاني

**س1:عرف ما يأتي:**

**1- الأدوات البرمجية للتحقيق الجنائي الرقمي. 2- استعادة الملفات المحذوفة. 3-البرمجيات الضارة.**

**4- سجلات النظام والتطبيقات. 5- أدوات التحقيق الجنائي مفتوحة المصدر.**

**س2: املى الفراغات الاتية بما يناسبها:**

**1- تعتمد أقراص ــــــــــ على التخزين المغناطيسي، بينما تعتمد أقراص ــــــــــ على ذاكرة الفلاش الإلكترونية.**

**2- تُعد سجلات النظام والتطبيقات مصدرًا أساسيًا في التحقيق الرقمي لأنها تعمل على تسجيل ــــــــــ و ــــــــــ و ــــــــــ.**

**3- من أشهر أدوات جمع الأدلة الرقمية المستخدمة في التحقيق الجنائي الرقمي برنامج ــــــــــ وبرنامج ــــــــــ .**

**4- تُستخدم أدوات تحليل الشبكات لمعرفة الاتصالات والبيانات المتبادلة عبر الإنترنت، ومن أمثلتها أداة ــــــــــ.**

**5- من أهم تحديات استرجاع الملفات من أقراص SSD استخدام أمر ــــــــــ وتقنية ــــــــــ .**

**6- تُعد أدوات التحقيق الجنائي الرقمي التجارية مرتفعة الكلفة لكنها تمتاز بتوفير ــــــــــ و ــــــــــ .**

**س3: اشرح باختصار دور الأدوات البرمجية في التحقيق الجنائي الرقمي وكيف تسهم في كشف الجرائم الإلكترونية.**

**س4: عدّد أنواع الأدوات البرمجية المستخدمة في التحقيق الجنائي الرقمي مع ذكر مثال لكل نوع.**

**س5: وضّح خطوات استعادة الملفات المحذوفة من الحاسوب وفق الإجراءات الجنائية الرقمية.**

**س6: اذكر أهم التحديات التي تواجه المحقق الجنائي عند استرجاع الملفات من الهواتف المحمولة.**

**س7: قارن بين أقراص HDD و SSD من حيث:**

**آلية الحذف - بقاء البيانات - إمكانية الاسترجاع.**

**س8: عدّد الأنواع الرئيسية للبرمجيات الضارة مع توضيح فكرة عامة عن وظيفة كل نوع.**

**س9: اشرح أهمية فحص سجلات النظام والتطبيقات في التحقيق الجنائي الرقمي ودورها في كشف الأنشطة المشبوهة.**

**س10: قدّم مقارنة بين الأدوات التجارية والأدوات مفتوحة المصدر في التحقيق الرقمي من حيث:**

**الكلفة - سهولة الاستخدام - الدعم الفني - القبول القانوني**

# الفصل الثالث

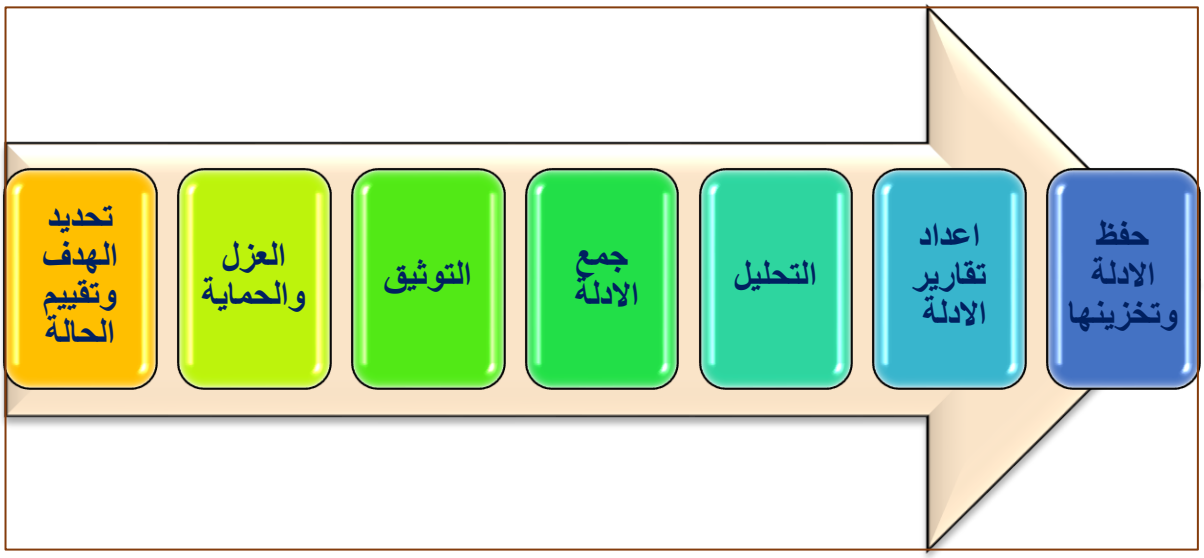
# إجراءات جمع الأدلة الرقمية وتحليلها

**المقدمة:**

يتناول هذا الفصل مفهوم التحقيق الجنائي الرقمي وأهميته في مواجهة تزايد الجرائم الرقمية الناتجة عن الاعتماد المتزايد على التقنيات الحديثة. يهدف إلى تزويد الطالب بالمعرفة والمهارات اللازمة لجمع وتحليل الأدلة الرقمية وفق أسس علمية تراعي الجوانب التقنية والقانونية والأخلاقية.

## 1-3 خطوات جمع الادلة الرقمية بطريقة صحيحة

يعد جمع الأدلة الرقمية المرحلة الأولى في التحقيق الجنائي الرقمي، ويهدف إلى الحصول على البيانات بطريقة قانونية تضمن سلامتها وصلاحيتها للتحليل. وفيما يلي اهم خطوات جمع الأدلة الرقمية وكما موضحة بالشكل (3-1):




**شكل (3-1) خطوات جمع الأدلة الرقمية**

### أولاً: تحديد الهدف وتقييم الحالة (Identification & Assessment)

تُعد هذه المرحلة الركيزة الأساسية في أي تحقيق رقمي (Digital Forensics)، إذ تضع الإطار العام للعمل وتوجّه الخطوات اللاحقة لجمع الأدلة وتحليلها. ويهدف هذا الجزء إلى فهم طبيعة الحادث الأمني، تحديد مصادر الأدلة المحتملة، تقييم المخاطر التي قد تهدد البيانات، والتأكد من شرعية الإجراءات التي سيتم اتخاذها.

**1- تحديد نوع الحادث أو الجريمة الرقمية**

تبدأ عملية التحقيق بفهم دقيق للواقعة؛ إذ يساعد تحديد نوع الجريمة الرقمية على وضع تصور واضح لماهية الأدلة التي يجب البحث عنها والأولويات التي يجب مراعاتها.

قد تشمل الحوادث الرقمية:

- اختراق أنظمة بهدف سرقة بيانات أو إحداث ضرر.
- ابتزاز إلكتروني مثل التهديد بنشر معلومات حساسة.
- حذف أو تعديل ملفات بشكل غير مصرح به.
- استخدام غير قانوني لحسابات أو أجهزة.

**2- تحديد الأجهزة والأنظمة المحتمل احتواؤها على الأدلة**

بعد فهم الحادث، يُصار إلى تحديد البيئة التي قد تحتوي أدلة رقمية ذات صلة. وتشمل هذه البيئة:

- أجهزة الكمبيوتر المكتبية أو المحمولة التي قد يكون تم تنفيذ الأنشطة عليها.
- الهواتف الذكية والأجهزة اللوحية المستخدمة للوصول إلى الحسابات أو تخزين الملفات.
- الخوادم (Servers) وقواعد البيانات التي تحتفظ بالسجلات المهمة.
- معدات الشبكات، مثل أجهزة التوجيه والجدران النارية، لما تحتويه من سجلات اتصال.
- الخدمات السحابية أو البريد الإلكتروني المرتبط بالحسابات المستهدفة.

يتم إعداد قائمة بهذه المصادر، مع توضيح سبب اعتبار كل مصدر مهمًا للتحقيق.

**3- تقييم المخاطر التي قد تهدد سلامة الأدلة**

يعتمد نجاح التحقيق على الحفاظ الكامل على الأدلة الرقمية دون تغيير أو فقدان. ولذلك يتم تقييم مجموعة من المخاطر المحتملة، مثل:

- استمرار استخدام الجهاز من قبل المستخدم أو المشتبه به، مما قد يؤدي إلى تغيير أو حذف بيانات مهمة.
- وجود برمجيات خبيثة قد تُخفي آثارها أو تُعدّل البيانات تلقائيًا.
- احتمال فقدان سجلات مهمة إذا تم إيقاف الخادم بطريقة غير آمنة.
- إمكانية قيام المهاجم بإتلاف الأدلة عن بُعد إذا بقي النظام متصلاً بالإنترنت.

يساعد تقييم هذه المخاطر في اتخاذ قرار سريع حول ضرورة عزل الجهاز، أو أخذ نسخ فورية من الذاكرة أو السجلات قبل ضياعها.

**4- تحديد الصلاحيات القانونية لجمع البيانات**

يجب أن تتم كل مرحلة من مراحل التحقيق الرقمي ضمن إطار قانوني يضمن شرعية الإجراءات ويحمي خصوصية الأفراد. وتشمل هذه الخطوة:

- الحصول على إذن رسمي من السلطات المختصة (مثل مراكز الشرطة أو الجهات القضائية).
- التأكد من وجود موافقة صريحة عند التحقيق في أجهزة أو حسابات ضمن بيئة العمل.
- الالتزام بالقوانين الوطنية المتعلقة بحماية البيانات والخصوصية.
- تحديد نطاق البحث بدقة لتجنب الوصول إلى معلومات غير مرتبطة بالقضية.

هذه الضمانات القانونية ضرورية لاعتماد الأدلة أمام القضاء، ولمنع أي طعن عليها لاحقًا.

ثانيا: العزل والحماية :

تعد مرحلة العزل والحماية خطوة محورية في اجراءات التحقيق الجنائي الرقمي، إذ تهدف إلى الحفاظ على الأدلة الرقمية في حالتها الأصلية دون أي تغيير قد يؤثر في قيمتها العلمية أو القانونية. وتكمن أهمية هذه المرحلة في منع أي تعديل أو تلف محتمل للأدلة، سواء كان ناتجًا عن استخدام بشري غير مقصود، أو عن برمجيات تعمل في الخلفية، أو عن إجراءات تقنية قد تؤدي إلى الكتابة فوق البيانات.

إن الالتزام بإجراءات العزل والحماية يضمن بقاء الأدلة موثوقة وقابلة للاستخدام في مراحل التحليل اللاحقة.

1- عزل الجهاز أو الشبكة عن الاتصال بالإنترنت:

يُعد الاتصال بالإنترنت من أبرز مصادر الخطر على الأدلة الرقمية، إذ قد يسمح للمهاجم بإزالة آثار الجريمة عن بُعد، أو يؤدي إلى تحديثات تلقائية لملفات النظام، أو استمرار عمل البرمجيات الخبيثة.

لذلك يقوم المحقق الرقمي بفصل كابل الشبكة وتعطيل الاتصال اللاسلكي (Wi-Fi)، لمنع الجهاز من التواصل مع أي مصادر خارجية، مما يساهم في تثبيت حالة الجهاز وقت وقوع الحادث.

2- منع استخدام الجهاز المشكوك به:

يجب منع تشغيل الجهاز أو استخدامه بأي شكل، لأن مجرد تسجيل الدخول أو تشغيل البرامج قد يؤدي إلى إنشاء ملفات جديدة أو تعديل السجلات (Logs) أو كتابة ملفات مؤقتة تُغيّر بنية القرص.

وبناءً على حالة الجهاز، يتم إيقاف تشغيله أو تركه في وضعه الحالي إذا كان يعمل، مع الالتزام بالمعايير المعتمدة في التحقيق الجنائي الرقمي.

3- إجراءات الحماية المتقدمة للأدلة:

تشمل مرحلة العزل والحماية أيضًا اتخاذ إجراءات تقنية متقدمة للحفاظ على سلامة الأدلة الرقمية، مثل إنشاء نسخة طبق الأصل من وسائط التخزين، والتحقق من سلامتها باستخدام قيم التجزئة، والاستعانة بأدوات منع الكتابة.

وسيتم تناول هذه الإجراءات بالتفصيل في قسم (3-2 تقنيات الحفاظ على سلامة الأدلة الرقمية).

ثالثا: التوثيق (Documentation):

يقصد بالتوثيق تسجيل جميع الإجراءات والخطوات التي يتم تنفيذها أثناء التحقيق الرقمي، بما يشمل جمع الأدلة وتحليلها وحفظها، وذلك بهدف ضمان تتبع الدليل والتحقق من سلامة الإجراءات. وسيتم تناول أساليب التوثيق وإعداد التقارير بالتفصيل في قسم (3-5 توثيق الأدلة الرقمية وإعداد التقارير النهائية).

رابعا: جمع الأدلة (Collection):

تُعد مرحلة جمع الأدلة المرحلة التي يتم فيها استخراج البيانات الرقمية من مصادرها المختلفة بطريقة فنية منظمة تضمن عدم إتلاف المعلومات أو تغييرها. وتختلف آليات الجمع باختلاف نوع المصدر، مثل أجهزة الحاسوب، والهواتف الذكية، والشبكات، والخدمات السحابية، وسيتم التوسع في هذه الإجراءات ضمن أقسام التحليل اللاحقة.

خامسًا: التحليل (Analysis):

تمثّل مرحلة التحليل الجانب الفني من التحقيق الرقمي، حيث يتم فحص البيانات المستخرجة وتفسيرها بهدف الوصول إلى أدلة رقمية ذات صلة بالحادث محل التحقيق. وتشمل هذه المرحلة مجموعة من الإجراءات، من أبرزها:

1- استعادة الملفات المحذوفة.

2- الكشف عن البرمجيات الخبيثة.

3- تحليل آثار استخدام الجهاز.

4- ربط الأحداث الزمنية لإنشاء خط زمني.

5- إعادة بناء سيناريو الحادث.

ويُعرض التحليل التفصيلي للأدلة المستخرجة من الحواسيب والهواتف والشبكات في الأقسام اللاحقة من هذا الفصل.

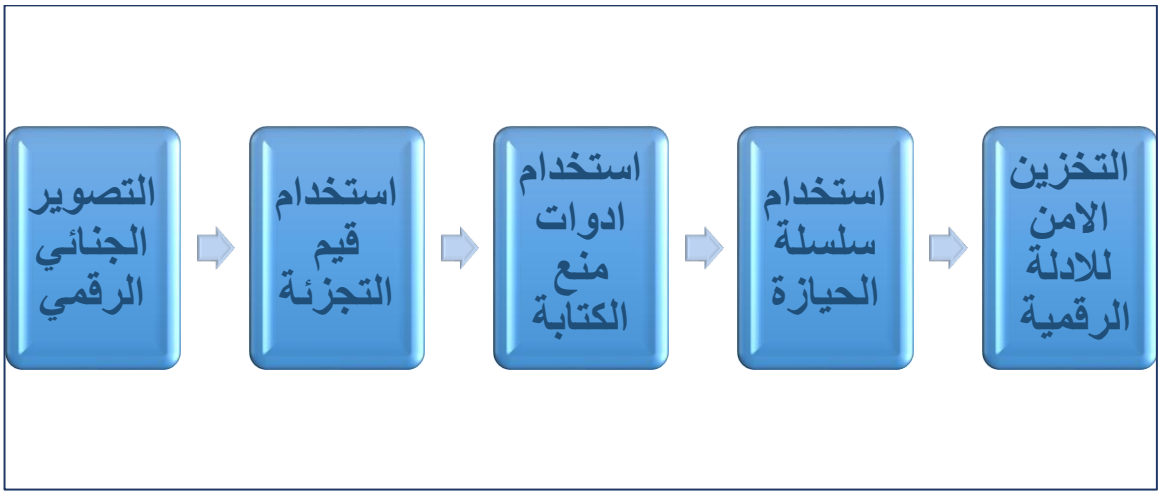
سادسًا: إعداد تقرير الأدلة (Reporting):

يمثل تقرير الأدلة الوثيقة الرسمية التي تُلخص نتائج التحقيق الرقمي، ويُعتمد عليه في عرض الأدلة والاستنتاجات أمام الجهات المختصة. وسيتم توضيح مكونات التقرير وآلية إعداده بشكل تفصيلي في قسم (3-5).

سابعًا: حفظ الأدلة وتخزينها (Storage & Archiving): تهدف هذه المرحلة إلى ضمان حفظ الأدلة الرقمية بشكل آمن للرجوع إليها عند الحاجة، سواء لاستكمال التحقيق أو لأغراض قانونية لاحقة. وسيتم تناول تقنيات التخزين الآمن للأدلة الرقمية بصورة أكثر تفصيلًا في قسم (3-2-4 التخزين الآمن للأدلة الرقمية).

## 2-3 تقنيات الحفاظ على سلامة الأدلة الرقمية

يقصد بسلامة الدليل الرقمي (Digital Evidence Integrity) الحفاظ على الدليل في حالته الأصلية منذ لحظة ضبطه وحتى انتهاء إجراءات التحقيق، دون أي تعديل أو حذف أو إضافة، سواء كان ذلك عن قصد أو غير قصد. وتُعد سلامة الدليل أساسًا لضمان موثوقية نتائج التحقيق الرقمي. وفيما يلي أهم التقنيات العملية المستخدمة لتحقيق ذلك، كما هو موضح في الشكل (2-3).




شكل (2-3) تقنيات الحفاظ على سلامة الأدلة الرقمية

وبالنسبة للتصوير الجنائي (Forensic Imaging):هو عملية إنشاء نسخة رقمية طبق الأصل (Bit-by-Bit) من وسيط التخزين، بحيث تشمل جميع البيانات المخزنة، بما فيها المساحات الفارغة والملفات المحذوفة، ويتم استخدام هذه النسخة لاحقًا في التحليل بدلًا من الدليل الأصلي.

والسؤال المهم لماذا نستخدم التصوير الجنائي

يُستخدم التصوير الجنائي للأسباب الآتية:

- العمل على نسخة بديلة دون المساس بالدليل الأصلي.
- حماية البيانات من التلف أثناء التحليل.
- الحفاظ على الدليل الأصلي في مكان آمن.

وبالنسبة لأدوات التصوير الجنائي

توجد أدوات متخصصة تُستخدم في المختبرات الجنائية الرقمية، من أشهرها: FTK Imager و EnCase، إضافة إلى أدوات مفتوحة المصدر مثل Guymager في أنظمة لينكس. وتمتاز هذه الأدوات بقدرتها على:

- إنشاء صورة كاملة ومتسلسلة لوسيط التخزين.
- تسجيل معلومات تفصيلية عن عملية النسخ.

**ومن الإجراءات الأساسية أثناء التصوير**

عند إجراء التصوير الجنائي يجب الالتزام بما يأتي:

- توصيل وسيط التخزين بجهاز التحقيق عبر أداة منع الكتابة قدر الإمكان.
- التأكد من تشغيل البرنامج في الوضع الجنائي (Forensic Mode).
- حفظ ملف الصورة في وسيط تخزين آمن ومخصص للتحقيقات.
- توثيق بيانات الوسيط وتاريخ ووقت التصوير واسم القائم بالعملية.

**رقم التمرين: 7** **الزمن المخصص: 3 ساعات**

اسم التمرين: استخدام برنامج FTK Imager لإنشاء نسخة طبق الأصل (Forensic Image)

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الاهداف التعليمية:**

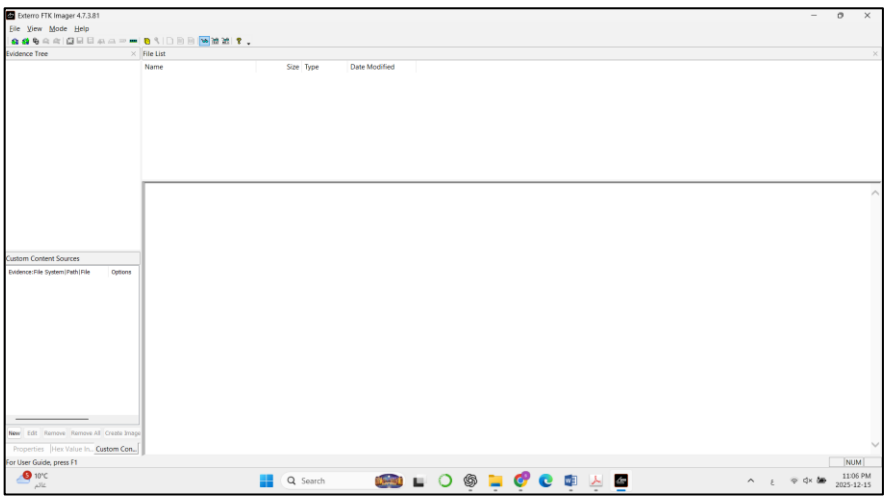
تعريف الطالب بآلية إنشاء نسخة جنائية رقمية باستخدام برنامج FTK Imager، والتحقق من سلامة الأدلة الرقمية، وتوثيق خطوات العمل وفق الأسس العلمية للتحقيق الجنائي الرقمي.

ثانياً: التسهيلات العلمية:

مختبر حاسوب مجهز، برنامج FTK Imager، وسائط تخزين رقمية تجريبية، وإشراف علمي أثناء تنفيذ التمرين.

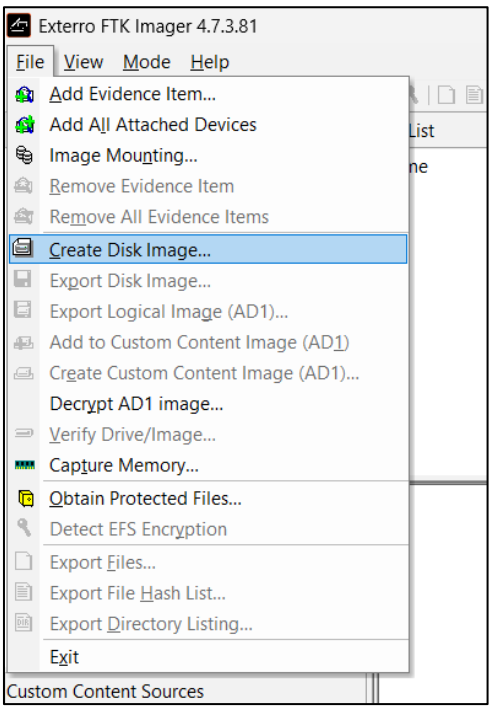
## ثالثا: خطوات تنفيذ التمرين

1- تشغيل برنامج **FTK Imager**.

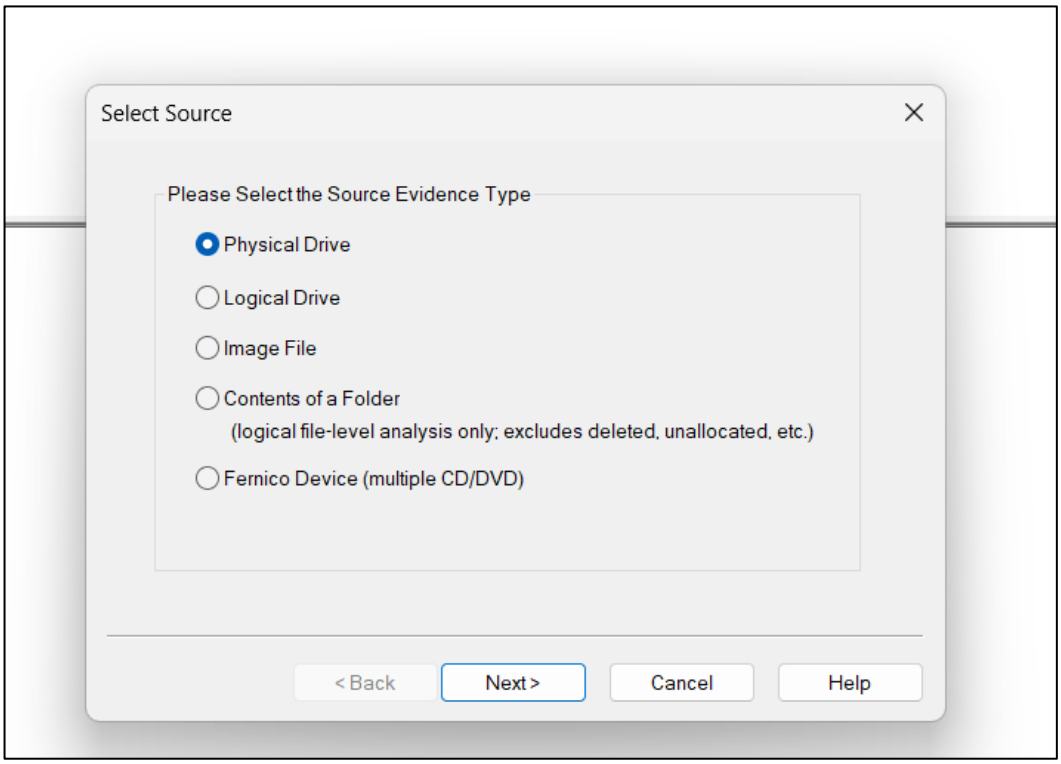


2- من القائمة اختر:

3- File → Create Disk Image:

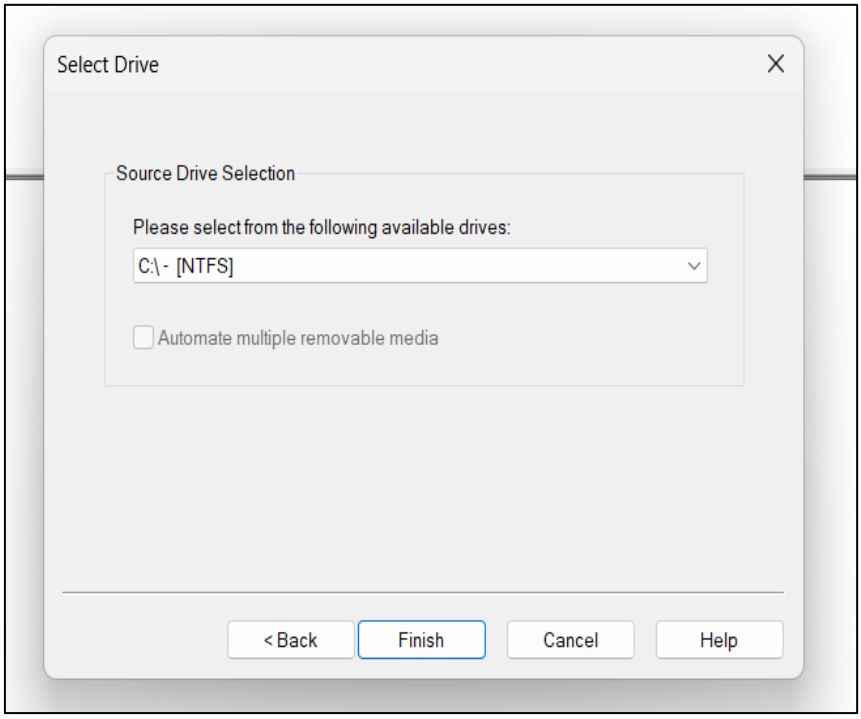



4- اختيار نوع المصدر:

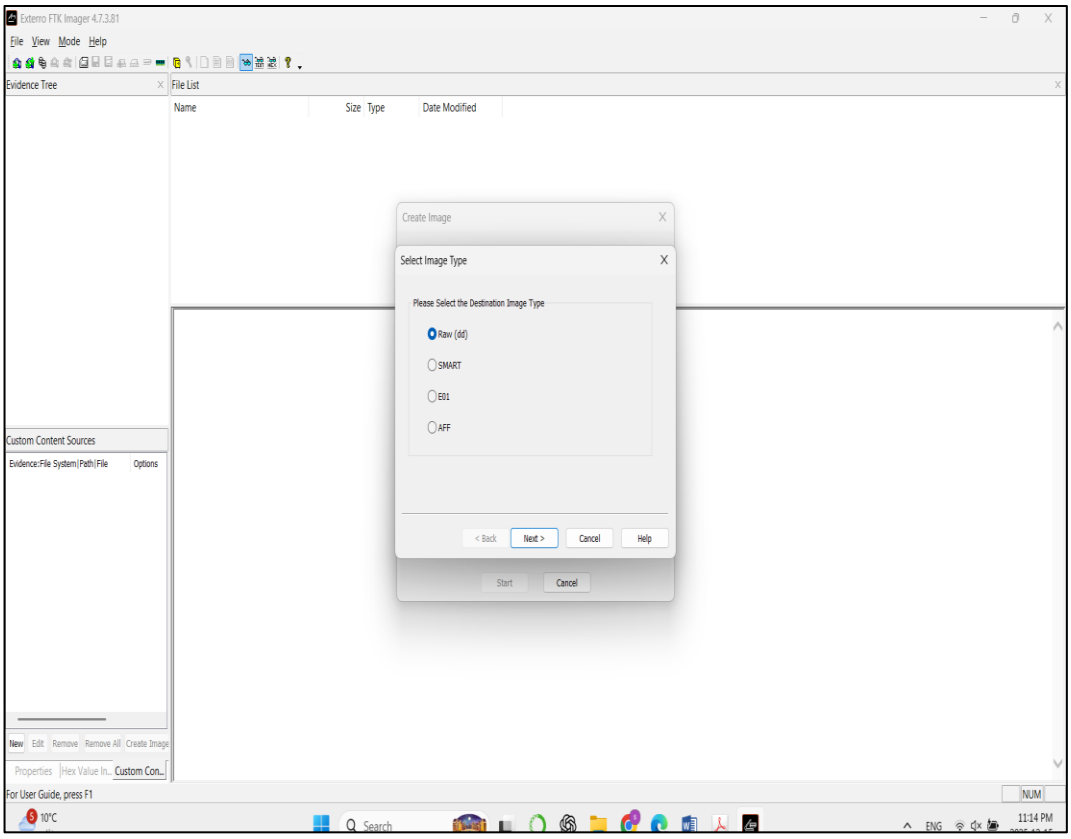



- Physical Drive قرص كامل
- Logical Drive قسم معين

5- تحديد القرص المطلوب نسخه:

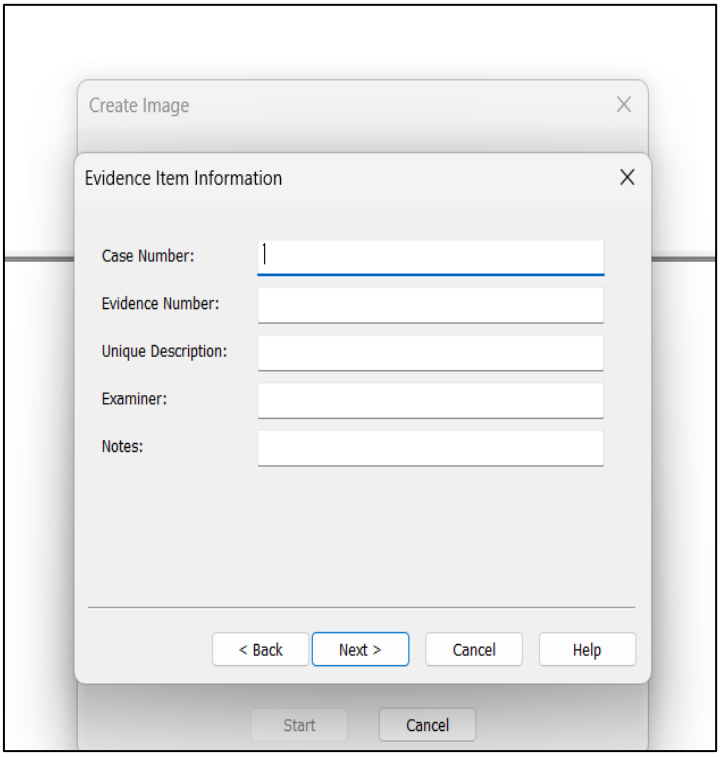



6- بعد ضغط finish تظهر قائمة لاختيار نوع ملف الصورة من add كما موضح ادناه:




يتم اختبار نوع (E10) لأنه الأكثر استخدامًا في التحقيقات الجنائية

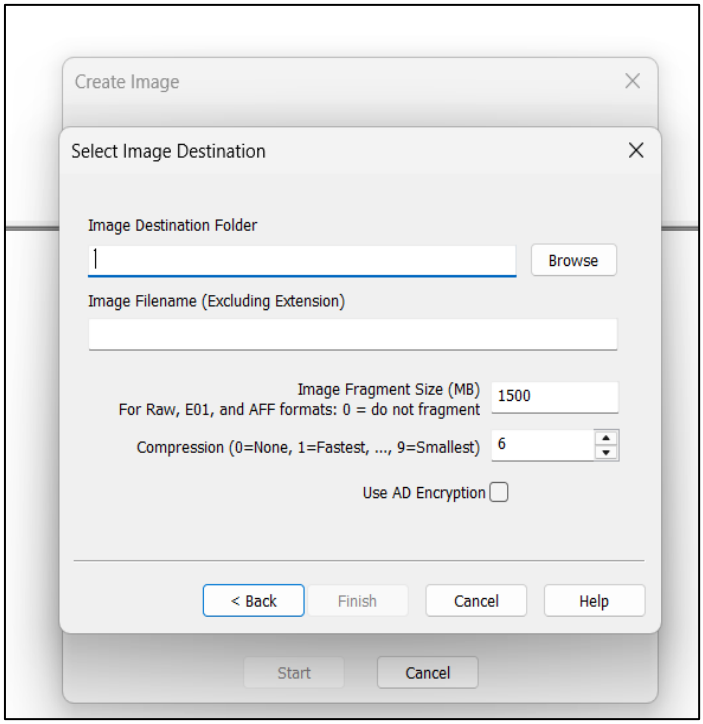
7- إدخال بيانات الدليل: بعدها يتم ادخال معلومات الدليل كما موضح بالشكل ادناه:




8- تحديد مكان حفظ النسخة: بعدها يتم تحديد مكان حفظ النسخة

9- تفعيل خيار **Verify Image after Creation**.

10- بدء عملية النسخ، وكما موضح بالشكل ادناه:



| **استمارة قائمة الفحص** | | | | |
|---|---|---|---|---|
| اسم الطالب: المرحلة: الثالثة<br>التخصص: | | | | |
| اسم التمرين: استخدام برنامج FTK Imager لإنشاء نسخة طبق الأصل رقم التمرين:7 | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | % 5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | % 15 | | |
| 3 | مراحل تنفيذ التمرين. | % 15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

### 1-2-3 استخدام قيم التجزئة (Hash Values) للتحقق من سلامة الدليل

تُستخدم قيم التجزئة للتحقق من سلامة الأدلة الرقمية، إذ تمثل قيمة رقمية فريدة تنتج عن تطبيق خوارزمية رياضية مثل MD5 أو SHA-1 أو SHA-256 على البيانات. ويؤدي أي تعديل في محتوى الدليل إلى تغيّر هذه القيمة، مما يسمح باكتشاف أي عبث أو تلف.

وعادةً يتم حساب قيم التجزئة في المراحل الآتية:

- عند ضبط الدليل الأصلي.
- بعد إنشاء النسخة الجنائية.
- قبل تقديم الدليل للجهة المختصة.

ويتم توثيق هذه القيم ضمن ملف القضية لضمان إمكانية الرجوع إليها عند الحاجة.

**رقم التمرين: 8** **الزمن المخصص: 3 ساعات**

اسم التمرين: فحص سلامة الأدلة الرقمية باستخدام برنامجHashCalc

**مكان التنفيذ: مختبر الحاسوب**

**أولاً: الأهداف التعليمية:**

تدريب الطالب على استخدام برنامج HashCalc لحساب قيم التجزئة والتحقق من سلامة الأدلة الرقمية وعدم تعرضها للتلاعب.

**ثانياً: التسهيلات العلمية:**

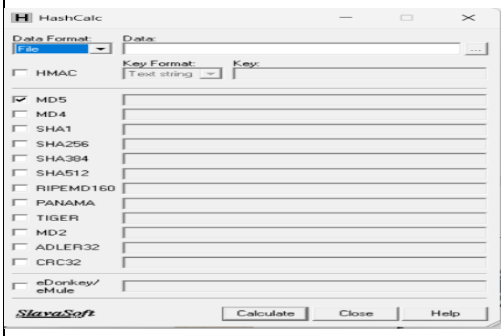
مختبر حاسوب مجهز، برنامج HashCalc، ملف دليل رقمي أو ملف صورة جنائية، وإشراف علمي.

خطوات تنفيذ التمرين:

1- ارتد بدلة العمل وشغل برنامج HashCalc.

2- ومن ثم قم باختيار خوارزمية التجزئة: MD5

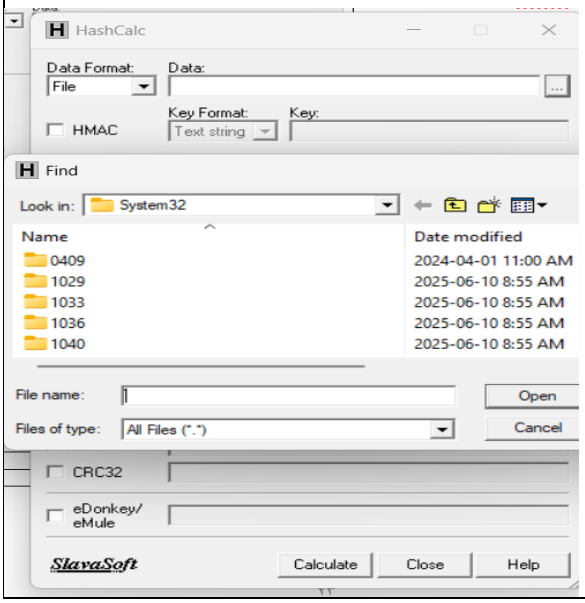
او SHA-1.




3- من الاختيارdata تحديد ملف الدليل أو ملف الصورة ومن ثم فتحه open

4- الضغط على Calculate.

5- مقارنة قيمة الـ Hash مع القيمة الأصلية.




| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب:<br>التخصص: | | | المرحلة: الثالثة | |
| اسم التمرين: فحص سلامة الأدلة الرقمية باستخدام برنامج HashCalc<br>رقم التمرين:8 | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

### 2-2-3 استخدام أدوات منع الكتابة (Write Blockers)

تُعد أدوات منع الكتابة من الوسائل الأساسية للحفاظ على سلامة الأدلة الرقمية، إذ تمنع أي عملية كتابة أو تعديل على وسيط التخزين أثناء الفحص، وتسمح بقراءة البيانات فقط، مما يعزز موثوقية إجراءات التحقيق.

#### 1-2-2-3 أنواع أدوات منع الكتابة

تنقسم أدوات منع الكتابة إلى نوعين رئيسيين:

**1- أدوات منع الكتابة المادية (Hardware Write Blockers):**

وهي أجهزة خارجية تعتمد على حماية على مستوى العتاد، وتُعد الأكثر أمانًا، ومن أشهرها: Tableau وWiebeTech.

**2- أدوات منع الكتابة البرمجية (Software Write Blockers):**

وهي برامج تمنع عمليات الكتابة عبر نظام التشغيل، مثل ( WriteProtect و Windows Forensic Environment WinFE)، وتُعد أقل موثوقية مقارنة بالأدوات المادية.

**رقم التمرين: 9** **الزمن المخصص: 3 ساعات**

اسم التمرين: استخدام أدوات Write Blockers أثناء استخراج الأدلة

أداة removable access tool (Ratool)

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الأهداف التعليمية:**

تعريف الطالب بدور أدوات Write Blockers في منع التعديل على الأدلة الرقمية، وتطبيق استخدامها أثناء استخراج الأدلة للحفاظ على سلامتها.

**ثانياً: التسهيلات العلمية:**

مختبر حاسوب مجهز، أدوات Write Blockers (مادية أو برمجية)، وسائط تخزين رقمية تجريبية، وإشراف علمي.

**خطوات تنفيذ التمرين:**

1- ارتد بدلة العمل فتح أداة removable access tool (Ratool) كما موضح بالشكل ادناه.

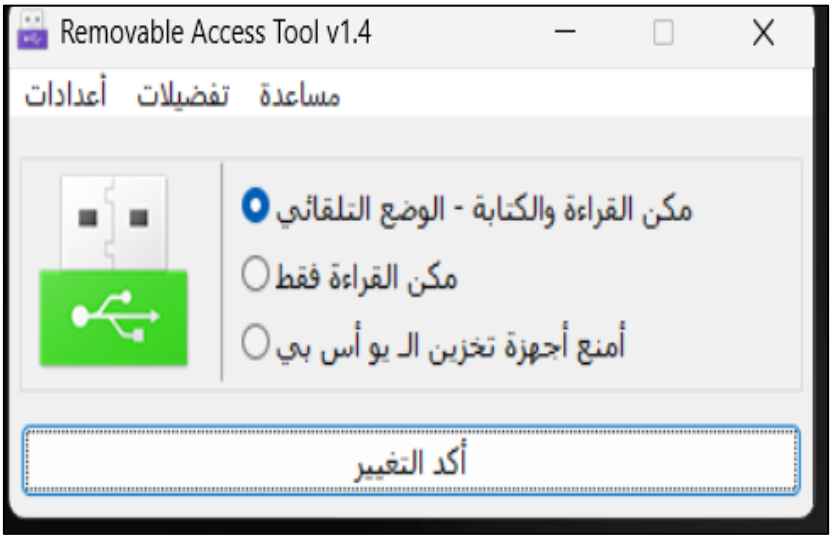
2- من الشكل الموضح نلاحظ ان:

- خيار: تمكين القراءة والكتابة – الوضع الافتراضي يسمح بالوصول الكامل إلى وسائط التخزين (قراءة وكتابة)، ويُستخدم في الحالات العادية ولا يُنصح به أثناء التحقيق الجنائي الرقمي
- خيار :تمكين القراءة فقط ويسمح بقراءة البيانات دون السماح بأي تعديل عليها، ويُعد الخيار المناسب لاستخدامه كـ Software Write Blocker أثناء فحص الأدلة الرقمية
- خيار: منع أجهزة التخزين USB أو CD

يقوم بمنع النظام من التعرف على وسائط التخزين القابلة للإزالة، ويُستخدم لحماية الجهاز من إدخال وسائط خارجية غير مصرح بها.

