

الجرائم الرقمية

الهدف العام من المقرر

يهدف المقرر إلى تعريف الطلاب بالتكنولوجيا والأدوات المستخدمة في هذا المجال وتعزيز قدراتهم على التعامل مع التحديات الأمنية الرقمية. وبشكل عام، يهدف مقرر الجرائم الرقمية إلى تزويد الطلاب بالمعرفة والمهارات اللازمة للعمل في مجال الأمن السيبراني والتحقيق في الجرائم الإلكترونية في القطاعات الحكومية والخاصة.

الأهداف التفصيلية للمقرر : أن يكون المتدرب قادراً على ان:

- فهم الجرائم الرقمية ونوعياتها وتحليلها، وكيفية التعرف على الأدلة الرقمية وتحليلها.
- فهم التهديدات الرقمية وكيفية تحديدها وحماية الأنظمة والشبكات والبيانات منها.
- فهم كيفية التحقيق في الجرائم الرقمية وجمع الأدلة الرقمية وتحليلها، وكيفية التعامل مع الأدلة الرقمية في القضايا الجنائية. فهم القوانين واللوائح المتعلقة بالجرائم الرقمية وكيفية تطبيقها.
- فهم الأخلاقيات المهنية والتصرف الأخلاقي في مجال الجرائم الرقمية وكيفية التعامل معها.

مقدمة

في عصر التكنولوجيا الحديثة، أصبحت الجرائم الرقمية تشكل تحدياً كبيراً للمجتمعات والدول على حد سواء. إن انتشار استخدام الإنترنت والأجهزة الذكية جعل العالم أكثر اتصالاً، لكنه أوجد أيضاً بيئة خصبة لنشوء أنواع جديدة من الجرائم. تهدف دراسة الجرائم الرقمية إلى تسليط الضوء على مفهوم هذه الجرائم واستعراض أنواعها المختلفة، بالإضافة إلى تحليل شامل للتشريعات والقوانين التي تحكمها. يتم التركيز أيضاً على دور الجرائم الرقمية في مجال الأمن السيبراني، من خلال التعرف على التقنيات والأدوات المستخدمة في التحقيق الرقمي وأساليب حماية البيانات. من خلال دراسة قضايا واقعية، نسعى إلى تقديم فهم عميق وشامل لهذه الظاهرة المعقدة، وتزويد الطلاب بالمعرفة اللازمة لتعزيز الأمن السيبراني ومواجهة التحديات بفعالية وأخلاقية.

5.....الوحدة الاولى

6.....مقدمة في الجرائم الرقمية.

7.....مفهوم الجرائم الرقمية وأنواعه.

10.....كيفية تأثيرها على الأفراد والمؤسسات.

12.....التحديات التي يواجهها المحققون والمدعين العامين في مجال مكافحة الجرائم الرقمية.

14.....الوحدة الثانية

15.....التعرف على الجرائم الرقمية.

دراسة أنواع الجرائم الرقمية المختلفة، مثل الاحتيال عبر الإنترنت والتسلل إلى الأنظمة والتجسس والتزيف الإلكتروني والابتزاز الرقمي وغيرها. يتم تناول كل نوع من هذه الجرائم بشكل تفصيلي، وكيف يمكن التعامل معها ومكافحتها.

22.....الوحدة الثالثة

23.....التحقيق في الجرائم الرقمية.

24.....كيفية جمع الأدلة الرقمية وتحليلها وتقييمها.

25.....كيفية إجراء التحقيقات الرقمية وجمع الأدلة والتعامل معها.

27.....الأدوات والتقنيات المستخدمة في جمع الأدلة الرقمية وكيفية تحليلها.

28.....كيفية تطبيق الأساليب القانونية المختلفة في مكافحة الجرائم الرقمية.

37.....الوحدة الرابعة

38.....الأمن السيبراني.

يتضمن هذا الموضوع دراسة مفهوم الأمن السيبراني وأهميته في مواجهة الجرائم الرقمية، وكذلك دراسة التهديدات السيبرانية والاستراتيجيات اللازمة لمكافحة هذه التهديدات.

40.....الوحدة الخامسة

41.....الحماية الرقمية.

41	يتم تناول الأساليب اللازمة لحماية الأنظمة والبيانات والشبكات وتأمينها من الهجمات السيبرانية، وكذلك كيفية رصد ومكافحة التهديدات السيبرانية.
43	الوحدة السادسة
44	الجرائم المرتبطة بوسائل التواصل الاجتماعي.
44	كيفية التعامل مع الجرائم المرتبطة بوسائل التواصل الاجتماعي مثل التحرش الجنسي والتشهير والابتزاز الرقمي، وكيفية الحماية منها ومكافحتها.
44	أساليب الوقاية والتحقق والتعامل مع هذه الجرائم.
45	كيفية تحديد المسؤولية القانونية
47	الوحدة السابعة
48	السياسات والقوانين المتعلقة بالجرائم الرقمية.
48	دراسة السياسات والقوانين المتعلقة بالجرائم الرقمية وكيفية تطبيقها.
50	دراسة القضايا القانونية المرتبطة بالجرائم الرقمية، مثل التحقق من الهوية الرقمية وإنشاء الأدلة الرقمية والحفاظ على الخصوصية الإلكترونية.
52	القوانين المحلية والدولية المتعلقة بالجرائم الرقمية وكيفية تطبيقها في العمل القضائي.
56	الوحدة الثامنة
57	مراجعة شاملة لمادة الجرائم الرقمية



الوحدة الاولى

مقدمة في الجرائم الرقمية.

مفهوم الجرائم الرقمية وأنواعه.

كيفية تأثيرها على الأفراد والمؤسسات.

التحديات التي يواجهها المحققون والمدعين العامين في مجال مكافحة الجرائم الرقمية.



مقدمة في الجرائم الرقمية.

الجرائم الإلكترونية شبح يهدد عالمنا الرقمي المترابط في ظلّ ثورة التكنولوجيا وانتشار الإنترنت، باتت تُهددنا ظاهرة خطيرة تُسمى "الجرائم الإلكترونية". وتتنوع هذه الجرائم وتتطور باستمرار، مستغلةً ثغرات التكنولوجيا الحديثة لتنفيذ مخططات خبيثة تلحق الضرر المادي والمعنوي بالأفراد والمؤسسات على حدٍ سواء.

لم يتم وضع تعريف واضح من قبل المشرع لـ الجرائم الإلكترونية وما زال هناك اختلاف حول ماهيتها ولكن يمكن اعتبارها بأنها سلوكيات غير قانونية يقدم على ارتكابها فرد أو مجموعة من الأفراد بواسطة الأجهزة الذكية والمواقع الإلكترونية بهدف تحقيق مكاسب مختلفة، ويكون ذلك عن طريق ابتزاز الضحية وتهديدها وتخريب صورتها أمام المجتمع الواقعي والافتراضي، أما بحسب وجهة النظر المجتمع الدولي فقد اعتبر الجريمة الإلكترونية بأنها ممارسات وأعمال تتعلق بجهاز الحاسوب تسعى لتحقيق مكاسب مادية أو شخصية أو التسبب بضرر.

يُعد سهولة الوصول إلى الإنترنت وانتشاره الواسع الأرض الخصبة لارتكاب هذه الجرائم، ممّا يُتيح للمجرمين استهداف ضحايا من جميع أنحاء العالم دون عناء. وتشمل سرقة البيانات الشخصية والمالية، والاحتيال الإلكتروني، ونشر المحتوى الضار، والاختراق، والابتزاز، والتجسس، وغيرها الكثير.

ولكن لا تقتصر خطورة هذه الجرائم على انتشارها الواسع فقط، بل تكمن أيضًا في صعوبة تعقب المجرمين وملاحقتهم، خاصةً مع تواجدهم في دول مختلفة. ناهيك عن سرعة انتشار المعلومات عبر الإنترنت ممّا يُساعد المجرمين على نشر المحتوى الضار أو المعلومات المضللة بسرعة فائقة.

ولذا، بات من الضروري اتخاذ خطوات وقائية حاسمة لمكافحة هذه الظاهرة المُقلقة. تقع مسؤولية حماية الفضاء الإلكتروني على عاتق الجميع، بدءًا من الأفراد الذين يجب عليهم توخي الحذر عند استخدام الإنترنت، مرورًا بالمؤسسات التي يجب عليها تعزيز أنظمة أمنها المعلوماتي، وصولًا إلى الحكومات التي يجب عليها سنّ القوانين والتشريعات اللازمة لمكافحة الجرائم الإلكترونية.

ولحماية أنفسنا من هذا الخطر المُحدق، يجب علينا اتباع خطوات وقائية أساسية، مثل استخدام كلمات مرور قوية وفريدة من نوعها لكل حساب، والحذر من رسائل البريد الإلكتروني والمواقع الإلكترونية المشبوهة، وعدم النقر على الروابط أو فتح المرفقات من مصادر غير موثوقة، وتثبيت برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة على جهازك، والحرص على تحديث نظام التشغيل وبرامجك بشكل دوري، والحذر بشأن ما تنشره على الإنترنت، وعدم مشاركة معلوماتك الشخصية أو المالية مع أي شخص لا تعرفه، والإبلاغ عن أي نشاط مشبوه لـ **authorities**.

إنّ مكافحة الجرائم الإلكترونية مسؤولية جماعية تتطلب تضافر الجهود من الأفراد والمؤسسات والحكومات. فمن خلال التوعية ونشر ثقافة الأمن الإلكتروني، والتعاون بين جميع الجهات المعنية، يمكننا الحدّ من مخاطر هذه الجرائم وحماية عالمنا الرقمي من براثن المجرمين.

مفهوم الجرائم الرقمية وأنواعه.

مفهوم الجرائم الإلكترونية (الجرائم المعلوماتية):

الجريمة الإلكترونية هي نشاط إجرامي يستهدف جهاز كمبيوتر أو شبكة كمبيوتر أو جهازاً متصلاً بالشبكة وتحاول استخدامهم. تقع معظم الجرائم الإلكترونية على أيدي لصوص أو مخترقين يودون كسب الأموال، وأحياناً نادرة أخرى يكون الهدف من وراء الجرائم الإلكترونية هو إلحاق الضرر بأجهزة الكمبيوتر لأسباب غير الربح، و يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة .

فتكون الجرائم المعلوماتية بهدف سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص، تتشابه الجريمة الإلكترونية مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة، ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة، فالجريمة الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الاتصال الحديثة والشبكات المعلوماتية.

أنواع الجرائم الرقمية

هناك العديد من أنواع الجرائم الإلكترونية التي تشتمل على سرقة الهوية أو البيانات أو المعلومات القيمة؛ واتلاف الأجهزة وتعطيل الخدمات عبر الإنترنت. ولعل أبرز أنواع الجرائم الإلكترونية هي ما يلي:

القرصنة أحد أساليب الجرائم الإلكترونية

تعد القرصنة واحدة من أكثر الجرائم الإلكترونية شيوعاً. وهي تعني الوصول غير المصرح به إلى البيانات وأنظمة الكمبيوتر أو الشبكات لسرقة المعلومات أو تعديل الملفات أو تعطيل الوظائف العادية للمواقع الإلكترونية.

الهندسة الاجتماعية

تعد هجمات الهندسة الاجتماعية أحد أكثر الأمثلة شيوعاً للجرائم الإلكترونية. وهي تعني الاحتيال والتلاعب العقلي بالأشخاص لتقديم معلومات حساسة مطلوبة لارتكاب عمليات احتيال عبر الإنترنت. يتصل مجرمو الإنترنت بالضحية المحتملة عبر الهاتف أو من خلال منصات الويب مثل مواقع المواعدة أو المسابقات أو الجوائز على الويب من أجل الحصول على المعلومات من الضحية، ومن ثم استخدامها لغرض السرقة.

هجمات DDOS (هجمات الحرمان من الخدمات)

يطلق عليها أيضاً هجمات الحرمان من الخدمات، وتقوم هذه الجريمة الإلكترونية على إرسال بيانات ضخمة غير لازمة على المواقع المستهدفة من أجل زيادة الضغط على المواقع مما يمنع وصول المستخدمين إليها. يتم توجيه هجمات DDOS في الغالب إلى خوادم الويب للشركات الكبيرة أو الكيانات الحكومية. حيث تحاول تعطل الشبكة وإسقاطها بحيث تصبح الخدمة عبر الإنترنت غير متاحة أو معطلة.

البرمجيات الخبيثة

البرامج الضارة هي نوع آخر من الجرائم الإلكترونية الحالية. هذه برامج ضارة مصممة بقصد مهاجمة أنظمة الكمبيوتر. تستخدم هذه البرامج الضارة لقفل الملفات المهمة على أجهزة الحاسوب ومن أجل فتحها تطلب مكافأة من صاحبها. ولعل أشهر هذه البرمجيات هي الفيروسات وأحصنة طروادة.

التصيد الاحتيالي من الجرائم الإلكترونية

جريمة أخرى من الجرائم الإلكترونية الشائعة. يعني التصيد الاحتيالي الحصول على معلومات قيمة من المستخدمين بطريقة مخادعة. حيث يتم جمع البيانات الخاصة بالضحية من خلال صفحة ويب احتيالية لها نفس مظهر الصفحة التي يعرفها الضحية بحيث توفر الأخيرة المعلومات التي يبحث عنها الجاني. يتم استخدام رسائل البريد الإلكتروني على سبيل المثال ويحمل اسم وشعار الشركة التي يعرفها الشخص، وعندما يطلب منه الضغط على الرابط تتم سرقة بياناته.

أحصنة طروادة

من بين أنواع الجرائم الإلكترونية تلك المعروفة باسم أحصنة طروادة. وهي تلك الأنواع من البرامج الضارة التي تظهر على أنها برامج مشروعة وغير ضارة، ولكن عند تنفيذها تكون قادرة على إتلاف ملفات البيانات أو سرقة المعلومات أو مقاطعة تشغيل الكمبيوتر. إنها واحدة من أخطر أمثلة الجرائم الإلكترونية.