اما زر (أكد التغيير) فيُستخدم لتطبيق الإعداد المحدد، ولا يصبح الخيار فعالًا إلا بعد الضغط على هذا الزر.

والأيقونة الجانبية رمزUSB ترمز إلى أن الأداة مخصصة للتحكم بأجهزة التخزين القابلة للإزالة.




3- الشكل المجاور يوضح قائمة تفضيلات وكالاتي:

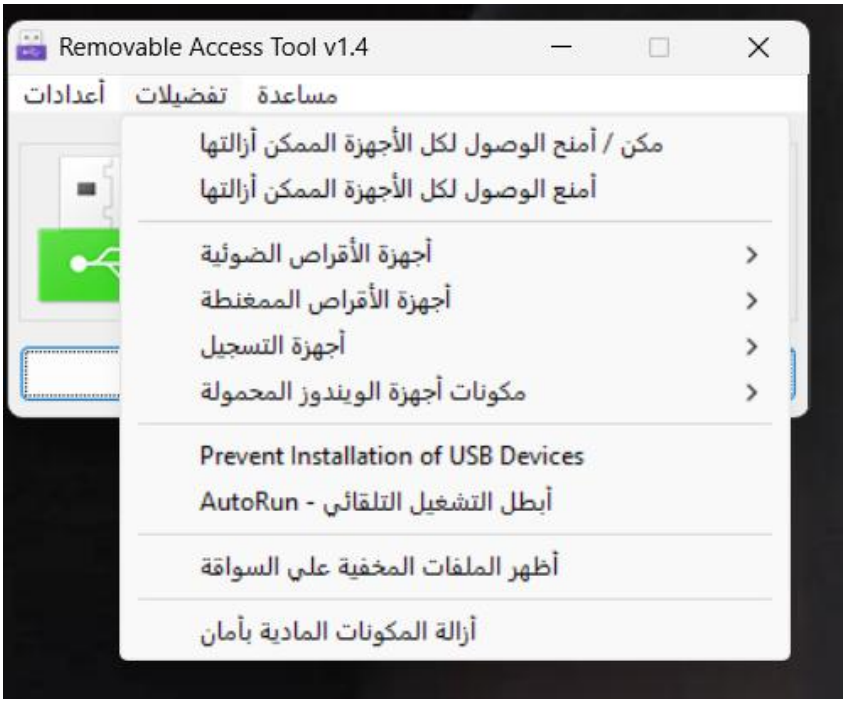
- منع / السماح بالوصول للأجهزة القابلة للإزالة: يستخدم لسماح أو منع الوصول إلى جميع أجهزة التخزين القابلة للإزالة، ويُستخدم لحماية النظام من إدخال وسائط غير مصرح بها أثناء التحقيق.
- أجهزة الأقراص الضوئية (CD / DVD): يُستخدم للتحكم في الوصول إلى الأقراص الضوئية
- أجهزة الأقراص المحمولة (USB Storage) ويسمح بالتحكم في وحدات التخزين المحمولة ويُستخدم لتفعيل وضع القراءة فقط ((Read-Only أثناء فحص الأدلة.

- اجهزة التسجيل: ويتحكم في السماح أو منع أجهزة التسجيل مثل: أجهزة النسخ، أجهزة التسجيل الخارجي. ويُستخدم لمنع نسخ البيانات أو تسريبها.
- مكونات أجهزة الواجهة المحمولة: يتيح التحكم في مكونات الأجهزة المحمولة المتصلة بالنظام، مثل الهواتف أو وحدات التخزين الخاصة بها، ويُستخدم لتقليل المخاطر الأمنية.

-revent Installation of USB Devices - : خيار يمنع تثبيت أي جهاز USB جديد على النظام، ويُعد إجراءً وقائيًا مهمًا في بيئات التحقيق الجنائي الرقمي.

– إيقاف التشغيل التلقائي AutoRun:يُستخدم لتعطيل خاصية التشغيل التلقائي للأجهزة، وذلك لمنع تشغيل أي ملفات ضارة فور توصيل وسيط التخزين.

- إظهار الملفات المخفية على السواقة:يتيح عرض الملفات المخفية داخل وسائط التخزين، وهو مفيد لاكتشاف ملفات مخفية أو آثار نشاط مشبوه.
- إزالة المكونات المادية بأمان: يُستخدم لفصل أجهزة التخزين بطريقة آمنة، مما يمنع تلف البيانات أو فقدان الأدلة الرقمية.



| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب:<br>التخصص : | | | المرحلة: الثالثة | |
| **اسم التمرين: استخدام أدوات Write Blockers أثناء استخراج الأدلة**<br>**( (أداة Ratool) (removable access tool))**<br>رقم التمرين:9 | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

### 3-2-3 التخزين الآمن للأدلة الرقمية

يقصد بالتخزين الآمن حفظ الأدلة الرقمية في بيئة محمية تضمن عدم تعرضها للتلف الفيزيائي أو التغيير الرقمي أو الوصول غير المصرح به، سواء أثناء التحقيق أو بعد انتهائه.

#### 3-2-3-1 أهداف التخزين الآمن

يهدف التخزين الآمن إلى:

1- حماية الأدلة من التلف أو الفقدان.

2- منع الوصول غير المصرح به.

3- الحفاظ على سلامة البيانات الرقمية.

4- ضمان إمكانية الرجوع إلى الأدلة عند الحاجة.

#### 3-2-3-2 أنواع التخزين الآمن

1) **التخزين الفيزيائي:**

- **حفظ وسائط التخزين في خزائن مغلقة.**
- **استخدام حقائب مضادة للكهرباء الساكنة.**
- **وضع ملصقات تعريف واضحة على كل دليل.**

2) **التخزين الرقمي:**

- **حفظ الأدلة داخل خوادم محمية.**
- **استخدام كلمات مرور قوية وتقنيات تشفير.**
- **تحديد صلاحيات الوصول للمختصين فقط.**

#### 3-2-3-3 إجراءات التخزين الآمن

1- عدم توصيل وسائط الأدلة بأجهزة غير مخصصة للفحص.

2- استخدام أنظمة مراقبة للدخول إلى غرفة الأدلة.

3- الاحتفاظ بنسخة احتياطية في موقع منفصل.

4- فحص سلامة الأدلة دوريًا باستخدام قيم التجزئة.

## 3-3 تحليل الأدلة المستخرجة من الحواسيب واجهزة الهاتف

تُركّز مرحلة تحليل الأدلة الرقمية على فحص البيانات المستخرجة وتفسيرها بهدف الوصول إلى معلومات تدعم فهم الحادثة الرقمية وتحديد المسؤوليات. ويتم تنفيذ التحليل وفق منهجية فنية منظمة لضمان دقة النتائج وإمكانية الاستفادة منها في التقرير النهائي.

ينقسم تحليل الأدلة الرقمية إلى قسمين رئيسيين:

- تحليل الأدلة المستخرجة من الحواسيب.
- تحليل الأدلة المستخرجة من الهواتف الذكية.

### 3-3-1 تحليل الأدلة المستخرجة من الحواسيب

تُعد الحواسيب من أهم مصادر الأدلة الرقمية، نظرًا لما تحتويه من ملفات وسجلات وأنشطة استخدام متنوعة. ويشمل تحليلها المراحل الآتية:

**1- التحضير لعملية التحليل**

قبل البدء في التحليل، يجب مراعاة ما يأتي:

- العمل على نسخة جنائية (Forensic Image) بدلًا من القرص الأصلي.
- التحقق من قيمة التجزئة (Hash) لضمان سلامة النسخة.
- استخدام محطة عمل جنائية مخصصة.
- توثيق خطوات التحليل والأدوات المستخدمة.

**2- تحليل نظام الملفات (File System Analysis)**

يتم فحص نظام الملفات للتعرّف على أنواع الملفات الموجودة، والملفات التي أُنشئت أو عُدلت حديثًا، والملفات المحذوفة وآثارها، والبيانات الوصفية (Metadata) ويساعد ذلك في تحديد نشاط المستخدم وإنشاء خط زمني للأحداث.

**3- استعادة الملفات المحذوفة**

يمكن باستخدام أدوات التحليل الجنائي استعادة الملفات المحذوفة من المساحات غير المستخدمة في القرص، ومعرفة خصائصها قبل الحذف، مما يسهم في الكشف عن الأدلة المخفية.

**4- تحليل سجلات النظام (System Logs)**

تشمل سجلات النظام معلومات مهمة مثل: سجلات الدخول والخروج، وسجلات تثبيت أو حذف البرامج، والسجلات الأمنية. ويساعد تحليلها في تحديد المستخدم وقت الحادث والكشف عن أي نشاط غير طبيعي.

**5- تحليل نشاط الإنترنت (Internet Activity)**

يتضمن تحليل نشاط الإنترنت فحص المواقع التي تم الوصول إليها والملفات التي تم تنزيلها وعمليات البحث كلمات المرور المحفوظة وملفات الارتباط (Cookies). ويساعد ذلك في فهم سلوك المستخدم أو ارتباطه بأنشطة مشبوهة.

**6- الكشف عن البرمجيات الخبيثة (Malware Detection)**

يتم فحص النظام لاكتشاف البرمجيات الخبيثة أو أدوات الاختراق باستخدام برامج متخصصة وأدوات تحليل الملفات التنفيذية.

**7- تحليل الملفات والوثائق**

يشمل ذلك فحص المستندات وتحليل البيانات الوصفية للصور والملفات، واستخراج الكلمات المفتاحية ذات الصلة بالقضية.

### 3-3-2 تحليل الأدلة المستخرجة من الهواتف الذكية

تُعد الهواتف الذكية مصدرًا مهمًا للأدلة الرقمية لاحتوائها على بيانات شخصية واتصالية ومعلومات مواقع.

**1- تحليل الرسائل وسجلات المكالمات**

يشمل فحص الرسائل النصية وتطبيقات المراسلة وسجلات المكالمات، مما يساعد في تحديد علاقات المستخدم وتوقيت الاتصالات.

**2- تحليل الصور والوسائط (Media Analysis)**

يتم تحليل محتوى الصور والوسائط إضافة إلى بياناتها الوصفية (EXIF) مثل وقت الالتقاط والموقع الجغرافي ونوع الجهاز.

**3- تحليل بيانات المواقع الجغرافية (Location Data)**

تشمل بيانات GPS والأبراج الخلوية وسجل المواقع، وتُستخدم لتتبع تحركات المستخدم.

**4- تحليل التطبيقات (App Analysis)**

يتضمن فحص تطبيقات التواصل الاجتماعي والبريد الإلكتروني والتطبيقات البنكية، واستخراج المحادثات والملفات وبيانات الحسابات.

**5- استعادة البيانات المحذوفة من الهاتف**

تُستخدم أدوات متخصصة مثل Cellebrite UFED و Magnet AXIOM لاستعادة البيانات المحذوفة، مما قد يكشف عن محاولات إخفاء الأدلة.

## 4-3 تحليل الشبكات وتحديد مصادر الهجمات

يُقصد بتحليل الشبكات فحص حركة البيانات المتبادلة داخل الشبكة أو بين الأجهزة والإنترنت، بهدف اكتشاف الأنشطة غير المشروعة مثل الاختراق أو التجسس أو سرقة البيانات أو نشر البرمجيات الخبيثة. وتكتسب هذه المرحلة أهمية خاصة لأن كثيرًا من الهجمات الإلكترونية تظهر آثارها في سجلات الشبكة وحزم البيانات أكثر من ظهورها داخل ملفات الأجهزة.

### 3-4-1 أهداف تحليل الشبكات في التحقيق الجنائي الرقمي

عند إجراء تحليل للشبكة، يسعى المحقق إلى:

1- معرفة كيف حصل الهجوم (طريقة الدخول).

2- تحديد مصدر الهجوم (IP أو جهاز مهاجم).

3- معرفة ما الذي تم استهدافه (خدمة، جهاز، حساب).

4- تحديد هل تم تسريب بيانات أم لا.

5- توثيق الوقت والتاريخ الذي حصل فيه الهجوم.

6- جمع أدلة رقمية يمكن استخدامها في التقرير النهائي.

### 3-4-2 مصادر الأدلة الشبكية

تعتمد عملية تحليل الشبكات في التحقيق الجنائي الرقمي على مجموعة من مصادر الأدلة الشبكية التي توفّر معلومات دقيقة عن حركة البيانات والاتصالات داخل الشبكة، وتُستخدم هذه المصادر لاكتشاف الأنشطة غير المشروعة وتحديد مصادر الهجمات الإلكترونية. ومن أهم هذه المصادر ما يأتي:

**1- ملفات التقاط الحزم (PCAP):** وهي ملفات تحتوي على تسجيل لحزم البيانات المتبادلة عبر الشبكة خلال فترة زمنية محددة، وتُستخدم لتحليل الاتصالات، وتحديد البروتوكولات المستخدمة، والكشف عن السلوكيات غير الطبيعية التي قد تشير إلى وجود هجوم إلكتروني.

**2- سجلات الجدار الناري (Firewall Logs):** تسجّل هذه السجلات الاتصالات المسموح بها والمرفوضة بين الشبكة الداخلية والخارجية، وتساعد في اكتشاف محاولات الوصول غير المصرح بها، وتحديد عناوين IP المشبوهة والمنافذ المستهدفة.

**3- سجلات الموجّهات (Router Logs):** توفّر معلومات عن مسارات حركة البيانات داخل الشبكة، وتُستخدم لتتبّع مصدر الاتصالات وتحديد اتجاهها، مما يساعد في كشف الهجمات الصادرة من داخل الشبكة أو خارجها.

**4- سجلات الخوادم:** تشمل سجلات خوادم الويب والبريد وقواعد البيانات، وتوضّح الطلبات الواردة إلى الخوادم، وأوقات الوصول، وعناوين الأجهزة المتصلة، مما يسهم في اكتشاف الهجمات التي تستهدف الخدمات الشبكية.

**5- سجلات أنظمة التشغيل:** هي السجلات التي ينشئها نظام التشغيل لتوثيق الأنشطة الشبكية والأمنية، مثل محاولات تسجيل الدخول والاتصال بالشبكة، وتُعد مصدراً مهماً لربط النشاط الشبكي بسلوك المستخدم أو الجهاز.

### 3-4-3 مفاهيم أساسية

حتى يتم تحليل الشبكات بصورة صحيحة ضمن التحقيق الجنائي الرقمي، يجب الإلمام بعدد من المفاهيم الأساسية المرتبطة بآلية عمل الشبكات والاتصالات، ومن أهمها ما يأتي:

**1- عنوان IP (Internet Protocol Address):** هو عنوان رقمي يُمنح لكل جهاز متصل بالشبكة، ويُستخدم للتعرّف على مصدر ووجهة البيانات، وقد يكون عنوانًا داخليًا ضمن الشبكة المحلية أو عنوانًا عامًا على الإنترنت.

**2- عنوان MAC (Media Access Control Address):** هو معرف فريد يُخصص لبطاقة الشبكة داخل الجهاز، ويُستخدم داخل الشبكات المحلية لتحديد الأجهزة بدقة.

- **المنافذ (Ports):** تمثل المنافذ نقاط اتصال تستخدمها الخدمات الشبكية المختلفة، حيث تعمل كل خدمة على منفذ محدد، مثل: منفذ رقم 80 لبروتوكول HTTP، ومنفذ رقم 443 لبروتوكول HTTPS، ومنفذ رقم 53 لبروتوكول DNS. وغالبًا ما تستهدف الهجمات الإلكترونية منافذ معينة مرتبطة بخدمات حساسة.

**3- البروتوكولات (Protocols):** البروتوكول هو مجموعة من القواعد التي تنظم عملية إرسال واستقبال البيانات بين الأجهزة، ومن أهم البروتوكولات المستخدمة في تحليل الشبكات:

- TCP: بروتوكول موثوق يضمن وصول البيانات كاملة وبالترتيب الصحيح.
- UDP: بروتوكول غير موثوق يُستخدم في الاتصالات السريعة.
- DNS: مسؤول عن تحويل أسماء النطاقات إلى عناوين IP.
- HTTP / HTTPS: بروتوكولات تصفح الويب، حيث يوفر HTTPS اتصالًا مشفّرًا.
- ICMP: يُستخدم لاختبار الاتصال بين الأجهزة، مثل أمر Ping.

### 3-4-4 خطوات تحليل الشبكات وتحديد مصدر الهجوم

تُعد عملية تحليل الشبكات من الإجراءات الأساسية في التحقيق الجنائي الرقمي، وتهدف إلى الكشف عن الأنشطة غير المشروعة داخل الشبكات وتحديد مصدر الهجوم اعتمادًا على الأدلة الرقمية المتاحة. وتتم هذه العملية وفق خطوات منهجية متسلسلة، كما يأتي:

**1- تحديد نطاق التحليل:** تبدأ عملية التحليل بتحديد نطاق التحقيق، ويشمل ذلك الشبكة أو الجهاز المستهدف، وطبيعة الحادثة، والفترة الزمنية المتوقعة لوقوع الهجوم، مما يساعد على تقليل حجم البيانات محل الفحص.

**2- جمع بيانات الشبكة:** يتم في هذه المرحلة جمع الأدلة الشبكية من مصادر متعددة، كما هو موضح في موضوع مصادر الأدلة الشبكية.

**3- تصفية البيانات وتحليلها:** نظرًا لكثرة البيانات الشبكية، تُطبّق عمليات تصفية لتحديد الحزم أو السجلات ذات الصلة بالاعتماد على عناوين IP أو المنافذ أو البروتوكولات أو الإطار الزمني، بهدف عزل النشاط المشبوه عن الحركة الطبيعية للشبكة.

**4- اكتشاف مؤشرات الهجوم:** يتم تحليل البيانات المصفاة لاكتشاف مؤشرات تدل على وجود هجوم إلكتروني، مثل تكرار محاولات الاتصال، أو استهداف منافذ حساسة، أو وجود اتصالات مع عناوين خارجية غير موثوقة.

**5- تتبع مصدر الهجوم:** بعد تحديد النشاط المشبوه، يتم تتبع مصدره من خلال تحليل عناوين IP ومقارنتها بعناوين الشبكة الداخلية والخارجية، إضافة إلى مراجعة سجلات DHCP وعناوين MAC عند الحاجة.

**6- توثيق النتائج:** تُختتم عملية التحليل بتوثيق النتائج بشكل منظم، ويتضمن ذلك وصف طبيعة الهجوم، ومصدره، وتوقيته، والأدلة الرقمية الداعمة، تمهيدًا لاستخدامها في التقرير النهائي..

### 3-4-5 مؤشرات الهجمات الشبكية

تُعرَّف مؤشرات الهجمات الشبكية بأنها علامات أو سلوكيات غير طبيعية تظهر في حركة الشبكة، وقد تدل على وجود هجوم إلكتروني أو نشاط غير مشروع. ومن أبرز هذه المؤشرات ما يأتي:

**1- تكرار محاولات الاتصال خلال فترة قصيرة:** يشير إلى قيام جهاز واحد أو عنوان IP بعدد كبير من محاولات الاتصال خلال وقت قصير، وغالبًا ما يدل ذلك على محاولة اختراق أو تخمين كلمات المرور.

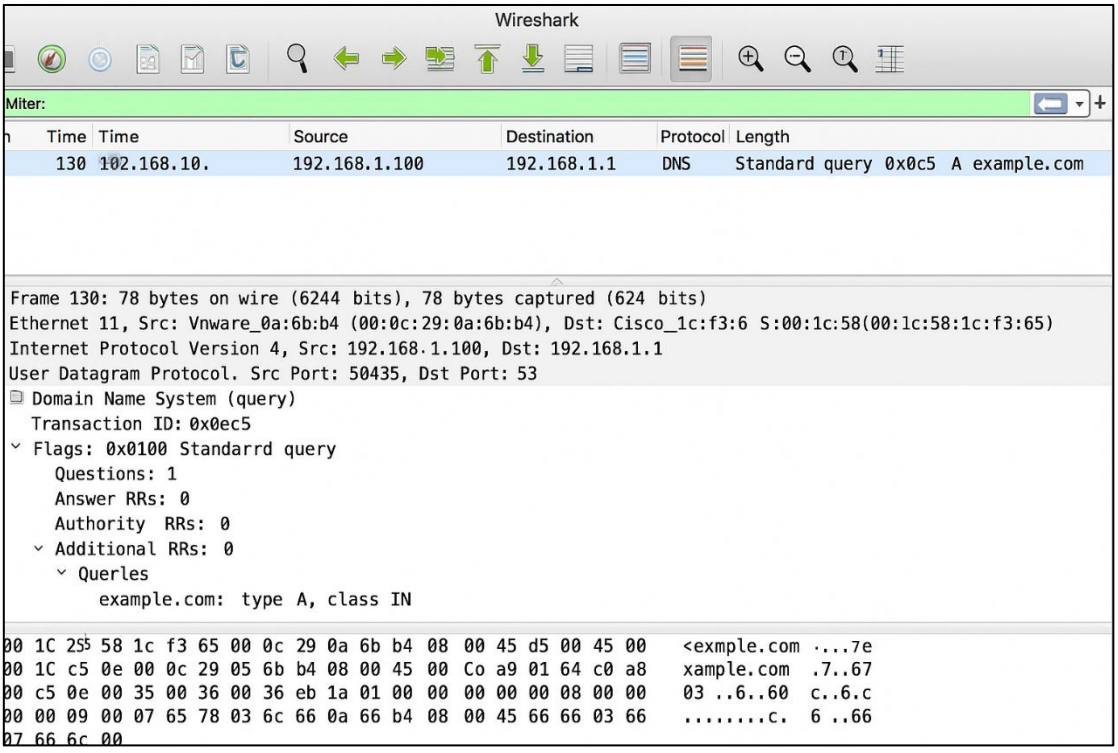
**2- استهداف منافذ حساسة:** تُعد المنافذ الحساسة هي المنافذ المرتبطة بخدمات مهمة داخل النظام، ويُعد تكرار الاتصال بهذه المنافذ مؤشرًا محتملًا على وجود محاولة اختراق. ويوضح جدول (3-1) أرقام المنافذ الشائعة المستهدفة.

**جدول (3-1) يبيّن أرقام المنافذ الشائعة.**

| رقم المنفذ | اسم الخدمة | الاستخدام |
|---|---|---|
| 22 | SSH | الاتصال الآمن والتحكم عن بُعد بالأجهزة |
| 80 | HTTP | تصفح مواقع الإنترنت غير المشفّرة |
| 443 | HTTPS | تصفح مواقع الإنترنت المشفّرة والآمنة |
| 53 | DNS | تحويل اسم الموقع إلى عنوان IP |
| 21 | FTP | نقل الملفات بين الأجهزة |
| 25 | SMTP | إرسال البريد الإلكتروني |
| 110 | POP3 | استلام البريد الإلكتروني |

**1- اتصالات غير معتادة مع عناوين خارجية:** عندما يتصل جهاز داخل الشبكة بعناوين خارجية غير معروفة أو مشبوهة، فقد يدل ذلك على وجود تحكم عن بُعد أو محاولة تسريب بيانات.

**2- طلبات DNS مشبوهة:** ظهور طلبات DNS لأسماء نطاقات غريبة أو غير معروفة قد يشير إلى برمجيات خبيثة تحاول الاتصال بخوادم خارجية.




**شكل (3- 3) يوضح طلب DNS داخل برنامج Wireshark**

3- نقل بيانات غير طبيعي: **زيادة مفاجئة في حجم البيانات المرسلة خارج الشبكة. وهذا قد يدل على سرقة أو تسريب معلومات.**

### 3-4-6 أنواع الهجمات التي يمكن اكتشافها عبر تحليل الشبكات

يمكن لتحليل الشبكات الكشف عن عدة أنواع من الهجمات الإلكترونية، من أبرزها ما يأتي:

1- فحص المنافذ (Port Scanning): يقوم المهاجم بمحاولة معرفة المنافذ المفتوحة على الجهاز أو الخادم، ويظهر ذلك على شكل اتصالات متعددة تستهدف منافذ مختلفة خلال فترة قصيرة.

2- هجمات تخمين كلمات المرور (Brute Force): تتضمن محاولات متكررة لتجربة كلمات مرور مختلفة، وتظهر عادةً في سجلات الشبكة أو الأنظمة على شكل محاولات دخول فاشلة متتالية.

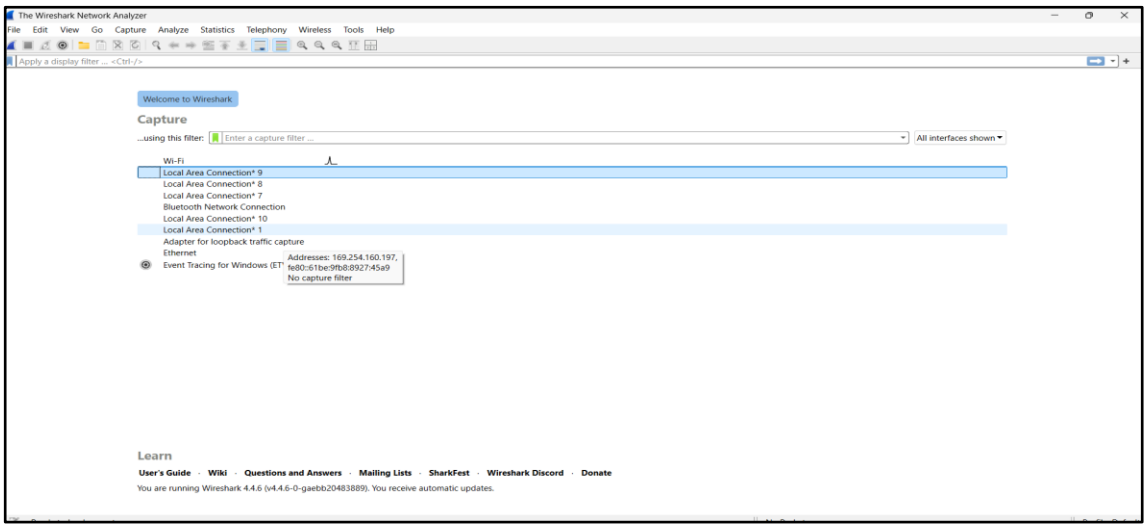
3- هجمات حجب الخدمة (DoS / DDoS): تهدف إلى إغراق الشبكة أو الخادم بعدد كبير من الطلبات، مما يؤدي إلى بطء الخدمة أو توقفها بشكل كامل.

4- التصيد الإلكتروني (Phishing): تعتمد على خداع المستخدم لحثّه على زيارة مواقع مزيفة أو إدخال بياناته الشخصية، وتظهر من خلال اتصالات مع مواقع مشبوهة أو روابط غير موثوقة.

5- تسريب البيانات (Data Exfiltration): يتم فيها نقل بيانات حساسة خارج الشبكة دون تصريح، ويظهر ذلك غالبًا على شكل حركة بيانات كبيرة وغير طبيعية.

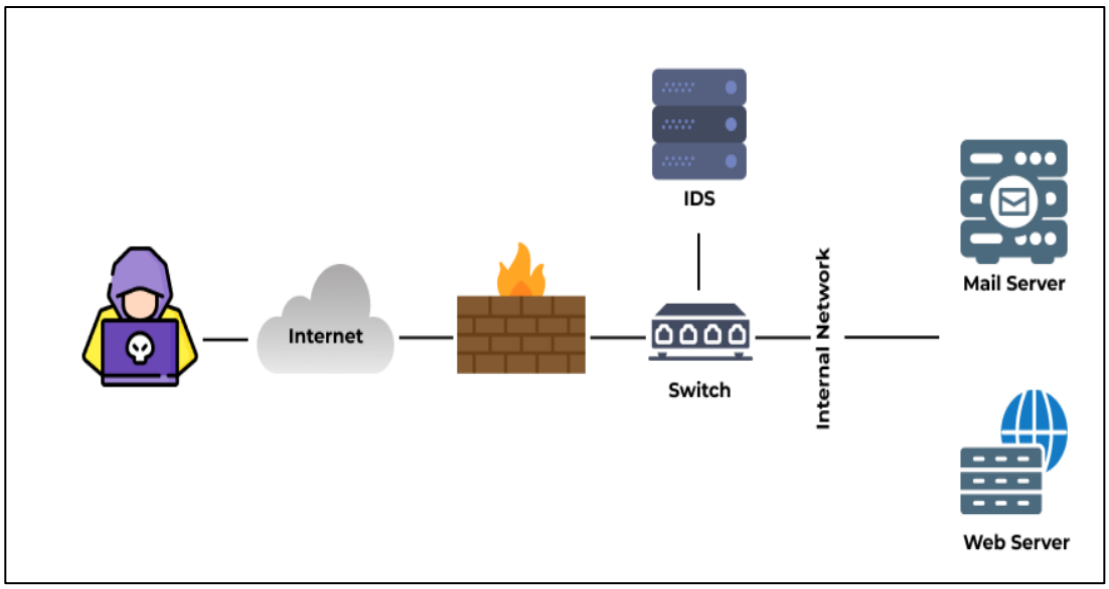
### 3-4-7 أدوات تحليل الشبكات:

**1- Wireshark :** وهي اداة تُستخدم لالتقاط وعرض وتحليل حزم البيانات داخل الشبكة، وتساعد في تحديد نوع الاتصال، وعناوين المصدر والوجهة، والبروتوكولات المستخدمة.




شكل (3-4) برنامج Wireshark

**2- انظمة كشف ومنع التسلل (IDS / IPS) مثل Snort:** أنظمة تُستخدم لمراقبة حركة الشبكة بشكل مستمر، والكشف عن الهجمات الإلكترونية تلقائيًا، وإصدار تنبيهات عند اكتشاف نشاط مشبوه.




**شكل (3-5) يوضح IDS بين الشبكة والإنترنت.**

**رقم التمرين: 10** **الزمن المخصص: 3 ساعات**

اسم التمرين: تحليل حركة البيانات عبر الشبكة باستخدام Wireshark

**مكان التنفيذ: مختبر الحاسوب**

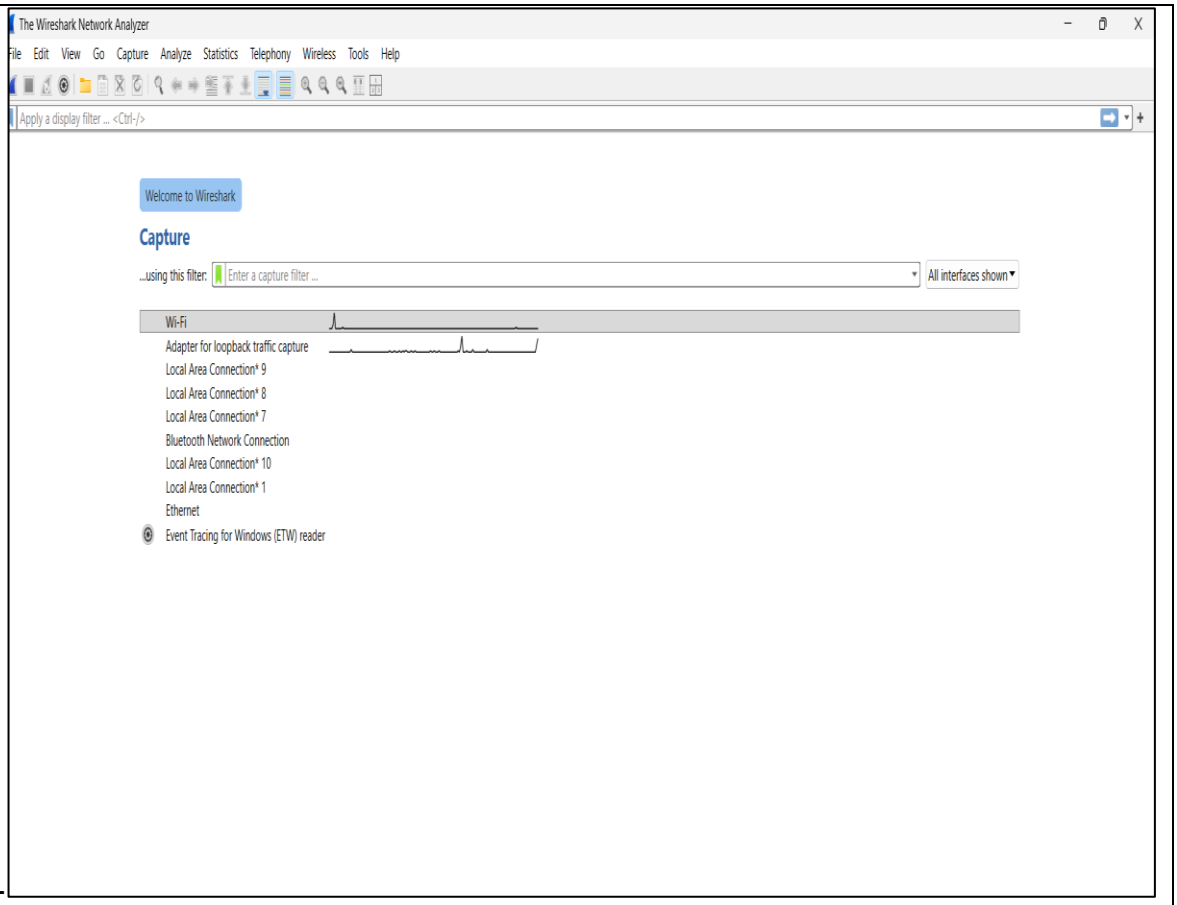
**أولاً: الأهداف التعليمية:**

تدريب الطالب على استخدام برنامج Wireshark في التقاط وتحليل حزم البيانات الشبكية، والتعرّف على البروتوكولات والاتصالات المشبوهة ضمن إطار التحقيق الجنائي الرقمي.

**ثانياً: التسهيلات العلمية:**

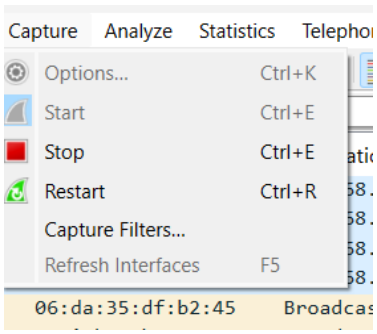
مختبر حاسوب مجهز، برنامج Wireshark، شبكة محلية أو اتصال إنترنت للتجربة، وملفات التقاط حزم (PCAP)، مع إشراف علمي أثناء التنفيذ.

1- ارتد بدلة العمل، اختيار واجهة الشبكة (Wi-Fi / Ethernet):

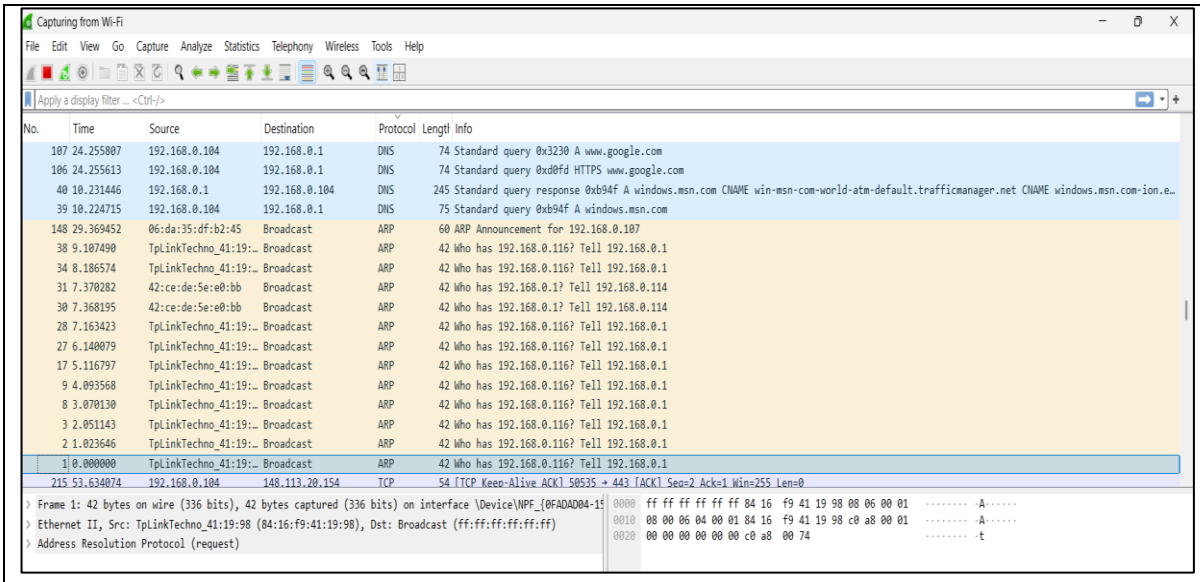



-

2- اضغط على قائمة capture الموضحة بالشكل ادناه:



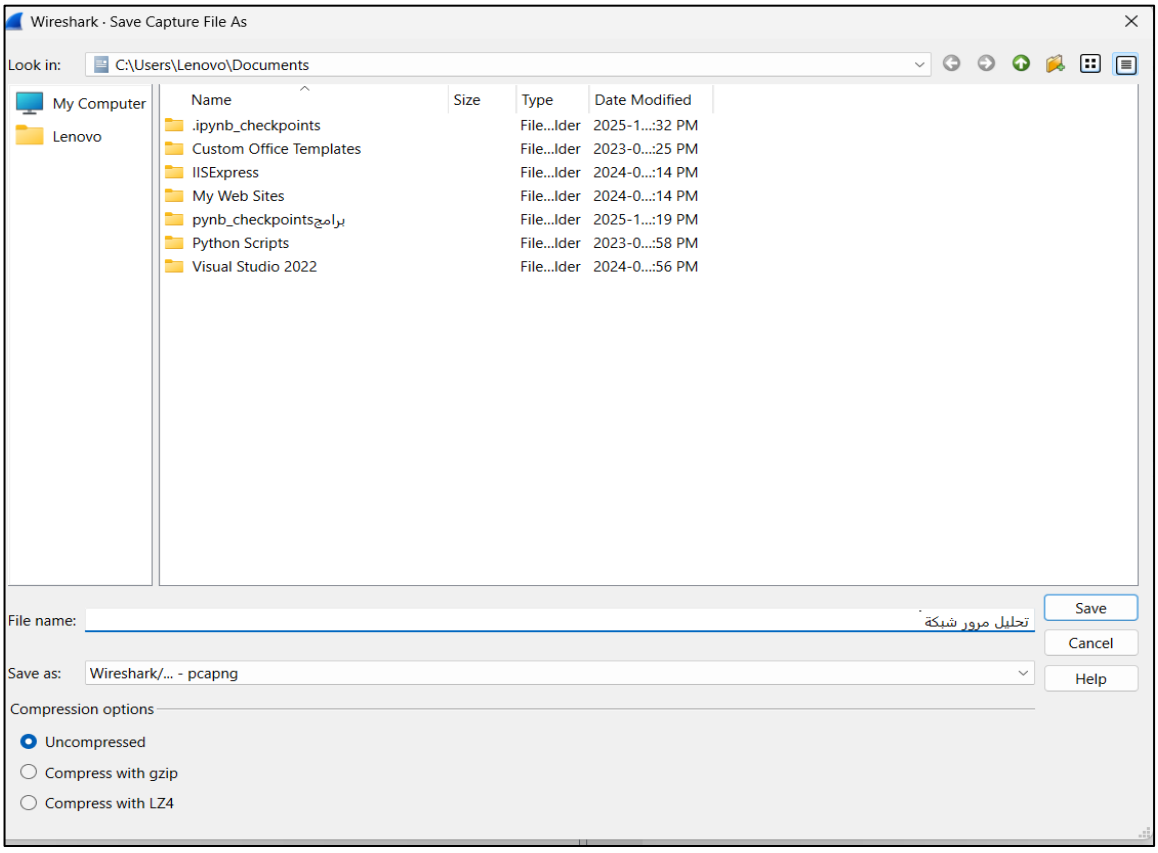

3- نضغط start، سوف تبدأ عملية التحليل وكما موضح ادناه:




- لتحليل عناوين IP، البروتوكولات، الحزم المشبوهة نختار capture filters.

- لإيقاف الالتقاط وحفظ الملف نختار stop.

سوف تظهر النافذة التالية نحدد مكان واسم ملف الحفظ وأيضا اختيار نوع الضغط :



| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب:<br>التخصص : | | | المرحلة: الثالثة | |
| **اسم التمرين: اسم التمرين: تحليل حركة البيانات عبر الشبكة باستخدام Wireshark.**<br>**رقم التمرين:10** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## 5-3 توثيق الادلة الرقمية واعداد التقارير النهائية

يقصد **بتوثيق الأدلة الرقمية** تسجيل جميع الإجراءات والخطوات التي يتم اتخاذها أثناء جمع الأدلة الرقمية وتحليلها وحفظها، منذ لحظة اكتشاف الدليل وحتى تقديم النتائج النهائية. ويهدف التوثيق إلى ضمان سلامة الأدلة الرقمية، ومنع التلاعب بها، ودعم موثوقية نتائج التحقيق. ويشمل التوثيق العلمي ما يأتي:

1- تسجيل وقت وتاريخ جمع الأدلة: يُدوّن المحقق وقت وتاريخ جمع كل دليل، مما يساعد في إنشاء تسلسل زمني دقيق للأحداث وتتبع انتقال الدليل بين الجهات المعنية.

2- تصوير موقع الأجهزة كما وُجدت: تُلتقط صور توثيقية لمكان وجود الأجهزة قبل التعامل معها، بما يشمل ترتيب الأسلاك، وحالة الشاشة، والبيئة المحيطة.

3- تسجيل بيانات الأجهزة والوسائط: يتم تدوين نوع الدليل، والأرقام التسلسلية، ونوع الوسيط الرقمي، وذلك لضمان إمكانية تتبّع الأدلة ومنع الالتباس بينها.