التنمر الإلكتروني

يعد التنمر الإلكتروني نوعاً آخر من الجرائم الإلكترونية اليوم. ويمكن تنفيذ المضايقات عبر الإنترنت من خلال البريد الإلكتروني أو الشبكات الاجتماعية، حيث يتم مهاجمة الضحية أو التشهير بها من خلال التعليقات أو المنشورات أو الرسائل المباشرة. إنها واحدة من أكثر الجرائم الإلكترونية انتشاراً وتزايداً في العالم.

سرقة كلمة مرور FTP

عندما تتم استضافة معلومات تسجيل الدخول إلى صفحة الويب على أجهزة كمبيوتر ضعيفة الحماية، يمكن للقراصنة الوصول إلى كلمات مرور FTP للدخول إلى محتوى الويب الخاص بالضحايا وتعديله أو التلاعب به.

حقن SQL

هذا نوع من الجرائم الإلكترونية للشفرات الضارة التي تسمح لمجرمي الإنترنت بمهاجمة أي قاعدة بيانات غير محمية. يتكون الهجوم من حقن أجزاء من كود SQL في نموذج ويب، مما يوفر للمتسلل وصولاً سهلاً إلى الواجهة الخلفية للموقع.

البرامج المقرصنة

يعد توزيع واستخدام برامج الكمبيوتر المقرصنة من أكثر الجرائم الإلكترونية شيوعاً. فقد تحتوي المواد غير المصرح بها على فيروسات متنقلة أو فيروسات أحصنة طروادة قد تضر بتشغيل أجهزة الكمبيوتر أو تضرر بها. لذا ينصح باستخدام البرامج من مصدرها الرسمي.

جرائم الابتزاز والتهديد للأفراد: والتي تكون من خلال ابتزاز الضحية وتهديدها بنشر معلومات خاصة أو صور أو فيديوهات في حال امتناع الضحية عن تنفيذ ما يتم طلبه.

التشهير الإلكتروني بحق الأشخاص من خلال الذم والتحقير والقذف ، وذلك عن طريق نشر معلومات عن شخص أو هيئة معينة تنسب إليها بشكل مباشر.

الجرائم الإلكترونية السياسية التي تعنى باستهداف الأمور السياسية الحساسة والهامة في الدولة، والتطفل على أمن الدولة وسرقة المعلومات من خلال انتهاك المواقع العسكرية والسياسية التابعة للدولة.

الجرائم الإلكترونية التي تمارس ضد الحكومات عن طريق الدخول الى مواقع الوزارات بهدف تدمير البنية التحتية لها.

الجرائم الإلكترونية لتزوير الهوية: وذلك من خلال انتحال شخصيات الافراد على مواقع التواصل بسرقة معلوماتهم الشخصية واستخدامها لأغراض غير قانونية.

جرائم الملكية: وتكون عن طريق نشر روابط تؤدي الى الوصول الى الأجهزة وسرقة ما فيها من بيانات وبرامج وتعطيل تلك الأجهزة اما بشكل كلي او جزئي.

السرقه المشفرة (حيث يقوم المتسللون بتعدين العملات المشفرة باستخدام موارد لا يملكونها).

التجسس الإلكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات الحكومة أو الشركة).

التدخل في الأنظمة بطريقة تعرض الشبكة للخطر.

انتهاك حقوق النشر.

المقامرة غير المشروعة.

بيع السلع غير المشروعة عبر الإنترنت.

تشمل الجرائم الإلكترونية الأمرين التاليين أو أحدهما على الأقل:

نشاط إجرامي يستهدف أجهزة الكمبيوتر باستخدام الفيروسات وأنواع أخرى من البرمجيات الخبيثة.

نشاط إجرامي يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى.

مرتكبو الجرائم الإلكترونية الذين يستهدفون أجهزة الكمبيوتر قد يصيبونها ببرمجية خبيثة لإتلاف الأجهزة أو إيقافها عن العمل، وقد يستخدمون تلك البرمجية الخبيثة في حذف البيانات أو سرقتها. يمكن كذلك أن يعمل مرتكبو الجرائم الإلكترونية على منع المستخدمين من استخدام موقع إلكتروني أو شبكة أو منع شركة تقديم خدمة برمجية من الوصول إلى عملائها، وهذا الأسلوب معروف باسم هجوم الحرمان من الخدمات (DoS) .

قد تشمل الجريمة الإلكترونية التي تستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى استخدام أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات أو الصور غير المشروعة.

غالبًا ما يفعل مرتكبو الجرائم الإلكترونية الأمرين في الوقت نفسه. قد يستهدفون أجهزة الكمبيوتر التي تحتوي على فيروسات أولاً ثم يستخدمونها لنشر البرمجيات الخبيثة على أجهزة أخرى أو عبر الشبكة. توجد كذلك بعض البلاد التي تضع فئة ثالثة من الجرائم الإلكترونية حيث يتم استخدام أجهزة كمبيوتر كملحق في الجريمة. من أمثلة ذلك استخدام أجهزة كمبيوتر لتخزين البيانات المسروقة.

دوافع ارتكاب الجرائم الرقمية

1. الربح المادي: يعتبر الحصول على المال هو الدافع الرئيسي لارتكاب الجرائم الرقمية لذلك يستخدم القراصنة السيبرانيون التقنيات الحاسوبية والإلكترونية للدخول إلى الأنظمة السيبرانية وسرقة المعلومات والبيانات والمال.
2. التجسس الصناعي: يقوم القراصنة السيبرانيون في بعض الأحيان بالاختراق الرقمية وسرقة المعلومات الحساسة من المؤسسات والشركات والحكومات وذلك للاستفادة من هذه المعلومات في التجسس الصناعي أو الاستفادة منها في تحقيق المكاسب المالية.
3. الانتقام: يمكن أن يكون الانتقام هو دافعًا لبعض المجرمين السيبرانيين، ويمكن أن يكون الانتقام من مؤسسة أو شخص ما بسبب خلاف سابق أو اعتقادات شخصية.
4. النشاط السياسي: يمكن استخدام التقنيات الحاسوبية والإلكترونية في النشاط السياسي.
5. كما قد يقوم بعض الأفراد بارتكاب الجرائم الرقمية للتأثير على القرارات السياسية أو التأثير على الرأي العام.
6. الاضطراب: قد يجد بعض الأفراد أنفسهم مضطرين لارتكاب الجرائم السيبرانية، مثل القراصنة الذين يريدون إظهار الثغرات الأمنية في الأنظمة السيبرانية والإنترنت ودفع المؤسسات لتقوية أمنها أو قد يكون الأفراد يريدون الكشف عن الجرائم والفساد، ويستخدمون التقنيات الحاسوبية والإلكترونية للكشف عنها وإظهارها للعالم.

كيفية تأثيرها على الأفراد والمؤسسات.

- سرقة الهوية في ازدياد عام لا يتوقف، وفقًا تقرير حالة مرونة الأمن السيبراني لعام 2021 من **Accenture** ، زادت الهجمات الأمنية بنسبة 31٪ من 2020 إلى 2021، وزاد عدد الهجمات لكل شركة من 206 إلى 270 على أساس سنوي. الهجمات على الشركات تؤثر على الأفراد أيضًا لأن العديد منهم يخزنون بيانات حساسة ومعلومات شخصية من العملاء.
- يمكن لهجوم واحد -سواء كان خرقًا للبيانات أو برمجيات خبيثة أو برنامج طلب فدية أو هجوم حرمان من الخدمات- يكلف الشركات من جميع الأحجام ما متوسطه 200 ألف دولار، وتخرج العديد من الشركات المتضررة من العمل في غضون ستة أشهر من الهجوم، وذلك وفقًا لشركة التأمين **Hiscox**.
- نشرت **Javelin Strategy & Research** دراسة عن احتيال الهوية في عام 2021 وجدت فيها أن خسائر الاحتيال في الهوية لذلك العام بلغت 56 مليار دولار.
- بالنسبة للأفراد والشركات، يمكن أن يكون تأثير الجريمة الإلكترونية عميقًا: ضررًا ماليًا في المقام الأول، ولكن أيضًا فقدان الثقة والإضرار بالسمعة.
- أولاً: جرائم تسبب الأذى للأفراد.**
- ومن خلالها يتم استهداف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات هامة تخص حساباته سواء البنكية أو على الإنترنت، وتتمثل هذه الجرائم في:

انتحال الشخصية: وفيها يستدرج المجرم الضحية ويستخلص منها المعلومات بطرق غير مباشرة، ويستهدف فيها معلومات خاصة من أجل الاستفادة منها واستغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أشخاص بعينهم وقلب الوسط رأساً على عقب، وإفساد العلاقات سواء الاجتماعية أو علاقات العمل.

تهديد الأفراد: يصل المجرم من خلال القرصنة وسرقة المعلومات إلى معلومات شخصية وخاصة جداً بالنسبة للضحية، ثم يقوم بابتزازها من أجل كسب الأموال وتحريضه للقيام بأفعال غير مشروعة قد يصاب فيها بأذى.

تشويه السمعة: يقوم المجرم باستخدام المعلومات المسروقة وإضافة بعض المعلومات المغلوطة، ثم يقوم بارسالها عبر الوسائط الاجتماعية أو عبر البريد الإلكتروني للعديد من الأفراد بغرض تشويه سمعة الضحية وتدميرهم نفسياً.

تحريض على أعمال غير مشروعة: يقوم المجرم باستخدام المعلومات المسروقة عن أفراد بعينهم واستغلالها في ابتزاز الضحايا بالقيام بأعمال غير مشروعة تتعلق بالدعارة وتجارة المخدرات وغسيل الأموال والعديد من الجرائم الإلكترونية الأخرى.

ثانياً: جرائم تسبب الأذى للمؤسسات.

1. اختراق الأنظمة:

وتتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات المتمثلة في الخسائر المادية والخسائر في النظم، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة.

كما يمكن سرقة المعلومات الخاصة بموظفين المؤسسات والشركات وتحريضهم وابتزازهم من أجل تدمير الأنظمة الداخلية للمؤسسات، وتثبيت أجهزة التجسس على الحسابات والأنظمة والسعي لاختراقها والسيطرة عليها لتحقيق مكاسب مادية وسياسية.

وتؤثر الجرائم الإلكترونية الخاصة باختراق الشبكات والحسابات والأنظمة بشكل سلبي على حالة الاقتصاد في البلاد، كما تتسبب في العديد من مشاكل تتعلق بتهديد الأمن القومي للبلاد إذا ما لم يتم السيطرة عليه ومكافحتهم بكل جدارة، وتمثل نسبة الجرائم الإلكترونية والجرائم المعلوماتية حول العالم 170%، وتزداد النسبة يوم بعد يوم مما يجعلنا جميعاً في خطر محقق بسبب الانتهاكات واختراق الأنظمة والحسابات.

اختراق المواقع الإلكترونية والسيطرة عليها، ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف لزعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة.

2. تدمير النظم:

يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.

أو تدمير الخادم الرئيسي الذي يستخدمه جميع من بالمؤسسة من أجل تسهيل الأعمال، ويتم ذلك من خلال اختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة والدخول على الحسابات جميعاً في نفس ذات الوقت، ويتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره وبالتالي تعطل الأعمال بالشركات والمؤسسات.

ثالثاً: جرائم الأموال.

1. الإستيلاء على حسابات البنوك:

وهي اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الائتمانية، ومن ثم الإستيلاء عليها وسرقة ما بها من أموال.

2. انتهاك حقوق الملكية الفكرية والأدبية:

وهي صناعة نسخ غير أصلية من البرامج وملفات المالتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات.

رابعاً: الجرائم التي تستهدف أمن الدولة.

1. برامج التجسس:

تنتشر العديد من برامج التجسس والمستخدم في أسباب سياسية والتي تهدد أمن وسلامة الدولة، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات، فيقوم أعداء الوطن بهدم أنظمة النظام والإطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

2. استخدام المنظمات الإرهابية لأسلوب التضليل:

ويعتمد الإرهابيون على استخدام وسائل الإتصال الحديثة وشبكة الإنترنت من أجل بث ونشر معلومات مغلوطة، والتي قد تؤدي لزعة الاستقرار في البلاد وإحداث الفوضى من أجل تنفيذ مصالح سياسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الإنتفاع بمصالح شخصية.

التحديات التي يواجهها المحققون والمدعين العامين في مجال مكافحة الجرائم الرقمية.

هناك العديد من العقبات التي يمكن مواجهتها أثناء التحقيقات في الجرائم الإلكترونية. ويتم إنشاء إحدى هذه العقبات من خلال عدم الكشف عن الهوية التي توفرها تكنولوجيا المعلومات والاتصالات للمستخدمين. ويمكن إخفاء الهوية الأفراد من الانخراط في الأنشطة دون الكشف عن أنفسهم و أفعال للآخرين.

وهناك العديد من تقنيات إخفاء الهوية التي يستخدمها مجرمو الإنترنت وأحد هذه الأساليب هو استخدام خوادم بروكسي. والخدام الوكيل هو خادم وسيط يستخدم لتوصيل عميل بخادم يطلب العميل موارد منه وتخفي جهات إخفاء الهوية أو الخوادم الوكيله المجهولة بيانات هوية المستخدمين عن طريق إخفاء عنوان بروتوكول الإنترنت الخاص بهم واستبداله بعنوان بروتوكول الإنترنت مختلف كما يمكن لمجرمي الإنترنت أيضاً استخدام شبكات عدم الكشف عن الهوية لتشفير حركة المرور وإخفاء عنوان بروتوكول الإنترنت ، في محاولة لإخفاء أنشطتهم ومواقعهم على الإنترنت. ومن الأمثلة المعروفة لشبكات إخفاء الهوية تور (Tor) وفريينيت (Freenet) ومشروع الإنترنت غير المرئي.

و يواجه المحققون والمدعين العامين في مجال مكافحة الجرائم الرقمية العديد من التحديات، منها:

1. التطور السريع للتكنولوجيا:

تتطور أساليب الجرائم الإلكترونية بسرعة فائقة، مما يتطلب من المحققين والمدعين العامين مواكبة هذه التطورات من خلال التدريب المستمر واكتساب المهارات الجديدة.

تصبح بعض الأدلة الرقمية قديمة بسرعة، مما قد يجعل من الصعب جمعها وتحليلها.

2. نقص الموارد:

غالباً ما تفتقر وكالات إنفاذ القانون إلى الموارد اللازمة لمكافحة الجرائم الإلكترونية، بما في ذلك الموظفين ذوي الخبرة والأدوات التكنولوجية المتقدمة.

قد يؤدي ذلك إلى صعوبة في التحقيقات وملاحقة مجرمي الإنترنت.

3. الأدلة الرقمية:

قد تكون الأدلة الرقمية هشة وقابلة للتلف، مما يتطلب معالجتها بعناية وحفظها بشكل صحيح.

قد يكون من الصعب جمع الأدلة الرقمية من الأجهزة والمواقع الإلكترونية الموجودة في نطاقات قضائية أجنبية.

قد تخضع قوانين حماية البيانات لقيود على كيفية جمع الأدلة الرقمية واستخدامها.

4. الاختصاص القضائي:

قد تكون الجرائم الإلكترونية عابرة للحدود، مما قد يجعل من الصعب تحديد الاختصاص القضائي للتحقيق والملاحقة القضائية.

قد يتطلب ذلك تعاونًا دوليًا بين وكالات إنفاذ القانون، مما قد يكون صعبًا بسبب الاختلافات في القوانين والإجراءات.

5. التشفير:

يستخدم مجرمو الإنترنت غالبًا التشفير لحماية بياناتهم، مما قد يجعل من الصعب على المحققين الوصول إلى الأدلة.

قد تمنع قوانين حماية الخصوصية وكالات إنفاذ القانون من كسر التشفير.

6. نقص الوعي:

قد لا يكون ضحايا الجرائم الإلكترونية على دراية بوقوع جريمة، أو قد لا يعرفون كيفية الإبلاغ عنها.

قد يكون لدى الجمهور العام أيضًا فهم محدود للجرائم الإلكترونية وكيفية حماية أنفسهم منها.

7. التعاون مع القطاع الخاص:

غالبًا ما يتم ارتكاب الجرائم الإلكترونية على منصات شركات التكنولوجيا، مما قد يتطلب تعاونًا بين وكالات إنفاذ القانون والقطاع الخاص.

قد تكون شركات التكنولوجيا مترددة في مشاركة البيانات مع وكالات إنفاذ القانون بسبب مخاوف الخصوصية.

8. قضايا الخصوصية:

يجب على المحققين والمدعين العامين الموازنة بين الحاجة إلى التحقيق في الجرائم الإلكترونية وحماية خصوصية الأفراد.

قد تؤدي بعض تقنيات التحقيق، مثل مراقبة الإنترنت، إلى مخاوف بشأن الخصوصية.

9. ملاحقة مجرمي الإنترنت:

قد يكون من الصعب ملاحقة مجرمي الإنترنت، خاصة إذا كانوا موجودين في دول ليس لديها اتفاقيات تسليم مع البلد الذي وقعت فيه الجريمة.

قد يستخدم مجرمو الإنترنت أيضًا هويات وهمية وشبكات افتراضية خاصة لإخفاء هويتهم وموقعهم.

على الرغم من هذه التحديات، يبذل المحققون والمدعون العامون جهودًا كبيرة لمكافحة الجرائم الإلكترونية ويتم استخدام تقنيات جديدة وتطوير أساليب جديدة للتحقيق والملاحقة القضائية.

يتم أيضًا بذل الجهود لزيادة الوعي بالجرائم الإلكترونية وكيفية الوقاية منها.

الوحدة الثانية

التعرف على الجرائم الرقمية.

دراسة أنواع الجرائم الرقمية المختلفة، مثل الاحتيال عبر الإنترنت والتسلل إلى الأنظمة والتجسس والتزييف الإلكتروني والابتزاز الرقمي وغيرها. يتم تناول كل نوع من هذه الجرائم بشكل تفصيلي، وكيف يمكن التعامل معها ومكافحتها.

التعرف على الجرائم الرقمية.

للتعرف على الجرائم الرقمية من أكثر التحديات تعقيداً التي تواجهها المجتمعات الحديثة. في عصر المعلومات، أصبح الإنترنت والمجتمعات الافتراضية جزءاً لا يتجزأ من حياتنا اليومية. بينما يوفر هذا الاتصال الرقمي العديد من الفوائد والفرص، إلا أنه يفتح أيضاً الأبواب لظهور أشكال جديدة من الجرائم. الجرائم الرقمية، التي تُعرف أيضاً بالجرائم الإلكترونية أو السيبرانية، تشمل مجموعة واسعة من الأنشطة غير القانونية التي تُرتكب عبر الإنترنت أو باستخدام التكنولوجيا الرقمية. تشمل هذه الجرائم الاحتيال الإلكتروني، اختراق الأنظمة، سرقة الهوية، التهديدات السيبرانية، والتجسس الإلكتروني، وغيرها من الأفعال الضارة وسوف نتعرف عليهم جميعاً.

يُعتبر الاحتيال الإلكتروني أحد أبرز أشكال الجرائم الرقمية. يمكن أن يتخذ الاحتيال الإلكتروني العديد من الأشكال، بما في ذلك التصيد الاحتيالي، حيث يتم خداع الأفراد للكشف عن معلومات حساسة مثل كلمات المرور أو أرقام بطاقات الائتمان من خلال رسائل بريد إلكتروني مزيفة أو مواقع ويب احتيالية. بالإضافة إلى ذلك، يمكن استخدام البرامج الخبيثة مثل الفيروسات وبرامج التجسس للوصول غير المصرح به إلى الأجهزة وسرقة البيانات أو تدميرها.

اختراق الأنظمة هو نوع آخر من الجرائم الرقمية حيث يقوم الأفراد أو المجموعات بالوصول غير المصرح به إلى شبكات الكمبيوتر أو الأجهزة بهدف سرقة المعلومات أو تعطيل الأنظمة. يمكن أن يكون الهدف من هذه الهجمات الحصول على بيانات حساسة، مثل السجلات المالية أو الأسرار التجارية، أو لتعطيل البنية التحتية الحيوية مثل الشبكات الكهربائية أو أنظمة النقل.

سرقة الهوية هي جريمة رقمية خطيرة يمكن أن يكون لها آثار مدمرة على الضحايا. في هذه الجريمة، يتم سرقة المعلومات الشخصية مثل أرقام الضمان الاجتماعي أو تفاصيل الحسابات المصرفية واستخدامها لفتح حسابات جديدة، إجراء عمليات شراء غير مصرح بها، أو ارتكاب جرائم أخرى تحت اسم الضحية. يمكن أن تؤدي سرقة الهوية إلى مشاكل مالية خطيرة وتلحق أضراراً بسمعة الضحية.

التهديدات السيبرانية تتضمن جميع الأنشطة التي تهدف إلى تعطيل الأنظمة أو البيانات، بما في ذلك الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية أو الأنظمة الحكومية. يمكن أن تكون هذه الهجمات مدمرة بشكل خاص لأنها يمكن أن تؤدي إلى فقدان البيانات الحيوية أو تعطيل الخدمات الأساسية. بالإضافة إلى ذلك، فإن الهجمات الموجهة من قبل الدولة يمكن أن تكون جزءاً من استراتيجية أوسع للحرب السيبرانية.

التجسس الإلكتروني هو جريمة رقمية تتضمن الوصول غير المصرح به إلى المعلومات السرية أو الحساسة من أجل الاستفادة منها بطرق غير قانونية. يمكن أن تكون هذه المعلومات تجارية، حيث تقوم الشركات بالتجسس على منافسيها للحصول على ميزة غير عادلة، أو حكومية، حيث تقوم الدول بالتجسس على بعضها البعض للحصول على معلومات استخباراتية.

مع تطور التكنولوجيا، تصبح الجرائم الرقمية أكثر تعقيداً وتنوعاً. على سبيل المثال، أصبح استخدام الذكاء الاصطناعي والتعلم الآلي في الهجمات السيبرانية أكثر شيوعاً، مما يزيد من تحديات اكتشاف ومنع هذه الهجمات. بالإضافة إلى ذلك، فإن ظهور العملات الرقمية مثل البيتكوين أدى إلى ظهور جرائم جديدة مثل عمليات الاحتيال بالعملات الرقمية وغسيل الأموال الإلكتروني.

الجرائم الرقمية لا تقتصر على الأفراد أو المجموعات الصغيرة فقط، بل يمكن أن تكون منظمات إجرامية كبيرة أو حتى دول. هذه الجهات يمكن أن تكون متطورة تقنياً ولديها الموارد اللازمة لتنفيذ هجمات معقدة ومنسقة. على سبيل المثال، يمكن أن تقوم هذه الجهات باستخدام البرمجيات الخبيثة مثل البرمجيات الفدية لتشفير بيانات الضحايا ومطالبتهم بفدية لفك التشفير.

التعامل مع الجرائم الرقمية يتطلب تعاوناً دولياً وتنسيقاً بين الحكومات والمؤسسات الأمنية. العديد من الجرائم الرقمية تتجاوز الحدود الوطنية، مما يجعل التعاون الدولي ضرورياً لملاحقة المجرمين وتقديمهم للعدالة. بالإضافة إلى ذلك، يجب أن يكون هناك تحديث مستمر للتشريعات والسياسات لمواكبة التطورات التكنولوجية السريعة.

التعليم والتوعية هما من الأدوات الأساسية في مكافحة الجرائم الرقمية. يمكن أن يساعد توعية الأفراد والمؤسسات بالمخاطر وكيفية حماية أنفسهم في تقليل فرص النجاح لهذه الجرائم. يجب أن يتضمن التعليم حول الجرائم الرقمية معلومات عن كيفية تحديد رسائل البريد الإلكتروني الاحتيالية، حماية المعلومات الشخصية، واستخدام البرامج الأمنية.

التكنولوجيا الأمنية تلعب دوراً حيوياً في مكافحة الجرائم الرقمية. تشمل هذه التكنولوجيا برامج مكافحة الفيروسات، الجدران النارية، أنظمة كشف التسلل، وتقنيات التشفير. هذه الأدوات يمكن أن تساعد في الكشف عن الأنشطة المشبوهة ومنع الوصول غير المصرح به إلى الأنظمة والبيانات.

الأخلاقيات في التكنولوجيا تعتبر جزءاً مهماً من مكافحة الجرائم الرقمية. يجب أن يكون لدى الأفراد والمؤسسات وعي بأهمية الاستخدام المسؤول للتكنولوجيا وأن يتجنبوا الانخراط في الأنشطة غير القانونية أو غير الأخلاقية. بالإضافة إلى ذلك، يجب أن تكون هناك معايير أخلاقية واضحة تحكم سلوك المهنيين في مجال تكنولوجيا المعلومات والأمن السيبراني.

في الختام، الجرائم الرقمية تمثل تحدياً كبيراً ومنتزاعاً في العالم المعاصر. تتطلب مواجهتها مجموعة من الإجراءات والتدابير، بما في ذلك تطوير التكنولوجيا الأمنية، تعزيز التعاون الدولي، تحديث التشريعات والسياسات، وتوعية الأفراد والمؤسسات بالمخاطر وكيفية الحماية منها. من خلال الجهود المشتركة، يمكننا العمل على الحد من تأثير هذه الجرائم وتعزيز الأمن السيبراني في جميع أنحاء العالم.

دراسة أنواع الجرائم الرقمية المختلفة، مثل الاحتيال عبر الإنترنت والتسلل إلى الأنظمة والتجسس والتزييف الإلكتروني والابتزاز الرقمي وغيرها. يتم تناول كل نوع من هذه الجرائم بشكل تفصيلي، وكيف يمكن التعامل معها ومكافحتها.

في العصر الرقمي الحديث، أصبحت الجرائم الرقمية متنوعة ومعقدة، مما يشكل تحدياً كبيراً للمجتمعات والحكومات على حد سواء. تتضمن الجرائم الرقمية مجموعة واسعة من الأنشطة غير القانونية التي تُرتكب عبر الإنترنت أو باستخدام التكنولوجيا الرقمية. في هذا السياق، سنقوم بدراسة أنواع مختلفة من الجرائم الرقمية، مثل الاحتيال عبر الإنترنت، التسلل إلى الأنظمة، التجسس الإلكتروني، التزييف الإلكتروني، والابتزاز الرقمي، وسنستعرض كيفية التعامل معها ومكافحتها:

الاحتيال عبر الإنترنت هو أحد أكثر أنواع الجرائم الرقمية شيوعاً وانتشاراً. يتضمن الاحتيال عبر الإنترنت أي عمل يهدف إلى خداع الأفراد أو الشركات من أجل الحصول على مكاسب مالية أو معلومات شخصية. هناك عدة أنواع من الاحتيال عبر الإنترنت، بما في ذلك التصيد الاحتيالي، الاحتيال في التسوق الإلكتروني، والاحتيال البنكي.

التصيد الاحتيالي: يحدث التصيد الاحتيالي عندما يقوم المهاجم بإرسال رسائل بريد إلكتروني تبدو وكأنها من مصادر موثوقة، مثل البنوك أو المؤسسات الحكومية، بهدف خداع المستخدمين للكشف عن معلوماتهم الشخصية مثل كلمات المرور وأرقام بطاقات الائتمان. لمكافحة التصيد الاحتيالي، يجب على الأفراد والشركات أن يكونوا حذرين من الرسائل غير المتوقعة التي تطلب معلومات شخصية أو مالية، ويجب عليهم التحقق من صحة الرسائل من خلال الاتصال بالمصدر مباشرة.

الاحتيال في التسوق الإلكتروني: يحدث هذا النوع من الاحتيال عندما يقوم المجرمون بإنشاء مواقع تسوق مزيفة أو استخدام منصات التسوق الشهيرة لبيع منتجات وهمية أو مسروقة. يمكن للمستهلكين حماية أنفسهم من خلال التسوق فقط من المواقع الموثوقة والتحقق من تقييمات البائعين.