4- توثيق سلسلة الحيازة (Chain of Custody): يقصد بها تسجيل جميع الأشخاص الذين تعاملوا مع الدليل منذ لحظة ضبطه وحتى تقديمه للجهات المختصة، بما يضمن عدم التشكيك في صحة الأدلة.

### 1-5-3 أهمية توثيق الأدلة الرقمية

تنبع أهمية توثيق الأدلة الرقمية من كونه:

يضمن سلامة الأدلة وعدم التلاعب بها.

يدعم القبول القانوني للأدلة الرقمية.

يحدد المسؤوليات ويعزز موثوقية نتائج التحقيق.

### 2-5-3 مراحل توثيق الأدلة الرقمية

يمر توثيق الأدلة الرقمية بعدة مراحل متسلسلة، تشمل ما يأتي:

**1- توثيق بيانات الدليل:** تسجيل نوع الدليل، ومكان العثور عليه، وتاريخ ووقت الضبط، وحالة الدليل عند اكتشافه، واسم الجهة أو الشخص الذي قام بجمعه.

**2- توثيق إجراءات جمع الدليل وإنشاء النسخة الجنائية:** تسجيل الخطوات المتبعة أثناء جمع الدليل وإنشاء النسخة الجنائية (Forensic Image)، لإثبات أن العمل تم على نسخة وليس على الدليل الأصلي.

**3- توثيق عمليات التحليل:** تسجيل جميع إجراءات التحليل الفني التي أُجريت على النسخة الجنائية، مع ذكر الأدوات المستخدمة والنتائج المستخلصة.

**4- توثيق سلسلة الحيازة:** تسجيل عمليات استلام وتسليم الدليل منذ جمعه وحتى انتهاء التحقيق.

### 3-5-3 إعداد التقارير النهائية في التحقيق الجنائي الرقمي

يُعد التقرير النهائي الوثيقة الرسمية التي تُعرض فيها نتائج التحقيق الجنائي الرقمي بصورة منظمة وواضحة، ويجب أن يتسم بالدقة والموضوعية ويُكتب بلغة علمية مهنية.

**ان مكونات التقرير النهائي تشمل:**

- مقدمة التقرير: تتضمن معلومات عامة عن القضية والجهة الطالبة للتحقيق وهدفه.
- وصف الأدلة الرقمية: توضيح نوع الأدلة التي تم فحصها ومصادرها وعلاقتها بالقضية.
- المنهجية المتبعة: شرح موجز للخطوات المتبعة أثناء التحقيق والأدوات المستخدمة.
- عرض النتائج: تقديم النتائج المكتشفة بشكل منظم ومدعوم بالأدلة الرقمية.
- الاستنتاجات: تفسير النتائج وربطها بالقضية دون إبداء آراء شخصية.
- الخاتمة والتوصيات: تلخيص النتائج وتقديم توصيات لتعزيز الأمن الرقمي ومنع تكرار الحوادث.

### 3-5-4 الأدوات المستخدمة في التوثيق وإعداد التقارير

تُستخدم مجموعة من الأدوات الرقمية لدعم عملية التوثيق وإعداد التقارير، من أبرزها:

- **Autopsy** : أداة جنائية رقمية لتحليل الأقراص والملفات واستخراج الأدلة من أنظمة التشغيل المختلفة.

- **FTK Imager** : أداة لإنشاء نسخ جنائية (Forensic Images) من الأقراص والوسائط الرقمية مع الحفاظ على سلامة الدليل.

- **Wireshark** : أداة لتحليل حركة الشبكة والتقاط الحزم بهدف فحص الاتصالات واكتشاف الأنشطة المشبوهة.

- **Notecase** : أداة لتدوين وتنظيم الملاحظات بشكل هرمي تُستخدم لتوثيق التحقيقات والمعلومات الجنائية.

**كما تحمي الأسوار المدن، يحمي الأمن السيبراني مستقبل المجتمعات الرقمية**

**رقم التمرين:11** **الزمن المخصص: 3 ساعات**

اسم التمرين: **توثيق مراحل التحقيق الجنائي الرقمي باستخدام Forensic Case Notes**

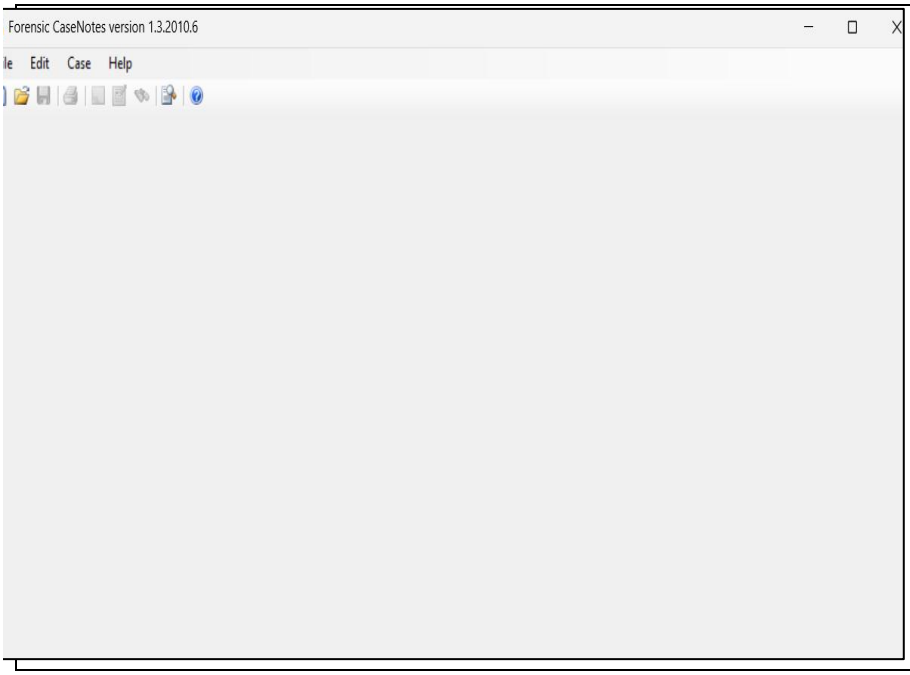
مكان التنفيذ: مختبر الحاسوب

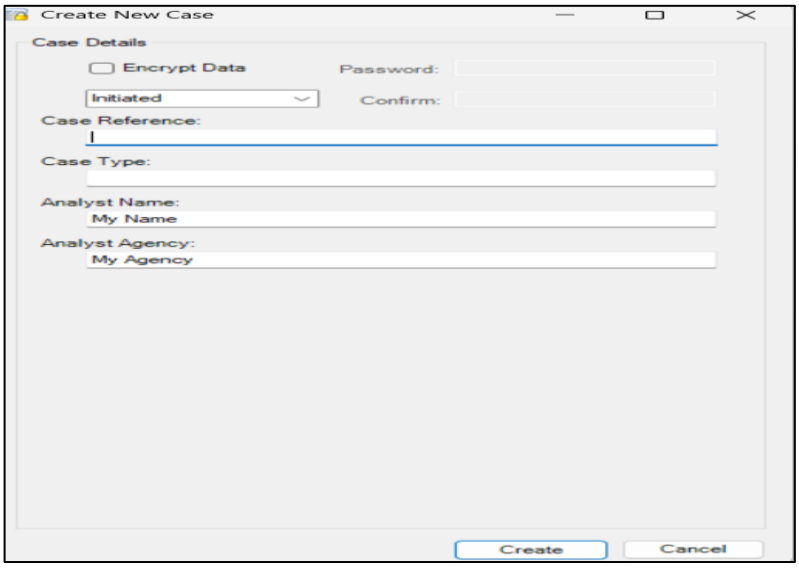
**اولاً: الأهداف التعليمية:**

تدريب الطالب على توثيق مراحل التحقيق الجنائي الرقمي بشكل منظم باستخدام Forensic Case Notes، مع تسجيل الإجراءات والنتائج بما يضمن سلامة الأدلة ومصداقية التحقيق.

**ثانياً: التسهيلات العلمية:**

مختبر حاسوب مجهز، برنامج أو نماذج Forensic Case Notes، أدلة رقمية تجريبية، وإشراف علمي أثناء تنفيذ التمرين.

| | |
|---|---|
| 1. ارتد بدلة العمل وشغل الحاسوب قم افتح أداة **forensic case notes** وسوف تظهر النافذة التالية: |  |

| | |
|---|---|
| 2-لإنشاء قضية جديدة، من قائمة file نختار الامر new حيث ستظهر النافذة الاتية: |  |
| **3- قم بأدخال التفاصيل التالية:** | - **تشفير البيانات Encrypt Data وفيها خيار لتشفير ملف القضية بالكامل حيث عند تفعيله يجب إدخال: كلمة المرور وتأكيد كلمة المرور وذلك لحماية بيانات القضية من الوصول غير المصرح به.**<br>- **حالة القضية case status: وفيها الحالة ال افتراضيةInitiated وتعني أن القضية تم إنشاؤها ولم يبدأ التحقيق بشكل كامل بعد ويمكن لاحقًا تغييرها مثلIn Progress / Closed..**<br>- **مرجع القضية Case Reference وهو حقل مهم لتعريف القضية ويُستخدم كرقم رسمي أو كود تتبع. مثال: 001-2025-DF**<br>- **نوع القضية case type: يحدد طبيعة القضية الجنائية الرقمية ومثال ذلك**<br>o Cyber Crime<br>o Data Breach<br>o Malware Investigation<br>o Network Forensics<br>- **اسم المحلل analyst name: وهو اسم الشخص المسؤول عن التحقيق.**<br>- **مؤسسة المحلل Analyst Agency وهي الجهة التي يتبع لها المحلل. مثل: University Name، Cyber Security Lab ، Digital Forensics Unit**<br>- **انشاء create: حيث يتم انشاء القضية رسميًا وبعد الضغط عليه يتم حفظ بيانات القضية يبدأ توثيق التحقيق.**<br>بعدها يتم توثيق أدوات الفحص المستخدمة ونتائج التحليل وقيم Hash. ثم حفظ وتصدير التقرير. |

| استمارة قائمة الفحص | | | | |
|---|---|---|---|---|
| اسم الطالب:<br>التخصص : | | | المرحلة: الثالثة | |
| **اسم التمرين: توثيق مراحل التحقيق الجنائي الرقمي باستخدام Forensic Case Notes**<br>**رقم التمرين:11** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## اسئلة الفصل الثالث

**س1: أكمل الفراغات التالية:**

1. تُستخدم أداة ــــــــــــ لمنع أي عملية كتابة على وسيط التخزين أثناء الفحص الجنائي.
2. يُطلق على السجل الذي يوضح انتقال الدليل بين الأشخاص اسم ــــــــــــ.
3. يُستخدم برنامج ــــــــــــ لتحليل حركة البيانات داخل الشبكة.
4. من أشهر خوارزميات التجزئة المستخدمة ــــــــــــ و ــــــــــــ.
5. يُعد توثيق وقت وتاريخ جمع الأدلة جزءًا من مرحلة ــــــــــــ.

**س2: عرف مايلي :**

الدليل الرقمي، التصوير الجنائي الرقمي، سلسلة الحيازة، قيم التجزئة

**س3: عدّد أنواع أدوات منع الكتابة (Write Blockers).**

**س4: اذكر أنواع الهجمات التي يمكن اكتشافها عبر تحليل الشبكات.**

**س5: ما وظيفة Wireshark؟**

**س6: ما المقصود بملفات PCAP؟**

**س7: ما أهمية تحليل سجلات النظام؟**

**س8: ما الهدف من التخزين الآمن للأدلة الرقمية؟**

**س9: عدد مع الشرح الموجز الأدلة المستخرجة من الهواتف الذكية.**

**س10: اشرح بالتفصيل خطوات تحليل الشبكات وتحديد مصدر الهجوم.**

**س10: ما هي الإجراءات الأساسية التي يجب الالتزام بها أثناء تصوير الادلة الجنائية الرقمية.**

# الفصل الرابع:

# أنواع الجرائم الإلكترونية ودور التحقيق الجنائي الرقمي

مقدمة

يشهد العالم تحولاً جذرياً في مفاهيم الجريمة التقليدية، حيث انتقل الصراع من ساحات الواقع المادي إلى الفضاء السيبراني الافتراضي. لم تعد الجريمة تتطلب تواجداً جسدياً للجاني في موقع الحدث، بل أصبح بالإمكان تنفيذ أعقد العمليات الإجرامية من خلف شاشات الحاسوب وعبر القارات. يتناول هذا الفصل تصنيفاً دقيقاً للجرائم الإلكترونية الحديثة، بدءاً من الجرائم المالية التي تستهدف الاقتصاد، مروراً ببرمجيات الفدية التي تشل حركة المؤسسات، وصولاً إلى الجرائم الأخلاقية التي تمس كرامة الإنسان. والأهم من ذلك، يسلط الفصل الضوء على دور "المحقق الجنائي الرقمي" كخط الدفاع الأخير الذي يعمل على تتبع الأثر الرقمي، تحليل الأدلة، وتقديم الجناة للعدالة.. تخيلوا أن الإنترنت مدينة عالمية ضخمة لا تنام، شوارعها هي الشبكات، ومبانيها هي المواقع الإلكترونية، وسكانها هم مليارات المستخدمين. وكما هو الحال في أي مدينة كبيرة، هناك من يسعى لاستغلال هذه البيئة لأغراض إجرامية.

في هذا الفصل، سيتم التعرف على الجانب المظلم من هذه المدينة الرقمية. سنتعرف على أخطر أنواع الجرائم الإلكترونية التي تواجه عالمنا اليوم، من سرقة الأموال بضغطة زر إلى تنظيم شبكات إجرامية عابرة للقارات. الأهم من ذلك، سنسلط الضوء على الدور الحاسم الذي يلعبه المحقق الجنائي الرقمي في كل نوع من هذه الجرائم

## 1-4 الجرائم المالية وغسيل الأموال الإلكتروني

تشكل الجرائم المالية وغسيل الأموال عبر الإنترنت العصب الرئيسي للاقتصاد الأسود في العالم الرقمي. إن خطورة هذه الجرائم لا تكمن فقط في الخسائر المادية الهائلة التي تتكبدها الدول والشركات، بل في قدرتها على التطور المستمر واستغلال الثغرات في بروتوكولات الأمان والتحويلات البنكية الدولية. إن فهم ميكانيكية عمل **غسيل الأموال الإلكتروني** بدءاً من الإيداع، مروراً بالتمويه، ووصولاً إلى الدمج يعد ركيزة أساسية لأي متخصص في مجال أمن المعلومات والتحقيق الجنائي الرقمي، ليكون قادراً على تتبع المسار المالي الرقمي وكشف الهوية الحقيقية للجناة مهما حاولوا التخفي خلف طبقات التشفير.

ومع تزايد اعتماد المؤسسات المالية والأفراد على الأنظمة الرقمية في إدارة أصولهم، ظهر نوع خطير من الجرائم يُعرف بـ **الجرائم المالية الإلكترونية** .(Cyber Financial Crimes) هذه الجرائم لا تقتصر فقط على السرقة المباشرة للأرصدة، بل تمتد لتشمل عمليات **غسيل الأموال الرقمي**، التي تستخدم تقنيات التشفير والعملات الافتراضية لإضفاء الشرعية على أموال مكتسبة من أنشطة إجرامية. يهدف هذا

الجزء من الفصل إلى تفكيك البنية التقنية لهذه الجرائم، وتوضيح الأساليب المبتكرة التي يستخدمها الجناة للتحايل على الرقابة المالية، والتقنيات المقابلة التي يستخدمها المحققون لكشف هذه المخططات

**تعريف الجريمة الإلكترونية (Cybercrime Definition):**

لا يوجد تعريف دولي موحد للجريمة الإلكترونية نظراً للتطور السريع في التقنية واختلاف القوانين بين الدول، ولكن يمكن تعريفها من عدة زوايا لتغطية المفهوم بشكل كامل لطلاب الحاسوب:

**هي أي فعل غير قانوني ينطوي على استخدام جهاز حاسوب أو شبكة معلوماتية أو أي جهاز تقني ذكي. في هذا النوع من الجرائم، تكون التكنولوجيا هي البيئة التي تحدث فيها الجريمة، أو الأداة التي تُرتكب بها. اما من الناحية التقنية والقانونية فتعرف على انها** نشاط إجرامي يتميز بطابع تقني، يهدف إلى الاعتداء على:

- **سرية المعلومات (Confidentiality):** مثل سرقة البيانات.
- **سلامة المعلومات (Integrity):** مثل تعديل البيانات أو تزويرها.
- **توافر المعلومات (Availability):** مثل هجمات قطع الخدمة .أو استخدام هذه التقنيات لارتكاب جرائم تقليدية (كالاحتيال والسرقة) بأسلوب حديث.

**تعريف غسيل الأموال الإلكتروني (Cyber Money Laundering):**

يُعرف غسيل الأموال الإلكتروني (أو تبييض الأموال الرقمي) بأنه: **عملية تقنية معقدة تهدف إلى إخفاء المصدر غير المشروع للأموال الناتجة عن أنشطة إجرامية (سواء كانت جرائم سيبرانية كالقرصنة، أو تقليدية كتجارة المخدرات) وإعادة ضخها في النظام المالي العالمي باستخدام القنوات الرقمية والإنترنت، لتبدو وكأنها أصول مشروعة وقانونية.** يختلف غسيل الأموال الإلكتروني عن التقليدي في استبدال الحقائب النقدية المادية بـ **البتات والبايتات (Bits and Bytes)**، واستغلال سرعة التحويلات الرقمية لتضليل العدالة.

**اما بالنسبة لمراحل غسيل الأموال الإلكترونية** فتتمثل بثلاث مراحل أساسية:

**1- مرحلة الإيداع أو التوظيف (Placement) :**هي المرحلة الأولى والأكثر خطورة بالنسبة للمجرم، حيث يتم إدخال الأموال "القذرة" إلى النظام المالي الرقمي. بدلاً من إيداع النقد في بنك، يقوم المجرمون بشراء عملات رقمية (Cryptocurrencies) مثل البيتكوين باستخدام بطاقات مسروقة، أو تحويل الأموال إلى حسابات في بنوك إلكترونية لا تتطلب إجراءات تحقق قوية من الهوية.

**2- مرحلة التمويه أو التعتيم (Layering):** تعد هذه المرحلة هي **"القلب التقني "**لعملية الغسيل، والهدف منها هو قطع الصلة تماماً بين المال ومصدره الإجرامي عبر تعقيد مسار التتبع.

**آلية التنفيذ تقنياً:**

إجراء آلاف التحويلات المتشعبة بين محافظ رقمية مختلفة في دول متعددة خلال دقائق.

استخدام خدمات **خلط العملات** :**(Crypto Mixers/Tumblers)** وهي برمجيات تقوم بخلط عملات المجرم بعملات مستخدمين آخرين شرعيين وتجزئتها وإعادة تجميعها، مما يجعل تتبع سلسلة الكتل (Blockchain Analysis) شبه مستحيل.

تحويل الأموال إلى عملات ألعاب (In-game Currency) ثم بيعها للاعبين آخرين.

**3- مرحلة الدمج (Integration):** هي المرحلة النهائية حيث تعود الأموال إلى المجرم في صورة "نظيفة" وقابلة للاستخدام علناً.

**آلية التنفيذ تقنياً:**

إنشاء متاجر إلكترونية وهمية وشراء سلع غير موجودة باستخدام الأموال المغسولة (يدفع المجرم لنفسه).

استخدام بطاقات خصم (Debit Cards) مشحونة بعملات رقمية لشراء أصول مادية (عقارات، سيارات).

## 1-1-4: أشكال الجرائم المالية الإلكترونية

تعتبر الجرائم المالية الإلكترونية مجالاً واسعاً ومتجدداً، ولذلك يجب تفكيكها إلى أشكال محددة للتعمق في دراسة آلياتها التقنية. هذه الجرائم لا تستهدف البنوك الكبرى فقط، بل يمكن أن تستهدف أي شخص منا. يمكن تصنيف الجرائم المالية الإلكترونية بناءً على الأصول التي تستهدفها وطريقة الوصول إليها الى الأنواع التالية:

**1- الاحتيال على بطاقات الدفع والائتمان (Card Fraud):** يهدف هذا النوع إلى سرقة المعلومات الخاصة ببطاقات الدفع (Credit and Debit Cards) لاستخدامها في عمليات شراء عبر الإنترنت أو سحب نقدي غير مشروع. وهذا يمكن ان يحصل باستخدام الأساليب التالية:

**أ. التخطي والإسقاط (Skimming and Carding):**

**التخطي (Skimming):** جريمة فيزيائية-رقمية، حيث يتم تركيب جهاز صغير (Skimmer) على قارئ البطاقات في الصراف الآلي (ATM) أو نقاط البيع (POS) لنسخ بيانات الشريط الممغنط للبطاقة. يُستخدم الحاسوب في هذه المرحلة لمعالجة البيانات المسروقة واستخراج الأرقام السرية التي تم التقاطها عبر كاميرات صغيرة.

**بيع البطاقات المسروقة :(Carding)** هي عملية تجارة البيانات المسروقة للبطاقات رقم البطاقة، تاريخ الانتهاء، ورمز CVV عبر الأسواق السرية في الإنترنت المظلم. يقوم المشترون باستخدام هذه البيانات لإجراء عمليات شراء سريعة (Card Not Present - CNP) قبل أن يكتشف صاحب البطاقة السرقة.

**ب. هجمات البريد الإلكتروني وسرقة معلومات الدخول**: تستهدف هذه الهجمات سرقة معلومات البطاقات التي تكون مخزنة في قواعد بيانات المتاجر الإلكترونية أو حسابات المستخدمين:

**- تصيد الحسابات (Phishing Attacks):** إرسال رسائل بريد إلكتروني مزورة تدعي أنها من بنك الضحية لسرقة بيانات الدخول، والتي قد تقود لاحقاً إلى الوصول لبطاقاته المربوطة بالحساب.

**-البرمجيات الخبيثة (Malware):** استخدام برامج Keyloggers لتسجيل كل ما يكتبه المستخدم على لوحة المفاتيح أثناء إدخال معلومات البطاقة في المتصفح.

**2- الاحتيال على الحسابات المصرفية وتحويل الأموال(Account & Wire Fraud) :**

هنا يتم استهداف الحساب البنكي مباشرة أو استغلال ضعف الإجراءات الأمنية في تحويل الأموال.

**أ. الاستيلاء على الحساب (Account Takeover - ATO):**

يتمكن المجرم من الوصول الكامل لحساب الضحية المصرفي عبر الإنترنت. عادةً ما يتم ذلك بعد سرقة بيانات الدخول عبر هجوم تصيد متطور أو عبر الحصول على كلمة المرور من بيانات مسربة في هجوم اختراق سابق (Data Breach) ، ثم استخدامها للدخول للحساب وإجراء تحويلات ضخمة.

**ب. الاحتيال عبر اختراق بريد الشركات (BEC - Business Email Compromise):**

يُعد هذا الشكل من أكثر الجرائم المالية تكلفةً وتعقيداً، حيث يعتمد على الهندسة الاجتماعية والدراية بهيكل الشركة. يقوم المخترق باختراق البريد الإلكتروني لشخصية قيادية (المدير التنفيذي أو المدير المالي) في شركة ما، ثم يرسل رسالة فورية إلى موظف في قسم الحسابات يطلب فيها تحويل مبلغ كبير وعاجل لحساب خارجي (هو حساب المخترق)، متذرعاً بضرورة الصفقة وسريتها. يُرسل التحويل دون علم الموظف بأنه مزور، ويصعب استعادة الأموال بعد مغادرتها النظام.

**جـ. تبديل بطاقة SIM (SIM Swapping):**

جريمة متطورة تستهدف التغلب على المصادقة الثنائية (2FA) التي تعتمد على الرسائل النصية .يقوم المهاجم بخداع شركة الاتصالات (Social Engineering) لنقل رقم هاتف الضحية إلى
شريحة (SIM Card) يملكها المهاجم. بمجرد حصوله على الرقم، يستطيع طلب إعادة تعيين كلمة المرور لأي حساب بنكي أو حساب عملات مشفرة للضحية، حيث تصل رسالة التحقق النصية إليه هو بدلاً من الضحية.

**3- الاحتيال الاستثماري وتلاعب الأسواق (Investment & Market Fraud):**

يتم استهداف المستثمرين الأفراد أو التلاعب بقيمة الأصول في الأسواق الرقمية.

**أ. مخططات بونزي الرقمية (Digital Ponzi Schemes):** يقوم المجرمون بإنشاء منصات استثمار إلكترونية (عادة ما تكون مزيفة للاستثمار في العملات المشفرة) تعد بعوائد خيالية غير واقعية. يدفعون

للمستثمرين الأوائل من أموال المستثمرين الجدد، وليس من أرباح فعلية، حتى يتم جمع مبلغ ضخم ثم يختفي المجرم بالمال.

**ب. التلاعب والرمي (Pump and Dump):** يستخدم المجرمون حسابات وهمية على وسائل التواصل الاجتماعي أو برامج مراسلة جماعية لشراء كميات كبيرة من أسهم منخفضة القيمة (أو عملة رقمية جديدة) ثم نشر أخبار كاذبة وإشاعات عنها لـ "ضخ (Pump) "سعرها. بمجرد ارتفاع السعر بسبب إقبال صغار المستثمرين، يقوم المجرمون بالبيع الفوري لـ "رمي (Dump) "السهم، مما يتسبب في خسائر فادحة للضحايا.

**دور التحقيق الجنائي الرقمي في الجرائم المالية:** يجب على المحقق الرقمي التركيز على:

**1- تحليل سجلات الخادم (Server Logs):** لتحديد عناوين IP المهاجمة في هجمات BEC وATO .

**2- تحليل البلوكشين (Blockchain Analysis):** في حالة العملات المشفرة، يتم استخدام أدوات متخصصة لتتبع المعاملات عبر سلاسل الكتل ومحاولة فك التشفير وربط المحافظ بهويات حقيقية.

**3- الاستجابة للحوادث (Incident Response):** العمل مع المؤسسات المالية بسرعة لتجميد الأموال وتحويلها قبل أن تتم عملية التعتيم (Layering) وتصبح الأموال غير قابلة للتتبع.

## 4-1-2: غسيل الأموال الإلكتروني: الغسالة الرقمية

تخيل أن مجرماً سرق مليون دولار عبر الإنترنت. هذه الأموال "قذرة" لأنها مرتبطة بجريمة. إذا حاول المجرم إيداعها مباشرة في حسابه، ستكتشف السلطات الأمر فوراً. هنا يأتي دور غسيل الأموال الإلكتروني. غسيل الأموال **(Money Laundering)** هو عملية إخفاء المصدر غير المشروع للأموال لجعلها تبدو وكأنها مكتسبة من مصدر شرعي.

**كيف تتم عملية غسيل الأموال الإلكتروني؟**

يمكن تلخيصها في ثلاث مراحل رئيسية:

**1- الإيداع (Placement): يتم إدخال الأموال "القذرة" إلى النظام المالي عن طريق:**

أ- العملات المشفرة **:**هي الطريقة المفضلة. يقوم المجرمون بشراء عملات مشفرة مثل البيتكوين **(Bitcoin)**أو العملات التي تركز على الخصوصية مثل المونيرو **(Monero)** والتي تخفي تفاصيل المعاملات (المرسل والمستقبل والمبلغ) بشكل افتراضي، مما يجعل تتبعها أصعب بكثير من البيتكوين.

ب- حسابات البغل **(Mule Accounts):** يقوم المجرمون بتجنيد أشخاص (يُطلق عليهم بغال الأموال) لاستخدام حساباتهم البنكية مقابل عمولة. يتم إيداع الأموال المسروقة في هذه الحسابات، ثم يقوم "البغل" بسحبها نقداً أو تحويلها حسب تعليمات المجرم.

**2- التغطية (Layering):** هذه هي مرحلة "الغسيل" الحقيقية، حيث يتم خلق شبكة معقدة من المعاملات لإخفاء أثر الأموال.

- التحويلات المتسلسلة وخدمات الخلاطات **(Mixers/Tumblers):** يتم تحويل الأموال بين مئات المحافظ الرقمية للعملات المشفرة في دول مختلفة خلال دقائق. ثم يتم استخدام خدمات "الخلاطات" التي تخلط عملاتهم المشفرة مع عملات آلاف المستخدمين الآخرين، مما يجعل تتبع المسار الأصلي للأموال شبه مستحيل.

- استخدام الرموز غير القابلة للاستبدال **(NFT**-Non-Fungible Tokens**):** يمكن للمجرمين ممارسة ما يسمى بـ التداول الوهمي (Wash Trading) يقومون بإنشاء عدة محافظ مجهولة، ثم يستخدمون الأموال غير المشروعة لبيع وشراء نفس الـ NFT بين هذه المحافظ بأسعار متزايدة. هذا لا يغسل الأموال فحسب، بل يرفع سعر الـ NFT بشكل مصطنع، ليتم بيعه لاحقاً إلى مشترٍ حقيقي بربح.

**3- الدمج (Integration):** تعود الأموال "النظيفة" إلى المجرم لتبدو وكأنها أرباح شرعية. يمكنه الآن استخدامها لشراء عقارات، سيارات، أو استثمارها في أعمال تجارية حقيقية دون إثارة الشكوك.

| المرحلة | الوصف | مثال رقمي |
|---|---|---|
| **الإيداع** | **إدخال الأموال غير الشرعية في النظام المالي.** | **شراء عملات مشفرة بمبلغ 100 ألف دولار تم سرقته من حسابات بنكية.** |
| **التغطية** | **إخفاء المصدر عبر معاملات معقدة.** | **تحويل البيتكوين عبر 50 محفظة مختلفة، ثم استخدام خدمة "خلاط" لتمويه المسار.** |
| **الدمج** | **إعادة الأموال "النظيفة" إلى المجرم.** | **بيع البيتكوين واستلام الأموال كـ "أرباح استثمار"، ثم شراء سيارة فاخرة.** |

**جدول 4-1: مراحل غسيل الأموال الإلكتروني**

## 4-1-3 دور المحقق الجنائي الرقمي

عند وقوع جريمة مالية، يتم استدعاء المحقق الجنائي الرقمي ليكون "المحقق الذي يتبع أثر الأموال" في العالم الرقمي. يتلخص دوره بالأتي:

- **تحديد نقطة الاختراق:** يستخدم المحقق أدوات مثل **Wireshark** لتحليل حركة مرور الشبكة المسجلة، وأدوات التحقيق الجنائي مثل **Autopsy** أو **EnCase** لإنشاء نسخة طبق الأصل من القرص الصلب للجهاز المصاب وتحليلها دون تغيير البيانات الأصلية.
- **تتبع مسار الأموال:** في العملات المشفرة وعلى الرغم من صعوبة المهمة، إلا أن جميع معاملات البيتكوين مسجلة في" بلوكتشين **(Blockchain)**. "يستخدم المحققون أدوات متخصصة لتحليل البلوكتشين مثل Chainalysis أو Elliptic لتتبع تدفق العملات بين

المحافظ الرقمية. الهدف هو الوصول إلى النقطة التي يحاول فيها المجرم تحويل العملة المشفرة إلى عملة حقيقية، وهي نقطة تتم عادة عبر منصات تداول تتطلب التحقق من الهوية - **(KYC Know Your Customer)**. هذه المنصات هي نقطة ضعف المجرمين، حيث يمكن للسلطات أن تطلب منها قانونياً الكشف عن هوية صاحب الحساب.

- **جمع الأدلة الرقمية:** يقوم المحقق بجمع وحفظ كل دليل رقمي بشكل سليم قانونياً، مع توثيق سلسلة العهدة**(Chain of Custody)** ، وهي سجل مفصل لكل شخص تعامل مع الدليل، ومتى، ولماذا، لضمان قبول الدليل في المحكمة.

## 2-4 الاحتيال الإلكتروني والاحتيال على الهوية

على عكس الجرائم التي تستهدف البنية التحتية للحاسوب (كالفيروسات)، يعتمد الاحتيال الإلكتروني على الخداع والتلاعب بالنفس البشرية. يتفرع هذا النوع من الجرائم إلى مسارين رئيسيين: الأول يهدف إلى الحصول على المال مباشرة (الاحتيال الإلكتروني)، والثاني يهدف إلى سرقة الشخصية والبيانات للوصول إلى منافع طويلة الأمد (الاحتيال على الهوية). لقد ربحت مليون دولار! فقط اضغط هنا للمطالبة بجائزتك." أو "تم تعليق حسابك البنكي، يرجى تحديث بياناتك فوراً عبر هذا الرابط." من منا لم ير مثل هذه الرسائل؟ هذه ليست عروضاً حقيقية، بل هي فخاخ متطورة نصبها محتالون رقميون يستخدمون الهندسة الاجتماعية **(Social Engineering)** كسلاح أساسي لهم. الهندسة الاجتماعية هي فن التلاعب النفسي بالبشر لدفعهم للقيام بأفعال معينة أو الكشف عن معلومات سرية. في هذا القسم، سنستكشف كيف يستغل المجرمون ثقتنا وفضولنا وخوفنا لإخداعنا، وكيف يمكن أن تتطور هذه الخدعة من سرقة بضعة دولارات إلى سرقة هويتنا الرقمية بالكامل.

### 4-2-1 أساليب الاحتيال الإلكتروني (Electronic Fraud)

**1- التصيد الإلكتروني (Phishing) وأنواعه:**

- التصيد العام: **(Phishing)** رسائل جماعية غير موجهة.
- التصيد الموجه: **(Spear Phishing)** هجوم مخصص يستهدف شخصاً أو شركة معينة.
- صيد الحيتان: **(Whaling)** يستهدف كبار الشخصيات في الشركات.
- التصيد عبر الرسائل النصية: **(Smishing)** استخدام الرسائل القصيرة (SMS) التي تحتوي على روابط خبيثة أو تطلب معلومات شخصية. مثال: "لقد تم تحديدك لاستلام طرد. يرجى تأكيد عنوانك ودفع رسوم توصيل بسيطة عبر الرابط التالي."
- التصيد الصوتي: **(Vishing)** استخدام المكالمات الهاتفية. قد يتصل بك شخص ينتحل صفة

موظف بنك ويخبرك بوجود مشكلة في حسابك ويطلب منك تأكيد معلوماتك الشخصية أو رقم بطاقتك الائتمانية.

**2-علامات التحذير من التصيد:**

- الشعور بالإلحاح أو التهديد" :حسابك سيغلق خلال 24 ساعة"!
- تحية عامة" :عزيزي العميل" بدلاً من اسمك الحقيقي.
- أخطاء إملائية ونحوية :الشركات الكبرى عادة ما تدقق رسائلها بعناية.

عنوان بريد إلكتروني غريب للمرسل :قد يبدو العنوان صحيحاً للوهلة الأولى، لكن عند التدقيق تجد اختلافات طفيفة (مثلاً servIce@paypaI.com :بدلاً من - service@paypal.com لاحظ حرف "I"الكبير بدلاً من "i" الصغير)

- روابط مشبوهة :قبل النقر، مرر مؤشر الماوس فوق الرابط لترى عنوان **URL** الحقيقي.

### 2-2-4: الاحتيال على الهوية (Identity Theft)

الاحتيال على الهوية (Identity Theft) هو جريمة رقمية يقوم فيها المهاجم بسرقة معلومات شخصية تخص شخصًا آخر، مثل الاسم، رقم الهوية، بيانات البطاقة البنكية، أو كلمات المرور، بهدف انتحال شخصيته واستخدامها في أنشطة غير قانونية. يمكن أن يستخدم المجرمون هذه المعلومات لفتح حسابات بنكية، إجراء عمليات شراء، أو حتى ارتكاب جرائم باسم الضحية، مما يسبب أضرارًا مالية وقانونية كبيرة للمتضرر.




هذه الجريمة أصبحت أكثر انتشارًا مع تزايد الاعتماد على الإنترنت، لذلك يعد الوعي والحذر عند مشاركة البيانات الشخصية أمرًا أساسيًا للوقاية منها. هنا، لا يكتفي المجرم بسرقة أموالك، بل يسرق "هويتك" في العالم الرقمي.

**اما بالنسبة لأنواع سرقة الهوية فهي:**

- سرقة الهوية المالية: النوع الأكثر شيوعاً، بهدف سرقة الأموال.

- سرقة الهوية الطبية: استخدام هوية شخص آخر للحصول على رعاية صحية أو أدوية.
- سرقة الهوية الإجرامية: ارتكاب جريمة ثم تقديم هوية الضحية للشرطة.
- سرقة هوية الأطفال **:**سرقة هوية طفل لفتح حسابات أو الحصول على قروض. هذه الجريمة خطيرة لأنها قد لا تُكتشف لسنوات عديدة حتى يكبر الطفل ويحاول الحصول على أول قرض أو وظيفة له.
- سرقة الهوية الاصطناعية **(Synthetic ID Theft):** يقوم المجرمون بدمج معلومات حقيقية (مثل رقم ضمان اجتماعي مسروق) مع معلومات مزيفة (اسم وعنوان وهمي) لإنشاء هوية جديدة تماماً "اصطناعية". هذه الهويات يصعب اكتشافها لأنها لا تطابق أي شخص حقيقي بشكل كامل.

### 3-2-4: دور المحقق الجنائي الرقمي

المحقق الجنائي الرقمي هو خبير متخصص في جمع وتحليل الأدلة الرقمية المتعلقة بالجرائم الإلكترونية. يستخدم أدوات وتقنيات متقدمة لفحص أجهزة الكمبيوتر، الهواتف الذكية، والشبكات، بهدف كشف الحقائق وتوثيق الأدلة الرقمية التي تثبت وقوع الجريمة.

**1- دوره في الاحتيال الإلكتروني (E-Theft):**

- **تحديد نوع الاحتيال** :المحقق يبدأ بتحديد طبيعة الاحتيال الإلكتروني، مثل الاحتيال عبر البريد الإلكتروني، الاحتيال في المعاملات المصرفية الإلكترونية، أو الاحتيال عبر مواقع التجارة الإلكترونية.
- **جمع الأدلة الرقمية** :يقوم المحقق بتحليل سجلات الدخول، رسائل البريد الإلكتروني، سجلات المعاملات المالية الرقمية، وتفريغ محتوى الأجهزة المستخدمة في الجريمة.
- **تحليل الأدلة** :استخدام تقنيات متقدمة مثل استرجاع البيانات المحذوفة، تحليل الشبكة، وتحليل البرمجيات الخبيثة (Malware) التي قد تكون مستخدمة في تنفيذ الاحتيال.
- **تتبع الجناة** :تتبع مصدر الهجوم أو عملية الاحتيال عبر تحليل عناوين الـIP ، وتحليل الأنماط الرقمية التي تساعد في كشف هوية الجناة أو مواقعهم.
- **تقديم تقارير دقيقة** :إعداد تقارير مفصلة تُستخدم في التحقيقات القضائية لدعم القضايا أمام المحاكم.

**2- دوره في الاحتيال على الهوية (Identity Theft)**

- **تحليل البيانات المسروقة** :فحص البيانات الرقمية التي تم الاستيلاء عليها مثل بيانات بطاقات الائتمان، كلمات المرور، أو المعلومات الشخصية.
- **تحديد طريقة السرقة** :التعرف على الطرق التي استخدمها المجرم للوصول إلى المعلومات

مثل التصيد الاحتيالي(Phishing) ، البرمجيات الخبيثة، أو اختراق قواعد البيانات.

- **استعادة الأدلة الرقمية** :استرجاع الأدلة المتعلقة بالهوية المسروقة من الأجهزة الرقمية ومواقع الإنترنت.
- **التعاون مع الجهات الأمنية** :العمل جنبًا إلى جنب مع الشرطة، وكالات إنفاذ القانون، والمؤسسات المالية لتأمين الأدلة وتحليلها بشكل قانوني.
- **التوصية بإجراءات الحماية** :بناءً على نتائج التحقيق، يقدم المحقق نصائح وإجراءات للوقاية من جرائم الاحتيال على الهوية مستقبلاً.

**3- التقنيات والأدوات المستخدمة**

- برامج تحليل البيانات الرقمية.
- أدوات استرجاع البيانات المحذوفة.
- برامج تحليل البرمجيات الخبيثة.
- أدوات تحليل الشبكات وسجلات الدخول.
- برامج التشفير وفك التشفير.

**4- أهمية دور المحقق الجنائي الرقمي**

- يضمن كشف الحقيقة في القضايا المتعلقة بالاحتيال الإلكتروني.
- يساعد في إعادة الحقوق للضحايا.
- يساهم في ردع الجرائم الإلكترونية من خلال تقديم أدلة واضحة.
- يعزز ثقة المستخدمين والمؤسسات في أمنهم الرقمي.
- تحليل رسائل التصيد :يقوم المحقق بتحليل" ترويسة البريد الإلكتروني (Email " (Header، وهي جزء مخفي من الرسالة يحتوي على معلومات تقنية قيمة عن مسار الرسالة من الخادم المصدر إلى صندوق بريد الضحية.
- فحص المواقع المزيفة :يقوم المحقق بتحليل الجهة التي قامت بتسجيل اسم النطاق (Domain)عبر سجلات .Whois حتى لو كانت المعلومات خاصة، يمكن للمحقق البحث عن أنماط في كيفية تسجيل النطاقات قد تقود إلى نفس الشخص أو المجموعة.
- تتبع المعاملات المالية :كما في الجرائم المالية، يتتبع المحقق مسار الأموال.
- استعادة البيانات والاتصالات :إذا تم استخدام برمجية خبيثة للسرقة، يقوم المحقق بتحليل جهاز الضحية لتحديد خوادم "القيادة والتحكم " التي يتواصل معها المجرم.

## 3-4 برامج الفدية **(Ransomware)**

لغرض فهم برامج الفدية بصورة واضحة لنفترض انك استيقظت صباحاً لتجد أن جميع أبواب منزلك قد أُغلقت بأقفال غريبة، وكل ممتلكاتك الثمينة داخل صناديق مقفلة. ثم تجد رسالة على الطاولة تقول: "إذا أردت مفاتيح الأقفال، عليك أن تدفع مبلغاً من المال". **هذا بالضبط ما تفعله برامج الفدية**، لكنها تفعل ذلك لأثمن ممتلكاتك في العصر الحديث وهو **بياناتك الرقمية**.