الاحتيال البنكي: يتضمن هذا النوع من الاحتيال سرقة المعلومات المصرفية أو التلاعب بالحسابات المصرفية عبر الإنترنت. يمكن للمؤسسات المالية مكافحة هذا الاحتيال من خلال تطبيق تقنيات الأمان مثل المصادقة الثنائية، ومراقبة الحسابات بانتظام للكشف عن أي نشاط خارج عن القانون.

التسلل إلى الأنظمة أو القرصنة: هو عملية الوصول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات بهدف سرقة البيانات أو التسبب في أضرار. يمكن أن يكون الهدف من التسلل هو سرقة المعلومات الحساسة، مثل البيانات المالية أو الأسرار التجارية، أو تعطيل الأنظمة والخدمات.

القرصنة الأخلاقية: يمكن أن يكون التسلل إلى الأنظمة مشروعًا في بعض الحالات عندما يتم تنفيذه من قبل "الهacker الأخلاقيين" الذين يختبرون أمان الأنظمة لتحسينها. تستخدم الشركات القرصنة الأخلاقية لتحديد الثغرات الأمنية وإصلاحها قبل أن يتمكن المهاجمون من استغلالها.

تأمين الأنظمة: يجب على المؤسسات تنفيذ تدابير أمان قوية لحماية أنظمتها من التسلل. يشمل ذلك استخدام جدران نارية، أنظمة كشف التسلل، وتشفير البيانات. بالإضافة إلى ذلك، يجب أن يكون لدى المؤسسات سياسات أمان قوية وتدريب الموظفين على أفضل ممارسات الأمان السيبراني.

التجسس الإلكتروني: هو عملية الوصول غير المصرح به إلى المعلومات السرية أو الحساسة بهدف استخدامها بطرق غير قانونية. يمكن أن تكون هذه المعلومات تجارية أو حكومية.

التجسس التجاري: تقوم الشركات بالتجسس على منافسيها للحصول على ميزة غير عادلة. يمكن أن يشمل ذلك سرقة الأسرار التجارية أو البيانات المالية الحساسة. لمكافحة التجسس التجاري، يجب على الشركات استخدام تقنيات الأمان المتقدمة لحماية بياناتها الحساسة.

التجسس الحكومي: تقوم الدول بالتجسس على بعضها البعض للحصول على معلومات استخباراتية. يمكن أن تشمل هذه المعلومات الأسرار العسكرية أو الاستراتيجية. لمكافحة التجسس الحكومي، يجب على الدول تعزيز أمن شبكاتها وتطبيقات البرمجيات، بالإضافة إلى مراقبة الأنظمة بانتظام للكشف عن أي أنشطة خارجة عن القانون.

التزييف الإلكتروني يتضمن إنشاء مستندات أو بيانات مزيفة بغرض الاحتيال أو التضليل. يمكن أن تشمل هذه الجريمة تزوير الهويات الرقمية، أو الوثائق المالية، أو المعلومات الحساسة.

تزييف الهوية الرقمية: يمكن للمجرمين استخدام الهوية الرقمية المزيفة للوصول إلى الأنظمة أو البيانات أو لإجراء عمليات شراء غير مصرح بها. يمكن مكافحة تزييف الهوية الرقمية من خلال استخدام تقنيات التحقق من الهوية مثل التوقيعات الرقمية والشهادات الإلكترونية.

تزييف الوثائق المالية: يمكن أن يشمل ذلك تزوير الفواتير أو الشيكات أو البيانات المصرفية. يمكن مكافحة تزييف الوثائق المالية من خلال استخدام تقنيات التحقق من الصحة مثل البصمة المائية الرقمية والتشفير.

الابتزاز الرقمي: يتضمن التهديد بالكشف عن معلومات حساسة أو التسبب في ضرر للأنظمة أو البيانات ما لم يتم دفع فدية. تشمل هذه الجريمة استخدام برامج الفدية، حيث يتم تشفير بيانات الضحايا ومطالبتهم بدفع فدية لفك التشفير.

برامج الفدية: برامج الفدية هي نوع من البرامج الضارة التي تقوم بتشفير بيانات الضحية وتطلب فدية لإعادة الوصول إليها. لمكافحة برامج الفدية، يجب على الأفراد والمؤسسات الاحتفاظ بنسخ احتياطية من البيانات بانتظام، وتحديث البرامج وأنظمة التشغيل للحماية من الثغرات الأمنية.

التوعية والتدريب: يجب توعية الأفراد والشركات حول كيفية التعرف على الهجمات المحتملة وكيفية الرد عليها. يشمل ذلك التدريب على كيفية التعامل مع رسائل البريد الإلكتروني المشبوهة واستخدام تقنيات الأمان الأساسية مثل برامج مكافحة الفيروسات والجدران النارية.

سرقة الهوية: تتضمن استخدام المعلومات الشخصية لشخص آخر دون إذنه بغرض الاحتيال. يمكن أن تؤدي هذه الجريمة إلى فتح حسابات مصرفية جديدة، إجراء عمليات شراء غير مصرح بها، أو حتى ارتكاب جرائم أخرى تحت اسم الضحية. حماية المعلومات الشخصية: يجب على الأفراد حماية معلوماتهم الشخصية من خلال استخدام كلمات مرور قوية وفريدة لكل حساب، وتمكين المصادقة الثنائية حيثما أمكن. يجب أيضاً مراقبة الحسابات المالية بانتظام للتحقق من أي نشاط غير عادي. الإبلاغ عن سرقة الهوية: في حالة اكتشاف سرقة الهوية، يجب الإبلاغ عنها فوراً للجهات المعنية مثل البنوك أو المؤسسات المالية، والسلطات القانونية.

التحرش الرقمي: يشمل استخدام التكنولوجيا لمضايقة أو تهديد الآخرين. يمكن أن يشمل ذلك إرسال رسائل تهديدية، نشر معلومات شخصية بشكل غير قانوني، أو التهديدات عبر وسائل التواصل الاجتماعي. الإبلاغ والحماية: يمكن مكافحة التحرش الرقمي من خلال التبليغ عن هذه الأنشطة إلى السلطات المختصة والمنصات المعنية، واستخدام إعدادات الخصوصية لحماية المعلومات الشخصية. التوعية والتعليم: يجب توعية الأفراد حول كيفية التعامل مع التحرش الرقمي وحثهم على عدم الرد على التهديدات والاحتفاظ بالأدلة للإبلاغ عنها.

التهديدات السيبرانية الموجهة للدول : تتضمن هذه التهديدات هجمات سيبرانية تستهدف البنية التحتية الحيوية للدول، مثل الشبكات الكهربائية، أنظمة النقل، والمؤسسات الحكومية. يمكن أن تكون هذه الهجمات مدمرة للغاية وتتطلب استجابة منسقة من قبل الدول والمؤسسات الأمنية.

التعاون الدولي: لمكافحة التهديدات السيبرانية الموجهة للدول، يجب تعزيز التعاون الدولي لمشاركة المعلومات حول التهديدات والهجمات المحتملة، وتطوير استراتيجيات مشتركة للرد على هذه الهجمات.

تحسين البنية التحتية للأمن السيبراني: يجب على الدول تحسين أمان البنية التحتية الحيوية من خلال تنفيذ تقنيات الأمان المتقدمة وتدريب العاملين على كيفية التعامل مع التهديدات السيبرانية.

الجرائم المالية الإلكترونية: تشمل الجرائم المالية الإلكترونية مجموعة واسعة من الأنشطة غير القانونية التي تهدف إلى سرقة الأموال أو التلاعب بالأسواق المالية. يمكن أن تشمل هذه الجرائم الاحتيال في بطاقات الائتمان، غسل الأموال عبر الإنترنت، والاحتيال في الأوراق المالية.

تقنيات الأمان المالية: لمكافحة الجرائم المالية الإلكترونية، يجب على المؤسسات المالية استخدام تقنيات أمان متقدمة مثل التشفير، أنظمة كشف الاحتيال، ومراقبة النشاط المالي بشكل دوري.

التشريعات والسياسات: يجب تحديث التشريعات والسياسات لمواكبة التطورات في الجرائم المالية الإلكترونية وضمان وجود عقوبات رادعة للمجرمين.

تقنيات مكافحة الجرائم الرقمية

تتطلب مكافحة الجرائم الرقمية مزيجاً من التكنولوجيا، السياسات، والتعليم، والتعاون الدولي. فيما يلي نظرة على أهم التقنيات والإجراءات التي تساعد في مكافحة هذه الجرائم:

1. التشفير

التشفير هو عملية تحويل البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح فك التشفير الصحيح. يعد التشفير أحد أكثر الوسائل فعالية لحماية البيانات الحساسة، سواء أثناء التخزين أو النقل.

تشفير البيانات: يجب تشفير البيانات الحساسة، مثل المعلومات الشخصية والمالية، لحمايتها من الوصول غير المصرح به. يستخدم التشفير الخوارزميات الرياضية لتحويل البيانات إلى نص غير مقروء، ولا يمكن فك التشفير إلا باستخدام المفتاح الصحيح.

تشفير الاتصالات: يستخدم التشفير لحماية الاتصالات عبر الإنترنت، مثل البريد الإلكتروني والتصفح والمكالمات الصوتية، من الاعتراض والتنصت. بروتوكولات مثل TLS (Transport Layer Security) و SSL (Secure Sockets Layer) تستخدم لتشفير البيانات المرسلة بين الخوادم والمتصفحات.

2. أنظمة كشف التسلل (IDS) ومنع التسلل (IPS)

تستخدم أنظمة كشف التسلل ومنع التسلل للكشف عن الأنشطة المشبوهة أو غير المصرح بها في الشبكات.

أنظمة كشف التسلل (IDS): تعمل على مراقبة حركة المرور في الشبكة وتحليلها للكشف عن الأنشطة غير العادية أو الهجمات المحتملة. تقوم بإعلام مسؤولي النظام عند اكتشاف تهديدات.

أنظمة منع التسلل (IPS): تقوم بمنع الأنشطة المشبوهة أو الهجمات فور اكتشافها. يمكنها أن تتخذ إجراءات تلقائية لحظر حركة المرور الضارة ومنع التسلل إلى الشبكة.

3. جدران نارية (Firewalls)

الجدران النارية تعمل كحاجز بين الشبكة الداخلية والشبكات الخارجية، مثل الإنترنت، لمنع الوصول غير المصرح به.

جدران نارية قائمة على البرامج: تُثبت على الأجهزة وتوفر حماية فردية من التهديدات. يمكنها مراقبة حركة المرور الواردة والصادرة وتصفية البيانات بناءً على قواعد محددة.

جدران نارية قائمة على الأجهزة: تُستخدم لحماية الشبكات الكبيرة وتعمل على مستوى الشبكة بالكامل. توفر حماية أكثر قوة وفعالية ضد التهديدات الخارجية.

4. التوقيعات الرقمية والشهادات الرقمية

التوقيعات الرقمية والشهادات الرقمية تستخدم للتحقق من صحة الوثائق والرسائل الإلكترونية.

التوقيعات الرقمية: توفر ضماناً بأن المستند أو الرسالة لم يتم تعديله وأنها صادرة عن المصدر الموثوق به. تستخدم التوقيعات الرقمية خوارزميات التشفير لضمان النزاهة والمصادقية.

الشهادات الرقمية: تصدرها سلطات التصديق (Certificate Authorities) وتستخدم للتحقق من هوية الأطراف المتصلة. توفر الشهادات الرقمية مستوى إضافياً من الأمان في الاتصالات عبر الإنترنت.

5. المصادقة الثنائية (Two-Factor Authentication)

المصادقة الثنائية تضيف طبقة إضافية من الأمان فوق كلمة المرور التقليدية. تتطلب من المستخدمين تقديم دليلين مستقلين للتحقق من هويتهم.

رموز المرور المؤقتة (One-Time Passwords): يتم إرسال رموز المرور المؤقتة إلى المستخدمين عبر الرسائل النصية أو التطبيقات المخصصة وتستخدم لمرة واحدة فقط.

التوثيق البيومتري: يشمل استخدام بصمات الأصابع، التعرف على الوجه، أو التعرف على الصوت للتحقق من هوية المستخدمين. يوفر مستوى عالٍ من الأمان لأنه يعتمد على الخصائص الفريدة للفرد.

6. أنظمة إدارة الهوية والوصول (IAM)

أنظمة إدارة الهوية والوصول توفر أدوات لإدارة والتحكم في الوصول إلى الموارد الرقمية. إدارة الهوية: تشمل إنشاء وإدارة الهويات الرقمية للمستخدمين، مثل حسابات المستخدمين وحقوق الوصول. إدارة الوصول: تشمل التحكم في من يمكنه الوصول إلى الموارد المختلفة وتحت أي ظروف. يمكن استخدام سياسات الوصول لتحديد الصلاحيات المطلوبة للوصول إلى البيانات أو الأنظمة.

7. برامج مكافحة الفيروسات والبرامج الضارة

برامج مكافحة الفيروسات والبرامج الضارة توفر حماية ضد الفيروسات والبرامج الخبيثة الأخرى. الكشف عن الفيروسات: تستخدم برامج مكافحة الفيروسات خوارزميات للكشف عن الفيروسات المعروفة من خلال التحقق من توقعات الفيروسات.

إزالة الفيروسات: يمكن للبرامج مكافحة الفيروسات إزالة الفيروسات المكتشفة وعزل الملفات المصابة لمنع الانتشار.

8. النسخ الاحتياطي والاسترداد

النسخ الاحتياطي والاسترداد توفر طريقة لحماية البيانات ضد الفقد أو التدمير.

النسخ الاحتياطي المنتظم: يجب إجراء نسخ احتياطي منتظم للبيانات الهامة لضمان إمكانية استردادها في حالة الفقد أو التدمير.

استراتيجيات الاسترداد: يجب تطوير استراتيجيات استرداد فعالة لضمان استعادة البيانات بسرعة وكفاءة في حالة حدوث أي طارئ.

9. التوعية والتعليم

التوعية والتعليم هما من أهم عناصر مكافحة الجرائم الرقمية. يتطلب الأمان السيبراني الفعال فهم الأفراد والشركات للتهديدات المحتملة وكيفية التصدي لها.

التدريب على الأمان السيبراني: يشمل تدريب الموظفين على أفضل ممارسات الأمان السيبراني، مثل التعرف على رسائل البريد الإلكتروني المشبوهة، وعدم تنزيل البرامج من مصادر غير موثوقة، وكيفية استخدام تقنيات الأمان الأساسية.

التوعية العامة: يشمل توعية الجمهور حول التهديدات السيبرانية وكيفية حماية المعلومات الشخصية، مثل استخدام كلمات مرور قوية وفريدة، وتجنب مشاركة المعلومات الحساسة عبر الإنترنت.

10. التعاون الدولي وتبادل المعلومات

التعاون الدولي وتبادل المعلومات يلعبان دورًا حاسمًا في مكافحة الجرائم الرقمية. تشمل الجهود الدولية التعاون بين الدول لمشاركة المعلومات حول التهديدات السيبرانية وتطوير استراتيجيات مشتركة للرد على هذه التهديدات.

منظمات الأمان السيبراني الدولية: مثل فريق الاستجابة لحوادث الأمان السيبراني (CERT) ومنظمة التعاون الاقتصادي والتنمية (OECD) التي تعمل على تعزيز التعاون الدولي في مجال الأمان السيبراني.

اتفاقيات التعاون: تشمل الاتفاقيات الدولية لتسهيل تبادل المعلومات حول التهديدات السيبرانية وتنسيق الردود على الهجمات السيبرانية.

11. البنية التحتية للأمان السيبراني

تعزيز البنية التحتية للأمان السيبراني يشمل تطبيق تقنيات الأمان المتقدمة وتطوير السياسات والإجراءات اللازمة لحماية الأنظمة والبيانات.

تقييمات الأمان: تشمل تقييمات دورية لأمان الأنظمة والشبكات لتحديد الثغرات الأمنية وإصلاحها.
سياسات الأمان: تشمل تطوير وتطبيق سياسات الأمان السيبراني لضمان حماية البيانات والأنظمة من التهديدات.

12. تقنيات الذكاء الاصطناعي والتعلم الآلي

تقنيات الذكاء الاصطناعي والتعلم الآلي يمكن أن تلعب دورًا مهمًا في مكافحة الجرائم الرقمية من خلال تحليل البيانات واكتشاف الأنماط غير العادية.

كشف التهديدات: يمكن استخدام تقنيات الذكاء الاصطناعي لتحليل البيانات واكتشاف الأنشطة المشبوهة أو التهديدات المحتملة.

الاستجابة التلقائية: يمكن لتقنيات الذكاء الاصطناعي اتخاذ إجراءات تلقائية للرد على التهديدات، مثل حظر حركة المرور الضارة أو تنبيه مسؤولي النظام.

مكافحة الجرائم الرقمية تتطلب استخدام مجموعة واسعة من التقنيات والإجراءات التي تهدف إلى حماية البيانات والأنظمة من التهديدات المتزايدة. من خلال استخدام التشفير، أنظمة كشف ومنع التسلل، الجدران النارية، التوقيعات الرقمية، المصادقة الثنائية، أنظمة إدارة الهوية والوصول، برامج مكافحة الفيروسات، النسخ الاحتياطي، التوعية والتعليم، التعاون الدولي، تعزيز البنية التحتية للأمان السيبراني، وتقنيات الذكاء الاصطناعي، يمكن للمؤسسات والأفراد تعزيز أمانهم السيبراني والتصدي للجرائم الرقمية بفعالية.

الوحدة الثالثة

التحقيق في الجرائم الرقمية.

كيفية جمع الأدلة الرقمية وتحليلها وتقييمها.

كيفية إجراء التحقيقات الرقمية وجمع الأدلة والتعامل معها.

الأدوات والتقنيات المستخدمة في جمع الأدلة الرقمية وكيفية تحليلها.

كيفية تطبيق الأساليب القانونية المختلفة في مكافحة الجرائم الرقمية.



التحقيق في الجرائم الرقمية.

اولا ماذا تعني بالتحقيق الجنائي Forensics ؟

عملية معقدة تتطلب دقة واحترافية عالية. باستخدام منهجية محددة وواضحة لجمع وتحليل وتقييم الأدلة الرقمية، يمكن للمحققين الرقميين تقديم أدلة قوية وموثوقة في المحاكم، مما يساهم في تحقيق العدالة. من الضروري اتباع الإجراءات القانونية والتقنية المناسبة لضمان سلامة الأدلة وفعاليتها في السياق القانوني.

ينبغي التأكد من:

1 توثيق وكتابة كل خطوة من خطوات التحقيق.

2 ضمان عدم تغيير الأدلة وعدم العبث بها.



أنواع التحقيق الجنائي الرقمي؟

Disk Forensics الأقراص

Memory Forensics ذاكرة التخزين

Network Forensics الشبكات

Email Forensics البريد الإلكتروني

Mobile Forensics أجهزة الجوال

هنالك أنواع ومجالات أخرى كثيرة للتحقيق الجنائي الرقمي البرامج الدرونز، الكلاود الانترنت الملفات الخبيثة.

منهجية التحقيق الجنائي الرقمي؟



منهجيته التحقيق تتكون من اربع مراحل و تبدأ بمرحلة جمع الأدلة و تحديد ما هي الامور التي يتم جمعها و منها ننتقل إلى المرحلة التالية و هي مرحلة حفظ الأدلة وفيها يتم معرفة طريقه الحفاظ على الأدلة و معرفة كيفية قرائه و نسخ الأدلة و من بعدها ننتقل لمرحلة التحليل و من خلالها تحليل الأدلة و معرفة ربطهم مع الحصول على نتائج مفيدة في التحقيق و منها نصل لأخر مرحلة و هي مرحلة إعداد التقارير و فيها يتم توثيق وكتابة كل شئ تم معرفة أثناء التحقيق .

هناك بعض الامور التي يجب أخذها في الاعتبار في عملية التحقيق الجنائي الرقمي و هي كالآتي:

ينبغي تحديد الأدوات التي سأستخدمها GUI or CLI -

هل هذه الحادثة الأمنية كانت Local أو عن بعد Remote

ما القانون Law المرتبط بهذه الحادثة الأمنية

كيفية جمع الأدلة الرقمية وتحليلها وتقييمها.

جمع الأدلة الرقمية هو الخطوة الأولى في عملية التحقيق الجنائي الرقمي، ويتضمن تأمين موقع الجريمة الرقمية واستخدام أدوات وتقنيات متخصصة لجمع البيانات دون تغييرها. الهدف هو ضمان سلامة الأدلة بحيث يمكن تحليلها وتقديمها في المحكمة لاحقاً.

تأمين موقع الجريمة الرقمية

عزل النظام: ضمان عدم تغيير الأدلة عن طريق عزل الأنظمة المصابة عن الشبكة لمنع أي تعديل أو حذف غير مقصود.

توثيق الموقع: تصوير وتوثيق الحالة الفعلية للأجهزة والمواقع الرقمية لضمان عدم فقدان أي تفاصيل مهمة.

استخدام الأدوات المناسبة

برامج جمع البيانات: مثل EnCase ، FTK ، و X1 Social Discovery لجمع وتحليل البيانات الرقمية.

أجهزة جمع البيانات: مثل Tableau Write Blockers التي تمنع تعديل البيانات أثناء جمعها.

جمع البيانات من المصادر المختلفة

أجهزة الكمبيوتر: استخراج الأقراص الصلبة، واستخدام أدوات استعادة البيانات لجمع المعلومات المخزنة.

الهواتف الذكية: استخدام برامج مثل Cellebrite لجمع البيانات من الأجهزة المحمولة.

الشبكات: استخدام أدوات تحليل الشبكات مثل Wireshark لجمع وتحليل حركة المرور الشبكية.

الإنترنت: استخراج البيانات من وسائل التواصل الاجتماعي، البريد الإلكتروني، والمواقع الإلكترونية.

حفظ الأدلة

التخزين الآمن: حفظ البيانات على أجهزة تخزين خارجية محمية بكلمات مرور وتشفير لضمان عدم التلاعب.

ضمان النزاهة: استخدام تقنيات التحقق من النزاهة مثل الخوارزميات التجزئة (MD5، SHA-256) لضمان عدم

تغيير البيانات أثناء النقل والتخزين.

كيفية إجراء التحقيقات الرقمية وجمع الأدلة والتعامل معها.

تتطلب هذه العملية مهارات متقدمة في التحليل الجنائي الرقمي ومعرفة بالأدوات والتقنيات المستخدمة لضمان نزاهة وسلامة الأدلة.

خطوات إجراء التحقيقات الرقمية:

التحضير والتخطيط

تحديد الأهداف والنطاق يتكون من

تحديد نوع الجرائم الرقمية المستهدفة.

تحديد المصادر المحتملة للأدلة الرقمية.

وضع خطة مفصلة للتحقيق تشمل جميع الخطوات المتوقعة.

تشكيل فريق التحقيق يتم من خلال:

تجميع فريق من الخبراء في مجالات التحليل الجنائي الرقمي، القانون، والأمن السيبراني.

تأمين الأدوات والتقنيات اللازمة.

جمع الأدلة الرقمية

تأمين موقع الجريمة الرقمية

عزل النظام: ضمان عدم تغيير الأدلة عن طريق عزل الأنظمة المصابة عن الشبكة لمنع أي تعديل أو حذف غير مقصود.

توثيق الموقع: تصوير وتوثيق الحالة الفعلية للأجهزة والمواقع الرقمية لضمان عدم فقدان أي تفاصيل مهمة.

استخدام الأدوات المناسبة

برامج جمع البيانات: مثل EnCase ، FTK ، و X1 Social Discovery لجمع وتحليل البيانات الرقمية.

أجهزة جمع البيانات: مثل Tableau Write Blockers التي تمنع تعديل البيانات أثناء جمعها.

جمع البيانات من المصادر المختلفة

أجهزة الكمبيوتر: استخراج الأقراص الصلبة، واستخدام أدوات استعادة البيانات لجمع المعلومات المخزنة.

الهواتف الذكية: استخدام برامج مثل Cellebrite لجمع البيانات من الأجهزة المحمولة.

الشبكات: استخدام أدوات تحليل الشبكات مثل Wireshark لجمع وتحليل حركة المرور الشبكية.

الإنترنت: استخراج البيانات من وسائل التواصل الاجتماعي، البريد الإلكتروني، والمواقع الإلكترونية.

حفظ الأدلة

التخزين الآمن: حفظ البيانات على أجهزة تخزين خارجية محمية بكلمات مرور وتشفير لضمان عدم التلاعب.

ضمان النزاهة: استخدام تقنيات التحقق من النزاهة مثل الخوارزميات التجزئة (MD5) ، (SHA-256) لضمان عدم تغيير البيانات أثناء النقل والتخزين.

تحليل الأدلة الرقمية

تحليل الملفات والبيانات

استعادة الملفات المحذوفة: استخدام أدوات استعادة البيانات مثل Recuva ، Photorec لاستعادة الملفات المحذوفة.

تحليل أنظمة التشغيل: فحص سجلات النظام (Event Logs) لاكتشاف الأنشطة غير العادية وتحليل ملفات الريجستري في نظام التشغيل Windows للحصول على معلومات عن البرامج المثبتة والنشاطات الأخيرة. تحليل الوثائق والصور: استخدام أدوات مثل Autopsy لتحليل محتوى الوثائق والصور واسترجاع البيانات المخفية.

تحليل الشبكات

مراقبة حركة المرور الشبكية: استخدام أدوات مثل Wireshark لتحليل حركة المرور وتحديد الاتصالات المشبوهة.

تحليل ملفات السجلات الشبكية: فحص ملفات السجلات الناتجة عن أجهزة التوجيه والخوادم للكشف عن الأنشطة غير العادية.

تقييم الأدلة الرقمية

تحقق النزاهة

التجزئة: التحقق من سلامة البيانات باستخدام الخوارزميات التجزئة (MD5) ، (SHA-256) لمقارنة التجزئات المولدة للأدلة مع التجزئات الأصلية للتأكد من عدم تغييرها.

توثيق الأدلة

تدوين الملاحظات: تدوين جميع الخطوات التي تم اتخاذها لجمع وتحليل الأدلة لضمان الشفافية والمصادقية.

توفير الوثائق الداعمة: جمع كل الوثائق الداعمة مثل التقارير الناتجة عن أدوات التحليل الجنائي.

إعداد التقارير

تقرير شامل: إعداد تقرير شامل يوضح جميع الأدلة المكتشفة والنتائج التي تم التوصل إليها، وتقديم الاستنتاجات المستندة إلى الأدلة وتقديم التوصيات للإجراءات المستقبلية.

تقديم الأدلة في المحكمة

ضمان القبول القانوني

الاتباع الصارم للبروتوكولات: اتباع البروتوكولات القانونية لجمع وتحليل الأدلة لضمان قبولها في المحكمة، وتقديم الأدلة بشكل يمكن فهمه من قبل القضاة والمحامين.

شهادة الخبراء

شهادة الخبراء الجنائيين: تقديم شهادات الخبراء الذين قاموا بجمع وتحليل الأدلة لتوضيح الإجراءات المتبعة وضمان نزاهة النتائج.

التحقيق الرقمي عملية متقدمة تتطلب معرفة تقنية وقانونية واسعة. يتطلب النجاح في هذا المجال اتباع منهجية صارمة لجمع الأدلة وتحليلها وتقييمها لضمان سلامتها وصحتها. باستخدام الأدوات والتقنيات المناسبة، يمكن للمحققين الرقميين تقديم أدلة قوية وموثوقة في المحاكم، مما يساهم في تحقيق العدالة. من الضروري أن يتم تنفيذ كل خطوة بدقة واحترافية لضمان قبول الأدلة واستخدامها بفعالية في السياق القانوني.

الأدوات والتقنيات المستخدمة في جمع الأدلة الرقمية وكيفية تحليلها.

برامج جمع البيانات الجنائية:

EnCase: أداة متكاملة لجمع وتحليل الأدلة الرقمية من أجهزة الكمبيوتر والشبكات. توفر واجهة مستخدم قوية وتمكن من استخراج البيانات بسهولة.