### 4-3-1 ما هي برامج الفدية وكيف تعمل؟

برامج الفدية **(Ransomware)** هي نوع من البرمجيات الخبيثة التي تقوم بتشفير **(Encrypting)** جميع الملفات الهامة. تستخدم برامج الفدية التشفير غير المتماثل **(Asymmetric Encryption)**. لكل ضحية، يتم إنشاء زوج من المفاتيح:

- المفتاح العام **(Public Key):** يكون متاحاً على جهاز الضحية ويستخدمه برنامج الفدية لتشفير الملفات. لا يمكن استخدام هذا المفتاح لفك التشفير.
- المفتاح الخاص **(Private Key):** هذا هو المفتاح السري الذي يمكنه فك التشفير. يتم تخزينه بأمان على خوادم المهاجم، وهو ما يطالبك بالدفع للحصول عليه.

بعد تشفير الملفات، تظهر رسالة على الشاشة (رسالة الفدية) تطالب الضحية بدفع مبلغ من المال.




**شكل (4-1): شاشة كمبيوتر مصابة ببرنامج فدية، تظهر رسالة الفدية الشهيرة مع عداد تنازلي ومطالبة بالدفع.**

### 4-3-2 طرق الانتشار وتطور الهجمات

- **طرق الانتشار:**

1. رسائل التصيد الإلكتروني **:**الطريقة الأكثر شيوعاً.
2. استغلال الثغرات الأمنية **:**مثل هجوم **WannaCry** الشهير الذي استغل ثغرة في نظام ويندوز للانتشار كدودة عبر الشبكات في عام 2017.
3. بروتوكول سطح المكتب البعيد **(RDP-Remote Desktop Protocol):** يخترق المهاجمون أجهزة الكمبيوتر (خاصة الخوادم) التي تتيح الوصول عن بعد بكلمات مرور

ضعيفة عبر هجمات القوة الغاشمة(Brute Force) ، ثم يقومون بتثبيت برنامج الفدية يدوياً.

❖ **تطور الهجمات: الابتزاز المزدوج والثلاثي**

1) الابتزاز المزدوج **:(Double Extortion)** قبل تشفير الملفات، يقومون بسرقة نسخة من البيانات الحساسة .ثم يهددون الضحية: "إما أن تدفع، أو سنقوم بنشر بياناتك على موقع التسريبات الخاص بنا على الشبكة المظلمة."

2) الابتزاز الثلاثي **:(Triple Extortion)** يضيف المهاجمون طبقة ثالثة من الضغط. بالإضافة إلى تشفير البيانات وتهديد نشرها، يقومون بشن هجوم حجب الخدمة (DDoS) على موقع الشركة لشل عملياتها بالكامل.

**دراسة حالة:** هجوم **Colonial Pipeline (2021)** تعرضت أكبر شركة لخطوط أنابيب الوقود في الولايات المتحدة لهجوم فدية من قبل عصابة .DarkSide أدى الهجوم إلى إغلاق الخطوط بالكامل، مما تسبب في نقص حاد في الوقود وحالة من الذعر في الساحل الشرقي للولايات المتحدة. اضطرت الشركة لدفع فدية تقدر بـ 4.4 مليون دولار (على الرغم من أن السلطات تمكنت لاحقاً من استعادة جزء منها). هذا الهجوم يوضح كيف يمكن لجريمة إلكترونية أن تؤثر على البنية التحتية الحيوية لدولة بأكملها.

### 4-3-3 دور المحقق الجنائي الرقمي

- الاحتواء والعزل **:**الخطوة الأولى والأكثر أهمية هي عزل الأجهزة المصابة عن بقية الشبكة.
- تحديد نوع الفدية **:**يستخدم المحقق أدوات ومواقع مثل **ID Ransomware** لتحديد السلالة الدقيقة للبرنامج الخبيث.
- تحليل نقطة الدخول **:**كيف دخل البرنامج الخبيث؟ هذا ضروري لمنع هجمات مستقبلية.
- البحث عن مفاتيح فك التشفير **:**يبحث المحقق في قواعد بيانات عالمية (مثل مشروع **"No More Ransom"**).
- استخبارات التهديدات **:(Threat Intelligence)** يستخدم المحققون المعلومات من الهجمات السابقة لنفس العصابة لفهم تكتيكاتهم وتقنياتهم وإجراءاتهم (TTPs - Tactics Techniques and Procedures)، مما يساعد في التحقيق الحالي.

## 4-4 الجريمة المنظمة عبر الإنترنت

عندما نسمع بمصطلح "الجريمة المنظمة"، قد نفكر في عصابات المافيا التقليدية. اليوم، تطورت هذه العصابات وأصبحت أكثر تنظيماً وخطورة بفضل الإنترنت. الجريمة المنظمة عبر الإنترنت هي النسخة الرقمية لهذه العصابات، حيث تعمل مجموعات من المجرمين معاً في هياكل تشبه الشركات تماماً، بهدف

تنفيذ هجمات إلكترونية واسعة النطاق وتحقيق أرباح تقدر بمليارات الدولارات. لم تعد الجريمة الإلكترونية مقتصرة على أفراد يعملون بمفردهم، بل أصبحت صناعة متكاملة.

### 4-4-1: هيكل وخصائص الجريمة المنظمة عبر الإنترنت

يمكن تشبيه عصابة الجريمة المنظمة بشركة ناشئة في وادي السيليكون، ولكن لأغراض تدميرية. لديها:

- "الإدارة العليا": القادة الذين يضعون الاستراتيجيات ويجنون معظم الأرباح.
- "قسم التطوير": مبرمجون موهوبون يطورون البرمجيات الخبيثة ويجدون ثغرات أمنية جديدة.
- "قسم العمليات": متخصصون في اختراق الشبكات وتنفيذ الهجمات.
- "قسم التسويق": محتالون يصممون وينفذون حملات التصيد.
- "القسم المالي": متخصصون في غسيل الأموال عبر العملات المشفرة.

### 4-4-2: الجريمة كخدمة (Crime-as-a-Service - CaaS)

**أحد أخطر تطورات الجريمة المنظمة هو نموذج "الجريمة كخدمة".**

- **Ransomware-as-a-Service (RaaS):** تقوم عصابة بتطوير برنامج فدية قوي، ثم تؤجره لمجرمين آخرين ("الشركات التابعة"). الأرباح يتم تقاسمها.
- **Phishing-as-a-Service:** يمكنك شراء حزمة تصيد جاهزة.
- **DDoS-as-a-Service:** يمكنك استئجار شبكة من الأجهزة المخترقة (Botnet) لشن هجوم حجب الخدمة الموزع.(DDoS)
- **Malware-as-a-Service:** يمكنك استئجار أو شراء برامج خبيثة مثل سارقي المعلومات أو أحصنة طروادة المصرفية.

### 4-4-3: الشبكة المظلمة (The Dark Web): سوق الجريمة

من المهم التمييز بين الويب العميق والويب المظلم:

- الويب السطحي **(Surface Web):** هو الإنترنت الذي نعرفه جميعاً، والذي يمكن الوصول إليه وفهرسته بواسطة محركات البحث مثل جوجل.
- الويب العميق **(Deep Web):** هو أي جزء من الإنترنت لا يمكن لمحركات البحث فهرسته. هذا يشمل معظم الإنترنت، مثل حسابك المصرفي عبر الإنترنت، بريدك الإلكتروني، قواعد البيانات الأكاديمية، إلخ. الوصول إليه يتطلب تسجيل الدخول.
- الويب المظلم **(Dark Web):** هو جزء صغير من الويب العميق تم إخفاؤه عمداً ويتطلب برامج خاصة للوصول إليه، مثل متصفح **Tor (The Onion Router)**. يعمل Tor عن طريق توجيه اتصالك عبر سلسلة من الخوادم المشفرة التي يديرها متطوعون حول العالم، مما يجعل من الصعب جداً تتبع مصدر الاتصال.

### 4-4-4 دور المحقق الجنائي الرقمي

الاختراق السري **(Undercover Operations):** يتسلل المحققون إلى منتديات الشبكة المظلمة.

- تحليل البرمجيات الخبيثة **(Reverse Engineering):** يقوم المحللون بتفكيك البرمجيات الخبيثة التي تطورها العصابة لفهم كيفية عملها، وتحديد خوادم القيادة والتحكم الخاصة بها، وربما العثور على أخطاء في الكود يمكن استغلالها لإنشاء أداة فك تشفير أو لتحديد هوية المطور.
- صعوبة الإسناد **(The Attribution Problem):** أحد أكبر التحديات هو تحديد المسؤول عن الهجوم بشكل قاطع. تستخدم العصابات والدول القومية تقنيات متقدمة لإخفاء هوياتهم، مثل استخدام خوادم مخترقة في دول أخرى كنقطة انطلاق لهجماتهم، مما يجعل من الصعب جداً إثبات من يقف وراء لوحة المفاتيح.

**جدول 4-2: مقارنة بين الجريمة المنظمة التقليدية والجريمة المنظمة عبر الإنترنت**

| وجه المقارنة | الجريمة المنظمة التقليدية | الجريمة المنظمة عبر الإنترنت (السيبرانية) |
|---|---|---|
| بيئة ارتكاب الجريمة | البيئة المادية الواقعية (الشوارع، الأماكن العامة، المباني، الحدود). | الفضاء السيبراني وشبكة الإنترنت (الدارك ويب، الشبكات، الأنظمة). |
| مسرح الجريمة | غالباً ما يكون محلياً أو يتطلب الانتقال المادي عبر الحدود (عابر للحدود). | غالباً ما يكون عالمياً ويتم عن بعد، مع صعوبة تحديد الموقع الجغرافي للجناة. |
| الأدوات المستخدمة | القوة الجسدية، الأسلحة، التزوير المادي، النقل المادي للسلع (مخدرات، بشر، أسلحة). | الأجهزة الإلكترونية (الحواسيب، الهواتف)، البرمجيات الخبيثة، أدوات الاختراق، التشفير. |
| طبيعة العنف | غالباً ما تتسم بـ العنف المباشر أو التهديد به (القتل، الاعتداء، الابتزاز الجسدي). | العنف فيها غالباً ما يكون غير مباشر، يعتمد على التأثير المادي (المالي) والنفسي. |
| الضحايا المستهدفون | أفراد أو مجموعات محددة ضمن نطاق جغرافي معين، أو مصالح مادية واضحة. | يمكن أن يكونوا ملايين الأشخاص أو المؤسسات في جميع أنحاء العالم في وقت واحد (الشركات، البنوك، الحكومات). |
| نوع الجرائم | الاتجار بالبشر، المخدرات، الأسلحة، غسيل الأموال التقليدي، الابتزاز، السطو المسلح. | الاحتيال الإلكتروني، انتحال الهوية، هجمات الفدية، القرصنة، سرقة البيانات، غسيل الأموال الرقمي. |
| مهارات الجناة | الخبرة الإجرامية في الميدان، التنظيم الهيكلي الصارم، الولاء التنظيمي. | الخبرة التقنية العالية في تكنولوجيا المعلومات والبرمجة واختراق الأنظمة. |
| صعوبة الاكتشاف والإثبات | أسهل نسبياً في الاكتشاف والإثبات (الشهود، البصمات، الأدلة المادية). | أكثر صعوبة بسبب إخفاء الهوية (الإخفاء)، عابرة الحدود، طبيعة الدليل الرقمي غير المادي. |

## 5-4 قضايا الجرائم الأخلاقية والخصوصية الرقمية

ليست كل الجرائم الإلكترونية تهدف إلى سرقة الأموال. هناك فئة من الجرائم تهاجم كرامة الإنسان وسلامته النفسية وخصوصيته. هذه الجرائم، التي يمكن أن نسميها" الجرائم الأخلاقية"، تستخدم قوة الإنترنت وسهولة الانتشار فيه كسلاح لنشر الكراهية، أو لممارسة التنمر، أو لابتزاز الضحايا، مسببة أضراراً نفسية عميقة قد تفوق الأضرار المالية. في هذا القسم، سنتناول هذه القضايا الحساسة ونفهم كيف ينتهك المجرمون خصوصيتنا الرقمية، وما هو دور المحقق الرقمي في تحقيق العدالة لضحايا لا تظهر جروحهم على أجسادهم.

### 1-5-4 :أنواع الجرائم الأخلاقية

**1- التنمر الإلكتروني** :(Cyberbullying) هو استخدام التكنولوجيا لمضايقة شخص آخر أو تهديده أو إحراجه بشكل متكرر. على عكس التنمر التقليدي الذي قد ينتهي بانتهاء اليوم الدراسي، فإن التنمر الإلكتروني يلاحق الضحية 7/24 عبر هاتفها وجهاز الكمبيوتر الخاص بها.

- ❖ مثال :قد يقوم مجموعة من الطلاب بإنشاء مجموعة دردشة سرية هدفها الوحيد هو السخرية من زميل لهم، ومشاركة صور تم التلاعب بها له، ونشر شائعات كاذبة عنه. هذا الهجوم الجماعي يمكن أن يكون له تأثير مدمر على نفسية الضحية.
- ❖ الأشكال:

- **Flaming:** خوض معارك كلامية غاضبة وعدائية في الأماكن العامة عبر الإنترنت مثل أقسام التعليقات.
- **Outing:** مشاركة أسرار شخص ما أو معلومات محرجة عنه علناً دون موافقته.
- **Exclusion:** استبعاد شخص ما عمداً من مجموعة عبر الإنترنت (مثل مجموعات الدردشة أو الألعاب) لجعله يشعر بالعزلة.

**2- الابتزاز الشخصي الإلكتروني** :(Sextortion) هو شكل خطير من أشكال الابتزاز. غالباً ما يبدأ السيناريو ببناء علاقة ثقة مزيفة. قد يتظاهر المجرم بأنه شخص في نفس عمر الضحية ويبدأ محادثة ودية عبر وسائل التواصل الاجتماعي. بعد كسب ثقة الضحية، يطلب منها إرسال صور أو مقاطع فيديو خاصة. بمجرد الحصول عليها، يكشف المبتز عن وجهه الحقيقي ويهدد بنشر هذه المواد على الإنترنت أو إرسالها إلى الأصدقاء والعائلة إذا لم تدفع الضحية مبلغاً من المال أو لم تقم بتنفيذ طلبات أخرى.

**3- خطاب الكراهية والتضليل**:(Hate Speech & Disinformation)

- ❖ خطاب الكراهية (**Hate Speech**): استخدام المنصات عبر الإنترنت لنشر محتوى يحرض

على الكراهية والعنف ضد مجموعات معينة على أساس العرق، أو الدين، أو الأصل. تستخدم الجماعات المتطرفة الإنترنت لتجنيد أعضاء جدد ونشر أيديولوجياتها السامة.

- ❖ التضليل **(Disinformation):** هو نشر معلومات كاذبة عمداً بهدف الخداع أو التلاعب بالرأي العام أو تحقيق مكاسب سياسية أو مالية. تكمن خطورته في سرعة انتشاره عبر خوارزميات وسائل التواصل الاجتماعي التي تفضل المحتوى المثير للجدل.

**4- التشهير الإلكتروني :Doxing**

- ❖ التشهير **(Defamation):** نشر معلومات كاذبة عن شخص ما بهدف الإضرار بسمعته.
- ❖ **Doxing:** هو اختصار لـ(dropping docs) ، ويعني البحث عن معلومات خاصة وحساسة عن شخص ما (مثل عنوان منزله الحقيقي، رقم هاتفه، مكان عمله، أسماء أفراد عائلته) ونشرها على الإنترنت بشكل علني. الهدف هو ترهيب الضحية وجعلها عرضة لمضايقات في العالم الحقيقي.

**5- تقنية التزييف العميق :(Deepfakes)** وهي استخدام الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صوت مزيفة تبدو واقعية للغاية. يمكن استخدام هذه التقنية لوضع وجه شخص ما على جسد شخص آخر في مقطع فيديو، أو لجعل شخصية عامة تقول أشياء لم تقلها أبداً. هذا يمثل تهديداً خطيراً للثقة والحقيقة، ويمكن استخدامه في التشهير، والاحتيال، ونشر الدعاية السياسية المضللة.

### 4-5-2 : الخصوصية الرقمية وبصمتك الرقمية

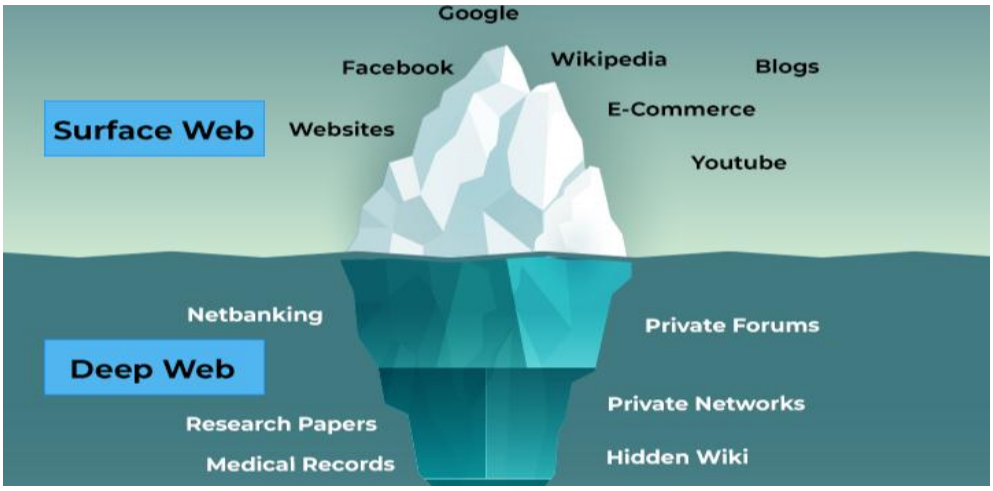
الخصوصية الرقمية **(Digital Privacy)** هي حقك في التحكم في من يمكنه جمع بياناتك الشخصية واستخدامها ومشاركتها. في كل مرة نستخدم فيها الإنترنت، نترك بصمات رقمية **(Digital Footprints)**.

1) البصمات النشطة **(Active Footprints):** هي البيانات التي تشاركها عن قصد، مثل منشوراتك على فيسبوك، تغريداتك على تويتر، أو الصور التي ترفعها على انستغرام.
2) البصمات الخاملة **(Passive Footprints):** هي البيانات التي تُجمع عنك دون وعي مباشر منك.

- ❖ مثال :عندما تستخدم تطبيق خرائط على هاتفك، فأنت لا تشارك موقعك بنشاط، لكن التطبيق يجمع بيانات موقعك الجغرافي في الخلفية. تجمع مواقع الويب عنوان IP الخاص بك، ونوع المتصفح الذي تستخدمه، والمدة التي قضيتها في كل صفحة.
- ❖ ملفات تعريف الارتباط **(Cookies):** هي ملفات نصية صغيرة تخزنها مواقع الويب على

جهازك. بعضها مفيد (مثل تذكر سلة التسوق الخاصة بك)، وبعضها الآخر (يسمى ملفات تعريف الارتباط للجهات الخارجية أو التتبع) يراقب نشاطك عبر مواقع متعددة لإنشاء ملف تعريف مفصل عنك لبيعه للمعلنين.

- مفهوم "مفارقة الخصوصية:(The Privacy Paradox) يشير هذا المصطلح إلى التناقض بين ما يقوله الناس عن الخصوصية وما يفعلونه بالفعل. يظهر العديد من المستخدمين قلقهم بشأن خصوصيتهم، لكنهم في نفس الوقت يشاركون كميات هائلة من المعلومات الشخصية على وسائل التواصل الاجتماعي مقابل الحصول على خدمات مجانية أو مزايا بسيطة. هذا السلوك يجعلهم أهدافاً سهلة لجمع البيانات والجرائم الإلكترونية.




**شكل (4-2 ): رسم توضيحي يمثل "جبل الجليد للبيانات الشخصية"، حيث الجزء العلوي هو البصمات النشطة، والجزء السفلي المخفي هو البصمات الخاملة**

### 4-5-3 : دور المحقق الجنائي الرقمي

التحقيق في هذه القضايا يتطلب مزيجاً من المهارات التقنية العالية والذكاء العاطفي.

- **التعامل مع الضحايا :**أول خطوة هي طمأنة الضحية وتوفير بيئة آمنة للإدلاء بالمعلومات. في قضايا مثل الابتزاز الجنسي، يكون الحفاظ على سرية وكرامة الضحية هو الأولوية القصوى. غالباً ما يعمل المحققون بالتنسيق مع الأخصائيين النفسيين لتقديم الدعم اللازم للضحية.

- **تحديد هوية المجهول:**

1- تحليل الحسابات المزيفة **:**بالتعاون مع شركات التواصل الاجتماعي، يمكن طلب سجلات الوصول (Access Logs)التي تحتوي على عناوين IP.

2- تحليل البيانات الوصفية **(Metadata):** الصور ومقاطع الفيديو تحتوي على بيانات وصفية مخفية (تسمى بيانات EXIF) قد تكشف عن نوع الكاميرا أو الهاتف المستخدم، وتاريخ ووقت التقاط الصورة، وأحياناً إحداثيات الموقع الجغرافي (GPS) إذا لم يتم حذفها. يمكن للمحقق استخدام أدوات متخصصة

لاستخراج هذه البيانات وتحليلها.

3- تحليل الأسلوب اللغوي **(Stylometry):** في بعض الحالات، يمكن تحليل أسلوب الكتابة (الكلمات المستخدمة، الأخطاء الإملائية المتكررة، بنية الجمل) للمساعدة في ربط حسابات مجهولة متعددة بنفس الشخص.

- ❖ **استعادة الأدلة المحذوفة :**يمتلك المحقق الرقمي الأدوات والتقنيات اللازمة لمحاولة استعادة الرسائل أو المنشورات المحذوفة من ذاكرة الأجهزة أو من النسخ الاحتياطية السحابية.
- ❖ **التحديات القانونية والأخلاقية :**يواجه المحققون تحديات كبيرة. إخفاء الهوية باستخدام شبكات VPNأو Tor يجعل التتبع صعباً. كما أن القوانين تختلف من بلد إلى آخر، مما يعقد طلب الأدلة من الشركات الأجنبية. يجب على المحقق الموازنة بين الحاجة إلى جمع الأدلة واحترام خصوصية الضحية وكرامتها.

وبعد أن تعرفنا على الجانب النظري لأنواع الجرائم الإلكترونية ودور المحقق الرقمي، حان الوقت لتطبيق بعض المهارات العملية الأساسية. تذكر دائماً، أن تصبح محققاً رقمياً ماهراً يتطلب الممارسة المستمرة. في هذين التمرينين، سنتعلم كيفية استخدام أداتين بسيطتين لكنهما قويتان جداً في مجال الأمن السيبراني والتحقيق الأولي.

تحذير هام **:**قم دائماً بإجراء هذه التمارين في بيئة آمنة. لا تقم أبداً بتحليل ملفات أو روابط تشك في أنها خبيثة بالفعل على جهاز الكمبيوتر الشخصي أو المدرسي الرئيسي دون إشراف متخصص. استخدم أجهزة افتراضية (Virtual Machines) أو أجهزة مخصصة للاختبار إذا أمكن.

**رقم التمرين:12** **الزمن المخصص: 3 ساعات**

اسم التمرين: **فحص البرمجيات الخبيثة بأستخدام Malwarebytes**

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الأهداف التعليمية:**

تعلم كيفية تثبيت واستخدام برنامج Malwarebytes وهو أحد أشهر البرامج المتخصصة في اكتشاف وإزالة البرمجيات الخبيثة، بما في ذلك برامج التجسس وبرامج الفدية.

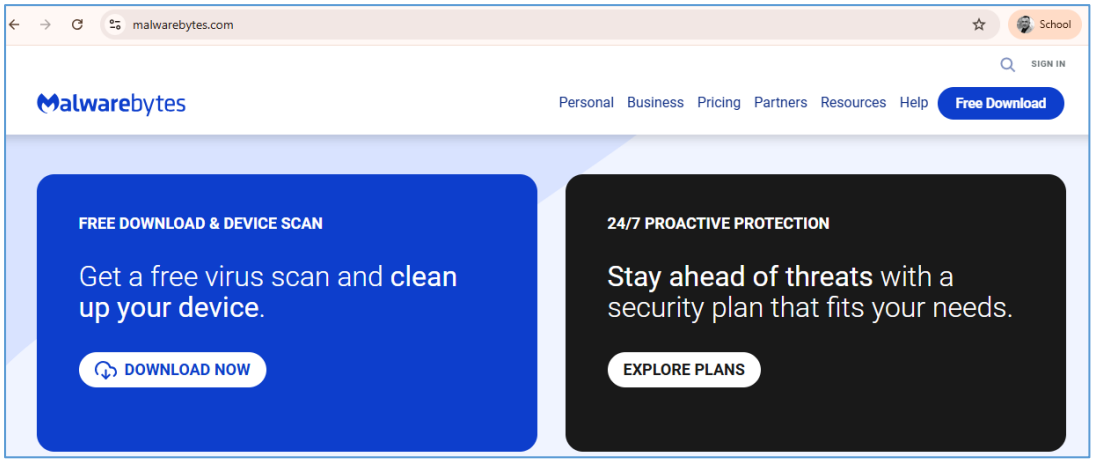
**ثانياً: التسهيلات العلمية:**

مختبر حاسوب مجهز، برنامج أو نماذج Malwarebytes، أدلة رقمية تجريبية، وإشراف علمي أثناء تنفيذ التمرين.

1- ارتد بدلة العمل.

**2- التحميل والتثبيت:**

- افتح متصفح الويب وانتقل إلى الموقع الرسمي https://www.malwarebytes.com/
- ابحث عن زر "Free Download" أو "تنزيل مجاني" وقم بتنزيل النسخة المجانية من البرنامج.




- بعد اكتمال التنزيل، افتح الملف الذي قمت بتنزيله واتبع تعليمات التثبيت البسيطة.

لقطة شاشة لموقع **Malwarebytes** الرسمي مع الإشارة إلى زر التنزيل المجاني

**3- فتح البرنامج وإجراء الفحص الأول:**

- بعد التثبيت، افتح برنامج Malwarebytes من سطح المكتب أو قائمة "ابدأ".
- ستظهر لك الواجهة الرئيسية للبرنامج. ستجد زراً كبيراً وواضحاً باسم "Scan" أو "فحص".
- انقر على زر "Scan". سيبدأ البرنامج فوراً في فحص جهاز الكمبيوتر الخاص بك.

**4- تحليل النتائج:**

- عند انتهاء الفحص، سيعرض البرنامج النتائج.
  - إذا تم العثور على تهديدات: سيعرض البرنامج قائمة بالملفات أو العناصر الخبيثة التي تم اكتشافها، مع تحديد نوع التهديد (Malware PUP - Potentially Unwanted Program etc.).

**5- عزل التهديدات:(Quarantine)**

- انقر على زر "Quarantine" أو "عزل".
- ماذا يعني العزل؟ يقوم البرنامج بنقل الملفات الخبيثة إلى منطقة آمنة ومعزولة داخل البرنامج.

وبالختام لا بد من معرفة ما هو **Malwarebytes** ؟

هو برنامج أمان لا يركز فقط على الفيروسات التقليدية، بل يتخصص في اكتشاف التهديدات "الحديثة" التي قد لا يكتشفها مضاد الفيروسات العادي. المحققون الرقميون يستخدمونه كأداة فحص أولية لتنظيف الأنظمة وتحديد طبيعة الإصابة.

**مناقشة وأسئلة:**

1. لماذا يعتبر استخدام برنامج متخصص مثل Malwarebytes مهماً إلى جانب مضاد الفيروسات العادي؟
2. ما الفرق بين "العزل (Quarantine) "و"الحذف(Delete) "؟
3. إذا اكتشف البرنامج تهديداً من نوع"PUP" ، ابحث على الإنترنت عن معنى هذا المصطلح.
4. كيف يمكن لنتائج فحص Malwarebytes أن تساعد المحقق الرقمي في بداية تحقيقه؟

| **استمارة قائمة الفحص** | | | |
|---|---|---|---|
| اسم الطالب: | | المرحلة: الثالثة | |
| التخصص : | | | |
| **اسم التمرين: فحص البرمجيات الخبيثة بأستخدام Malwarebytes.**<br>**رقم التمرين:12** | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وتحميل وتثبيت البرنامج. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

**رقم التمرين:13** **الزمن المخصص: 3 ساعات**

**اسم التمرين: تحليل هجوم تصيد إلكتروني باستخدام أداة تحليل ترويسة البريد الالكتروني:**

**(Email Header Analyzer)**

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الأهداف التعليمية:**

فهم ماهية ترويسة البريد الإلكتروني، وتعلم كيفية استخراجها، واستخدام أداة عبر الإنترنت لتحليلها وكشف معلومات عن مرسل رسالة تصيد مشبوهة.

**ثانياً: التسهيلات العلمية:**

مختبر حاسوب مجهز، بريد الكتروني Gmail،انترنت ومتصفح كروم، وإشراف علمي أثناء تنفيذ التمرين.

1- ارتد بدلة العمل.

**ما هي ترويسة البريد الإلكتروني (Email Header) ؟**

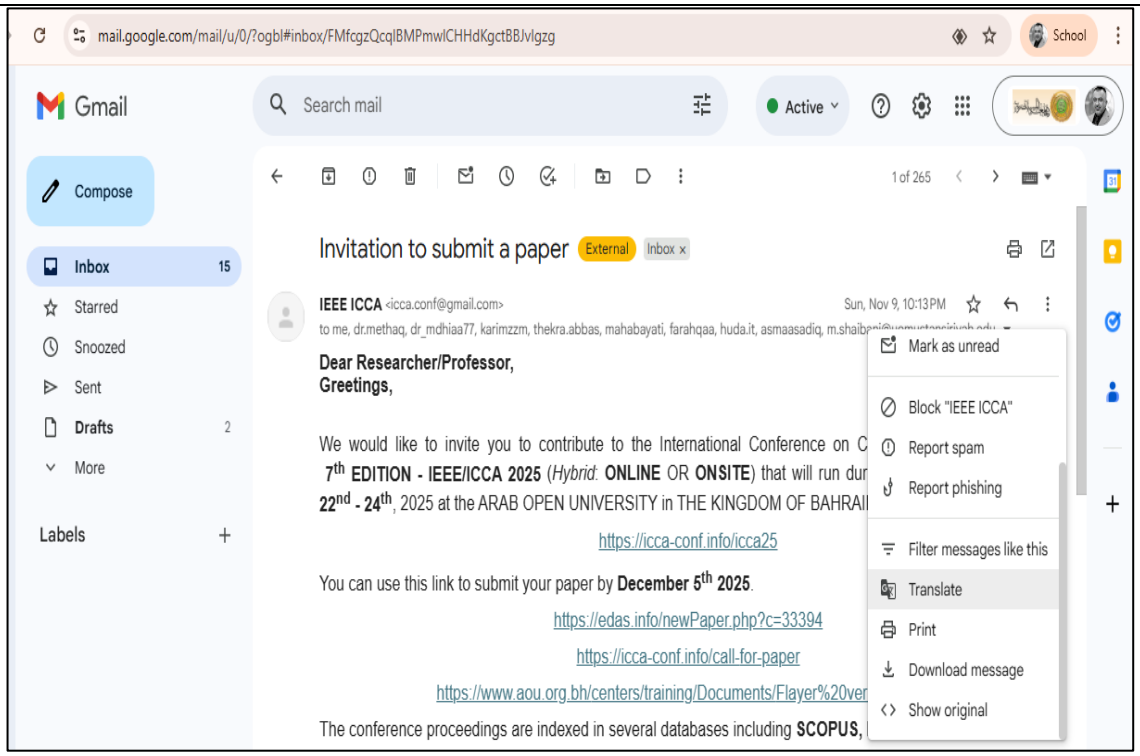
البريد الإلكتروني هو رسالة ورقية داخل ظرف. ما تراه عادة (المرسل، الموضوع، النص) هو الرسالة نفسها. أما الترويسة فهي كل المعلومات المكتوبة على الظرف: من أين جاءت، وما هي مكاتب البريد (الخوادم) التي مرت بها في طريقها إليك.

- تحتوي الترويسة على معلومات تقنية مثل عنوان IP للمرسل، والخوادم التي عالجت الرسالة أثناء انتقالها.
- يمكن استخدام هذه المعلومات لتتبع مصدر البريد الإلكتروني أو التحقق من مصداقيته.
- كما تُستخدم في التحقيقات الرقمية وتحليل الرسائل المزعجة أو رسائل التصيد الاحتيالي.

**الخطوات:**

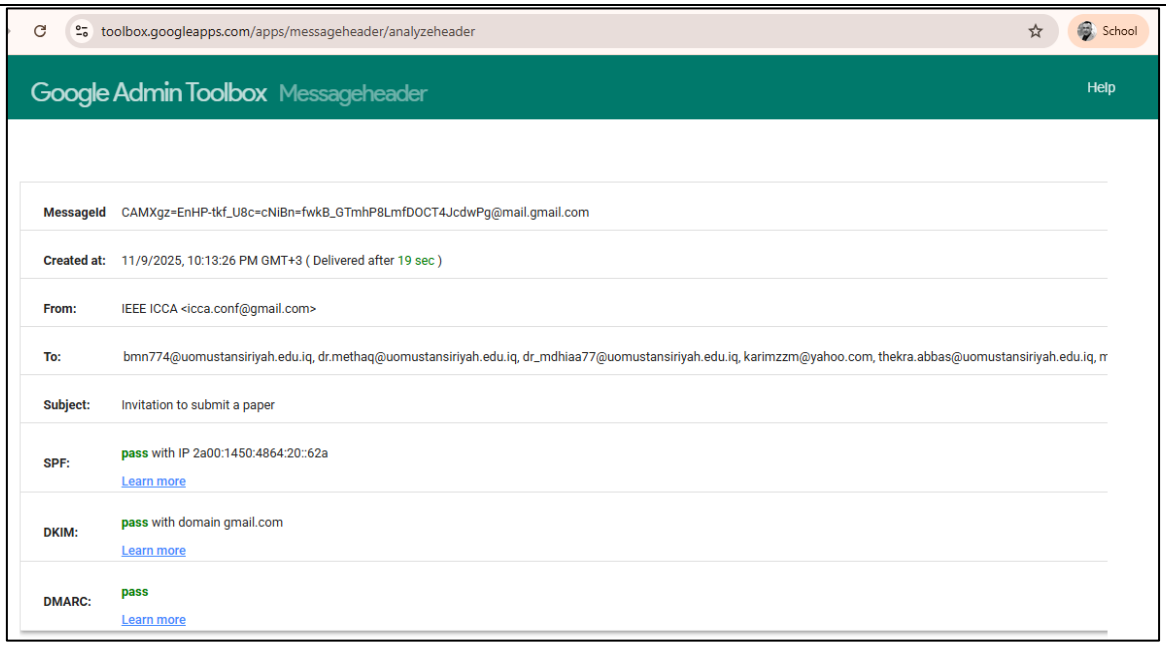
2. **استخراج ترويسة البريد:**

- في **Gmail:** افتح البريد الإلكتروني، انقر على النقاط الثلاث بجانب زر "رد"، واختر "Show original" أو "إظهار الأصل".
- في **Outlook:** افتح البريد الإلكتروني، انقر على "File" > "Properties". ستجد الترويسة في قسم"Internet headers" .




لقطة شاشة توضح كيفية الوصول إلى **"Show original"** في **Gmail**

1. **استخدام أداة تحليل الترويسة:**
   - ❖ افتح متصفح الويب وابحث عن **"Google Messageheader"** أو انتقل مباشرة إلى : https://toolbox.googleapps.com/apps/messageheader/
   - ❖ ستجد مربع نص كبير.
2. **لصق وتحليل الترويسة:**
   - ❖ انسخ ترويسة بريد إلكتروني كاملة والصقها في المربع.
   - ❖ انقر على زر."ANALYZE THE HEADER ABOVE"
3. **تفسير النتائج:**
   - ❖ ستقوم الأداة بتقديم النتائج في جدول منظم.
   - ❖ ما الذي تبحث عنه؟
     - ▪ **SPF DKIM DMARC:** هذه هي سجلات التحقق من الهوية. إذا رأيت "FAIL" أو "فشل" بجانبها، فهذه علامة حمراء كبيرة.
     - ▪ مسار الرسالة **(Hop):** هذا هو الجزء الأهم. يعرض الجدول كل خادم مرت به الرسالة، من الأسفل (المصدر) إلى الأعلى (وجهتك). بجانب كل خادم، سترى عنوان **IP** الخاص به .عنوان IP المصدر هو الدليل الأهم.




لقطة شاشة لنتائج تحليل ترويسة في أداة **Google** ، مع إبراز سجلات التحقق **(SPF)** ومسار الرسالة وعناوين**IP**

| **استمارة قائمة الفحص** | | | | |
|---|---|---|---|---|
| اسم الطالب: | | | المرحلة: الثالثة | |
| التخصص : | | | | |
| **اسم التمرين: اسم التمرين: تحليل هجوم تصيد إلكتروني باستخدام أداة تحليل ترويسة البريد الالكتروني . رقم التمرين:13** | | | | |
| ت | الخطوات | الدرجة القياسية | درجة الاداء | الملاحظات |
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تشغيل الحاسوب وفتح المتصفح. | %15 | | |
| 3 | مراحل تنفيذ التمرين | %15 | | |
| 4 | المناقشة | %10 | | |
| 5 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص: | | التاريخ | | التوقيع |

## اسئلة الفصل الرابع

س1: ضع كلمة (صح) أمام العبارة الصحيحة وكلمة (خطأ) أمام العبارة الخاطئة وصحح الخطأ ان وجد:

1. تعتمد الجرائم المالية الإلكترونية فقط على سرقة الأموال المباشرة دون استخدام وسائل تمويه رقمية.
2. تُعد مرحلة التمويه (Layering) المرحلة الأهم في غسيل الأموال الإلكتروني لأنها تهدف إلى قطع الصلة بين المال ومصدره الإجرامي.
3. التصيد الموجه (Spear Phishing) يستهدف شريحة عشوائية من المستخدمين دون تخصيص.
4. تستخدم برامج الفدية التشفير غير المتماثل، حيث يحتفظ المهاجم بالمفتاح الخاص.
5. يمكن للمحقق الجنائي الرقمي استخدام تحليل البلوكشين لتتبع معاملات العملات المشفرة رغم صعوبة المهمة.

س2: أكمل العبارات الاتية بما يناسبها:

1. تُعرف عملية إخفاء المصدر غير المشروع للأموال وإعادة إدخالها في النظام المالي باسم _____ الإلكتروني.
2. تُسمى الحسابات التي يستخدمها المجرمون لتحريك الأموال المسروقة مقابل عمولة بـ _____ .
3. يُطلق على أسلوب الاحتيال الذي يعتمد على خداع الضحية نفسياً مصطلح _____ الاجتماعية.
4. يُستخدم متصفح _____ للوصول إلى الشبكة المظلمة Dark Web .
5. تُعرف السجلات التي توثق التعامل مع الدليل الرقمي لضمان قبوله قانونياً باسم _____ العهدة.

س3: ناقش مراحل غسيل الأموال الإلكتروني موضحاً الأساليب التقنية المستخدمة في كل مرحلة، مع بيان دور المحقق الجنائي الرقمي في مواجهتها.

س4: اشرح أساليب الاحتيال الإلكتروني (Phishing) وأنواعه، مع توضيح علامات التحذير التي تساعد المستخدم والمحقق الرقمي على اكتشافه.

س5: بيّن دور المحقق الجنائي الرقمي في التعامل مع هجمات برامج الفدية، بدءاً من الاستجابة الأولية وحتى جمع الأدلة الرقمية.

# الفصل الخامس

# التوجهات المستقبلية في التحقيق الجنائي الرقمي

## 5 – 1 التحقيق الجنائي السحابي وانترنت الاشياء

مع التقدم التكنولوجي المتسارع، أصبحت الخدمات السحابية وإنترنت الأشياء (IoT) جزءًا لا يتجزأ من حياتنا اليومية، ومما لا شك فيه إلى ان الاستخدام الواسع لهذه الخدمات ترافقها تحديات أمنية وقانونية كبيرة وهذا ما ساهم في ظهور تخصص جديد في علوم الجرائم الرقمية يُعرف بـالتحقيق الجنائي السحابي الذي يمثل أحد أهم التخصصات الحديثة في مجال أمن المعلومات والعدالة الجنائية الرقمية.

ومع تعاظم الاعتماد على الخدمات السحابية، تزداد أهمية هذا المجال لضمان محاربة الجرائم السيبرانية بطريقة فعّالة ومحترفة. هذا التخصص يرتبط ارتباطًا وثيقًا بأجهزة إنترنت الأشياء ومع ذلك لا يزال هذا النوع من التحقيقات يواجه تحديات قانونية وتقنية كبيرة، مما يتطلب تطوير الأطر التشريعية والقانونية ، وتدريب الكوادر الأمنية، وتعزيز التعاون الدولي بين الجهات المختصة ومزودي الخدمات السحابية.

ولدراسة العلاقة بين التحقيق الجنائي الرقمي في بيئات الحوسبة السحابية وإنترنت الأشياء لا بد عزيزي الطالب من التعرف على مفهوم التحقيق الجنائي السحابي وإنترنت الأشياء ودراسة اهدافها وأهم التحديات التي تواجه المحققين في هذا المجال. وهذا ما سنتعرف عليها في الفقرات التالية.