FTK (Forensic Toolkit): تستخدم لتحليل الملفات واستعادة البيانات المحذوفة، وتحتوي على مجموعة واسعة من الأدوات لتحليل الأدلة الرقمية.

X1 Social Discovery: أداة متخصصة في جمع البيانات من وسائل التواصل الاجتماعي والمواقع الإلكترونية.

أجهزة جمع البيانات:

Tableau Write Blockers: تمنع تعديل البيانات أثناء جمعها من الأقراص الصلبة وأجهزة التخزين الأخرى، مما يحافظ على سلامة الأدلة.

أدوات تحليل الشبكات:

Wireshark: أداة تحليل حركة المرور الشبكية تتيح للمحققين مراقبة وتحليل حركة البيانات على الشبكة، مما يساعد في اكتشاف الأنشطة المشبوهة.

برامج استعادة البيانات:

Recuva: برنامج لاستعادة الملفات المحذوفة من أجهزة الكمبيوتر والأقراص الصلبة.

Photorec: أداة مفتوحة المصدر لاستعادة الملفات المحذوفة من مختلف أنواع وسائط التخزين.

أدوات جمع البيانات من الهواتف الذكية:

Cellebrite: تستخدم لاستخراج وتحليل البيانات من الهواتف المحمولة والأجهزة الذكية، بما في ذلك الرسائل النصية وسجلات المكالمات والصور.

التقنيات المستخدمة في جمع الأدلة الرقمية

تصوير الأقراص:

إنشاء صورة رقمية كاملة للقرص الصلب أو جهاز التخزين، مما يتيح للمحققين العمل على نسخة طبق الأصل دون التأثير على البيانات الأصلية.

التجزئة والتحقق من النزاهة:

استخدام خوارزميات التجزئة مثل MD5 و SHA-256 لإنشاء بصمة رقمية للأدلة، مما يساعد في التحقق من عدم تغيير البيانات أثناء جمعها وتحليلها.

عزل الأنظمة:

فصل الأجهزة المشتبه بها عن الشبكة لضمان عدم تغيير البيانات أو فقدانها.

كيفية تحليل الأدلة الرقمية

تحليل الملفات والبيانات:

استعادة الملفات المحذوفة: استخدام أدوات مثل Recuva و Photorec لاستعادة البيانات المحذوفة وفحصها.

تحليل سجلات النظام: فحص سجلات الأحداث وملفات الريجستري في نظام التشغيل لتتبع النشاطات المشبوهة واكتشاف التغييرات غير المصرح بها.

تحليل حركة المرور الشبكية:

مراقبة وتحليل البيانات الشبكية: استخدام أدوات مثل Wireshark لمراقبة حركة المرور الشبكية وتحليل البيانات المرسلة والمستلمة على الشبكة، مما يساعد في اكتشاف الهجمات والتسللات.

كيفية تطبيق الأساليب القانونية المختلفة في مكافحة الجرائم الرقمية.

مكافحة الجرائم الرقمية تتطلب اتباع مجموعة من الأساليب القانونية لضمان حماية البيانات والأدلة الرقمية وضمان تحقيق العدالة. هذه الأساليب تتنوع من حيث التشريعات، الإجراءات القانونية، والتعاون الدولي.

التشريعات والقوانين الوطنية

أ. قوانين مكافحة الجرائم الإلكترونية

قوانين مكافحة القرصنة: تمنع وتجرم الأفعال التي تشمل اختراق الأنظمة والشبكات بدون إذن.

قوانين حماية البيانات الشخصية: مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تضع معايير صارمة لحماية البيانات الشخصية ومعالجة الانتهاكات.

ب. تشريعات الأمن السيبراني

القوانين الخاصة بالأمن السيبراني: تفرض على الشركات والمؤسسات تنفيذ تدابير أمنية لحماية البنية التحتية الرقمية من الهجمات الإلكترونية.

القوانين المتعلقة بالإبلاغ عن الحوادث: تلزم المؤسسات بالإبلاغ عن الحوادث الأمنية إلى السلطات المختصة.

الإجراءات القانونية والتحقيقات الجنائية

أ. إجراءات جمع الأدلة

أوامر التفتيش والمصادرة: تستصدرها المحاكم للسماح للسلطات بجمع الأدلة من المواقع الرقمية والأجهزة الإلكترونية.

إجراءات الحفظ: تحافظ على سلامة الأدلة الرقمية لضمان قبولها في المحكمة.

ب. تحليل الأدلة وتقديمها

التجزئة والتحقق من النزاهة: استخدام تقنيات التحقق من النزاهة لضمان عدم تغيير الأدلة.

التوثيق المفصل: تسجيل كل خطوة في عملية جمع وتحليل الأدلة لضمان الشفافية والنزاهة.

التعاون الدولي

أ. اتفاقيات التعاون الدولي

اتفاقية بودابست بشأن الجرائم الإلكترونية: توفر إطارًا قانونيًا للتعاون بين الدول في مكافحة الجرائم الإلكترونية.

الاتفاقيات الثنائية ومتعددة الأطراف: تعزيز التعاون بين الدول لتبادل المعلومات والأدلة والمساعدة في التحقيقات العابرة للحدود.

ب. التعاون مع المنظمات الدولية

الإنتربول: يوفر دعمًا للدول الأعضاء في التحقيقات المتعلقة بالجرائم الإلكترونية وتنسيق الجهود الدولية.

اليوروبول: يساعد الدول الأوروبية في مكافحة الجرائم الإلكترونية من خلال توفير الموارد والخبرات.

الإجراءات الوقائية والتوعوية

أ. التوعية والتدريب

التدريب على الأمن السيبراني: توفير دورات تدريبية للموظفين وأفراد المجتمع لتعزيز الوعي بأهمية الأمن السيبراني وكيفية حماية البيانات.

حملات التوعية العامة: توعية الجمهور بالمخاطر الرقمية وطرق الحماية منها.

ب. الضوابط والتدابير الأمنية

استخدام التقنيات الحديثة: مثل التشفير والجدران النارية وأنظمة الكشف عن التسلل لحماية البيانات والشبكات.

تنفيذ السياسات الأمنية: وضع سياسات وإجراءات داخلية لضمان أمان المعلومات والتعامل الفعال مع الحوادث.

الملاحقات القانونية والعقوبات

أ. تقديم المتهمين للمحاكمة

الإجراءات القضائية: اتباع الإجراءات القانونية اللازمة لتقديم المشتبه بهم إلى المحاكمة وضمان حقوقهم في الدفاع.

شهادات الخبراء: تقديم شهادات الخبراء في التحقيقات الرقمية لدعم القضايا في المحاكم.

ب. العقوبات والتدابير

العقوبات الجنائية: تشمل السجن والغرامات للأفراد المدانين بالجرائم الرقمية.

العقوبات الإدارية: تشمل العقوبات المفروضة على الشركات والمؤسسات التي تفشل في الالتزام بتدابير الأمن السيبراني.

تطبيق الأساليب القانونية المختلفة في مكافحة الجرائم الرقمية يتطلب تكاملاً بين التشريعات الوطنية، الإجراءات القانونية، والتعاون الدولي. من خلال تعزيز التشريعات، تنفيذ الإجراءات الوقائية، وتنسيق الجهود الدولية، يمكن تحقيق مستوى أعلى من الأمان الرقمي وحماية البيانات، وبالتالي مكافحة الجرائم الإلكترونية بفعالية.



فى البداية قم بتحميل برنامج اوتوبسي (Autopsy) على ويندوز من رابط التحميل الآتى:

[/https://www.autopsy.com/download](https://www.autopsy.com/download)

قضية سرقة فنية وتشويه في المعرض الوطني في واشنطن العاصمة.

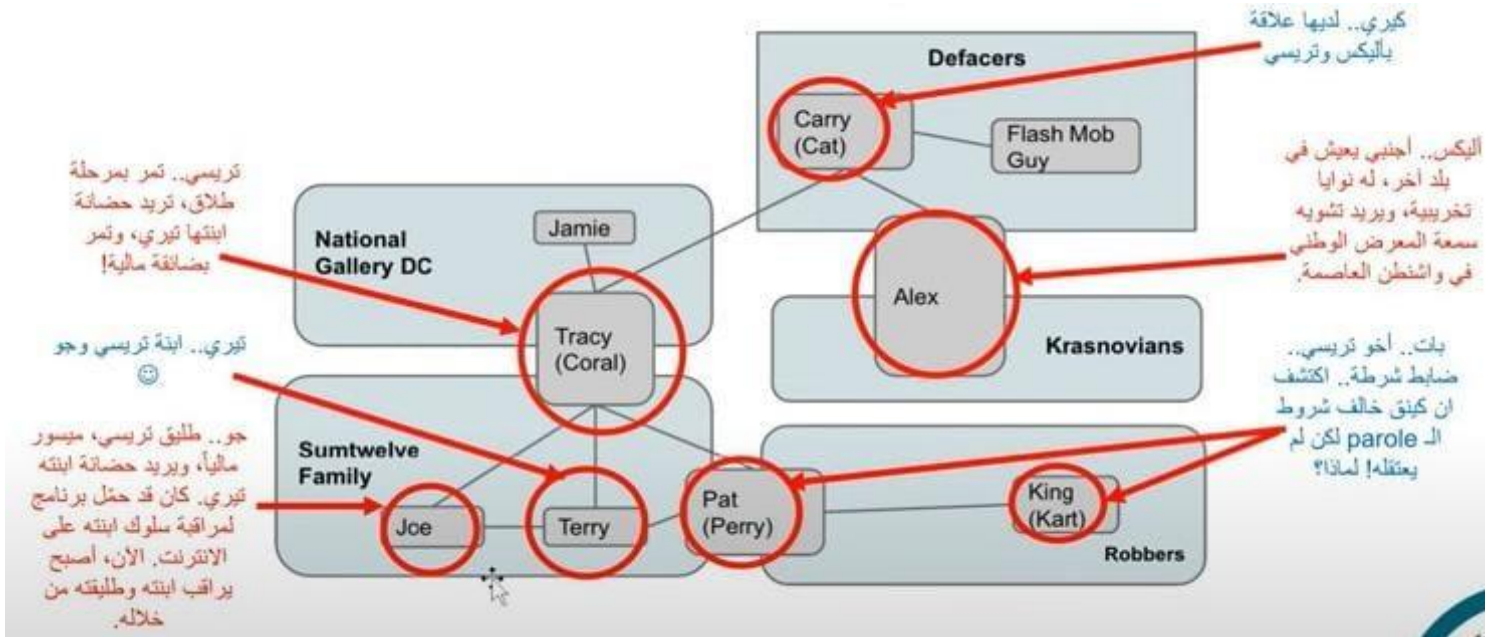


اضغط هنا لفتح رابط التمرين

تفاصيل القضية يوجد مجموعة من الأطراف ف القضية وهى كالآتى:

- اليكس .. Alex أجنبي يعيش في دولة أخرى.. لديه أغراض تخريبية ويريد الإضرار بسمعة المعرض الوطني في واشنطن.
- اتصل بكيري Carry وطلب منها المساعدة كبري تعرف موظفة في المعرض، اسمها تريسي.
- تريسي Tracy ، تمر بضائقة مالية وظروف عائلية... وتحتاج المال لتدفع أقساط مدرسة ابنتها الباهضة الثمن .
- جو Joe طليق تريسي.. كان قد حمل أداة المراقبة سلوك ابنته على الانترنت. لاحظ أن تريسي تخطط الأمر ماء وقام بإبلاغ الشرطة.
- تيري Terry .. ابنة تريسي وجو.. تفضل البقاء في مدرستها الحالية ولا تريد خسارة أصدقائها.. أخبرت أمها أنها تفضل العيش مع والدها إذا كان هو سيعمل لها عدم تغيير المدرسة .

رسم توضيحي بالأشخاص المشتبه فيهم في القضية وعلاقتهم معاً



سوف نحاول ربط الأدلة من خلال ايفون تريسي قوم بتحميل بيانات هاتف تريسي كما هو موضح بالصورة من رابط التمرين في الأعلى

afford to pay the tuition.

Evidence

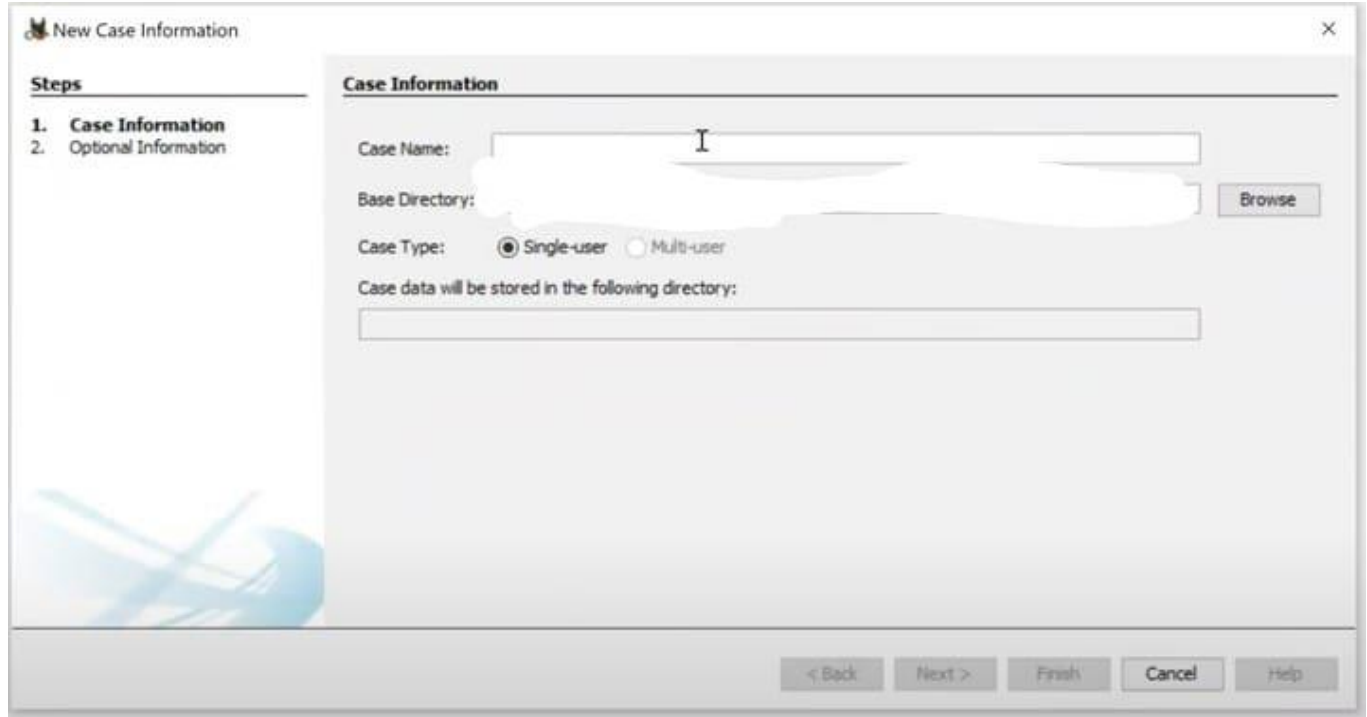
The seized evidence has been processed for you by the ingest team of the crime laboratory. You have been provided with the following data:

- Carry's phone on 2012-07-15 [ZIP] [FTK Logical Dump]
- Carry's tablet on 2012-07-16 [E01] [TAR]
- Email messages generated by the spyware installed on Tracy's Macbook Air and that were periodically emailed to Joe [ZIP]
- Tracy's phone on 2012-07-15 (encase) [L01] [ZIP]
- **Tracy's phone on 2012-07-15 (other extraction tool) [EQ1] [tar]**
- Tracy's external hard drive [E01]
- Tracy's home computer [E01] [E02]
- Exterior Network Packet Dumps
 - exterior 2012-07-06 exterior-2012-07-06.pcap
 - exterior 2012-07-09 exterior-2012-07-09.pcap
 - exterior 2012-07-10 exterior-2012-07-10.pcap
 - exterior 2012-07-12 exterior-2012-07-12.txt
- Interior Network Packet Dumps
 - interior 2012-07-06 interior-2012-07-06.pcap
 - interior 2012-07-09 interior-2012-07-09.pcap
 - interior 2012-07-10 interior-2012-07-10.pcap
 - interior 2012-07-12 interior-2012-07-12.txt

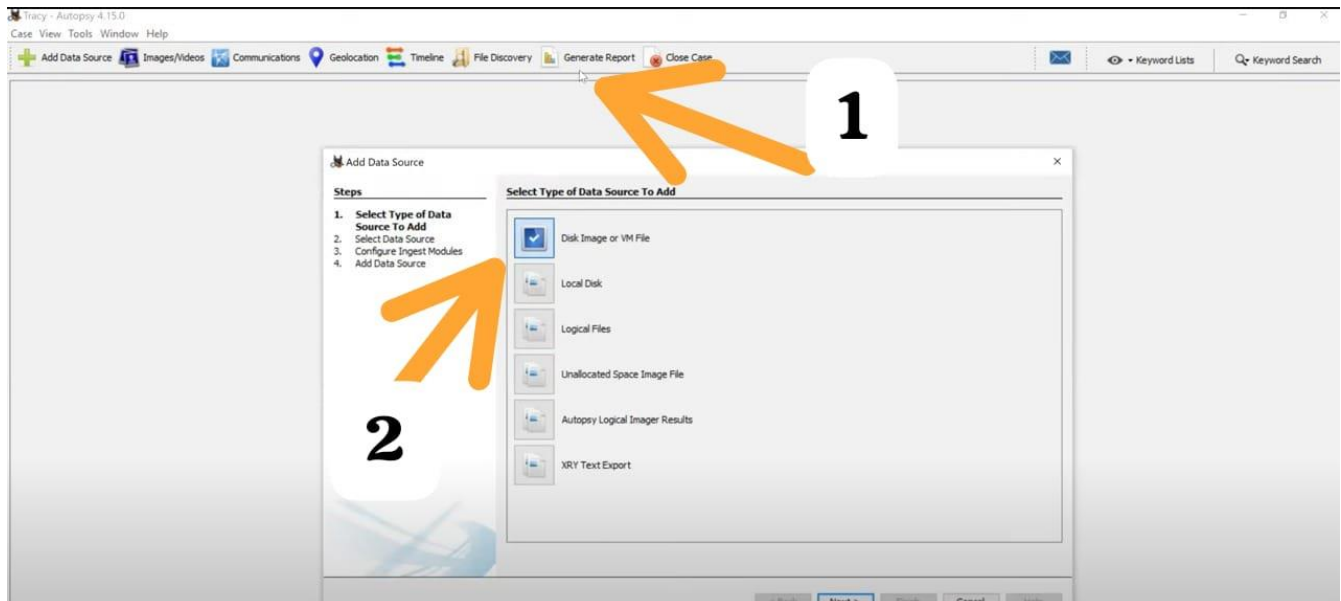
ومن ثم سوف نقوم بتشغيل البرنامج بعد تحميله على الويندوز و سوف نختار (New case)



ومن ثم نتابع مع خطوات تكوين الحالة من اختيار مكان حفظها على الحاسب و اسم الحالة كما موضح في الصورة التالية



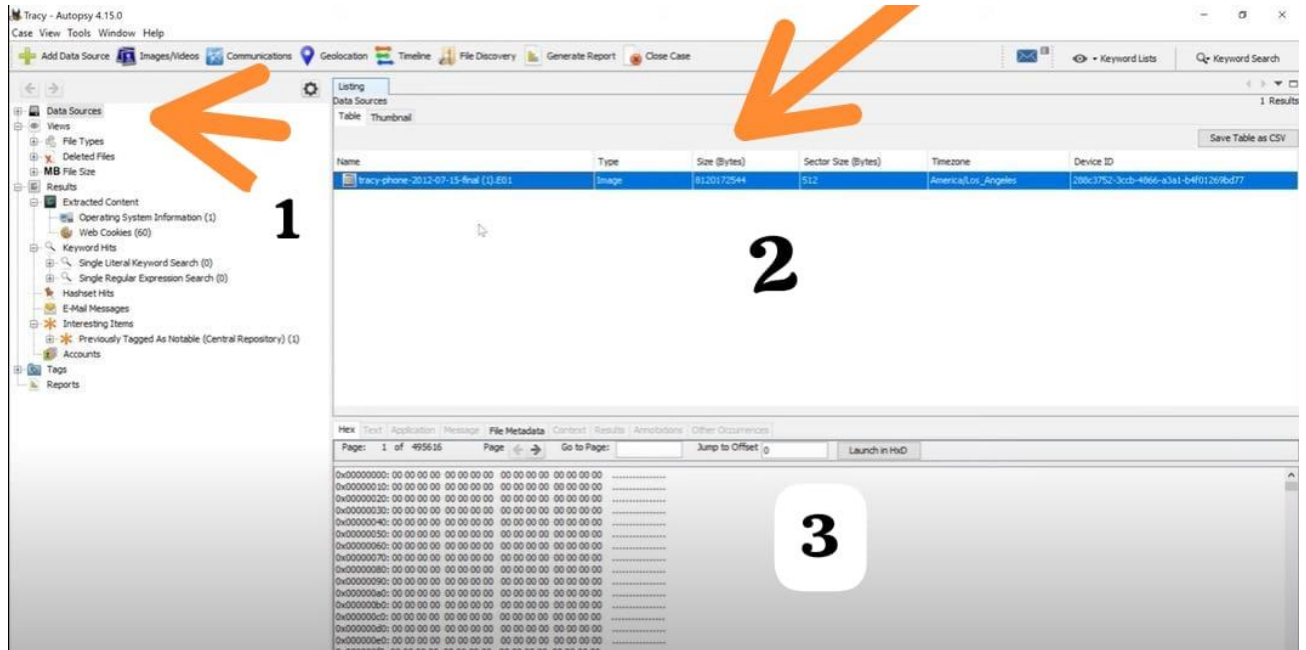
من **Generate Report** سوف يساعد في استخراج تقرير و الخطوة الثانية نختار **disk image** وسوف نقوم بتحميل صورت بيانات هاتف تريسي التي قومنا بتحميلها من رابط التمرين.



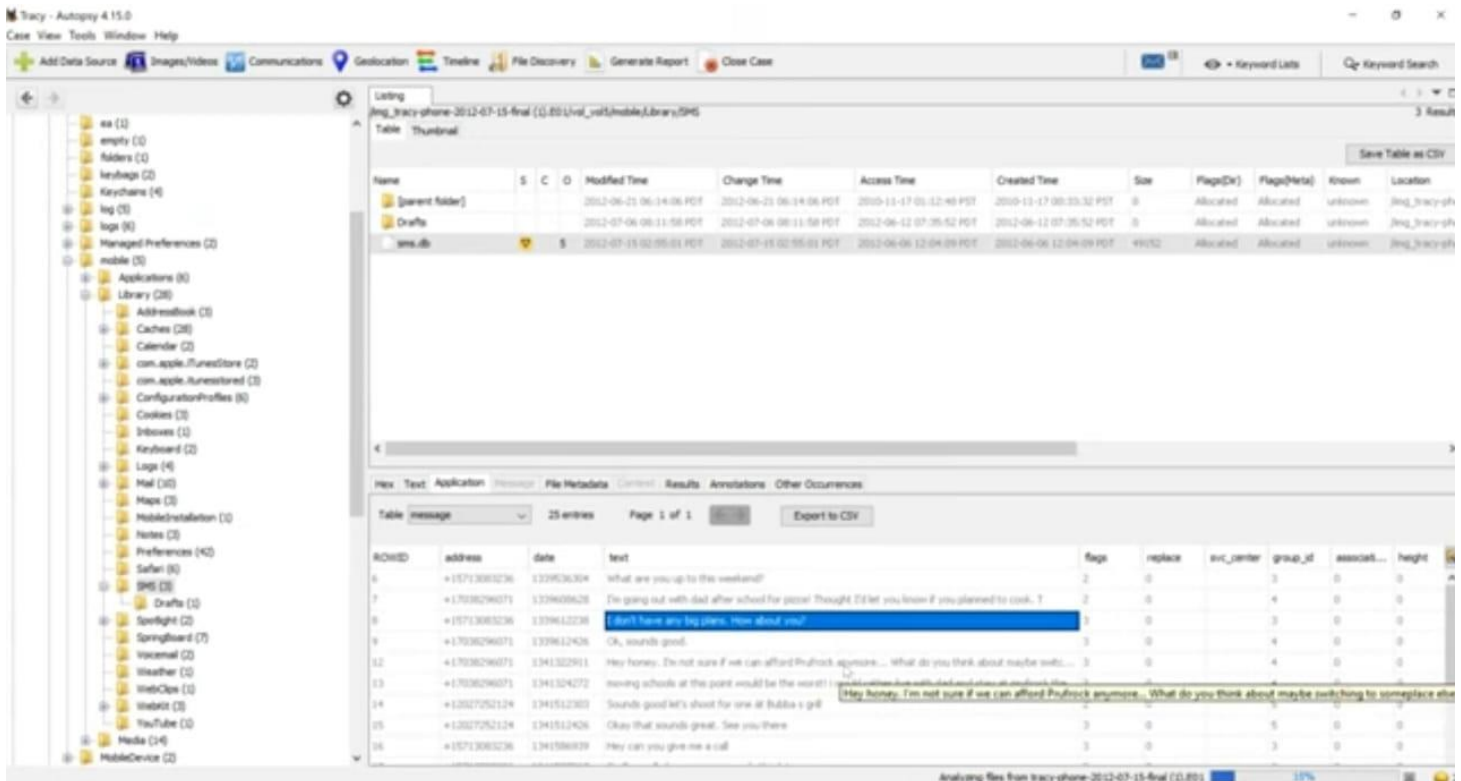
الخطوة الثالثة من تحميل بيانات تريسي و هي اختيار **path** الخاص ببياناتها ثم اتابع باقي الخطوات من **next** ولكن لا تنسى اضافته علامه عند **Fat file systems ignore orphan file in** المضافة بالأعلى.

The screenshot shows the 'Add Data Source' window with the 'Select Data Source' tab active. On the left, a 'Steps' list shows: 1. Select Type of Data Source To Add, 2. Select Data Source (current step), 3. Configure Ingest Modules, and 4. Add Data Source. The main area contains a 'Path' field with 'C:\' and a 'Browse' button. Below this is a checked checkbox for 'Ignore orphan files in FAT file systems'. Further down are dropdown menus for 'Time zone' (set to '(GMT-8:00) America/Los_Angeles') and 'Sector size' (set to 'Auto Detect'). There are also input fields for 'Hash Values (optional)': MD5, SHA-1, and SHA-256. A note at the bottom reads: 'NOTE: These values will not be validated when the data source is added.' At the bottom right, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

الخطوة التالية يظهر واجهة البرنامج و تنقسم إلى 1 ويوجد بيها جميع الملفات التي دم إدراجها على البرنامج و بالنظر إلى الجزء الثاني يمكننا قرائه ملف ايفون تريسي من خلاله و بالأسفل حيث رقم 3 يوجد لدينا تفاصيل البيانات بالكامل.



ومن ثم سوف نقوم بفتح الرسائل التي في هاتف تريسي ونرى تريسي تحدث مع أصدقائها و سوف نرى رساله من شقيق تريسي يطلب منها مراجعه ايميل يسمى **needs** و من خلال هذا المسدج سوف نذهب الى ملفات الأيميلات لنرى ماذا يوجد في هذا الايميل و سوف نرى ان هذا الإيميل يمكن استخدامه كدليل في التحقيق الجنائي و من هنا يمكننا تجميع الادلة لتقديمها في التقرير الجنائي.



الوحدة الرابعة

الأمن السيبراني.

يتضمن هذا الموضوع دراسة مفهوم الأمن السيبراني وأهميته في مواجهة الجرائم الرقمية، وكذلك دراسة التهديدات السيبرانية والاستراتيجيات اللازمة لمكافة هذه التهديدات.

الأمن السيبراني.