### 5-1-1 مفهوم التحقيق الجنائي السحابي

التحقيق الجنائي السحابي (Cloud Forensics) وهي احدى مجالات علم الأدلة الجنائية الرقمية وفرع متخصص من فروع التحقيق الرقمي الذي يهدف إلى استخراج وجمع وتحليل وحفظ الأدلة الرقمية الموجودة ضمن بيئات الحوسبة السحابية بطريقة قانونية وتقنية دقيقة ويمكن اعتمادها في المحاكم مثل خدمات (Microsoft Azure) و (Google Cloud) و (Amazon Web Services) . وفيما يلي بعض خصائص التحقيق الجنائي السحابي:-

1. **التوزيع المكاني للبيانات:** البيانات قد تكون موزعة في أكثر من دولة.
2. **الملكية المشتركة:** المعلومات قد تكون مشتركة بين المستخدمين ومزود الخدمة.
3. **الديناميكية:** البيانات تتغير بسرعة، مما يصعّب عمليات التحفظ عليها.
4. **الافتراضية:** معظم البيانات في البيئة السحابية لا تُخزَّن على أجهزة تقليدية.

#### أهداف التحقيق الجنائي السحابي

يمكن تلخيص اهداف التحقيق الجنائي السحابي فيما يلي :-

1. تحديد النشاطات المشبوهة في البيئة السحابية.

2. جمع الأدلة الرقمية بطريقة قانونية وسليمة.
3. تحليل الأنشطة الرقمية ومطابقتها مع الإجراءات الجنائية.
4. التوثيق والحفاظ على الأدلة لضمان صلاحيتها في المحكمة.
5. دعم استعادة البيانات في حالات الهجمات أو الاختراق.

**اما بالنسبة لمراحل التحقيق الجنائي السحابي**

لكي تستطيع عملية التحقيق الجنائي السحابي اداء ادوارها في جمع وتحليل الأدلة الرقمية الموجودة في بيئة الحوسبة السحابية بطريقة قانونية يجب ان تمر العملية بالمراحل المتسلسلة الاتية :-

1. **التعرف والتحديد:** تحديد مصدر الحادث أو النشاط غير المشروع وتحديد أنظمة الحوسبة السحابية المعنية.
2. **الجمع:** جمع البيانات الرقمية ذات العلاقة من الخوادم أو السجلات السحابية، مع الالتزام بسلسلة الحيازة (Chain of Custody).
3. **التحليل:** تحليل البيانات لاكتشاف طبيعة الجريمة، والجهات المتورطة فيها، أو الأنشطة المشبوهة.
4. **التوثيق والعرض:** إعداد تقارير مفصلة بالأدلة، بطريقة مفهومة قانونيًا وتقنيًا، لتقديمها في المحكمة.

**اما بالنسبة للتحديات التي تواجه التحقيق الجنائي السحابي**

ان التحقيق الجنائي السحابي يواجه تحديات تقنية وقانونية عديدة ويمكن اجمالها في النقاط التالية :-

1. **التوزيع الجغرافي للبيانات:**
2. **قضايا الخصوصية:**
3. **التشفير والتشفير الذاتي:**
4. **نقص المعايير:**
5. **التعاون مع مزودي الخدمات:**

**اما الأدوات والتقنيات المستخدمة في التحقيق الجنائي السحابي فهي:**

هنالك مجموعة من الادوات والتقنات التي تستخدم في التحقيق الجنائي السحابي هذه الادوات والتقنيات يمكن تصنيفها الى ثلاثة اقسام رئيسة :-

1. **أدوات لجمع الأدلة:** وهي عبارة عن مجموعة من الادوات والبرامج والمنصات التي تستخدم لجمع وتحليل الأدلة الرقمية من مصادر متنوعة مثل (اداة التحليلات الجنائية FTK Imager) و (برنامج تحليل الأدلة الرقمية EnCase Forensics) و (منصات تحليل البيانات السحابية والتواصل الاجتماعي Magnet AXIOM).

2. **أدوات تتبع الأنشطة السحابية:** وهي عبارة عن مجموعة من الادوات والخدمات والمنصات التي تستخدم لتتبع الأنشطة السحابية مثل خدمة (AWS CloudTrail) **وسجلات** الأنشطة (Audit Logs Google Cloud) **ومنصة** مراقبة نشاطات الموارد **(**Azure Monitor**).**
3. **أدوات إدارة سلسلة الحيازة:** مثل برنامج (CaseGuard) المدعوم **بالذكاء الاصطناعي والمصمم لتحرير المعلومات الحساسة تلقائيًا من مقاطع الفيديو وملفات الصوت والصور والمستندات، وبرنامج (**Chainkit**) التي تستخدم** لضمان تتبع الأدلة خلال التحقيق.

### 2-1-5 مفهوم إنترنت الأشياء (IoT)

إنترنت الأشياء IoT (Internet of Things) هو نظام من الأجهزة المادية المترابطة التي تتصل وتبادل البيانات عبر الإنترنت، مثل الكاميرات والساعات الذكية، السيارات المتصلة، وحتى الأجهزة المنزلية.... الخ. هذه الأجهزة لها ميزتان رئيسيتان وهي الاتصال بالإنترنت بالإضافة إلى التقنيات المدمجة كالبرامج وأجهزة الاستشعار. أحدثت أجهزة إنترنت الأشياء ثورةً في مجال تقنية المعلومات وسهّلت في الأتمتة والتعاون بين مختلف القطاعات، مثل الرعاية الصحية والزراعة والنقل والتصنيع وهذا ساهم في زيادة عدد المستخدمين بشكل ملحوظ وبالتالي زيادة في التحديات والتهديدات الأمنيّة التي تتعلق بمشكلات الأمان وعدم كفاية الحماية ومخاطر القرصنة بالاضافة الى مشكلة التوافق، ونقص التوحيد القياسي، وضمان الخصوصية وأمن البيانات. علاوة على ذلك فإن هذا التوسع في استخدام أجهزة إنترنت الأشياء شملت مختلف جوانب الحياة بما في ذلك الأنشطة الإجرامية لذا ومن منظور علم التحقيقات الجنائية الرقمية، يقدم إنترنت الأشياء تحديات جديدة بسبب الترابط بين الأجهزة والبرامج والسُحب الرقمية والأطراف الخارجية الأخرى التي تدير الأجهزة ولزيادة الحاجة للتحليل الجنائي لإنترنت الأشياء وإدارة الأدلة الرقمية بشكل صحيح في الإجراءات القضائية نشىء فرع جديد في التحليل الجنائي الرقمي يعرف باسم التحقيق الجنائي لإنترنت الأشياء (IoT Forensics).

### 3-1-5 التحقيق الجنائي الرقمي (Digital Forensics)

وهو علم جمع وتحليل الأدلة الرقمية بطريقة قانونية لتقديمها في المحكمة. وبعبارة اخرى التحقيق الجنائي الرقمي هو تطبيق العلم والقانون على الأدلة الرقمية بهدف جمعها وتحليلها وحفظها بطريقة قابلة للتقديم في المحكمة وتشمل الأدلة الموجودة على أجهزة الحواسيب، والهواتف الذكية، والأجهزة اللوحية، ووسائط التخزين الأخرى، وكذلك البيانات المخزنة على السحابة. وتكمن اهم التحديات الأمنية في التحقيقات الجنائية الرقمية فيما يلي :-

1. **التشفير:**
2. **الكميات الضخمة للبيانات.**

3. **أدوات تحقيق غير محدثة.**
4. **نقص الكفاءات المتخصصة.**
5. **ضعف التنسيق بين الجهات الأمنية والتقنية.**

## 5-1-4 التحقيق الجنائي وإنترنت الأشياء (IoT Forensics)

علم التحقيق الجنائي لإنترنت الأشياء هي فرع من فروع التحقيق الجنائي الرقمي، تُعنى باستخدام أي عمليات وإجراءات تتعلق بالتحقيق الجنائي الرقمي لاستعادة الأدلة الرقمية الصادرة عن جهاز أو أكثر من أجهزة إنترنت الأشياء، لغرض حفظها أو تحديدها أو استخراجها أو توثيقها من اجل إعادة بناء الأحداث المتعلقة بإنترنت الأشياء. يهدف التحقيق الجنائي لإنترنت الأشياء إلى توسيع نطاق التحقيق الجنائي الرقمي، مع التركيز بشكل رئيسي على إعادة بناء الأحداث التي تتضمن تحديد المعلومات والأدلة الرقمية واستخراجها من الأجهزة التابعة لمجال إنترنت الأشياء، باستخدام عملية سليمة من الناحية الجنائية ومقبولة قانونيًا. ويمكن تقسيم العملية بأكملها زمنيًا إلى ست مراحل مختلفة (تحديد الأدلة، جمع الأدلة ، حفظ الأدلة ، تحليل الأدلة ، تحديد مصدر الهجوم وعرض الأدلة). كما موضح في الشكل (5-1).



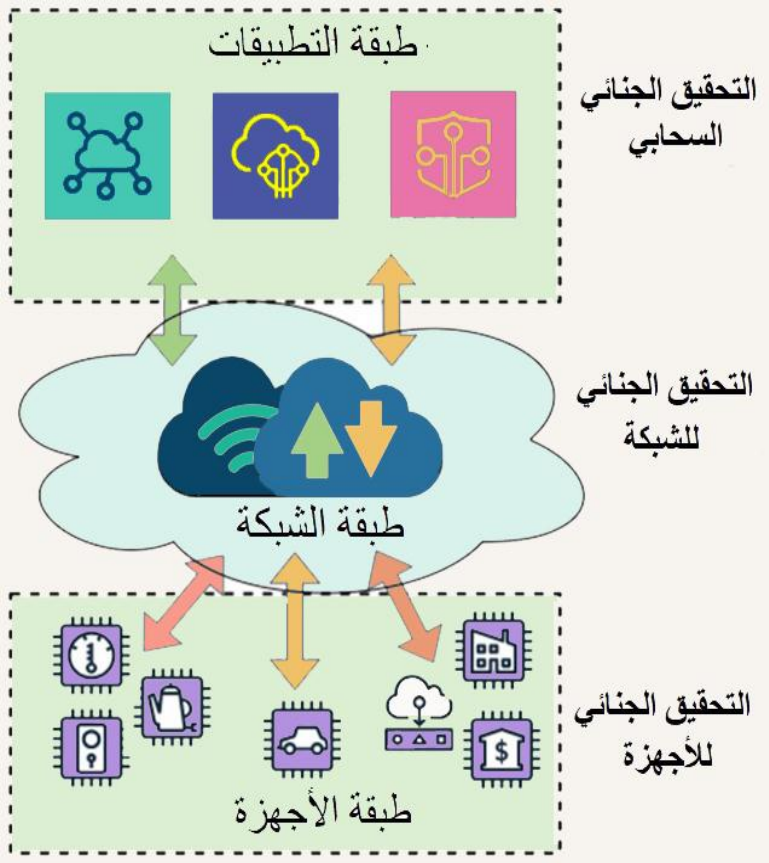

**الشكل (5-1) المخطط التسلسلي لمراحل التحقيق الجنائي الرقمي لأجهزة إنترنت الأشياء**

## 5-1-5 مكونات بنية إنترنت الأشياء ذات الصلة بالتحقيق

1. **الأجهزة الطرفية (Edge Devices):** أجهزة الاستشعار والكاميرات والساعات.
2. **بوابات الاتصال (Gateways):** تربط الأجهزة بالإنترنت.
3. **السحابة (Cloud):** لتخزين وتحليل البيانات.
4. **التطبيقات (Applications):** واجهات الاستخدام التي تُظهر البيانات وتتحكم بها.

### 6-1-5 طبقات التحقيق الجنائي لإنترنت الأشياء

غالبًا ما يتضمن التحقيق الجنائي لإنترنت الأشياء مراعاة بيانات الأدلة من نطاقات الشبكة غير المتجانسة، والتي يجب جمعها معًا أثناء عملية التحقيق. لهذا الغرض قدمت دراسة التحقيق الجنائي لإنترنت الأشياء على أنه مزيج من ثلاث طبقات تحقيق جنائي رقمي هي (التحقيق الجنائي للجهاز التحقيق الجنائي للشبكة التحقيق الجنائي للسحابة). ويهدف هذا التصنيف إلى تقسيم البحث إلى مشاكل فرعية محددة في مجال التحقيق الجنائي لإنترنت الأشياء والذي يعرض فئات إنترنت الأشياء المرتبطة مباشرةً بطبقات التحقيق الجنائي الرقمية الثلاث والشكل (5-2) يوضح طبقات التحقيق الجنائي الرقمي .




الشكل (5-2) يوضح طبقات التحقيق الجنائي الرقمي

وفيما يلي شرحا موجزا لمراحل طبقات التحقيق الجنائي الرقمي :-

1- طبقة التحقيق الجنائي للأجهزة: ويهدف الى تحديد واستخراج الأدلة من أجهزة إنترنت الأشياء (أي من ذاكرة الجهاز).

2- طبقة التحقيق الجنائي للشبكة: ويهدف الى تحديد واستخراج الأدلة من سجل الشبكة، وتتبعات حركة مرور الأجهزة، وأنماط الاتصال.

3- **طبقة التحقيق الجنائي السحابي: ويهدف الى استقراء المعلومات في السحابة التي تستخدمها الأجهزة. وذلك لأن أجهزة إنترنت الأشياء عادةً ما تكون محدودة الذاكرة، لذا فإن معظم المعلومات تُخزَّن في خدمات سحابية خاصة هذه الخدمات قد تحتوي على كميات هائلة من انشطة الاجهزة والتي يمكن تقديمها كأدلة محتملة.**

### 5-1-7 أهمية التحقيق الجنائي في إنترنت الأشياء

تتلخص أهمية التحقيق الجنائي في إنترنت الأشياء في القضايا التالية :-

1- **مصدر غني للأدلة الرقمية.**

2- **انتشار الأجهزة.**

3- **تحديات جنائية.**

### 5-1-8 التحديات التي تواجه التحقيق الجنائي في إنترنت الأشياء

1- **التنوع الهائل للأجهزة:** وهذا يجعلها تختلف في أنظمتها، صيغها، وقدراتها على حفظ البيانات.

2- **البيانات اللامركزية**: حيث تكون البيانات مخزنة في أماكن مختلفة (الجهاز، السحابة، التطبيق).

3- **ضعف الأمن**: كثير من أجهزة إنترنت الأشياء تفتقر لحماية كافية، ما يسهل التلاعب بالأدلة.

4- **عدم وجود معايير موحدة:** لا توجد بروتوكولات تحقيق موحدة لكل أجهزة إنترنت الأشياء.

5- **التقادم السريع للتكنولوجيا:** تطور الأجهزة بسرعة يسبق تطور أدوات التحليل الجنائي.

## 5 – 2 الذكاء الاصطناعي والتعليم الالي في التحقيق الجنائي الرقمي

يتنم استخدام الذكاء الاصطناعي في العمل الشرطي والأمني في مجالات مختلفة ، وغالبا ماً يندرج تحت استراتيجية المدن الذكية، والتي من ضمن أهدافها استخدام التقنيات المتطورة لضمان أمن وسلامة السكان في المدينة. وتشمل تقنيات الذكاء الاصطناعي على كاميرات المراقبة الذكية التي لديها القدرة على تحليل الصور والفيديوات لاكتشاف أماكن تواجد المشبوهين أو المطلوبين والأمور غير الطبيعية وتنبيه مركز التحكم مباشرةً. بالاضافة الى استخدام تقنية التعليم الالي في مجال الأمن الإلكتروني، واستخدام الطائرات الذكية بدون طيار والتي تسمى (سمارت درونز) للمراقبة الجوية، وتقوم بعض الجهات الشرطية الرائدة حالياً باستخدام الذكاء الاصطناعي وتقنياته المختلفة في محاربة الجريمة، من خلال الاعتماد على تقنياته الذكية في مجال التحقيق الجنائي للكشف عن العديد من الجرائم من أهمها الجرائم الإلكترنية .

### 5-2-1 دور الذكاء الاصطناعي في تطوير التحقيقات الجنائية الرقمية

لقد دخل الذكاء الاصطناعي إلى عمق علم الجريمة ، فأعاد تشكيل العلاقة بين الجاني، والضحية، ورجل الأمن، والمحقق. وذلك بفضل قدرته الهائلة على تحليل البيانات واستنتاج الأنماط، فأصبح من الممكن

قراءة السلوك الإجرامي من زوايا غير تقليدية، بل أحيانًا حتى قبل أن يتحول هذا السلوك إلى فعل ملموس. ونعد (الشرطة التنبؤية) أحد أهم إنجازات الذكاء الاصطناعي في مجال تطوير التحقيقات الجنائية الرقمية حيث تقوم هذه التقنية بتحليل قواعد بيانات الجرائم السابقة، وربطها بمعلومات عن المواقع الجغرافية، والوقت، وأنماط السلوك، لتحديد الأماكن والأوقات الأكثر عرضة لوقوع الجريمة وهذا يسمح للشرطة بنشر قواتها بطريقة أكثر كفاءة واستباقًا. ومن جهة أخرى يُستخدم الذكاء الاصطناعي في تحليل السلوك الرقمي للمشتبه بهم، من خلال تتبع أنشطتهم عبر الإنترنت، وتحليل تعبيراتهم اللغوية، ومراقبة تفاعلاتهم عبر وسائل التواصل. ويمكن للخوارزميات اليوم أن ترصد مؤشرات على وجود توجه عدواني، أو تخطيط محتمل لارتكاب جريمة، خاصة في قضايا الإرهاب أو الجرائم المنظمة أو الاعتداءات الرقمية.

وفي ميدان التحقيق الجنائي، بات الذكاء الاصطناعي أداة لا تُقدّر بثمن في تحليل الأدلة الجنائية الرقمية، مثل تسجيلات الفيديو، وسجلات الهواتف، والكاميرات الأمنية، وحتى بيانات الموقع الجغرافي (GPS). وخوارزميات التعرف على الوجه حيث يمكنها تحليل آلاف الساعات من الفيديو بدقة مذهلة، والتقاط تفاصيل يصعب على العين البشرية ملاحظتها، مثل تحركات غير متناسقة، أو إشارات جسدية مريبة، أو حتى التغيّر في ملامح الوجه تحت الضغط. كما يُستخدم الذكاء الاصطناعي في بناء ملفات نفسية للمجرمين المحتملين، من خلال تحليل سلوكياتهم السابقة، ومستوى التعليم، والبيئة الاجتماعية، والعوامل النفسية، وتطوير برامج تأهيلية للمجرمين داخل السجون، ويمكن تلخيص أهمية الذكاء الاصطناعي في التحقيقات الجنائية الرقمية من خلال الامور التالية:

1- **تحليل البيانات الضخمة بسرعة وفعالية.**
2- **رصد الأنشطة المشبوهة والتنبؤ بالجريمة.**
3- **استعادة البيانات المحذوفة والمخفية.**
4- **تحليل الأدلة الرقمية بدقة عالية.**
5- **تحليل الاتصالات الإلكترونية وتعقب الجرائم الإلكترونية.**

## 2-2-5 التحديات التي تواجه استخدام الذكاء الاصطناعي في التحقيقات الجنائية الرقمية

ان الذكاء الاصطناعي أصبح الحجر الأساس في التحقيقات الجنائية الرقمية، من حيث اسهامه في تحليل الأدلة بسرعة وكفاءة، وكشفه عن الأنشطة الإجرامية المخفية. ورغم هذه الطفرة التكنولوجية فان تطبيقات الذكاء الاصطناعي في التحقيقات الجنائية الرقمية لا تخلو من تحديات أخلاقية وقانونية عديدة وكما يلي:-

1- **الخصوصية وحماية البيانات.**

2- **إمكانية التلاعب والتزييف.**

3- **الاعتماد المفرط على الذكاء الاصطناعي.**

4- **التطور المستمر للجرائم الإلكترونية.**

### 3-2-5 التعلم الآلي (Machine learning)

التعلم الآلي هو فرع من فروع الذكاء الاصطناعي وعلوم الحاسوب يركز على استخدام البيانات والخوارزميات من أجل تقليد الطريقة التي يتعلم بها الإنسان والعمل على تحسينها بشكل تدريجي . ويمكن تلخيص أجزاء التعليم الآلي فيما يلي :

1. **البيانات (Data):** وهي المادة الخام التي يتعلم منها النماذج الذكية قد تكون هذه البيانات رقمية نصوص صور اصوات ....الخ .
2. **المتغيرات والميزات:** وهي الخصائص او الصفات المستخرجة من البيانات والتي تستخدمها النماذج الذكية في اتخاذ قرارتها وتنبؤاتها.
3. **الخوارزمية (Algorithm):** هي الطريقة او القاعدة التي تستخدمها النماذج الذكية للتعلم من البيانات.

### 4-2-5 تطبيقات التعلم الآلي في التحقيق الجنائي

يمثل التعلم الآلي أداة ثورية في مجال التحقيقات الجنائية حيث يساهم في تحليل البيانات الجنائية. وفيما يلي اهم المجالات التي يمكن ان يستخدم فيها التعلم الآلي في التحقيقات الجنائية

1. **تحليل الأدلة الرقمية.**
2. **التعرف على الوجوه والصور.**
3. **التعرف على الصوت.**
4. **تحليل النصوص.**
5. **التنبؤ بالجريمة.**
6. **تحليل الشبكات الإجرامية.**

### 5-2-5 فوائد التعلم الآلي في التحقيق الجنائي

يمكن تلخيص فوائد التعلم الآلي في التحقيق الجنائي في الامور التالية :-

1. **تسريع التحقيقات:** تقليل الوقت اللازم لتحليل الأدلة.
2. **دقة أعلى:** تقليل الأخطاء البشرية في التحليل.
3. **توقع الجرائم:** المساهمة في الوقاية قبل وقوع الجريمة.
4. **تحسين إدارة الموارد:** توجيه جهود الشرطة إلى المناطق أو الحالات ذات الأولوية.

### 5-2-6 تحديات ومخاطر التعلم الآلي في التحقيق الجنائي

كما اشرنا سابقا ان التعلم الآلي يمثل أداة ثورية في مجال التحقيقات الجنائية اذا تم استخدامه بشكل عادل وشفاف وتحت رقابة قانونية وهنالك مجموعة من التحديات والمخاطر التي تواجه التعلم الآلي ويمكن اجمال هذه التحديات والمخاطر بالاتي :-

1. **التحيز في الخوارزميات.**
2. **الخصوصية.**
3. **الأدلة القابلة للطعن.**
4. **الاعتماد المفرط.**

### 5-2-7 أخلاقيات التعلم الآلي في التحقيق الجنائي

يعد أخلاقيات التعلم الآلي في التحقيق الجنائي موضوعا بالغ الاهمية لان استخدام النماذج الذكية في هذا المجال يمكن ان يكون له تاثير مباشرة على حياة الافراد وحقوقهم القانونية عند استخدامها في لتحقيقات مثل التنبؤ بالجريمة أو التعرف على المشتبة بهم فيجب الالتزام بمعايير أخلاقية دقيقة للحفاظ على العدالة والشفافية والخصوصية فلذا يجب أن يتم تنفيذها بعناية وهذا يتم من خلال :-

1. **العدالة وعدم التحيز.**
2. **الخصوصية وسرية البيانات.**
3. **الشفافية وقابلية التفسير.**
4. **الاعتماد المحدود على الآلة.**
5. **المسؤولية والمساءلة.**
6. **الجودة والدقة.**

## 5 – 3 تحسين الامن السيبراني في التحقيق الجنائي الرقمي

في ظل تزايد الاعتماد على التكنولوجيا في مختلف جوانب الحياة، ظهرت تحديات جديدة تتعلق بالأمن السيبراني خصوصًا في مجال التحقيق الجنائي. وذلك لان التحقيق الجنائي في العصر الرقمي لم يعد يعتمد على الأدلة المادية فقط، بل أصبح يتطلب قدرات وتقنيات عالية وأمنًا سيبرانيًا متينًا لحماية الأدلة وتحقيق العدالة. لذلك فان تحسين الأمن السيبراني لم يعد خيارًا بل ضرورة أساسية في مواجهة الجرائم الحديثة.

تهدف عملية تحسين الأمن السيبراني في التحقيق الجنائي الرقمي لتحقيق الاتي :-

1. الحفاظ على الأدلة و منع العبث بها أو فقدانها.
2. تعزيز ثقة المحاكم بالأدلة الرقمية.

3. تسريع عمليات التحقيق.
4. الحد من الجرائم الإلكترونية مستقبلاً.

### 5-3-1 مفهوم الأمن السيبراني

الأمن السيبراني هي عبارة عن مجموعة من العمليات والممارسات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية. ان مفهوم الأمن السيبراني ظهر مع تطور وزيادة استخدام التقنيات الخاصة بالشبكات والانظمة والانترنت والتي صاحبتها تطورا في الجرائم ايضا ، واظهرت انواع جديدة من الجرائم تُعرف بـ(الجرائم السيبرانية) ، والتي تتطلب آليات مختلفة في التحقيق تختلف عن الجرائم التقليدية. ومع ازدياد الاعتماد على الأدلة الرقمية، أصبح من الضروري تطوير قدرات المحققين الجنائيين في التعامل مع البيانات الرقمية بشكل آمن وسليم. ولذا أصبحت الهجمات السيبرانية والجرائم الرقمية من أكبر التحديات التي تواجه الأفراد والمؤسسات. وللتصدي لهذه التحديات ، تأتي ضرورة تحسين دور الامن السيبراني في التحقيق الجنائي الرقمي للاستجابة للحوادث كأحد أهم المجالات في أمن المعلومات.

### 5-3-2 أهمية الأمن السيبراني في التحقيق الجنائي الرقمي

يُعد الأمن السيبراني عنصرًا أساسيًا في حماية عمليات التحقيق من التلاعب، أو الاختراق، أو التسريب. وتكمن أهميته فيما يلي:

1. الحفاظ على سرية المعلومات والتحقيقات الجارية.
2. ضمان نزاهة الأدلة الرقمية ومنع العبث بها.
3. تأمين أدوات وتقنيات التحليل الجنائي من الهجمات المحتملة.
4. ضمان الامتثال للقوانين واللوائح المتعلقة بالخصوصية والبيانات.

### 5-3-3 التهديدات السيبرانية التي تواجه التحقيقات الجنائية الرقمية

تعد الجرائم السيبرانية التي تستهدف الأفراد والمؤسسات والدول من اهم التحديات الناتجة عن الاعتماد على الفضاء السيبراني في مختلف مجالات الحياة. وقد أصبح التحقيق الجنائي الرقمي ضرورة لكشف هذه الجرائم، إلا أن هذا النوع من التحقيقات تواجه العديد من المخاطر والتهديدات التي يمكن اجمالها بالاتي :-

1. الهجمات المتعمدة على أدلة رقمية (مثل حذفها أو تشفيرها ببرمجيات الفدية).
2. التجسس السيبراني على سير التحقيق.
3. البرمجيات الخبيثة التي تصيب أدوات التحليل.
4. الثغرات الأمنية في أنظمة إدارة الأدلة.

### 4-3-5 استراتيجيات تحسين الامن السيبراني في التحقيق الجنائي الرقمي

ان إجراء التحقيقات الرقمية بالوسائل التقليدية لم تعد كافية خصوصا مع تصاعد التهديدات الإلكترونية، فأصبح من الضروري دمج ممارسات الأمن السيبراني في كل مرحلة من مراحل التحقيق الجنائي الرقمي وذلك من خلال تطبيق استراتيجيات تحسين الامن السيبراني التي تعزز مصداقية الأدلة الرقمية، وحماية سير التحقيق، وضمان تحقيق العدالة. وفيما يلي مجموعة من استراتيجيات التي يمكن تطبيقها لتحسين الامن السيبراني في التحقيق الجنائي الرقمي :-

1- **التدريب والتأهيل.**
2- **تشفير البيانات.**
3- **تطبيق مبدأ الوصول المحدود.**
4- **تطوير البنية التحتية.**
5- **التعاون الدولي.**
6- **استخدام الذكاء الاصطناعي.**
7- **التوثيق والمراقبة المستمرة.**
8- **الامتثال للمعايير القانونية والأخلاقية.**

## 5 – 4 قوانين وتشريعات جديدة في الادلة الرقمية

لا شك ان الأدلة المستخرجة من الأجهزة الإلكترونية والأنظمة الرقمية تختلف جوهرياً عن الأدلة التقليدية ومع التوسع في الفضاء الرقمي، تزداد الحاجة لتشريعات واضحة وأدوات تقنية متطورة، بالاضافة الى الكوادر المؤهلة لضمان استخدام الأدلة الرقمية بطريقة قانونية وعلمية تحفظ العدالة وتكافح الجريمة بكفاءة. وهذا يتطلب وجود إطار قانوني وتشريعي ينظم هذه العمليات ويكفل الحقوق ويضبط المسؤوليات من خلال منظومة تشريعية متكاملة وقابلة للتطوير وتحمي الحقوق وتضمن الأمن وتشجع على الابتكار. ويمكن اعتبار القوانين والتشريعات جديدة في الادلة الرقمية بمثابة العمود الفقري لأي تحول رقمي ناجح، للأسباب التالية:

1. ضمان حماية البيانات الشخصية.
2. تنظيم التعاملات الإلكترونية.
3. تحديد المسؤوليات القانونية عند حدوث خروقات أو أعطال.
4. تعزيز الثقة العامة في الأنظمة الرقمية الحكومية.
5. مكافحة الجرائم الإلكترونية.

6. حماية حقوق المواطنين الرقمية.

ويمكن اجمال أبرز القوانين والتشريعات المرتبطة بالادلة الرقمية فيما يلي :-

1. **قوانين حماية البيانات الشخصية.**
2. **قوانين المعاملات الإلكترونية.**
3. **قوانين الأمن السيبراني.**
4. **قوانين حرية المعلومات.**
5. **قوانين الهوية الرقمية والتوقيع الرقمي.**

## 5 – 5 اتجاهات المستقبل والابتكارات في التحقيق الجنائي الرقمي

مع التحول الرقمي المتسارع والتطور المستمر في تقنيات المعلومات والاتصالات، أصبح التحقيق الجنائي الرقمي مجالًا ديناميكيًا يتطلب مواكبة الابتكار المستمر لمواجهة التحديات المعقدة والمتجددة في تطور أدوات وأساليب الجريمة الرقمية (مثل الهجمات السيبرانية، الابتزاز الرقمي، والتحايل الإلكتروني). وهذا يتطلب استجابة أمنية تحقق أعلى مستويات الفعالية والدقة، وهو ما يقود إلى استكشاف واستخدام تقنيات متقدمة مثل الذكاء الاصطناعي، والتعليم الالي، وتحليلات البيانات الضخمة في التحقيق الجنائي الرقمي.

ان التحقيق الجنائي الرقمي في المستقبل لن يكون فقط أداة لمعالجة الجرائم، بل سيكون منظومة متكاملة قائمة على الذكاء الاصطناعي والتعاون الدولي، والتحقيقات الاستباقية. وفيما يلي مجموعة العوامل التي تدفع للتغيير وتطوير الاتجاهات المستقبلية في هذا المجال :

1. ازدياد الجرائم السيبرانية من حيث الكم والنوع.
2. تعقيد تقنيات التشفير ووسائل الإخفاء.
3. توسع بيئات البيانات (الحوسبة السحابية، إنترنت الأشياء).
4. ظهور أدوات الذكاء الاصطناعي التوليدي التي يمكن إساءة استخدامها.
5. الحاجة إلى أدوات تحليل أسرع وأكثر ذكاءً لمواكبة البيانات الضخمة.

### 5-5-1 التقنية الحديثة في أدوات التحقيق الرقمي

في ظل التطور المتسارع للتكنولوجيا وازدياد تعقيد الجرائم الرقمية، يشهد مجال التحقيق الجنائي الرقمي تحولاً كبيراً نحو تبنّي اتجاهات مستقبلية مبتكرة تهدف إلى تعزيز الكفاءة والدقة في كشف الجرائم وتحليل الأدلة الرقمية. ومع تنامي الاعتماد على تحليلات البيانات الضخمة، والذكاء الاصطناعي، والحوسبة

السحابية، لم تعد الأدوات والأساليب التقليدية كافية لمواجهة التحديات الجديدة التي تفرضها البيئة الرقمية الحديثة. وفيما يلي ابرز الاتجاهات المستقبلية في التحقيق الجنائي الرقمي :-

1. **الذكاء الاصطناعي.**
2. **التحقيق الجنائي السحابي.**
3. **تحقيقات إنترنت الأشياء.**
4. **التحقيق في العملات الرقمية.**
5. **التعلم الآلي والتحقيق الرقمي الاستباقي.**
6. **أتمتة التحقيقات.**
7. **تحقيقات الواقع الافتراضي.**
8. **تحليل الوسائط المتعددة المتقدمة.**
9. **التحقيق العابر للحدود.**

## 2-5-5 التحديات المستقبلية للتحقيق الجنائي الرقمي

مع التوسع المستمر في الاعتماد على التكنولوجيا الرقمية في جميع جوانب الحياة، تتعاظم التحديات التي تواجه التحقيق الجنائي الرقمي، مما يستدعي استعداداً استباقياً لمواجهة مستقبل يتسم بتعقيد الجرائم وتطور أدوات المجرمين. ففي الوقت الذي تُستخدم فيه تقنيات متقدمة مثل الذكاء الاصطناعي، والحوسبة السحابية، والعملات الرقمية، وأجهزة إنترنت الأشياء، بات المحقق الرقمي يواجه بيئة متغيرة يصعب مواكبتها بالوسائل التقليدية. ومن أبرز التحديات المستقبلية التي تواجه المحقق الرقمي هو

1. تطور أساليب إخفاء الأدلة والتشفير
2. زيادة حجم وتعقيد البيانات.
3. صعوبة الوصول إلى الأدلة المخزنة عبر الحدود الجغرافية.
4. الحاجة الملحة إلى تحديث القوانين.
5. تطوير الكوادر البشرية المؤهلة للتعامل مع الأدلة الرقمية بأعلى مستويات الدقة والمهنية
6. الخصوصية وحماية الحقوق الرقمية.

## 3-5-5 المهارات المستقبلية للمحقق الجنائي الرقمي

في ظل التطور المستمر في تقنيات المعلومات والاتصالات، يتزايد اعتماد أجهزة إنفاذ القانون على الخبرات الرقمية في مواجهة الجرائم الحديثة. ومع تعقّد البيئة الرقمية وتطور أساليب الجريمة الإلكترونية، أصبحت المهارات التقليدية للمحقق الجنائي غير كافية وحدها، مما أفرز حاجة متزايدة إلى

تطوير مهارات مستقبلية متخصصة تواكب تحديات العصر الرقمي. تشمل هذه المهارات القدرة على تحليل البيانات الضخمة، وفهم تقنيات الذكاء الاصطناعي، والتعامل مع أنظمة الحوسبة السحابية، وتحليل الأدلة من أجهزة إنترنت الأشياء والعملات الرقمية. كما أصبح من الضروري أن يمتلك المحقق الجنائي الرقمي كفاءة في الأمن السيبراني، والتشفير، واسترجاع البيانات المحذوفة، وفهم التشريعات الرقمية العابرة للحدود. ولا تقتصر المهارات المستقبلية على الجانب التقني فقط، بل تشمل أيضاً المهارات التحليلية والتفكير النقدي، والقدرة على التواصل والتنسيق مع جهات متعددة، إضافة إلى الالتزام بأخلاقيات المهنة والمعايير القانونية الدولية.

### 4-5-5 التوصيات والاستعداد للمستقبل

في ظل التوسع الهائل في التقنيات الرقمية وتنامي تهديدات الجرائم الإلكترونية، يواجه المحقق الجنائي الرقمي مستقبلاً يتطلب مستوى أعلى من الجاهزية، والتخطيط، والتطوير المستمر. ولم يعد كافياً الاكتفاء بالمهارات الحالية أو الأساليب التقليدية، بل أصبح من الضروري وضع رؤية مستقبلية واضحة تتضمن توصيات واستعدادات ممنهجة تمكّن المحقق من أداء دوره بكفاءة في بيئة تقنية سريعة التغير. وفيما يلي بعض التوصيات الخاصة للاستعداد المستقبلية في مجال التحقيق الجنائي الرقمي:-

1. استثمار في البحث والتطوير في مجال الأدلة الرقمية.
2. تحديث مستمر للتشريعات والقوانين لمواكبة الأدلة الناشئة.
3. تدريب الكوادر الأمنية والقضائية على الأدوات المتقدمة.
4. تعزيز التعاون الدولي في مشاركة البيانات والتحقيقات.

اعتماد منصات ذكاء اصطناعي موثوقة تضمن الشفافية في نتائج التحليل.

**رقم التمرين:14** **الزمن المخصص: 3 ساعات**

**اسم التمرين: استخدام (AWS Cloud Trial) لفحص سجلات النشاط في الحوسبة السحابية.**

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الأهداف التعليمية:**

عرض وفحص وتحليل سجلات النشاط (Activity Logs) داخل بيئة الحوسبة السحابية دون كتابة أي أكواد، وفهم كيفية تتبع العمليات الناجحة والفاشلة وتأثير الصلاحيات على أمن النظام.

**ملاحظة:-** استخدام Google Cloud Logging (Logs Explorer) كبديل مجاني عن الاداة (AWSCloudTrail)، كونها غير مجانية، دون كتابة أكواد, تعمل مباشرة عبر المتصفح، ولا تحتاج تثبيت.

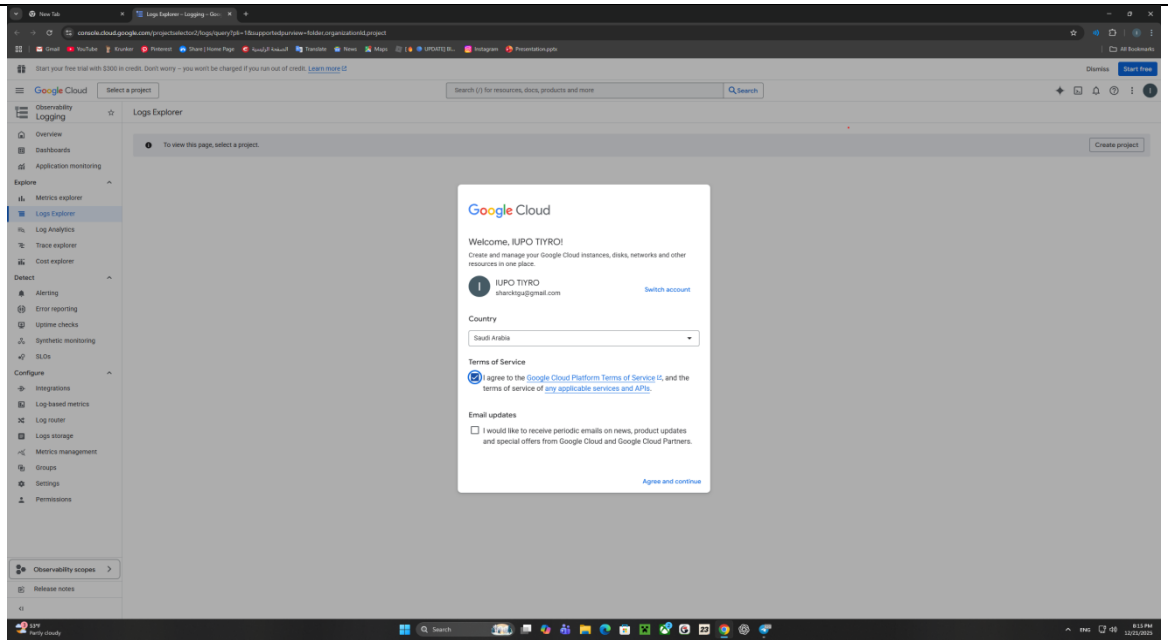
**ثانياً: التسهيلات العلمية:**

**المتطلبات الاساسية:**

- ✓ جهاز حاسوب لابتوب مع متصفح إنترنت.
- ✓ حساب مجاني في منصة Google وGoogle Cloud Project.
- ✓ جدول أو ورقة لتسجيل ملاحظات الطالب حول النشاطات المشبوهة والطبيعية.
- ✓ يمكن تجربة منصة Google Cloud Free Tier – Cloud Logging كبديل، مجاني ضمن حدود (FreeTier)، ولا تحتاج كتابة أكواد إذا استخدمت واجهة ( Logs Explorer) لعرض وتحليل سجلات النشاط

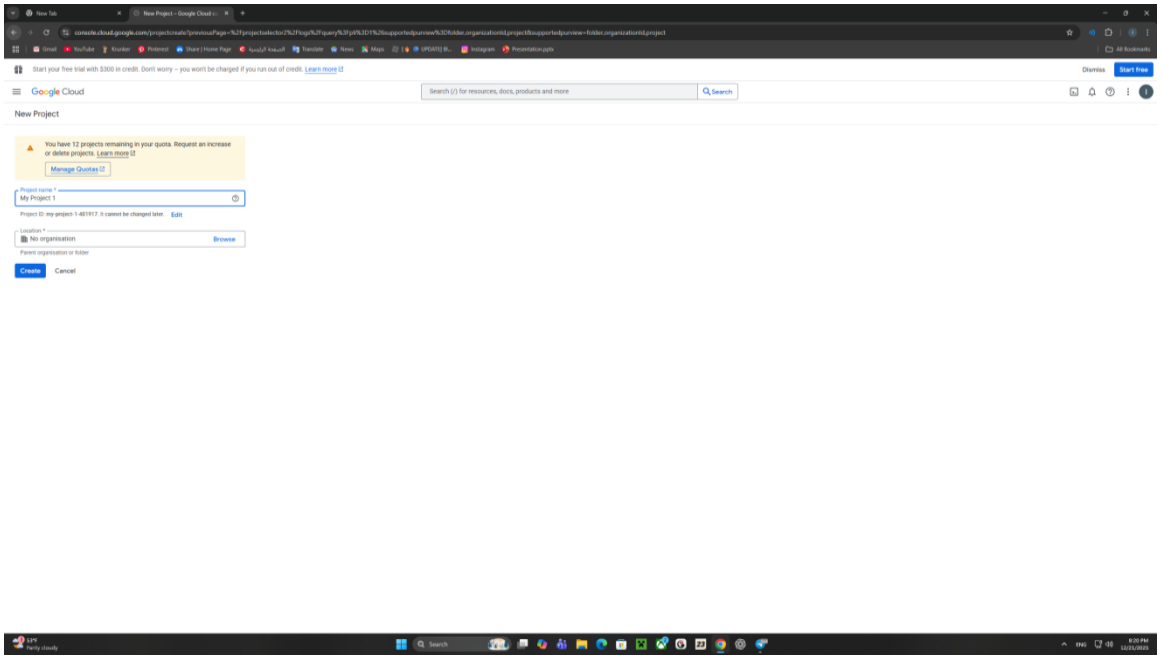
**الخطوة 1:** ارتد بدلة العمل ثم:

الدخول الى الواجهة المجانية لتحليل سجلات النشاط على Google Cloud بدون كود وتسجيل الدخول بحساب Google الخاص بك، ثم استخدام Logs Explorer لعرض وتحليل سجلات النشاط مباشرة عبره المنصة Google Cloud Logs Explorer – Free Tier بالضغط على الرابط الخاص https://console.cloud.google.com/logs كما في الشكل (5 – 3):



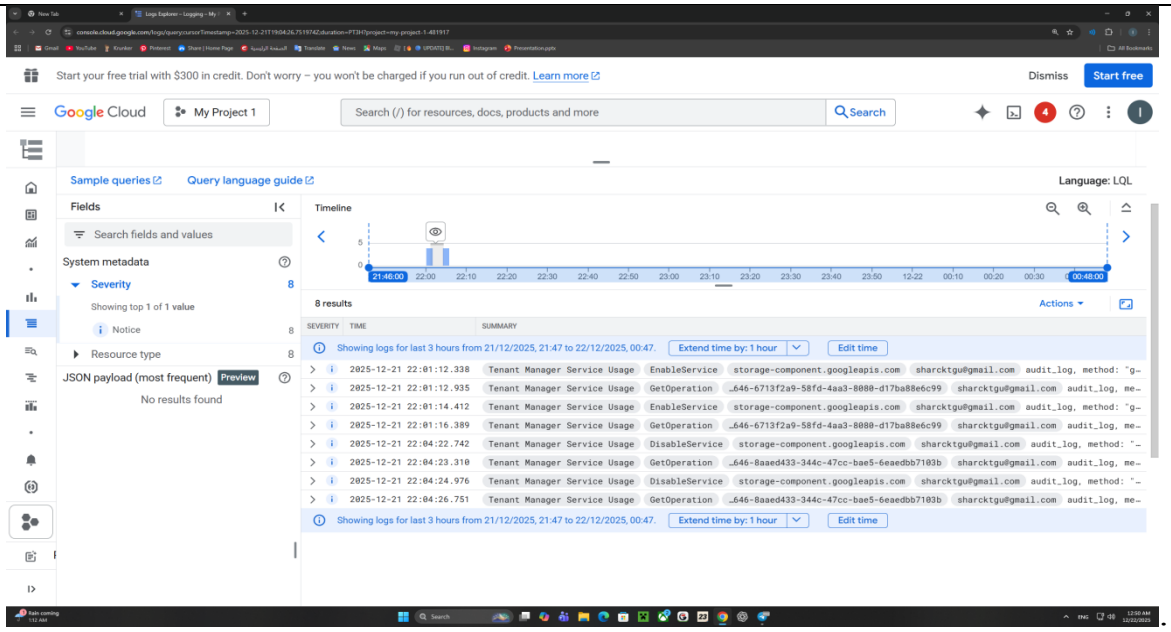

**الشكل (5 – 3)**

**الخطوة 2:** أدخل اسم المشروع في الحقل المخصص (Project Name) في هذا التمرين سنختار اسم المشروع (My Project 1). اما الحقل Organization إذا كان مطلوبًا سنختار ( No Organization)، أو اتركه فارغًا.ثم اضغط على المفتاح (Create) لإنشاء المشروع، بعد ذلك سيتم فتح لوحة التحكم الخاصة بالمشروع الجديد (Project Dashboard). كما في الشكل (5 –4):



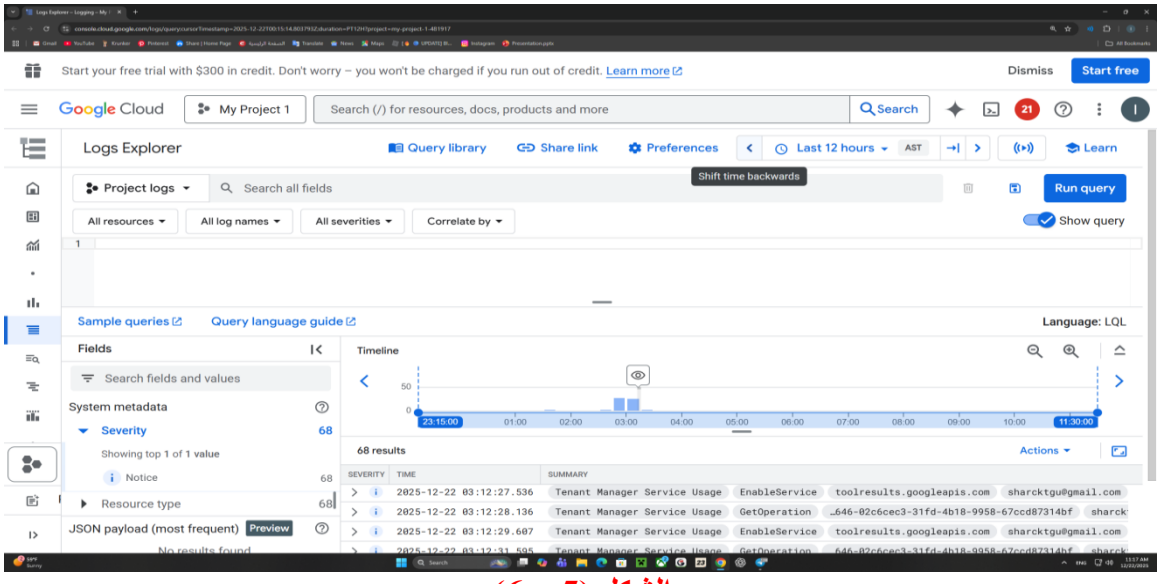

**الشكل (5 –4)**

**الخطوة 3:** اضغط على Logs Explorer لفتح واجهة استعراض السجلات. داخل المشروع في Google Cloud، وهو المكان الذي ستتمكن منه من فحص سجلات النشاط (Activity Logs) دون الحاجة لأي أكواد. ستظهر لوحة لتصفية السجلات حسب (الخدمة، الوقت، والنوع) ويمكنك البدء في تحليل سجلات النشاط كما هو هدف التمرين كما في الشكل (5 – 5):



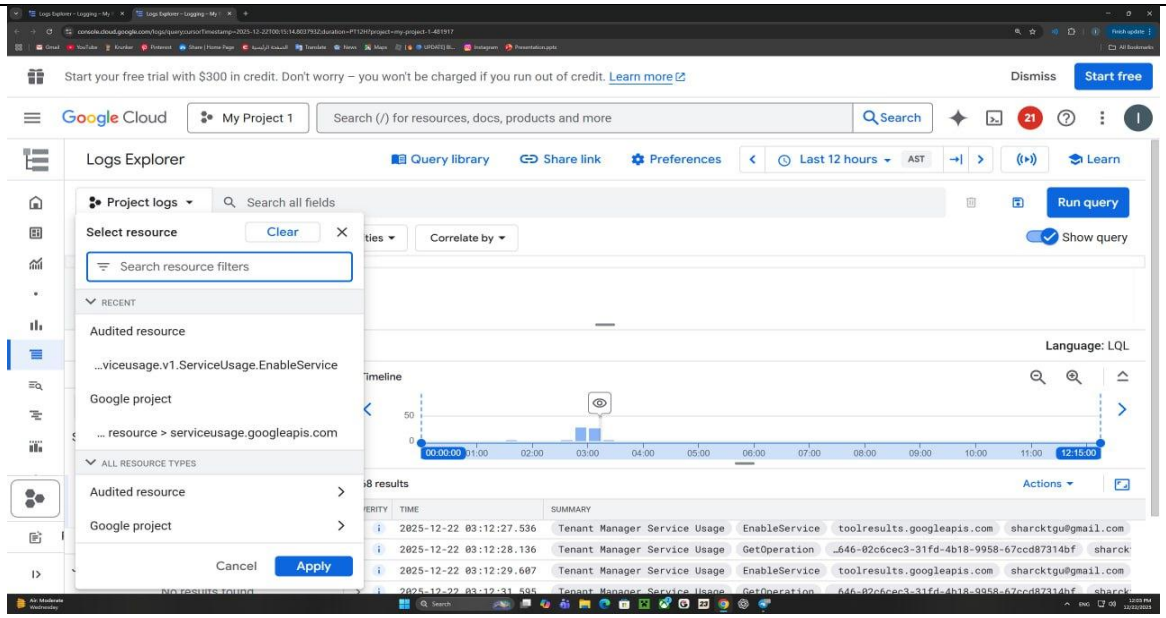

**الشكل (5 – 5)**

**الخطوة 4:** في واجهة Logs Explorer، توجد مجموعة من الخدمات و المورد الذي من الممكن فحص سجلاتها وقبل ذلك يجب ان يتم تحديد نطاق الوقت في الحقل Shift time backwards المخصص في شريط التبويب Logs Explorer . نتستطيع اختيار الفترة الزمنية المراد تحليل سجلاتها مثلاً (آخر ساعة، يوم، أسبوع) وهذا يساعد على تضييق نتائج السجلات وتركيز التحليل على النشاط المطلوب. ثم نضغط على المفتاح Run Query لعرض كل السجلات المرتبطة بالخدمة والفترة المحددة. عندها يمكننا رؤية الأحداث والنشاطات المرتبطة بالمشروع ومن قام بالنشاط، ومتى حدث، ونوع العملية وكما في الشكل (5 – 6):



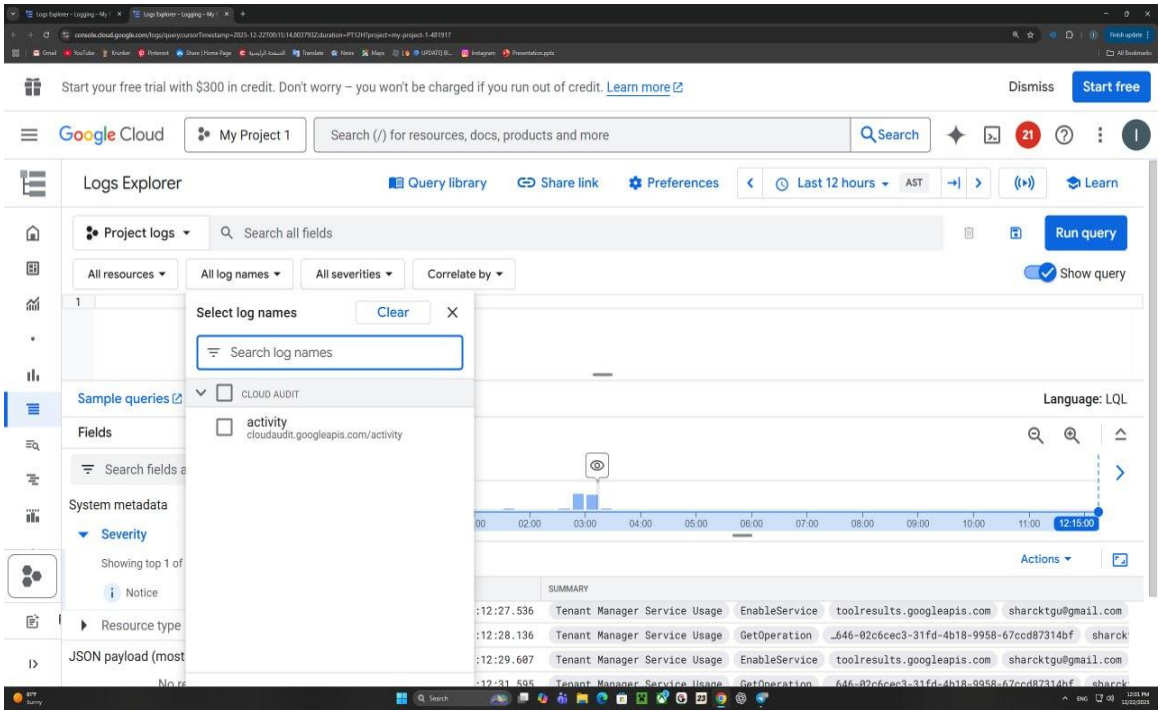

**الشكل (5 – 6)**

**الخطوة 5:** كما شرنا سابقا ان في واجهة Logs Explorer، توجد مجموعة من الخدمات و المورد الذي من الممكن فحص السجلات على اساسها وسنبدأ بالمورد (All resources) ويتم فيها اختيار أي مورد (Resource) نريد عرض سجلاته، مثل الخوادم أو قواعد البيانات. بعد اختيار الخدمة التي نريد عمل فحص لسجلاتها نضغط المفتاح Apple لاضافته كما موضح في الشكل (5 – 7):



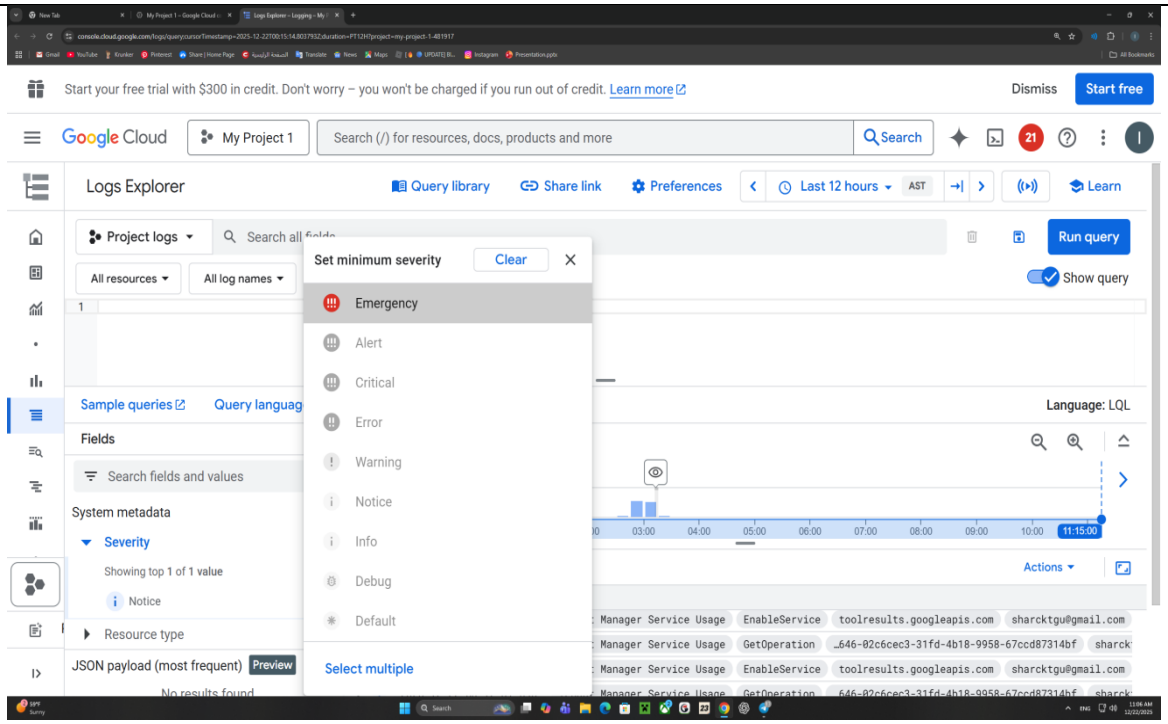

**الشكل (5 – 7)**

**الخطوة 6:** اختيار نوع السجل الدخول الذي تريد تحليله، مثل سجلات النشاط أو سجلات الأخطاء. وذلك من الضغط على المفتاح (All log names)، وبعد اختيار السجل نضغط المفتاح Apple لاضافته كما موضح في الشكل (5 – 8):



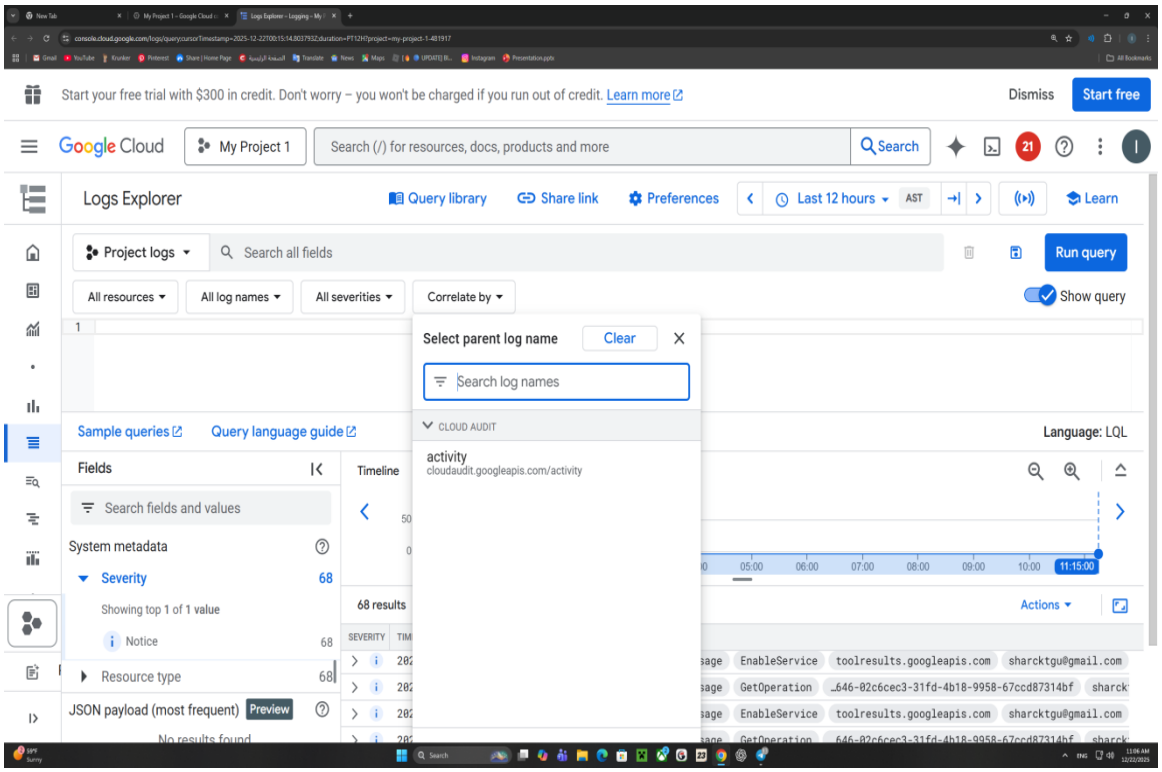

**الشكل (5 – 8)**

**الخطوة 7:** يمكن اختيار مستوى تصنيف الخطورة او درجاتها (Low Medium High)، من خلال القائمة All severities كما موضح في الشكل (5 – 9):




**الشكل (5 – 9)**

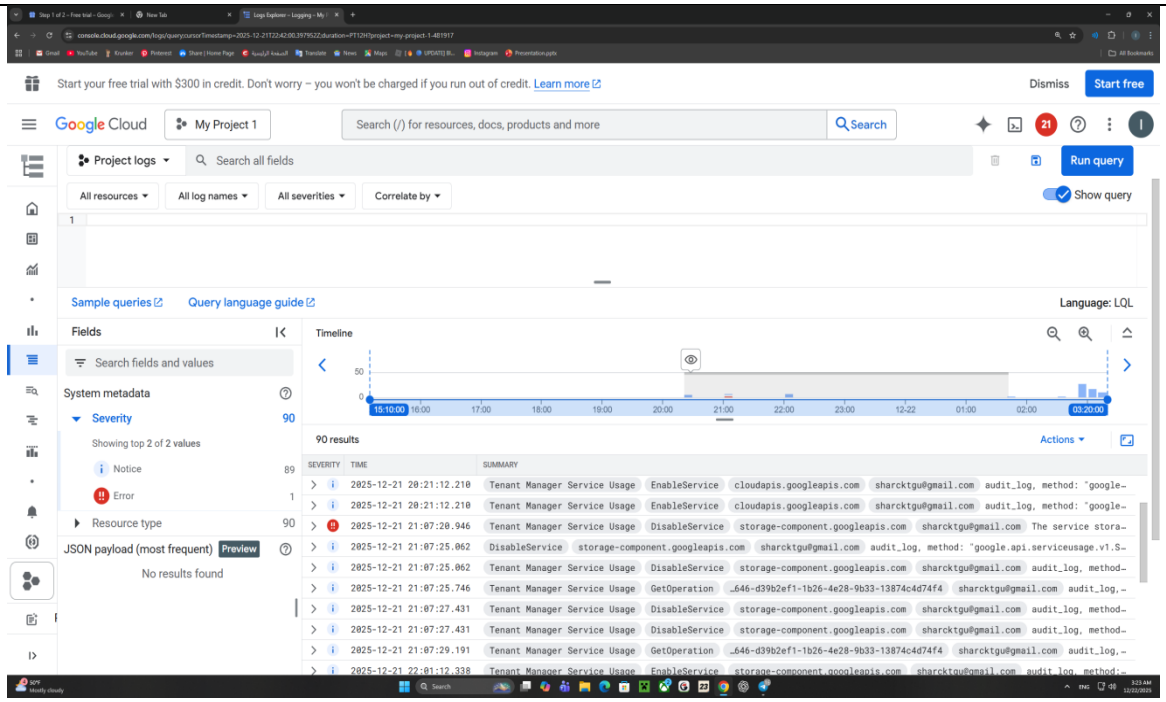
**الخطوة 8:** ربط وتحليل السجلات حسب معيار محدد مثل المستخدم أو الخدمة، لمعرفة الأنماط أو الأنشطة المشبوهة من خلال القائمة Correlate by كما موضح في الشكل (5 – 10):




**الشكل (5 – 10)**

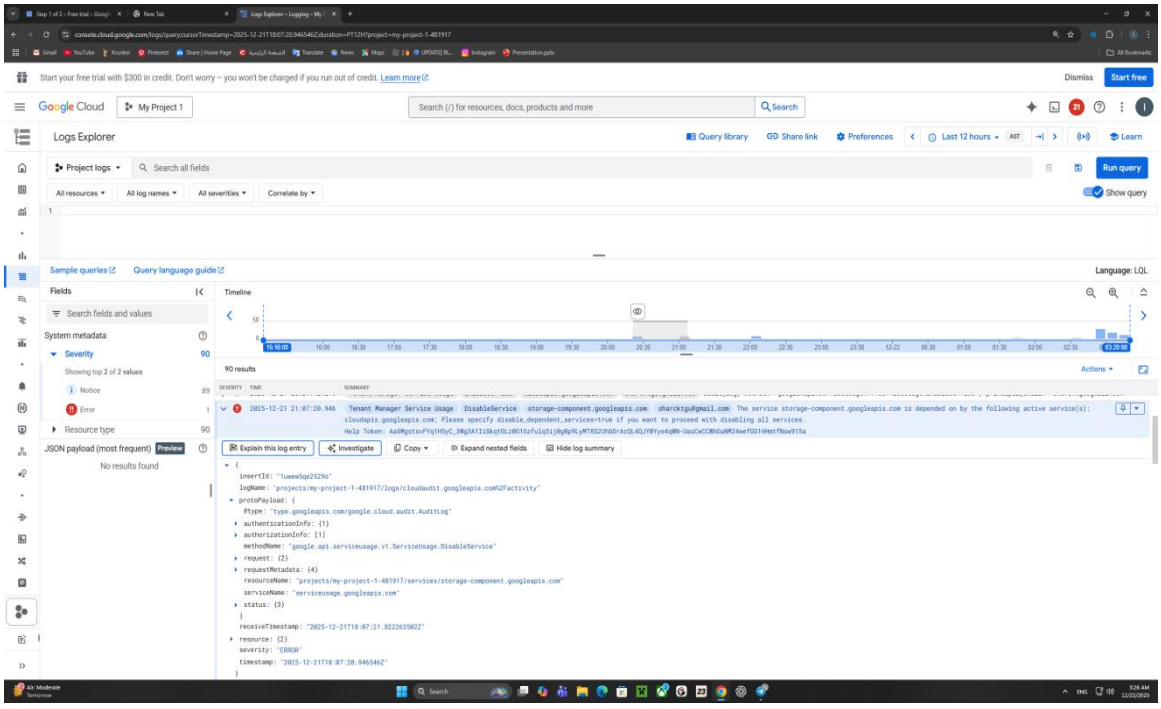
ملاحظة:- هذه الخيارات تساعدك على تصفية السجلات وتحليلها بطريقة منظمة وسريعة.

**الخطوة 9:** بعد تحديد الاختيارات نضغط على المفتاح Run Query للحصول على السجلات التي يتم تحليلها في الخطوة التالية كما موضح في الشكل (5 – 11):




**الشكل (5 – 11)**

**الخطوة 10:** في هذه المرحلة سنتعرف على عملية تحليل بيانات من خلال عرض سجلات موجودة أصلًا وقراءة الأحداث مثلا (تسجيل الدخول فتح واجهات استعلام Logs نفسه تفعيل خدمات) هذه تسمى System Logs او Background والتحليل الحقيقي للبيانات (Analysis) يكون عندما، يتم ربط الحدث بفاعل (Who) وتحدد الزمن (When) تحدد المورد (What Resource)، تفسر السبب (Why) مثلاً (من الذي أنشأ VM وفي أي وقت ومن أي IP وهل الحدث طبيعي أم مشبوه) و هذا السجل يمثل حدثًا إداريًا حقيقيًا تسمى فلترة السجلات (هنا يبدأ التحليل). سنختار السجل المؤشر باللون الاحمر لتحليها كما موضح في الشكل (5 – 12):




**الشكل (5 – 12)**

**الخطوة 11:**

بعد اختيار السجل سنقوم بصياغة تحليل احترافي للسجل وكأننا محققون رقميون من خلال التعرف على مستويات الخطورة Severities مثل (INFO = معلومات WARNING = تحذير ERROR = خطأ CRITICAL = خطير جدًا).

سجل تدقيق (Audit Log) هذا من Google Cloud تخبرنا أن هناك محاولة لتعطيل خدمة Cloud Storage داخل المشروع، وأن هذه المحاولة فشلت ونتج عنها خطأ (ERROR). بمعنى ان شخص أو نظام حاول إيقاف خدمة مهمة، لكن العملية لم تنجح.

logName: cloudaudit.googleapis.com/activity

هذا سجل نشاط إداري (Activity Log) يعني تغيير إعدادات أو خدمات داخل المشروع.

methodName: ServiceUsage.DisableService

الإجراء الذي تم تنفيذه هو محاولة تعطيل خدمة في المشروع.

resourceName: storage-component.googleapis.com

الخدمة المستهدفة هي Cloud Storage (خدمة تخزين سحابية مهمة).

serviceName: serviceusage.googleapis.com

الجهة التي نفّذت الطلب هي خدمة إدارة الخدمات في Google Cloud.

"severity: "ERROR

العملية فشلت ونتج عنها خطأ (إما بسبب صلاحيات، أو لأن الخدمة مطلوبة ولا يمكن إيقافها).

timestamp / receiveTimestamp

وقت تنفيذ المحاولة ووقت تسجيلها في السجلات.

الخلاصة للطالب (سطر واحد): هذا السجل يوضح محاولة فاشلة لتعطيل خدمة Cloud Storage داخل المشروع، وتم تسجيلها كخطأ أمني في سجلات التدقيق.

**النتيجة المتوقعة**

أن يتعلّم الطالب عمليًا كيفية تتبّع وتحليل سجلات النشاط داخل بيئة سحابية حقيقية، ويفهم كيف يتم تسجيل كل إجراء يتم على المشروع (مثل تفعيل أو تعطيل خدمة) داخل Activity Logs، مع القدرة على قراءة الرسائل وفهم معناها الأمني. ومن خلال ذلك يكتسب الطالب مهارة ربط الأحداث الزمنية بالمستخدم والخدمة المتأثرة، والتمييز بين السلوك الطبيعي والأخطاء أو الأنشطة غير المتوقعة، وهي مهارة أساسية في التحقيق الجنائي الرقمي ومهام محلل الأمن السيبراني في البيئات السحابية.

**المناقشة**

1. ما فائدة سجلات النشاط في مراقبة أمن المشروع السحابي؟
2. لماذا نحدد الزمن قبل تحليل السجلات؟
3. هل المحاولة الفاشلة تُعد حدثًا أمنيًا؟ ولماذا؟
4. ما أهمية مستويات الخطورة في السجلات؟
5. كيف نحدد (من، متى، ماذا، لماذا) من سجل واحد؟

| استمارة الفحص<br>تمرين رقم 14 | | | |
|---|---|---|---|
| الجهة الفاحصة: | | | |
| اسم الطالب : | المرحلة الثالثة | التخصص : الامن السيبراني | |
| اسم التمرين : استخدام (AWS CLOUD TRIAL) لفحص سجلات النشاط في الحوسبة السحابية | | | |

| ت | الخطوات | الدرجة القياسية % 50 | درجة الاداء %50 | الملاحظات |
|---|---|---|---|---|
| 1 | ارتداء بدلة العمل | %5 | | |
| 2 | تسجيل الدخول بحساب Google الى واجهة Google Cloud | %5 | | |
| 3 | أنشاء المشروع في Google Cloud ثم استخدام Logs Explorer لاجراء الاختبارات عليها | %5 | | |
| 4 | فحص سجلات النشاط (Activity Logs) | %5 | | |
| 5 | اختيار الفترة الزمنية المراد تحليل سجلاتها | %5 | | |
| 6 | اختيار المورد (Resource) المراد عرض سجلاته ثم اختر نوع السجل الدخول الذي تريد تحليله | %5 | | |
| 7 | اختيار مستوى تصنيف الخطورة او درجاتها | %5 | | |
| 8 | اجراء عملية التحليل للحصول على السجلات وقراءة الأحداث | %5 | | |
| 9 | المناقشة | %5 | | |
| 10 | الزمن المخصص | %5 | | |
| المجموع | | | | |
| اسم الفاحص | | التوقيع | | |

**رقم التمرين15** **الزمن المخصص: 3 ساعات**

**اسم التمرين: استخدام أدوات مفتوحة المصدر مثل (TENSOR FLOW) لتدريب نموذج يتنبأ بسلوكيات مشبوهة.**

**مكان التنفيذ: مختبر الحاسوب**

**اولاً: الأهداف التعليمية:**

تعريف الطلبة عمليًا على كيفية استخدم الذكاء الاصطناعي لاكتشاف السلوكيات المشبوهة قبل أن تتحول إلى هجوم إلكتروني، بمعنى نجعل النظام نفسه يتعلم ويراقب.

**ثانياً: التسهيلات العلمية:**

**المتطلبات الاساسية:**

- ✓ جهاز حاسوب منصب علية نظام التشغيل (Windows 11) ومتصل بالانترنت.
- ✓ استخدام الاداة (**TENSOR FLOW**) والتي هي مكتبة برمجية طورتها (Google) تستخدم لبناء نموذج ذكاء صناعي مناسبة للتعليم والتجارب العلمية.
- ✓ **النموذج:** هو برنامج ذكي يتعلم من البيانات وليس مجرد اوامر ثابتة، حيث يتم تغذيتها بمجموعة من البيانات الافتراضية، مثلا وقت الدخول الى لنظام، عدد المحاولات، نوع العملية (قراءة، حذف، تعديل) ، هذه البيانات تكون جاهزة او منشاة لاغراض تعليمية، وبعدها يبدأ يتوقع اشياء جديدة على اساسها.
- ✓ استخدام الاداة (TensorFlow Playground)، للشرح والعرض البصري فقط (تعليمي)، بدون تنفيذ نموذج حقيقي.

الخطوة 1:ارتد بدلة العمل ثم قم بإنشاء نموذج تصنيف (Classification Model) بسيط يتنبأ بالسلوكيات المشبوهة، من خلال تجهيزها بالبيانات الافتراضية ، وهذا يجعل النموذج عبارة عن طبقات، كل طبقة تتعلم جزء من السلوك، كما موضح في الجدول رقم (5 – 1)، وهذه الطبقات هي :

- طبقة ادخال البيانات: تستقبل البيانات (معلومات عن سلوك المستخدم)
- طبقات التحليل: البحث عن الانماط التكررة (دخول متكرر، وقت متاخر....الخ)
- طبقة القرار: اعطاء نتيجة (0 = سلوك طبيعي ، 1 = سلوك مشبوه)

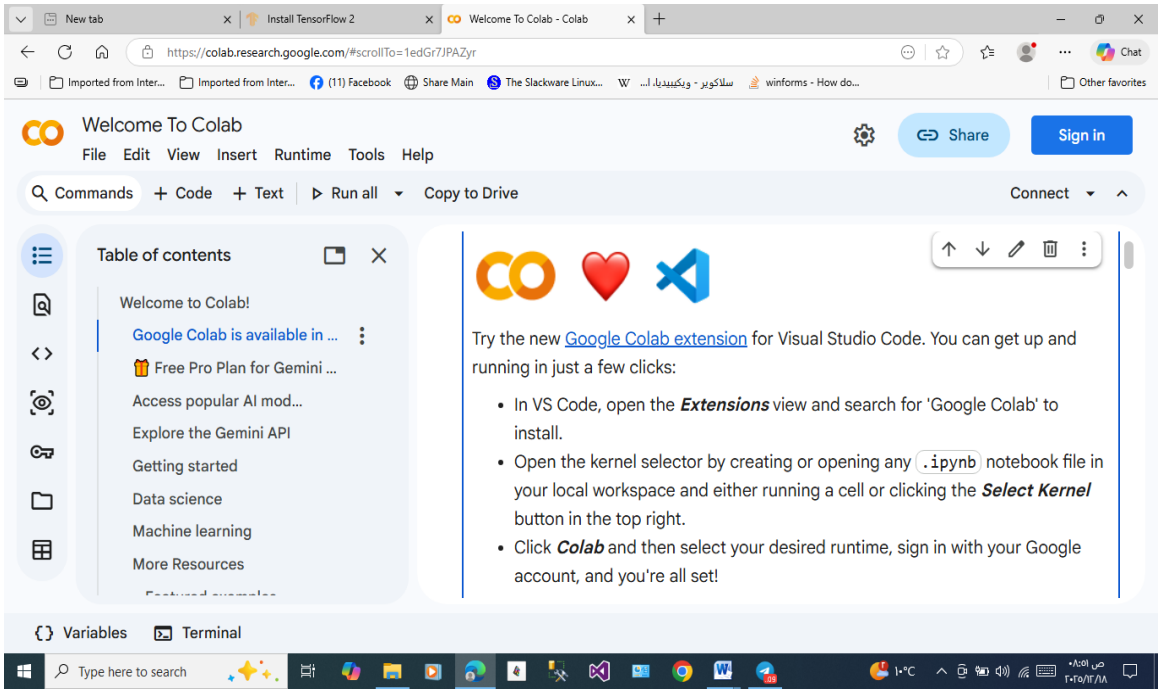
| النتيجة | نوع العملية | عدد المحاولات | وقت الدخول |
|---|---|---|---|
| طبيعي | قراءة | 1 | صباحًا |
| مشبوه | دخول | 5 | ليلًا |
| طبيعي | تعديل | 1 | ظهرًا |
| مشبوه | حذف | 7 | فجرًا |

**الجدول رقم (5 – 1)**

**الخطوة 2:**

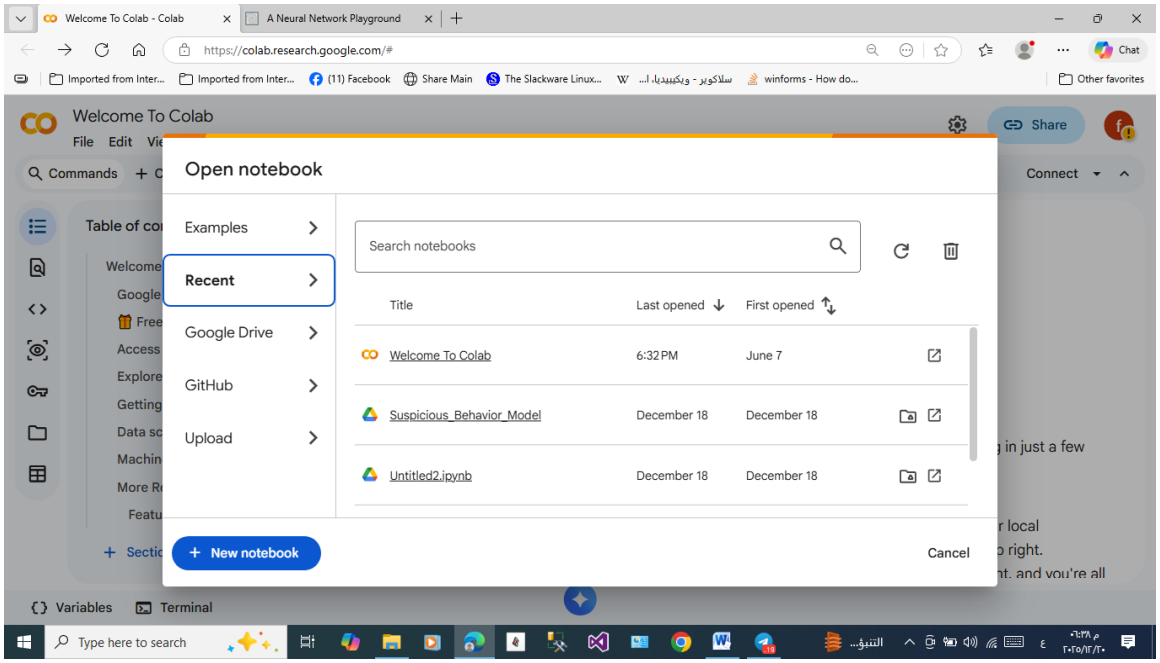
لاستخدام الاداة (TENSOR FLOW) بدون تثبيتها على الحاسبة عبر (Google Colab)، اضغط الرابط

(https://colab.research.google.com)، فتظهر الواجهة كما في الشكل (5 – 13):



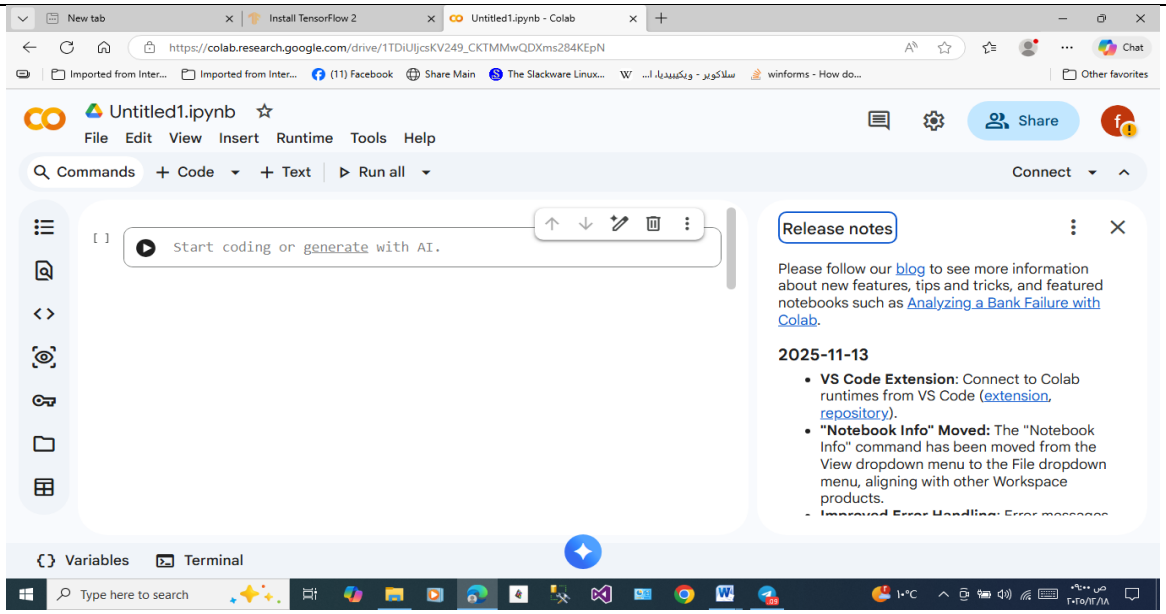

**الشكل (5 – 13)**

**الخطوة 3:** قم بعملية تسجيل الدخول الى (TENSOR FLOW) من خلال حساب (Gmail). بعد ان تتم عملية الدخول بنجاح تظهر الصفحة (Open notebook) كما في الشكل (5 – 14):



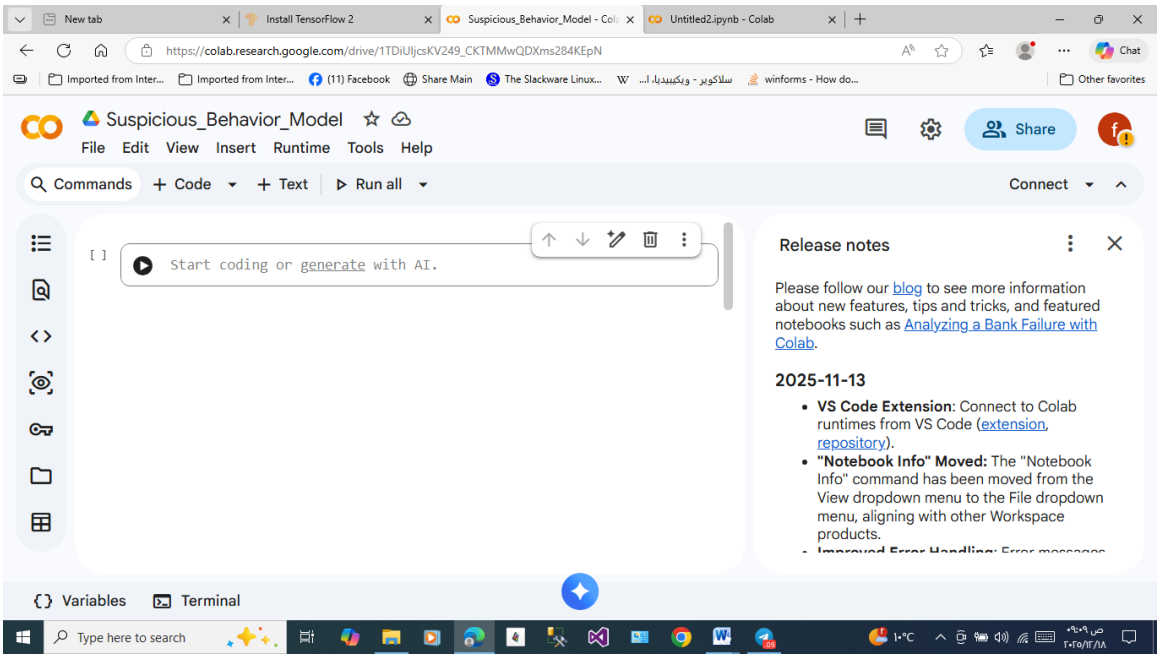

**الشكل (5 – 14)**

**الخطوة 4:** في صفحة (Open notebook) نضغط على (New notebook+)، فتظهر الصفحة (Untitled.ipynb)، كما في الشكل (5 – 15):




**الشكل (5 – 15)**

**الخطوة 5:** في اعلى الصفحة اضغط على اسم الملف والتي تكون عادة (Untitled.ipynb)، وقم بتغيرها الى اسم تستطيع حفظة وبسهولة تقدر الرجوع له عند الحاجة مثل (Student_Model)، في هذا التمرين سنختار الاسم (Suspicious_Behavior_Model) كما في الشكل (5 – 16).

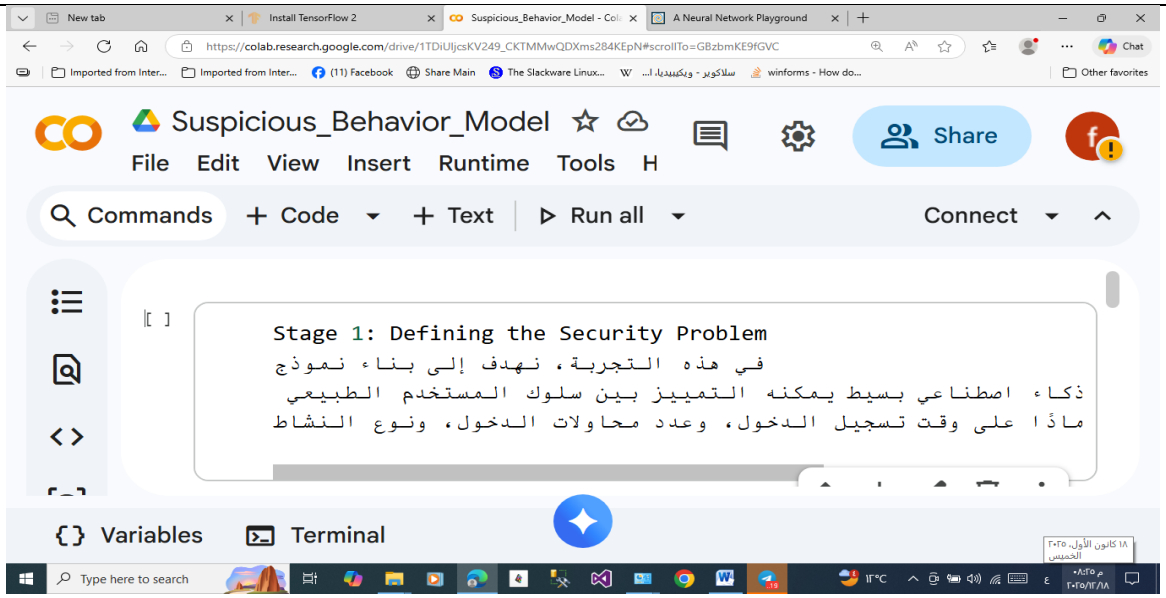



**الشكل (5 – 16)**

**الخطوة 5:** اضافة الخلايا (Stege) تتم عملية اضافة الخلايا من خلال الضغط على المفتاح (Code) في الشريط العلوي، والكتابة في الخلية يتم عبر الضغط على المفتاح (Text)، وكما يلي:-

**الخلية 1: تعريف المشكلة الامنية (Defining the security problem):**

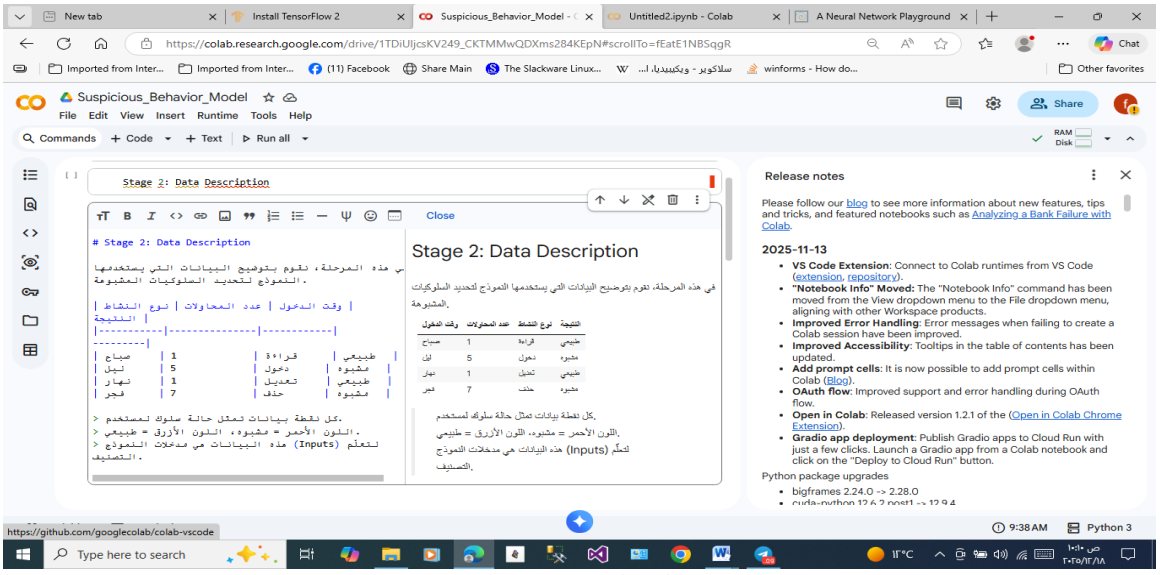
نضغط المفتاح (Code) لاضافة (الخلية 1)، وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي للمشكلة الامنية المراد من نموذج ذكاء اصطناعي اثباتها وهي (التمييز بين سلوك الطبيعي والسلوك المشبوه للمستخدم، وذلك اعتمادًا على وقت تسجيل الدخول، وعدد محاولات الدخول، ونوع النشاط)، وكما موضح في الشكل (5 – 17).




**الشكل (5 – 17)**

**الخلية 2: وصف البيانات (Data Description)**

نضغط المفتاح (Code) لاضافة (الخلية 2)، وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع لوصف البيانات، وادراج بيانات الجدول رقم (5 – 1)، كما موضح في الشكل (5 – 18):




**الشكل (5 – 18)**

**الخلية 3 : تصميم النموذج (Model Design)**

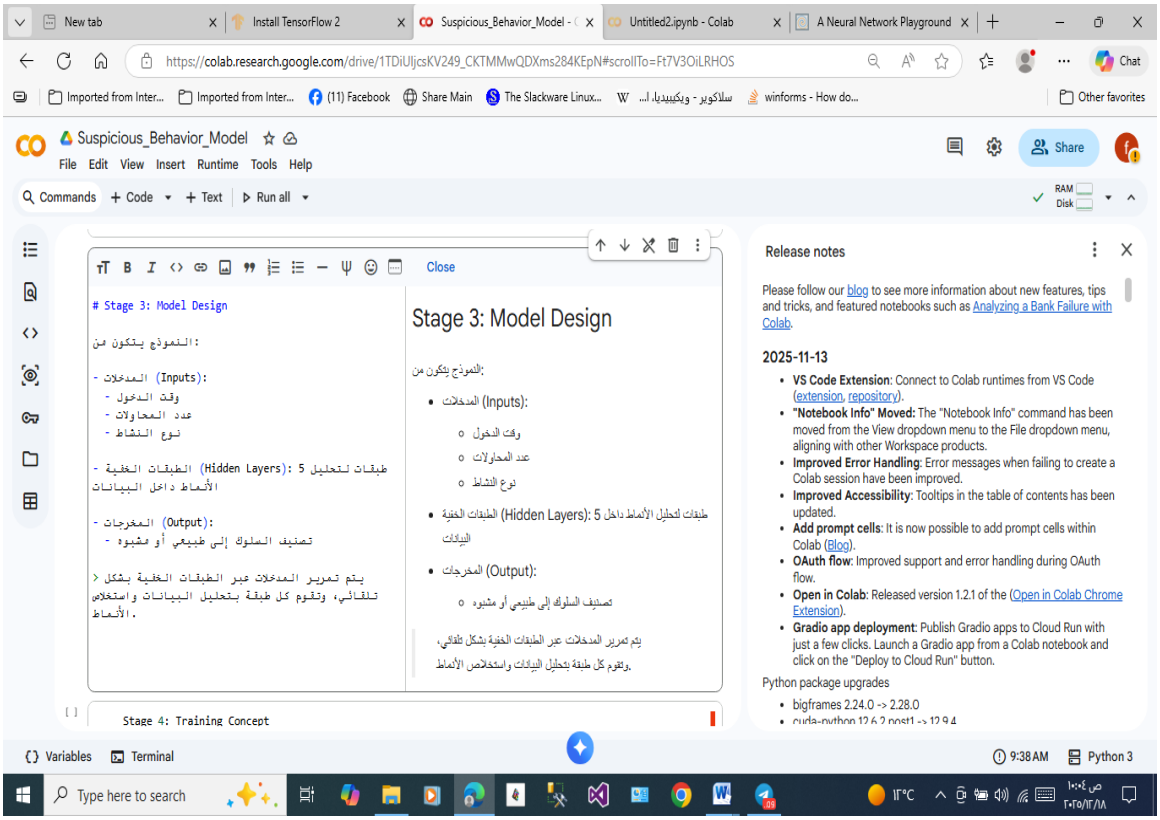
نضغط المفتاح (Code) لاضافة (الخلية 3)، وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي لتصميم النموذج كما موضح في الشكل (5 – 19) ، اما مكونات النموذج الرئيسة :-

المدخلات (Inputs): وهي المعلومات التي تعطى للنموذج مثل (وقت الدخول، عدد المحاولات، نوع النشاط، .....الخ)

الطبقات الخفية (Hidden Layers): وظيفة هذه الطبقات تحليل المدخلات، واكتشاف العلاقات والأنماط بينها مثلا (وقت متاخر، محاولات كثيرة، .....الخ).

المخرجات (Output): النتيجة النهائية التي يعطيها النموذج لتصنيف السلوك (طبيعي أم مشبوه).

الخلاصة (البيانات تدخل، تمر عبر الطبقات للتحليل، ويخرج قرار واضح ، طبيعي او مشبوه).




**الشكل (5 – 19)**

**الخلية 4: فكرة التدريب (Training Concept)**

نضغط المفتاح (Code) لاضافة (الخلية 4)، وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي لفكرة تدريب النموذج على كيفية التميّز بين السلوك الطبيعي و السلوك المشبوه. وكما موضح في الشكل (5 – 20). ويمكن تلخيص فكرة التمرين فيما يلي:-

1- البيانات: كل سجل يحتوي مدخلات (وقت الدخول، عدد المحاولات، نوع النشاط)، ومع نتيجة صحيحة تسمى (Label)

2- التدريب: النموذج يكرّر قراءة البيانات عدة مرات تسمى (Epochs) الهدف هو تقليل الخطأ.

3- التحسين: يقارن النموذج ناتجه بالنتيجة الصحيحة، ويصحّح أخطاءه، ويتحسّن مع كل تكرار ويصبح أدق وأذكى في التمييز ،وبهذه الحالة يكون النموذج قادرا على ان يتعلّم من أخطائه؛ وكلما تدرّب أكثر، تحسّن أداؤه، وأصبح أدق في اكتشاف السلوك المشبوه.

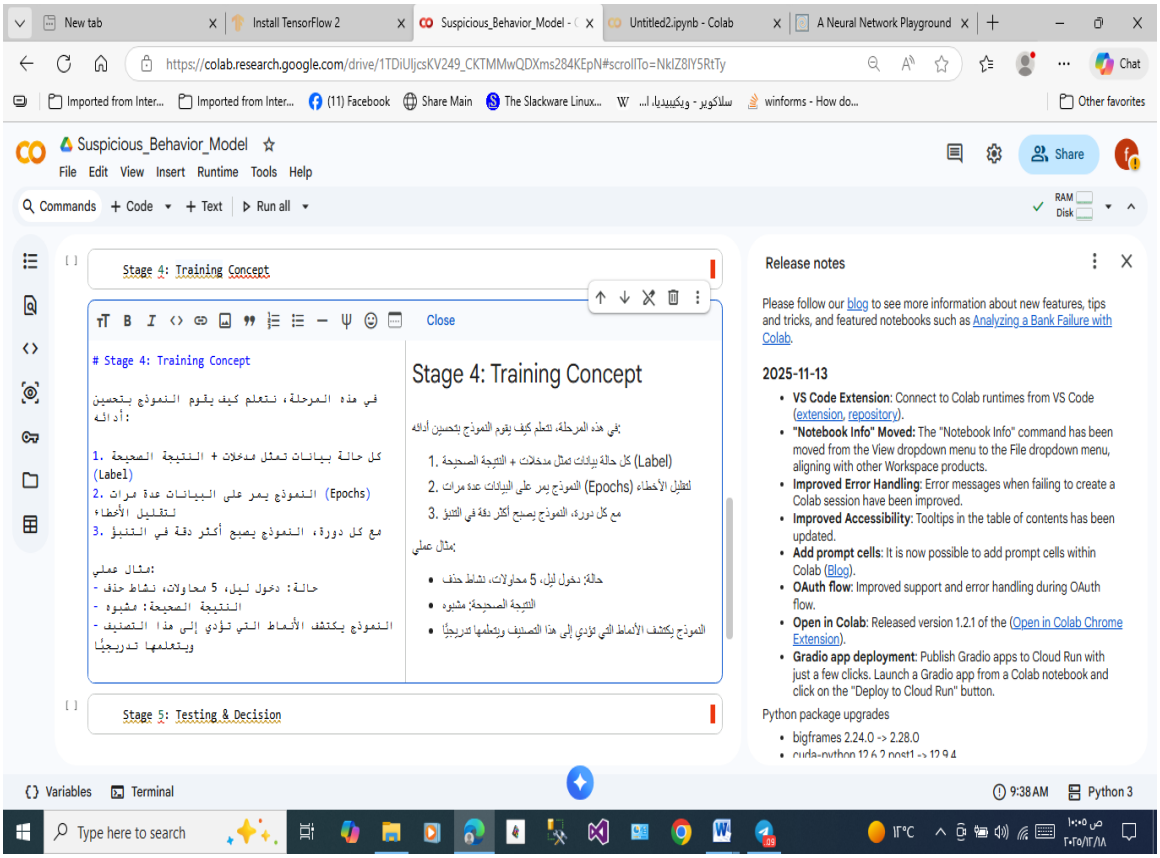
**ملاحظة:-**

Label: التسمية الصحيحة للبيانات (مثل: طبيعي أو مشبوه).

Epoch: عدد مرات مرور النموذج على نفس البيانات للتعلّم وتحسين الدقة.

هذه المصطلحات عالمية، وستصادفكم في أي مادة ذكاء اصطناعي أو أمن سيبراني فيها تحليل سلوك أو سجلات،

لذلك نتعلمها هنا بشكل مبسط وعملي.




**الشكل (5 – 20)**

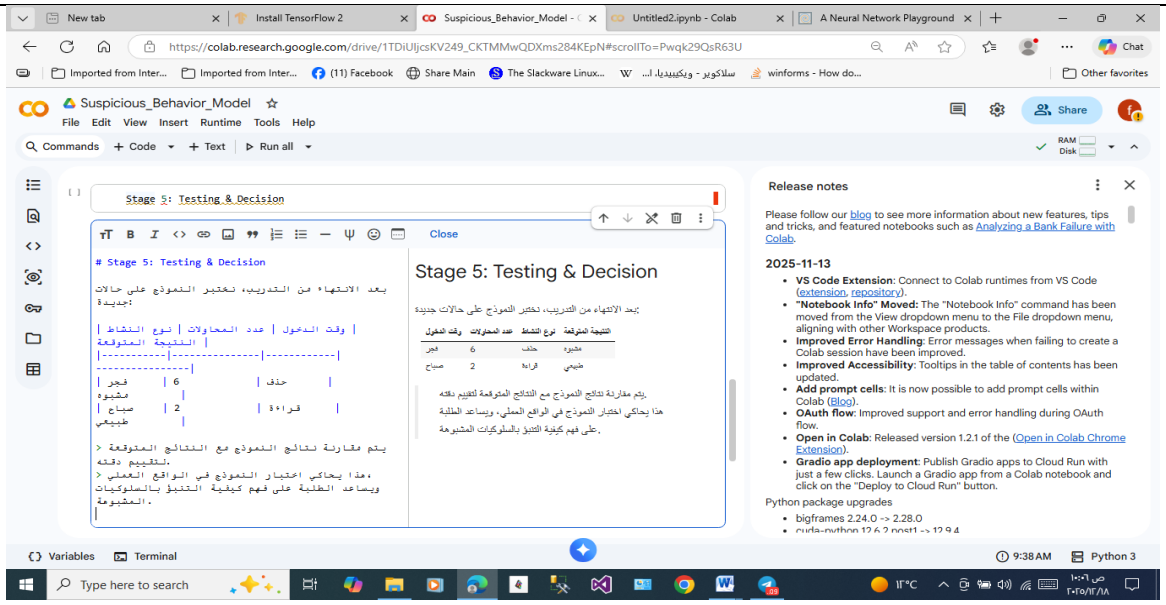
**الخلية 5: الاختبار واتخاذ القرار (Testing & Decision)**

نضغط المفتاح (Code) لاضافة (الخلية 5)، وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي لاختبار النموذج على بيانات جديدة لم يسبق له رؤيتها وهي بيانات الموجودة في الجدول رقم (5 – 2)، فيقوم النموذج بتحليل البيانات الجديدة ويعطي قرارا هل السلوك طبيعي ام مشبوه. وهذا يحاكي اختبار النموذج في الواقع العملي، ويساعد الطلبة على فهم كيفية التنبؤ بالسلوكيات المشبوهة. وكما موضح في الشكل (5 – 21):

وبالتالي نستطيع ان نقارن قرار النموذج بالنتيجة المتوقعة، لنعرف هل النموذج دقيق؟ وهل يمكن الاعتماد عليه لاكتشاف السلوك غير الطبيعي كما يحدث في التحقيقات الامنية الواقعية.

| النتيجة | نوع العملية | عدد المحاولات | وقت الدخول |
|---|---|---|---|
| مشبوه | حذف | 6 | فجرًا |
| طبيعي | قراءة | 2 | صباحًا |

**الجدول رقم (5 – 2)**




**الشكل (5 – 21)**

**الخلية 6: تجربة تفاعلية باستخدام (Interactive Playground Experience)**

نضغط المفتاح (Code) لاضافة (الخلية 6)، كما في الشكل (5 – 22). وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي لربط النموذج بالجانب التفاعلي البصري الذي سنشاهدة عبر الضغط على الرابط (https://playground.tensorflow.org)، والخاص باستخدام المقطع الوصفي عبر الاداة ( TensorFlow Playground)، وكما يلي :-

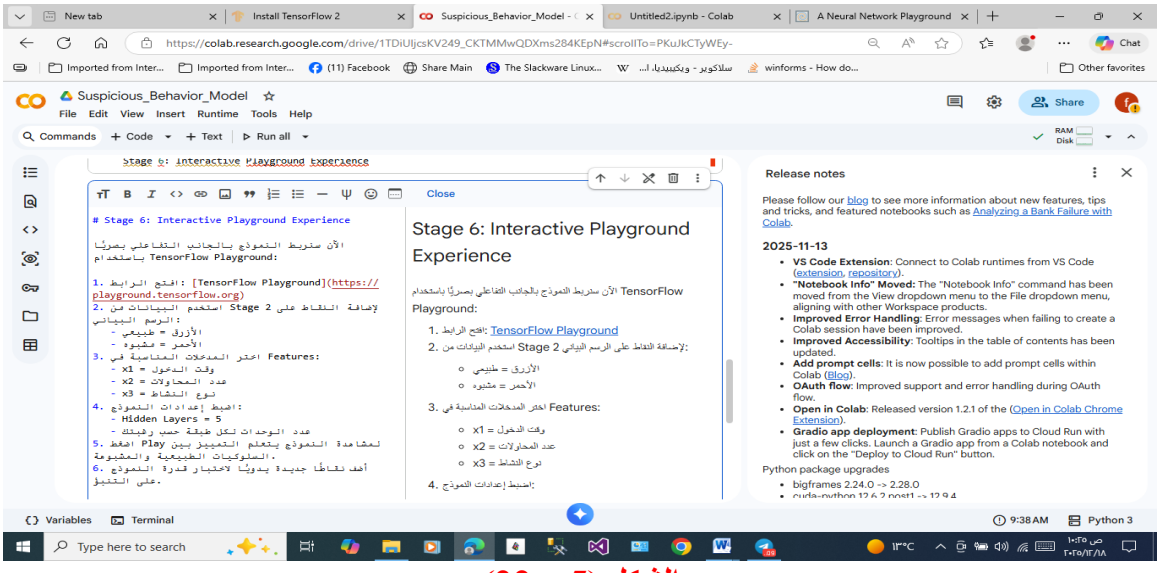
1- استخدم البيانات من (الخلية 2) لإضافة النقاط على الرسم البياني، (الأزرق = طبيعي) ، (الأحمر = مشبوه).

2- اختر المدخلات المناسبة في Features:

- x1 = وقت الدخول ، x2 = عدد المحاولات ، x3 = نوع النشاط.

3- اضبط إعدادات النموذج: (Hidden Layers = 5) عدد الوحدات لكل طبقة حسب رغبتك

4- اضغط (Play) لمشاهدة النموذج يتعلم التمييز بين السلوكيات الطبيعية والمشبوهة.

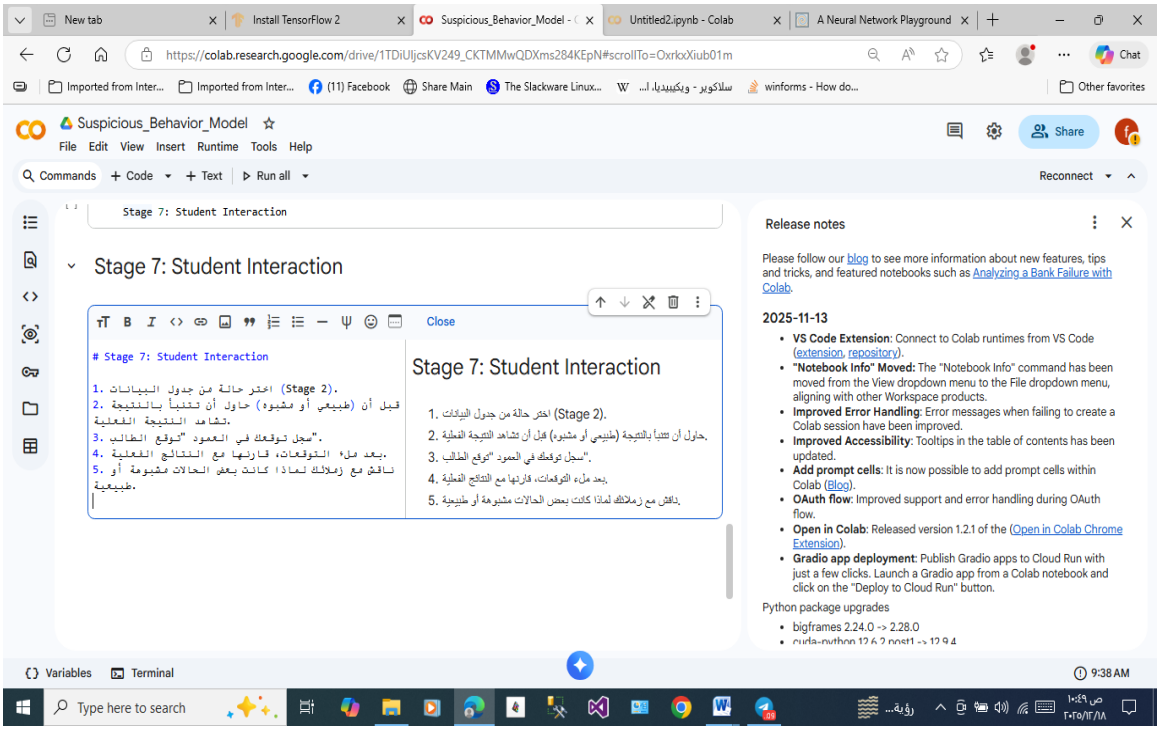



**الشكل (5 – 22)**

**الخلية 7: تفاعل الطلبة (Student Interaction)**

نضغط المفتاح (Code) لاضافة (الخلية 7)، كما في الشكل (5 – 23). وبعد اظافتها، نضغط المفتاح (Text)، ثم ندرج أي مقطع وصفي لتفاعل الطلبة وكما يلي:-

1. يقوم الطالب باختيار حالة من جدول البيانات (المرحلة 2).
2. يحاول الطالب أن يتنبأ بالنتيجة (طبيعي أو مشبوه) قبل أن يشاهد النتيجة الفعلية.
3. يقوم الطالب بتسجيل توقعه.
4. بعد ملء التوقعات في عمود النتيجة ، يقوم الطالب بمقارنتها مع النتائج الفعلية.
5. تجري عملية المناقشة بين الطلاب لماذا كانت بعض الحالات مشبوهة أو طبيعية.



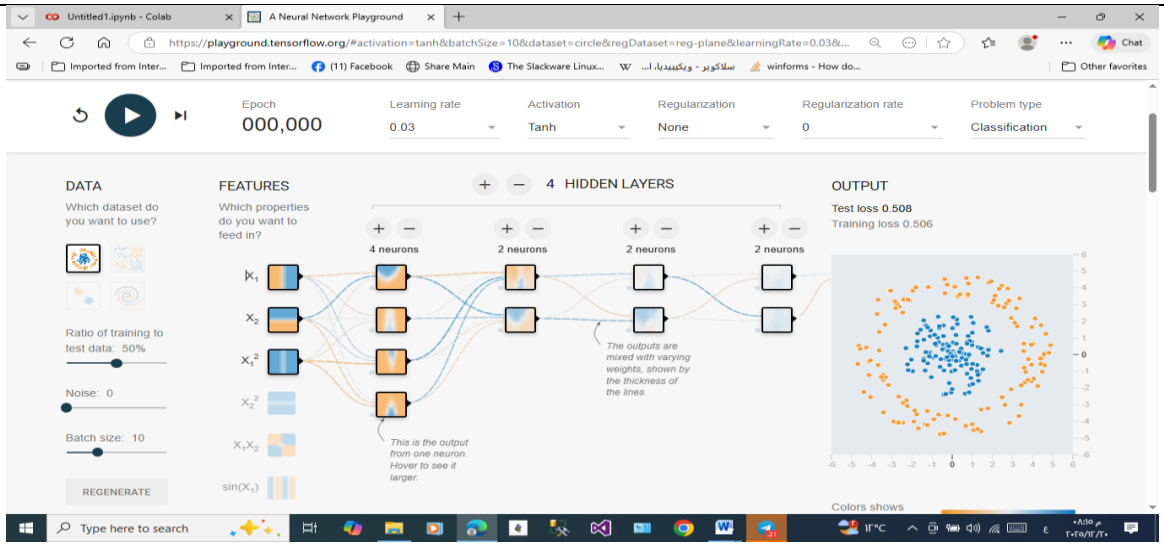

**الشكل (5 – 23)**

**الخطوة 6:** بعد الانتهاء من عملية ملء الخلايا يتم تشغيل النموذج من خلال الضغط على المفتاح (Run all).

ستلاحظ ان النموذج لا يعمل وهذا بسبب عدم كتابة الاكواد البرمجية التي هي فوق مستوى الطلبة في هذه المرحلة.

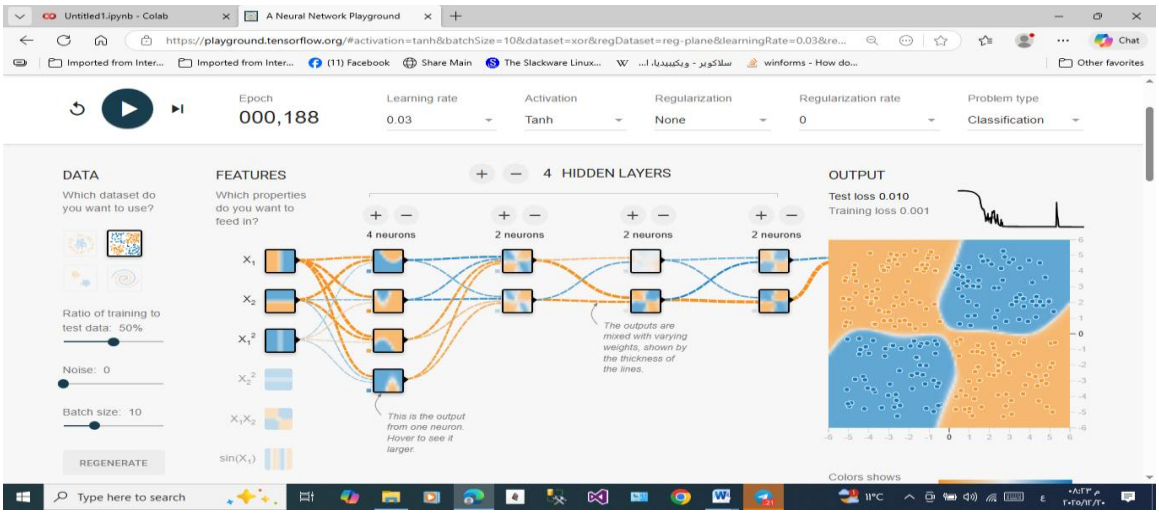
لذا سنلجاء الى استخدام الاداة (Tensorflow.playground) ، لاجراء عملية محاكاة لتوضيح ما يجري فعلا عند اختبار النموذج في (TENSOR FLOW). وذلك بالضغط على الرابط

(https://playground.tensorflow.org)، الذي تمت الاشارة الية عند تكوين (الخلية 6). وبعد الضغط على الرابط تظهر واجهة الاداة (Tensorflow.playground) كما في الشكل (5 – 24).




**الشكل (5 – 24)**

**الخطوة 7:** نضغط على مفتاح التشغيل (Run). وعند التشغيل سيظهر تحليل البيانات الطبيعية باللون الازرق والبيانات المشبوهة باللون الاحمر، وكما هو واضح في الشكل (5 – 25).




**الشكل (5 – 25)**

**ملاحظة مهمة :-** ان ما تقوم به هو ربط تعليمي (محاكاة) فقط، ونستطيع ان نقول ان (X1 يمثّل وقت الدخول) و (X2 يمثّل عدد المحاولات)، ونحن نستخدم المحاور كتمثيل بصري وليس كبيانات حقيقية. لان أداة (Playground) هي اداة عرض وفهم فقط، وليس نظام إدخال بيانات حقيقية.

**النتيجة المتوقعة**

الطالب يتعلم ويجرب نموذجًا عمليًا لتصنيف السلوكيات المشبوهة، ويشاهد النتائج مباشرة بصريًا، مع القدرة على إدخال بيانات جديدة لاختبار النموذج، وفهم كيفية تأثير كل مدخل على القرار النهائي، دون الحاجة لكتابة كود برمجي.

**المناقشة:**

1. كيف يتعلّم النموذج التمييز بين السلوك الطبيعي والمشبوه؟
2. ما دور البيانات (وقت الدخول، عدد المحاولات، نوع النشاط) في قرار النموذج؟
3. لماذا نحتاج إلى بيانات تدريب وبيانات اختبار منفصلة؟
4. هل يمكن للنموذج أن يخطئ؟ وما أسباب الخطأ المحتملة؟
5. كيف يمكن استخدام هذا النوع من النماذج في الأمن السيبراني عمليًا؟

| استمارة الفحص<br>تمرين رقم 15 | | | | |
|---|---|---|---|---|
| الجهة الفاحصة: | | | | |
| اسم الطالب : | المرحلة الثالثة | التخصص : الامن السيبراني | | |
| اسم التمرين: استخدام أدوات مفتوحة المصدر مثل (TENSOR FLOW) لتدريب نموذج يتنبأ بسلوكيات مشبوهة | | | | |
| ت | الخطوات | الدرجة القياسية 50 % | درجة الاداء 50% | الملاحظات |
| 1 | ارتد بدلة العمل | 5% | | |
| 2 | تسجيل الدخول بحساب Google الى واجهة TENSOR FLOW | 5% | | |
| 3 | تسجيل الدخول الى (TENSOR FLOW) من خلال حساب (Gmail). ثم الدخول الى (Untitled.ipynb). | 5% | | |
| 4 | إنشاء نموذج تصنيف (Classification Model) بسيط يتنبأ بالسلوكيات المشبوهة، واعطائها الاسم المناسب | 10% | | |
| 5 | اضافة الخلايا (Stege) ، والكتابة فيها ثم شغل النموذج ، وسجل الملاحظات. | 5% | | |
| 6 | اجراء عملية محاكاة باستخدام الاداة (Tensorflow.playground) | 5% | | |
| 7 | التشغيل برنامج المحاكاة، وتسجيل الملاحظات عند تحليل البيانات (الطبيعية باللون الازرق والبيانات المشبوهة باللون الاحمر) | 5% | | |
| 8 | المناقشة | 5% | | |
| 9 | الزمن المخصص | 5% | | |
| المجموع | | | | |
| اسم الفاحص | | التوقيع | | |

**رقم التمرين16** **الزمن المخصص: 3 ساعات**

**اسم التمرين: اجراء تدريبات عملية بأستخدام منصة محاكاة مثل ( CYBER DEFENDER) .**

**مكان التنفيذ: مختبر الحاسوب**

اولاً: الأهداف التعليمية:

تمكين الطلبة من تطبيق مفاهيم الأمن السيبراني عمليًا داخل بيئة محاكاة آمنة، لفهم كيفية اكتشاف وتحليل الهجمات والسلوكيات المشبوهة دون التأثير على أنظمة حقيقية.

ومن الجدير بالذكر ان ننوه الى ان هنالك بعض المعايير التي تم اعتمادها في تنفيذ هذا التمرين وكان من الواجب الاشارة اليها قبل البدء بالتمرين:

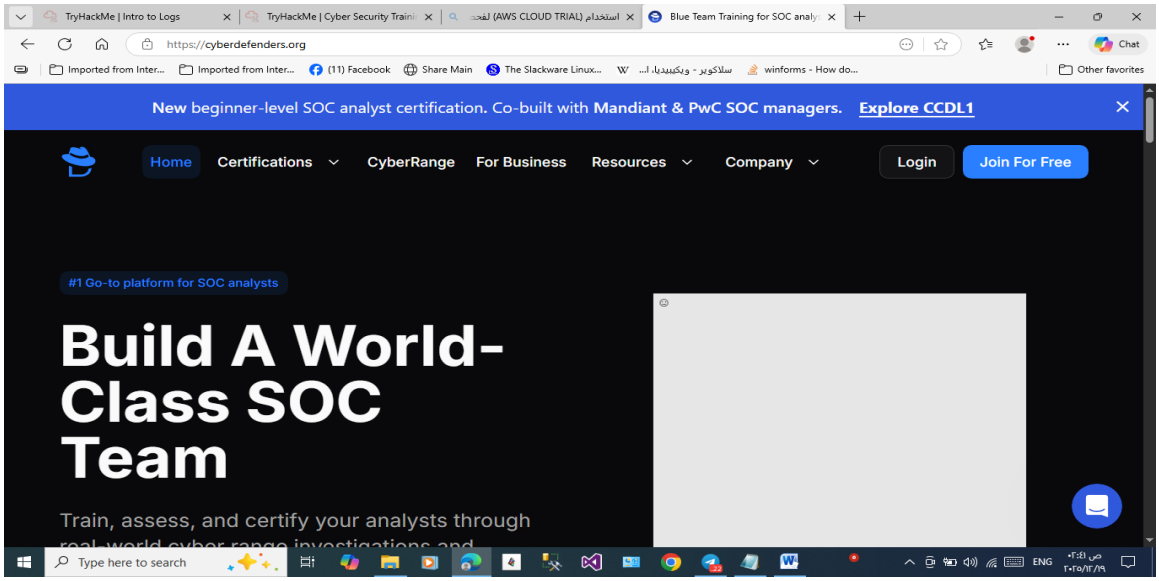
1. تم الالتزام باستخدام الحسابات المجانية فقط لذا تم استبدل المنصة (Cyber Range) بالمنصة (Cyber Defenders) والتي تؤدي نفس الغرض, والمناسبة فعلاً لعنوان التمرين.
2. الأداة المختارة هي CyberDefenders – Free Labs , لانها تعتبر مختبرات تحليل سجلات وتحقيق رقمي (قريبة جدًا من CloudTrail) , والقسم (Free Labs) مجاني, ولا تحتاج كتابة أكواد, وتركّز على التفكير والتحليل.
3. عدم إدخال أي بيانات شخصية حقيقية
4. تنفيذ التمرين داخل المنصة المخصصة دون الخروج عنها
5. التركيز على فهم الفكرة وليس سرعة الإنجاز

ثانياً: التسهيلات العلمية:

المتطلبات الاساسية:

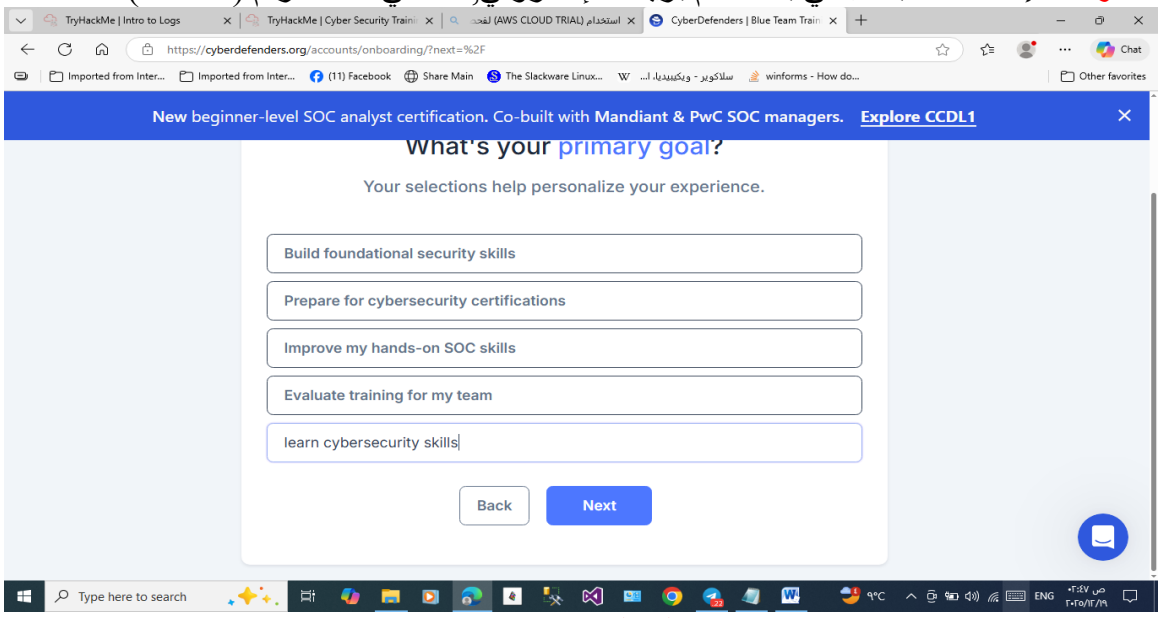
- جهاز حاسوب منصب علية نظام التشغيل (Windows 11) ومتصل بالانترنت، متصفح ويب حديث.
- حساب مجاني على منصة Cyber Defenders.
- معرفة أساسية بمفاهيم الأمن السيبراني.

**الخطوة 1:** ارتد بدلة العمل ثم قم بتشغيل الحاسوب والدخول إلى منصة (Cyber Defenders), ثم اضغط على (Join for free) كما في الشكل رقم (5–24) عبر الرابط (https://cyberdefenders.org) .




**الشكل (5 – 24)**

**الخطوة 2:** إنشاء حساب مجاني باستخدام بريدك الإلكتروني, كما في الشكل رقم (5 – 25):



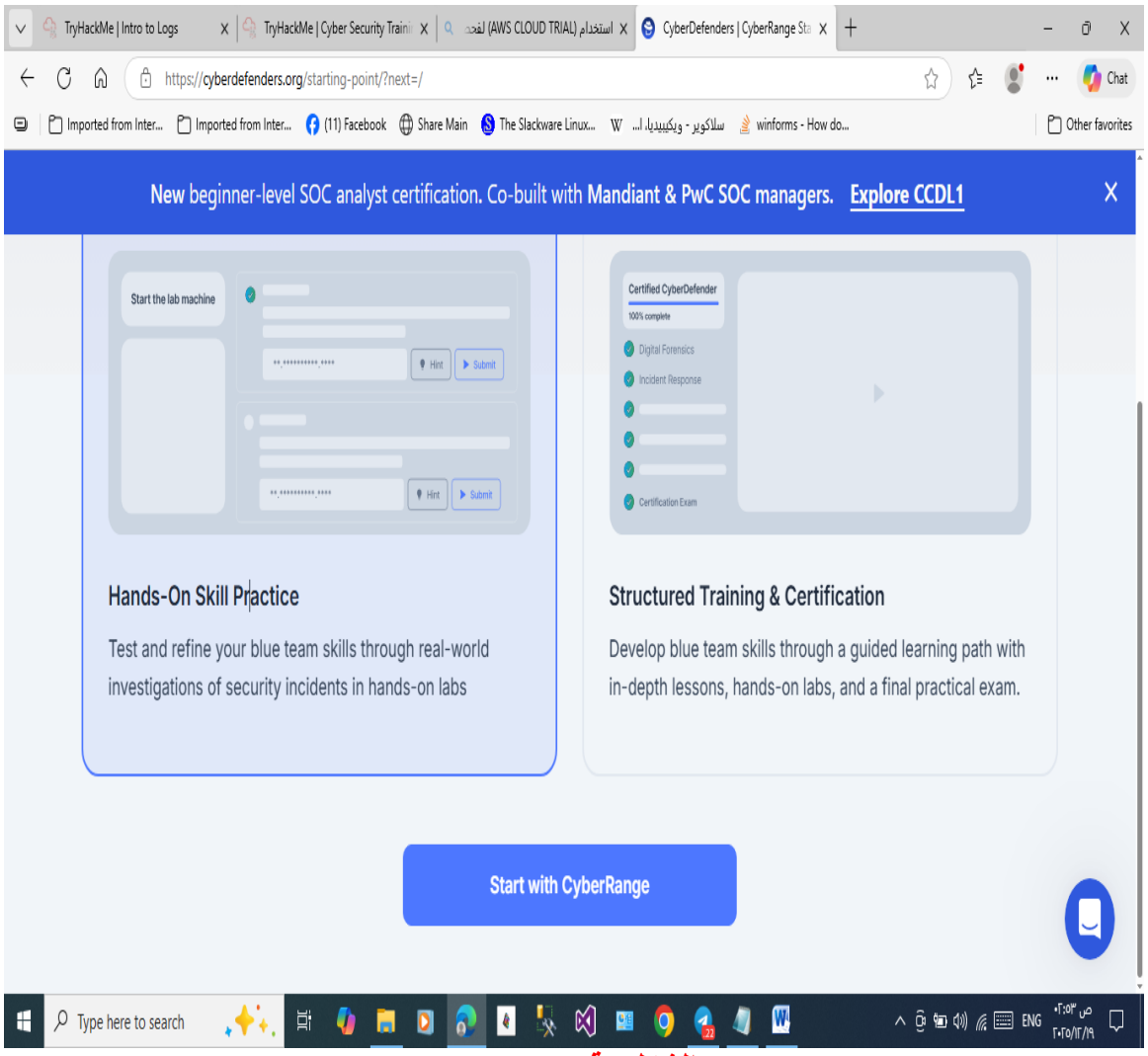

**الشكل (5 – 25)**

**الخطوة 3:** في هذه الخطوة سيتم التعامل مع مجموعة من الصفحات ذات العناوين المختلفة, التي هي تضع محددات وصفية لطبية النشاط المراد القيام به في المنصة, وكما يلي:-

- في الصفحة ذات العنوان (Which best describes you?), نختار الوصف الأقرب لك، مثلاً (Student / Learner), ثم اضغط Next أو Continue للمتابعة.
- في الصفحة ذات العنوان (What is your primary goal), نختار الخيار الأقرب لهدفك

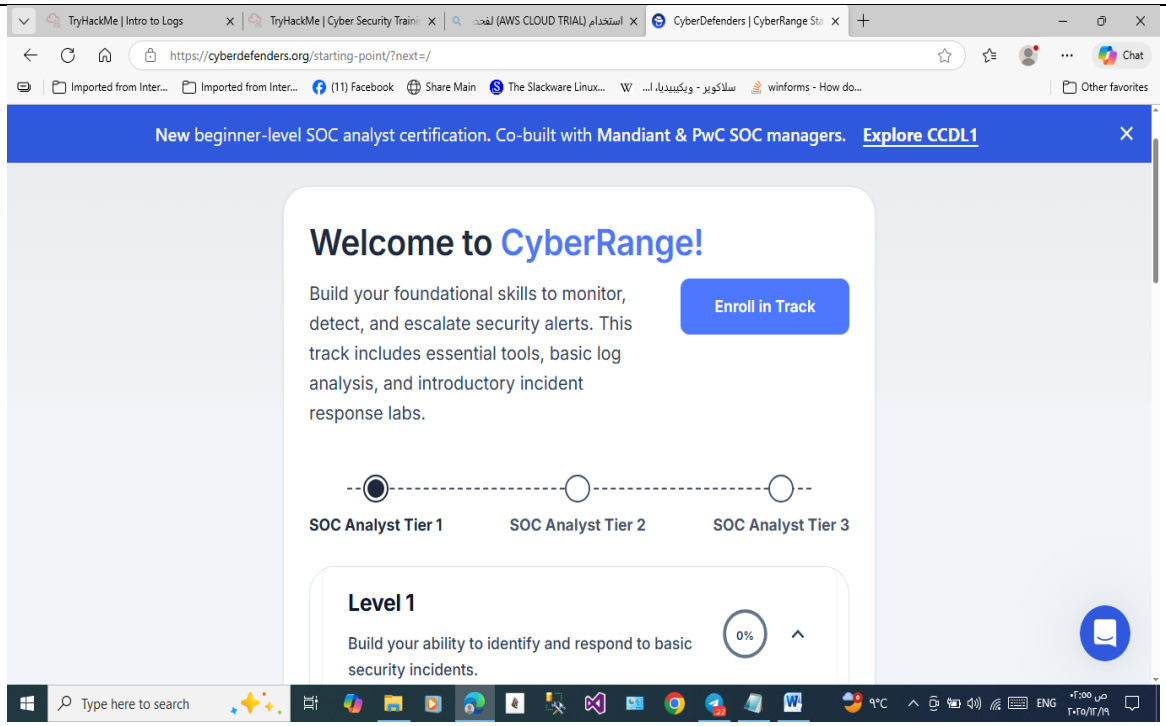
التعليمي، مثلاً (Learn Cybersecurity Skills), ثم اضغط Next أو Continue للمتابعة.

- في الصفحة ذات العنوان (How did you hear about cyber defenders?), يتم اختيار أي خيار مناسب أو حتى (Other) إذا لم يكن الخيار موجود، ثم اضغط Next أو Continue للمتابعة. تظهر الصفحة ذات العنوان (Chooses your starting point), وفيها اختياران. سوف نختار (Start the lab machine), ثم نضغط (Start with Cyber Range) كما في الشكل رقم (5 – 26):



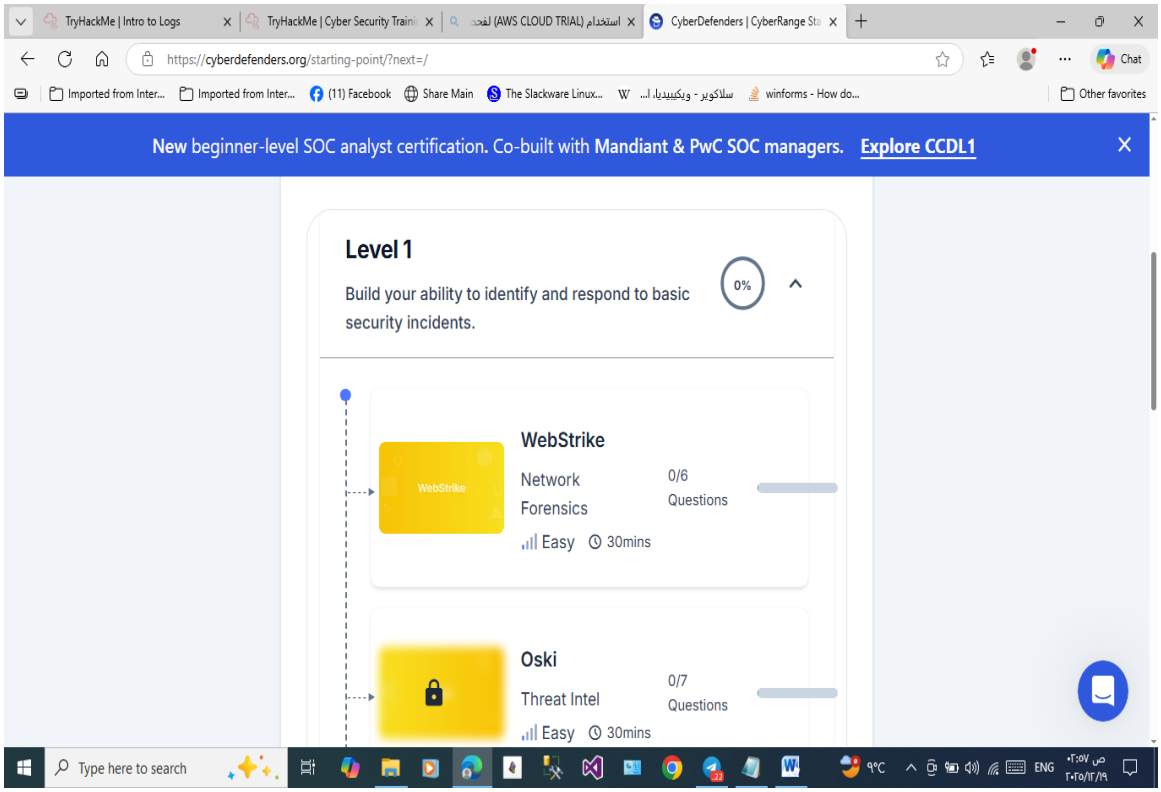

**الشكل رقم (5 – 26)**

**الخطوة 4:** في الصفحة ذات العنوان (Welcome to cyberrange), اختار ( Hands on skill practice), الآن وصلت إلى البيئة الأساسية للتمارين العملية (Cyber Range). اضغط على (1 Level) لبدء أول تمرين عملي داخل (Cyber Range) مباشرة دون الحاجة لأي شهادة أو مسار طويل، كما في الشكل رقم (5 – 27).



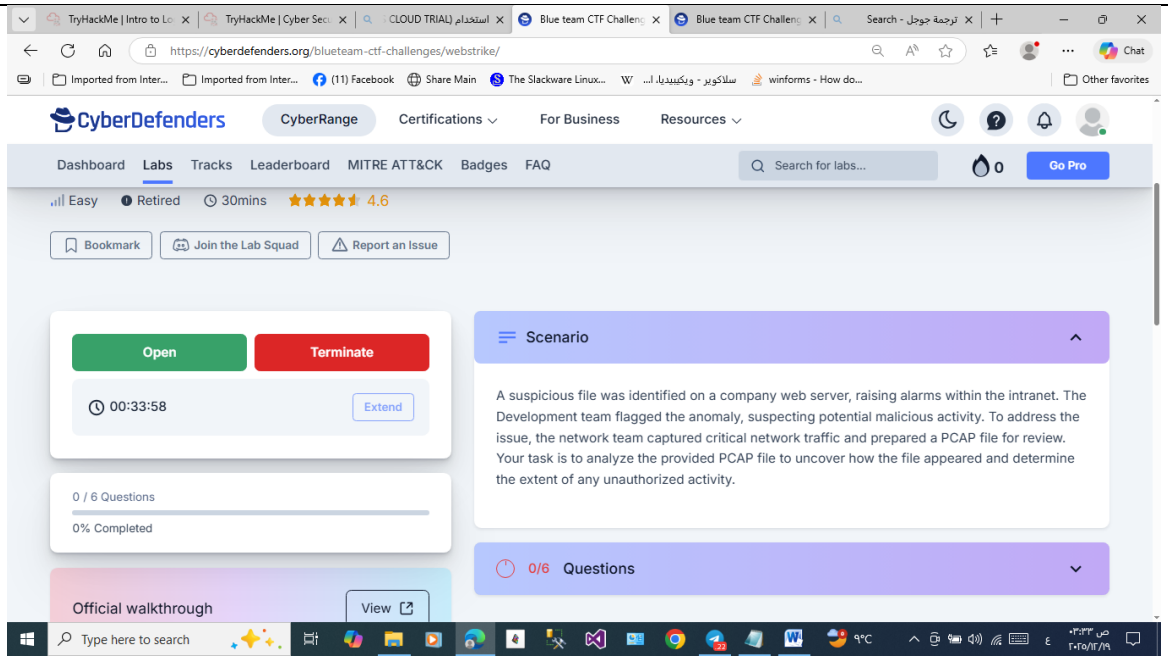

**الشكل (5 – 27)**

**الخطوة 5:** في هذه الصفحة يتم اختيارَ (Webstrike) وهومناسب ويركّز على تحليل سجلات وسلوك مشبوه، كما في الشكل رقم (5 – 28):



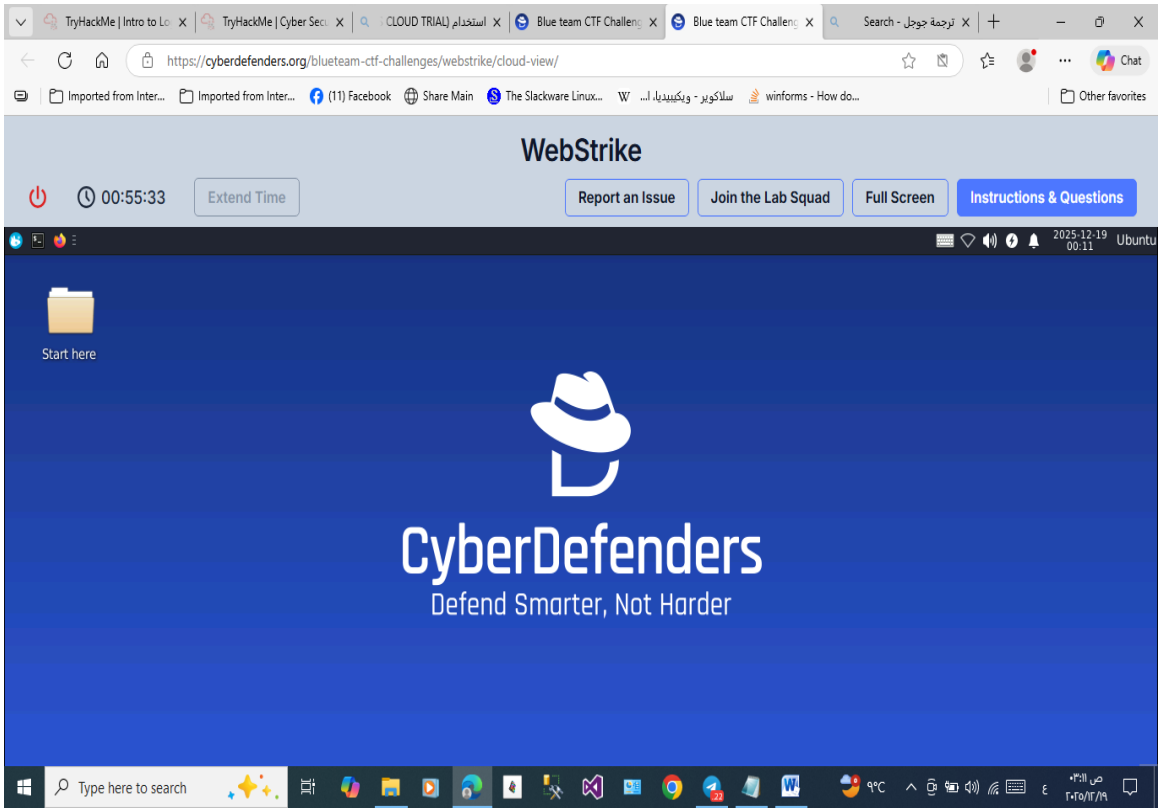

**الشكل (5 – 28)**

**الخطوة 6:** في هذه الصفحة (Webstrike lab) وهومناسب ويركّز على تحليل سجلات وسلوك مشبوه، كما في الشكل رقم (5 – 29). ثم نضغط على (Open).



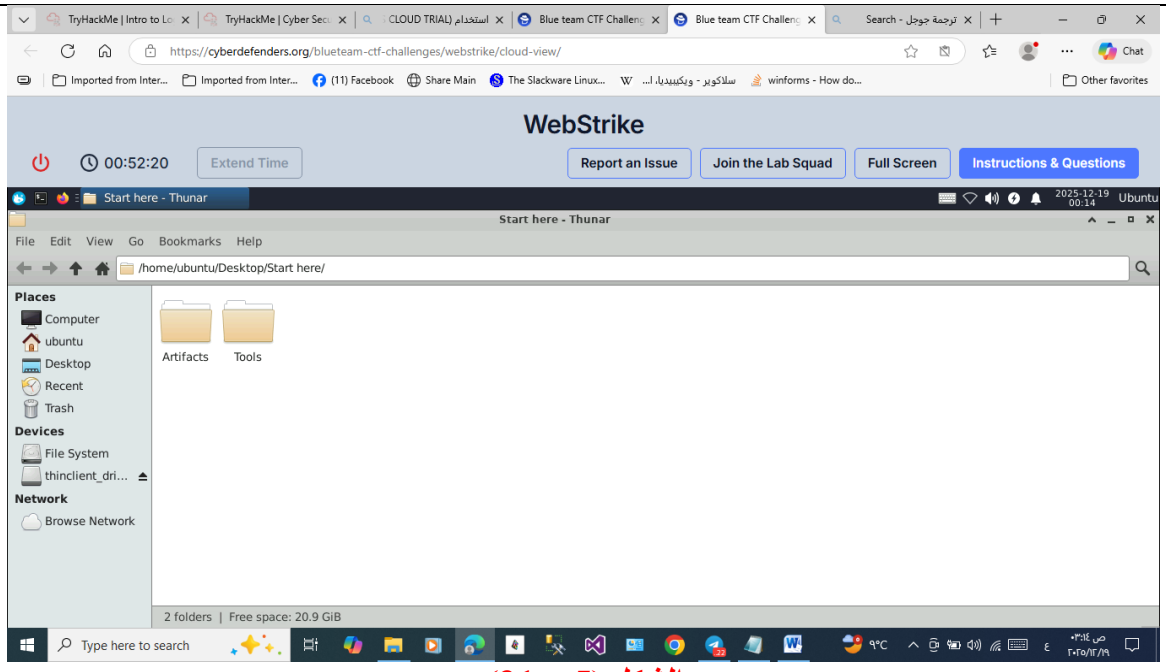

**الشكل (5 – 29)**

**الخطوة 6:** في الصفحة (Cyber defender)، يظهر الفولدر(Start here), كما في الشكل رقم (5 – 30):



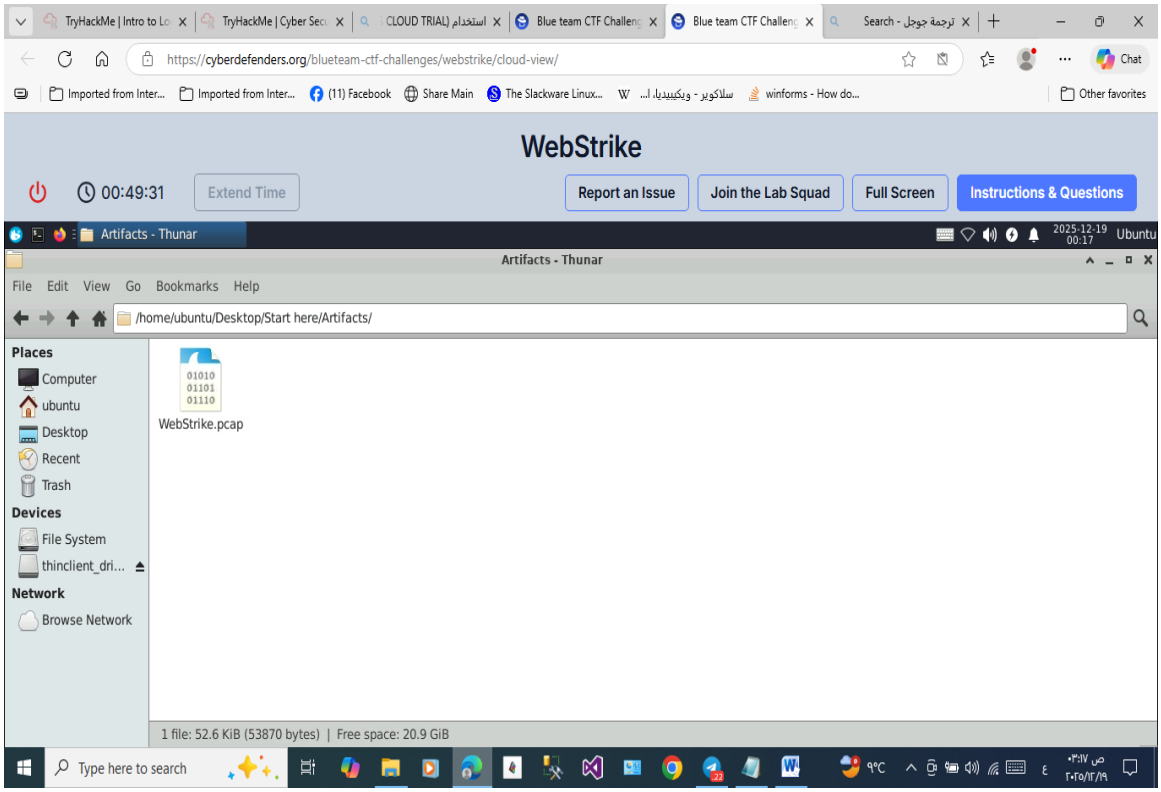

**الشكل (5 – 30)**

**الخطوة 7:** في الصفحة (Cyber defender), ننقر مرتين على الفولدر(Start here), فتظهر الشاشة (Web strike), وفيها الفولدرات عدد 2 , (Tools) و (Artifacts)، كما في الشكل رقم (5 – 31).



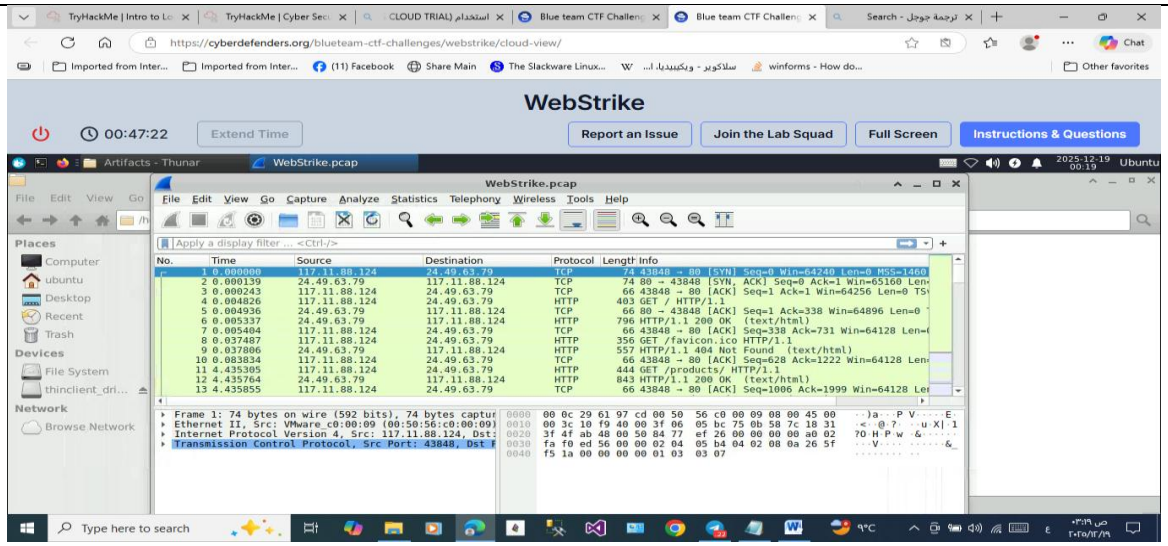

**الشكل (5 – 31)**

**الخطوة 8:** في الصفحة (Web strike)، ننقر مرتين على الفولدر (Artifacts)، فيظهر الملف (Webstrike.pcap) كما في الشكل رقم (5 – 32):




**الشكل (5 – 32)**

**الخطوة 9:** ننقر مرتين على ملف (Webstrike.pcap) لفتحه أو تنزيله حسب الخيارات المتاحة. هذا الملف يحتوي على سجلات الشبكة أو النشاط الأمني الذي ستقوم بتحليله في التمرين كما في الشكل رقم (5 – 33):




**الشكل (5 – 33)**

**الخطوة 9:** في هذه الفقرة سنركّز على فهم فكرة التحقيق وليس عمل الأداة, حيث نقوم بعملية تحليل البيانات التي تساعد على فهم بيئة التحقيق الأمني وطريقة التعامل مع الأدلة الرقمية. ومن الجدير بالذكر ان ملف (Webstrike.pcap) يحتوى على سجل نشاط شبكة (Network Log) التي تستخدم لرصد واكتشاف نشاط الويب المشبوه. وأن كل ملف أو(Artifact) في المختبر يمثل دليلاً لتحليل النشاط الأمني, ويتم التحليل باستخدام مجموعة من الادوات (Tools), كما يلي :

**عمود النشاط (Source):** ويقصد به عنوان الجهاز الذي بدأ الاتصال واقعيًا, إذا تكرر نفس الـ(Source) كثيرًا, فهذا يعني ان هذه الجهة هي نفسها التي تقوم بالنشاط, و بذلك يكون عنوان جهاز المستخدم هو عنوان جهاز المهاجم.

**عمود الوقت (Time) :** ويقصد به وقت حدوث كل اتصال واقعيًا, فالنشاط في وقت غير اعتيادي (ليلًا، خارج الدوام) قد يكون مشبوهًا.

**عمود البروتكول (Protocols):** ويقصد به نوع البروتوكول المستخدم واقعيا, اذا كانت من نوع (HTTP / HTTPS) فهو طبيعي غالبًا, اما اذا كانت بروتوكولات غريبة أو غير متوقعة فهذا مؤشر خطر.

**عمود الطول (Length):** ويقصد به طول الطلب المستخدم واقعيا, فاذا كانت الطلبات صغيرة ومتكررة جدًا فيكون احتمال فحص أو هجوم, اما اذا كانت الطلبات ذات أحجام غير طبيعية فهذا يعني تهريب بيانات.

**عمود المعلومات (Info):** وهو وصف مختصر لما حدث في كل اتصال, مثلا رسائل خطأ متكررة, تعني النظام يحاول الوصول لشئ ولا ينجح , وهذا يدل على فحص او محاولة اختراق. او طلبات غير معتادة للمستخدم العادي مثل طلب ملفات ادارية او صفحات حساسة, وهذا يعني نشاط مشبوه, او محاولات وصول متعددة في وقت قصير (خلال ثواني), وهذا يعني هجوم تخمين كلمات المرور.

**النتيجة المتوقعة**

الطالب يتعلم تحليل سجلات الشبكة الملتقطة مسبقًا (Log/PCAP Analysis) لفهم من قام بالنشاط، متى حدث، وهل هو طبيعي أم مشبوه. العملية تحاكي التحقيق الأمني الواقعي، حيث يتم تشخيص النشاط بربط عدة أعمدة معًا مثل المصدر، الوقت، نوع الاتصال وحجمه، وليس الاعتماد على حقل واحد فقط.

**المناقشة:**

1. ما الفرق بين التدريب داخل Cyber Range والعمل على نظام حقيقي؟

2. أي حقل في ملف الـ PCAP كان أكثر دلالة على السلوك المشبوه؟ ولماذا؟
3. كيف يساعد تكرار نفس الـ Source في كشف المهاجم؟
4. لماذا لا يكفي الاعتماد على حقل واحد (مثل الوقت أو البروتوكول) لاتخاذ قرار أمني؟
5. كيف تحاكي هذه المختبرات دور المحقق الجنائي الرقمي في الواقع؟

| استمارة الفحص<br>تمرين رقم 16 | | | | |
|---|---|---|---|---|
| **الجهة الفاحصة:** | | | | |
| **اسم الطالب :** | **المرحلة الثالثة** | **التخصص : الامن السيبراني** | | |
| **اسم التمرين : اجراء ندريبات عملية بأستخدام منصة محاكاة مثل (CYBER DEFENDERS)** | | | | |
| **ت** | **الخطوات** | **الدرجة القياسية % 50** | **درجة الاداء %50** | **الملاحظات** |
| **1** | **ارتداء بدلة العمل** | **%5** | | |
| **2** | **الدخول وإنشاء حساب مجاني على منصة (Cyber Defenders)** | **%5** | | |
| **3** | **التعامل مع الصفحات ذات العناوين المختلفة, لوضع محددات وصفية لطبية النشاط المراد القيام به في المنصة .** | **%5** | | |
| **4** | **الوصول إلى البيئة الأساسية للتمارين العملية, لبدء أول تمرين عملي داخل (Cyber Range) مباشرة.** | **%5** | | |
| **5** | **اختيار (Webstrike lab) لتحليل السجلات وسلوكيات المشبوه.** | **%5** | | |
| **6** | الوصول الى صفحة (Cyber defender), والتعامل مع الفولدر والملفات الموجودة فيها. | **%5** | | |
| **7** | تشغيل الملف (Webstrike.pcap) وتسجيل الملاحظات | **%5** | | |
| **8** | **المناقشة** | **%10** | | |
| **9** | **الزمن المخصص** | **%5** | | |
| **المجموع** | | | | |
| **اسم الفاحص** | | **التوقيع** | | |

## اسئلة الفصل الخامس

**س1: عرف ما يلي:-**

**إنترنت الأشياء IoT، التحقيق الجنائي الرقمي ، طبقة التحقيق الجنائي للشبكة ، التعلم الآلي ،التنبؤ بالجريمة ، الخوارزمية**

**س2: عدد خصائص التحقيق الجنائي السحابي.**

**س3: عدد اهم اهداف التحقيق الجنائي السحابي.**

**س4: عدد مع الشرح مراحل التحقيق الجنائي السحابي.**

**س5: عدد التحديات التي تواجه التحقيق الجنائي السحابي.**

**س6: عدد الأدوات والتقنيات المستخدمة في التحقيق الجنائي السحابي.**

**س7: ما هي اهم التحديات الأمنية في التحقيقات الجنائية الرقمية؟**

**س8: ارسم المخطط التسلسلي لمراحل التحقيق الجنائي الرقمي لأجهزة إنترنت الأشياء**

**س9: عدد وبشكل متسلسل مراحل التحقيق الجنائي الرقمي لأجهزة إنترنت الأشياء**

**س10: عدد مكونات بنية إنترنت الأشياء ذات الصلة بالتحقيق**

**س11: ما هي طبقات التحقيق الجنائي لإنترنت الأشياء؟**

**س12: وضح التحديات التي تواجه التحقيق الجنائي في إنترنت الأشياء**

**س13: وضح أهمية الذكاء الاصطناعي في التحقيقات الجنائية الرقمية**

**س14: عدد اهم التحديات التي تواجه استخدام الذكاء الاصطناعي في التحقيقات الجنائية الرقمية.**

**س15: عدد مع شرح موجز للعناصر أساسية لأجزاء التعليم الآلي.**

**س16: ما هي اهم المجالات التي يمكن ان يستخدم فيها التعلم الآلي في التحقيقات الجنائية؟**

**س17: ما هي فوائد التعلم الآلي في التحقيق الجنائي؟**

**س18: ما هي اهدف عملية تحسين الأمن السيبراني في التحقيق الجنائي الرقمي ؟**

**س19: هي ابرز الاتجاهات المستقبلية في التحقيق الجنائي الرقمي؟**

**س20: عدد اهم التوصيات الخاصة للاستعداد المستقبلية في مجال التحقيق الجنائي الرقمي.**

## الفهرست


| الموضوع | الصفحة |
|---|---|
| المقدمة | 3 |
| الفصل الأول: اساسيات التحقيق الجنائي الرقمي | 4 |
| 1-1 تعريف التحقيق الجنائي الرقمي | 4 |
| 2-1 تاريخ التحقيق الرقمي وتطوره | 4 |
| 1-2-1 المرحلة التمهيدية | 5 |
| 2-2-1 مرحلة التأسيس المبكر | 5 |
| 3-2-1 مرحلة النمو والتوسع | 5 |
| 4-2-1 مرحلة التطور | 6 |
| 3-1 اهمية التحقيق الجنائي في مكافحة الجرائم الالكترونية | 6 |
| 4-1 المبأدى الاساسية للتحقيق الجنائي الرقمي | 7 |
| 1-4-1 فروع التحقيق الجنائي الرقمي | 8 |
| 2-4-1 مصادر الادلة الرقمية | 9 |
| 3-4-1 الاجراءات القياسية للتحقيق الجنائي الرقمي | 11 |
| 5-1 التحديات القانونية والاخلاقية في التحقيقات الرقمية | 11 |
| تمرين رقم 1: فحص وتحليل عينات مشبوهة بأستخدام Visual Total | 13 |
| تمرين رقم 2: تهيئة أداة Autopsy وانشاء حالة تحقيق رقمية | 16 |
| اسئلة الفصل الاول | 22 |
| الفصل الثاني: ادوات وتقنيات التحقيق الجنائي الرقمي | 23 |
| 1-2 الادوات البرمجية للتحقيق الرقمي | 23 |
| تمرين رقم 3: استخدام الاداة Autopsy لتحليل بيانات الاجهزة | 26 |
| 2-2 استرجاع الملفات المحذوفة | 30 |
| تمرين رقم 4: استخدام FTK Imager لاسترجاع الملفات المحذوفة من القرص الصلب | 36 |
| 3-2 فحص سجلات النظام والتطبيقات | 40 |
| تمرين رقم 5: تحليل سجلات نظام التشغيل وسجلات التطبيقات لتحديد النشاطات المشبوهة | 44 |
| 4-2 البرمجيات الضارة | 47 |
| 5-2 مقارنة بين ادوات التحقيق الجنائي الرقمي التجارية والمفتوحة المصدر | 49 |
| تمرين رقم 6: مقارنة بين ادوات التحقيق الجنائي الرقمي التجارية والمفتوحة المصدر | 51 |

| | |
|---|---|
| اسئلة الفصل الثاني | 54 |
| الفصل الثالث: إجراءات جمع الأدلة الرقمية وتحليلها | 55 |
| المقدمة | 55 |
| 3-1 خطوات جمع الادلة الرقمية بطريقة صحيحة | 55 |
| 3-2 تقنيات الحفاظ على سلامة الأدلة الرقمية | 59 |
| تمرين رقم 7: استخدام برنامج FTK Imager لانشاء نسخة طبق الاصل | 60 |
| 3-2-1 استخدام قيم التجزئة للتحقق من سلامة الدليل | 65 |
| تمرين رقم 8: فحص سلامة الأدلة الرقمية بأستخدام HashCalc | 65 |
| 3-2-2 استخدام ادوات منع الكتابة | 67 |
| 3-2-2-1 انواع ادوات منع الكتابة | 67 |
| تمرين رقم 9: استخدام ادوات منع الكتابة اثناء استخدام الادلة | 67 |
| 3-2-3 التخزين الامن للادلة الرقمية | 71 |
| 3-2-3-1 اهداف التخزين الامن | 71 |
| 3-2-3-2 انواع التخزين الامن | 71 |
| 3-2-3-3 إجراءات التخزين الامن | 71 |
| 3-3 تحليل الادلة المستخرجة من الحواسيب واجهزة الهاتف | 71 |
| 3-3-1 تحليل الادلة المستخرجة من الحواسيب | 72 |
| 3-3-2 تحليل الأدلة المستخرجة من الهواتف الذكية | 73 |
| 3-4 تحليل الشبكات وتحديد مصادر الهجمات | 73 |
| 3-4-1 اهداف تحليل الشبكات في التحقيق الجنائي الرقمي | 74 |
| 3-4-2 مصادر الادلة الشبكية | 74 |
| 3-4-3 مفاهيم اساسية | 75 |
| 3-4-4 خطوات تحليل الشبكات وتحديد مصدر الهجوم | 75 |
| 3-4-5 مؤشرات الهجكمات الشبكية | 76 |
| 3-4-6 انواع الهجمات التي يمكن اكتشافها عبر تحليل الشبكات | 77 |
| 3-4-7 ادوات تحليل الشبكات | 78 |
| تمرين رقم 10: تحليل حركة البيانات عبر الشبكة بأستخدام Wireshark | 79 |
| 3-5 توثيق الادلة الرقمية واعداد التقارير النهائية | 82 |
| 3-5-1 اهمية توثيق الادلة الرقمية | 82 |

| | |
|---|---|
| 2-5-3 مراحل توثيق الادلة الرقمية | 82 |
| 3-5-3 اعداد التقارير النهائية في التحقيق الجنائي الرقمي | 82 |
| 4-5-3 الادوات المستخدمة في التوثيق واعداد التقارير | 83 |
| تمرين رقم 11: توثيق مراحل التحقيق الجنائي الرقمي | 83 |
| اسئلة الفصل الثالث | 87 |
| الفصل الرابع: أنواع الجرائم الالكترونية ودور التحقيق الجنائي الرقمي | 88 |
| مقدمة | 88 |
| 1-4 الجرائم المالية وغسيل الاموال الالكتروني | 88 |
| 1-1-4 اشكال الجرائم المالية الالكترونية | 90 |
| 2-1-4 غسيل الاموال الالكتروني: الغسالة الرقمية | 92 |
| 3-1-4 دور المحقق الجنائي الرقمي | 93 |
| 2-4 الاحتيال الالكتروني والاحتيال على الهوية | 94 |
| 1-2-4 اساليب الاحتيال الالكتروني | 94 |
| 2-2-4 الاحتيال على الهوية | 95 |
| 3-2-4 دور المحقق الجنائي الرقمي | 96 |
| 3-4 برامج الفدية Ransomware | 97 |
| 1-3-4 ما هي برامج الفدية وكيف تعمل؟ | 98 |
| 2-3-4 طرق الانتشار وتطور الهجمات | 98 |
| 3-3-4 دور المحقق الجنائي الرقمي | 99 |
| 4-4 الجريمة المنظمة عبر الانترنت | 99 |
| 1-4-4 هيكل وخصائص الجريمة المنظمة عبر الانترنت | 100 |
| 2-4-4 الجريمة كخدمة | 100 |
| 3-4-4 الشبكة المظلمة | 100 |
| 4-4-4 دور المحقق الجنائي | 101 |
| 5-4 قضايا الجرائم الاخلاقية والخصوصية الرقمية | 102 |
| 1-5-4 أنواع الجرائم الاخلاقية | 102 |
| 2-5-4 الخصوصية الرقمية وبصمتك الرقمية | 103 |
| 3-5-4 دور المحقق الجنائي الرقمي | 104 |
| تمرين رقم 12: فحص البرمجيات الخبيثة بأستخدام Malwarebytes | 105 |

| | |
|---|---|
| تمرين رقم 13: تحليل هجوم تصيد الكتروني بأستخدام أداة تحليل ترويسة البريد الالكتروني | 108 |
| اسئلة الفصل الرابع | 111 |
| الفصل الخامس: التوجهات المستقبلية في التحقيق الجنائي الرقمي | 112 |
| 1-5 التحقيق الجنائي السحابي وانترنت الاشياء | 112 |
| 1-1-5 مفهوم التحقيق الجنائي السحابي | 112 |
| 2-1-5 مفهوم انترنت الاشياء TOT | 114 |
| 3-1-5 التحقيق الجنائي الرقمي | 114 |
| 4-1-5 التحقيق الجنائي وانترنت الاشياء | 115 |
| 5-1-5 مكونات بنية انترنت الاشياء ذات الصلة بالتحقيق | 115 |
| 6-1-5 طبقات التحقيق الجنائي لانترنت الاشياء | 116 |
| 7-1-5 اهمية التحقيق الجنائي في انترنت الاشياء | 117 |
| 8-1-5 التحديات التي تواجه التحقيق الجنائي في انترنت الاشياء | 117 |
| 2-5 الذكاء الاصطناعي والتعليم الالي في التحقيق الجنائي الرقمي | 117 |
| 1-2-5 دور الذكاء الاصطناعي في تطوير التحقيقات الجنائية الرقمية | 117 |
| 2-2-5 التحديات التي تواجه استخدام الذكاء الاصطناعي في التحقيقات الجنائية الرقمية | 118 |
| 3-2-5 التعلم الالي | 119 |
| 4-2-5 تطبيقات التعلم الالي في التحقيق الجنائي | 119 |
| 5-2-5 فوائد التعليم الالي في التحقيق الجنائي | 119 |
| 6-2-5 تحديات ومخاطر التعليم الالي في التحقيق الجنائي | 119 |
| 7-2-5 اخلاقيات التعلم الالي في التحقيق الجنائي | 120 |
| 3-5 تحسين الامن السيبراني في التحقيق الجنائي الرقمي | 120 |
| 1-3-5 مفهوم الامن السيبراني | 121 |
| 2-3-5 اهمية الامن السيبراني في التحقيق الجنائي الرقمي | 121 |
| 3-3-5 التهديدات السيبرانية التي تواجه التحقيقات الجنائية الرقمية | 121 |
| 4-3-5 استراتيجيات تحسين الامن السيبراني في التحقيق الجنائي الرقمي | 121 |
| 4-5 قوانين وتشريعات جديدة في الادلة الرقمية | 122 |
| 5-5 اتجاهات المستقبل والابتكارات في التحقيق الجنائي الرقمي | 123 |
| 1-5-5 التقنية الحديثة في ادوات التحقيق الرقمي | 123 |
| 2-5-5 التحديات المستقبلية للتحقيق الجنائي الرقمي | 124 |

| | |
|---|---|
| 3-5-5 المهارات المستقبلية للمحقق الجنائي الرقمي | 124 |
| 4-5-5 التوصيات والاسعداد للمستقبل | 125 |
| تمرين رقم 14: استخدام AWS Cloud Trial لفحص سجلات النشاط في السجلات السحابية | 125 |
| تمرين رقم 15: استخدام ادوات مفتوحة المصدر لتدريب نموذج يتنبأ بسلوكيات مشبوهة | 133 |
| تمرين رقم 16: اجراء تدريبات عملية بأستخدام منصة محاكاة مثل CYBER RANGE | 143 |
| اسئلة الفصل الخامس | 151 |
| الفهرس | 152 |

# تم بحمده تعالی