يعتبر الأمن السيبراني أحد أهم المجالات في العصر الرقمي الحديث، حيث يتزايد الاعتماد على التكنولوجيا في جميع جوانب الحياة. يهدف الأمن السيبراني إلى حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية والتهديدات السيبرانية المختلفة. في هذه الوحدة، سنتناول مفهوم الأمن السيبراني وأهميته، بالإضافة إلى التهديدات السيبرانية والاستراتيجيات اللازمة لمكافحتها.

يتضمن هذا الموضوع دراسة مفهوم الأمن السيبراني وأهميته في مواجهة الجرائم الرقمية، وكذلك دراسة التهديدات السيبرانية والاستراتيجيات اللازمة لمكافحة هذه التهديدات.

مفهوم الأمن السيبراني

الأمن السيبراني هو مجموعة من الممارسات والتقنيات والعمليات المصممة لحماية الأنظمة والشبكات والبرمجيات من الهجمات الإلكترونية. يشمل الأمن السيبراني حماية البيانات من الوصول غير المصرح به، والتلف، والسرقة، والتهديدات الأخرى.

أهمية الأمن السيبراني

حماية البيانات الشخصية: مع تزايد حجم البيانات الشخصية المخزنة رقميًا، يصبح الأمن السيبراني ضروريًا لحماية الخصوصية ومنع سرقة الهوية.

حماية البنية التحتية الحيوية: تشمل البنية التحتية الحيوية قطاعات مثل الطاقة، والمياه، والاتصالات، والتي تتطلب حماية مشددة لمنع تعطيلها نتيجة للهجمات السيبرانية.

ضمان استمرارية الأعمال: تحمي الإجراءات الأمنية السيبرانية المؤسسات من التوقف عن العمل نتيجة للهجمات، مما يضمن استمرارية العمليات التجارية.

منع الخسائر المالية: الهجمات السيبرانية يمكن أن تؤدي إلى خسائر مالية كبيرة نتيجة لسرقة البيانات المالية أو تعطيل العمليات التجارية.

التهديدات السيبرانية؟

البرمجيات الخبيثة (Malware)

تشمل الفيروسات، والديدان، وأحصنة طروادة، التي تهدف إلى إتلاف أو تعطيل الأنظمة والشبكات.

الهجمات بالتصيد الاحتيالي (Phishing)

تهدف إلى خداع الأفراد للكشف عن معلومات حساسة مثل كلمات المرور أو البيانات المالية عن طريق رسائل البريد الإلكتروني المزيفة أو المواقع الوهمية.

الهجمات بالحرمان من الخدمة (DDoS)

تتضمن إغراق الشبكات أو الخوادم بكمية هائلة من البيانات لمنعها من تقديم الخدمات للمستخدمين العاديين.

الهجمات بالحقن (SQL Injection)

تتضمن إدخال تعليمات برمجية خبيثة في قواعد البيانات عبر تطبيقات الويب، مما يسمح للمهاجمين بالوصول إلى البيانات الحساسة.

التحديات الداخلية (Insider Threats)

تشمل الموظفين أو المستخدمين الذين يسيئون استخدام الوصول المصرح لهم به لتنفيذ هجمات أو تسريب معلومات. الاستراتيجيات لمكافحة التهديدات السيبرانية

التوعية والتدريب

توعية الموظفين والمستخدمين حول التهديدات السيبرانية وطرق الوقاية منها عبر برامج التدريب والتوعية المستمرة.

استخدام الجدران النارية وأنظمة كشف التسلل (IDS/IPS)

تطبيق تقنيات الجدران النارية وأنظمة كشف التسلل لمنع الوصول غير المصرح به واكتشاف الهجمات في مراحلها المبكرة.

التشفير

استخدام تقنيات التشفير لحماية البيانات أثناء التخزين والنقل، مما يجعل من الصعب على المهاجمين الوصول إليها وفهمها. الحفاظ على تحديث الأنظمة والبرمجيات بشكل منتظم لضمان حماية الأجهزة من الثغرات الأمنية التي يمكن استغلالها.


الأمن السيبراني هو عنصر أساسي لحماية الأنظمة والشبكات في العصر الرقمي. من خلال فهم التهديدات السيبرانية وتطبيق الاستراتيجيات المناسبة لمكافحتها، يمكن للأفراد والمؤسسات حماية بياناتهم وضمان استمرارية أعمالهم. هذه الوحدة تقدم نظرة شاملة على أهمية الأمن السيبراني والوسائل المتاحة لتحقيقه.



الوحدة الخامسة

الحماية الرقمية.

يتم تناول الأساليب اللازمة لحماية الأنظمة والبيانات والشبكات وتأمينها من الهجمات السيبرانية، وكذلك كيفية رصد ومكافحة التهديدات السيبرانية.



الحماية الرقمية.

في عالم اليوم الذي يعتمد بشكل متزايد على التكنولوجيا الرقمية، أصبحت الحماية الرقمية ضرورة حتمية لكل الأفراد والمؤسسات. مع تزايد التهديدات السيبرانية، تتطلب حماية الأنظمة والبيانات والشبكات تبني استراتيجيات وأدوات متقدمة لضمان سلامة المعلومات والأصول الرقمية. تهدف هذه الوحدة إلى تقديم فهم شامل للأساليب والتقنيات المستخدمة في تأمين البيانات الرقمية ورصد ومكافحة التهديدات الإلكترونية بشكل فعال.

يتم تناول الأساليب اللازمة لحماية الأنظمة والبيانات والشبكات وتأمينها من الهجمات السيبرانية، وكذلك كيفية رصد ومكافحة التهديدات السيبرانية.

الأساليب اللازمة لحماية الأنظمة والبيانات والشبكات

التشفير: التشفير المتناظر وغير المتناظر: تُستخدم هذه الأساليب لتأمين البيانات أثناء نقلها وتخزينها، بحيث يمكن قراءتها فقط من قبل الأطراف المخولة.

البروتوكولات الآمنة: مثل HTTPS و SSL/TLS لتأمين الاتصالات عبر الإنترنت.

إدارة الهوية والوصول: (IAM) أنظمة التحكم في الوصول: تحديد من يمكنه الوصول إلى المعلومات والموارد بناءً على هوياتهم وصلاحياتهم.

المصادقة الثنائية (2FA) والمصادقة متعددة العوامل: (MFA) تعزيز أمان الحسابات من خلال إضافة طبقات إضافية من التحقق.

الجدران النارية وأنظمة كشف التسلل (IDS) ومنع التسلل: (IPS)

الجدران النارية: تمنع الوصول غير المصرح به إلى الشبكات من خلال مراقبة وتصفية حركة البيانات الواردة والصادرة.

أنظمة كشف التسلل ومنع التسلل: تكتشف وتستجيب للأنشطة المشبوهة والهجمات المحتملة في الوقت الفعلي.

تحديث البرمجيات وإدارة التصحيحات:

التحديثات الدورية: الحفاظ على الأنظمة محدثة لضمان حماية الأجهزة من الثغرات الأمنية المعروفة.

إدارة التصحيحات: تطبيق التصحيحات الأمنية الفورية لمعالجة نقاط الضعف المكتشفة.

النسخ الاحتياطي واستعادة البيانات:

النسخ الاحتياطي المنتظم: الحفاظ على نسخ احتياطية محدثة من البيانات لضمان القدرة على استعادة المعلومات في حالة فقدان أو التلف.

اختبار استعادة البيانات: التأكد من فعالية عمليات النسخ الاحتياطي والاستعادة من خلال اختبارات دورية.

كيفية رصد ومكافحة التهديدات السيبرانية

مراقبة الأنظمة والشبكات:

أنظمة إدارة الأحداث والمعلومات الأمنية: (SIEM) تجميع وتحليل البيانات من مصادر متعددة للكشف عن الأنماط غير الطبيعية والتهديدات المحتملة.

الأدوات التحليلية: استخدام التحليلات التنبؤية والتعلم الآلي لتحديد الهجمات قبل وقوعها.

الاستجابة للحوادث السيبرانية:

خطط الاستجابة للطوارئ: وضع إجراءات محددة للتعامل مع الحوادث السيبرانية بسرعة وفعالية.

فرق الاستجابة للحوادث: (IRT) تشكيل فرق متخصصة للاستجابة الفورية والتخفيف من تأثير الهجمات.

التدريب والتوعية:

تدريب الموظفين: تقديم برامج تدريبية لتعليم الموظفين كيفية التعرف على التهديدات السيبرانية والتعامل معها.

حملات التوعية: نشر الوعي حول أفضل الممارسات الأمنية وكيفية تجنب الوقوع ضحية للهجمات الإلكترونية.

التدقيق والاختبار الأمني:

التدقيق الأمني الدوري: تقييم الأنظمة والشبكات بانتظام لتحديد الثغرات الأمنية.

اختبارات الاختراق: محاكاة الهجمات السيبرانية لاختبار قوة الأنظمة وتحديد نقاط الضعف.

إن حماية الأنظمة والبيانات والشبكات تتطلب مزيجًا من التقنيات المتقدمة والإجراءات الوقائية والاستجابة السريعة للتهديدات. من خلال تبني استراتيجيات الحماية الرقمية الفعالة وتطبيق الأساليب المناسبة، يمكن تحقيق مستوى عالٍ من الأمان السيبراني وضمان سلامة المعلومات الحيوية في العصر الرقمي.

الوحدة السادسة

الجرائم المرتبطة بوسائل التواصل الاجتماعي.

كيفية التعامل مع الجرائم المرتبطة بوسائل التواصل الاجتماعي مثل التحرش الجنسي والتشهير والابتزاز الرقمي، وكيفية الحماية منها ومكافحتها.

أساليب الوقاية والتحقق والتعامل مع هذه الجرائم.

كيفية تحديد المسؤولية القانونية.

الجرائم المرتبطة بوسائل التواصل الاجتماعي.

الجرائم المرتبطة بوسائل التواصل الاجتماعي تشمل مجموعة من الأنشطة الإجرامية التي تتم عبر منصات التواصل الاجتماعي مثل التحرش الإلكتروني، والتجسس، ونشر المعلومات الكاذبة، والترويج للمخدرات أو المواد المحظورة، وانتهاكات الخصوصية، والتحريض على الكراهية أو العنف، بالإضافة إلى الاحتيال وسرقة الهوية.

كيفية التعامل مع الجرائم المرتبطة بوسائل التواصل الاجتماعي مثل التحرش الجنسي والتشهير والابتزاز الرقمي، وكيفية الحماية منها ومكافحتها.

للتعامل مع الجرائم المرتبطة بوسائل التواصل الاجتماعي مثل التحرش الجنسي، التشهير، والابتزاز الرقمي، يمكن اتباع بعض الإجراءات التالية:

1. **التوعية والتثقيف:** تعلم وفهم كيفية استخدام منصات التواصل الاجتماعي بشكل آمن، والتعرف على السلوكيات المشكوك فيها والتي يمكن أن تؤدي إلى جرائم رقمية.
 2. **حماية الخصوصية:** ضبط إعدادات الخصوصية على حساباتك لتقليل من الوصول إلى المعلومات الشخصية من قبل الأشخاص غير المرغوب فيهم.
 3. **الابتعاد عن التفاعل السلبي:** تجنب التفاعل مع المحتويات غير اللائقة أو الخبيثة التي يمكن أن تؤدي إلى التحرش أو التشهير.
 4. **الإبلاغ والتبليغ:** استخدام خيارات الإبلاغ والتبليغ المتاحة على منصات التواصل الاجتماعي للإبلاغ عن أي نشاط مشبوه أو غير لائق.
 5. **التعاون مع السلطات:** في حالة التعرض لجريمة رقمية مثل التحرش أو الابتزاز، يجب الاتصال بالسلطات المختصة للمساعدة في معالجة المشكلة وتتبع المتسببين.
 6. **الاحتفاظ بالأدلة:** إن أمكن، الاحتفاظ بالرسائل أو الصور أو أي دليل يمكن أن يساعد في التحقيقات القانونية.
- الحماية من هذه الجرائم تتطلب توعية مستمرة واستخدام ذكاء رقمي للحفاظ على سلامتك الشخصية والمهنية عبر الإنترنت.

أساليب الوقاية والتحقق والتعامل مع هذه الجرائم.

للقاية والتحقق والتعامل مع جرائم وسائل التواصل الاجتماعي مثل التحرش الجنسي والتشهير والابتزاز الرقمي، يمكن اتباع الإجراءات التالية:

الوقاية:

توعية الذات والتعليم: تعلم ما يمكنك عن كيفية استخدام الإنترنت ووسائل التواصل الاجتماعي بشكل آمن. تعرف على السلوكيات الخطرة والتحذيرات الأساسية.

حماية الخصوصية: ضبط إعدادات الخصوصية على حساباتك للتحكم في من يمكنه رؤية معلوماتك الشخصية والمحتويات التي تشاركها.

استخدام كلمات المرور القوية: استخدام كلمات مرور قوية ومعقدة للحسابات الخاصة بك وتغييرها بانتظام.

التفكير قبل المشاركة: قبل نشر أو مشاركة أي معلومات أو صور على وسائل التواصل الاجتماعي، فكر في التأثيرات المحتملة لهذه الأفعال.

تقييم الطلبات والمطالبات: كن حذرًا عندما تتلقى طلبات أو رسائل غريبة أو غير مألوفة، وتجنب الرد على المطالبات الشخصية أو المالية.

التحقق:

فحص الحسابات والأنشطة: قم بفحص حساباتك الاجتماعية بانتظام للتأكد من عدم وجود نشاط غير مألوف أو غير مصرح به.

التحقق من الهوية: تأكد من هوية ومصادقية الأشخاص الذين تتفاعل معهم عبر الإنترنت قبل مشاركة معلومات شخصية أو حساسة.

التقارير والإبلاغ: استخدم خيارات الإبلاغ المتاحة على منصات التواصل الاجتماعي للإبلاغ عن أي نشاط مشبوه أو غير لائق.

التعامل:

الابتعاد عن التفاعل السلبي: تجنب التفاعل مع المحتوى السلبي أو الضار الذي يمكن أن يؤدي إلى التحرش أو الابتزاز.

الابتعاد عن الأساليب المؤذية: تجنب الوقوع في فخ التهديدات أو الابتزاز عبر الإنترنت، ولا ترد على مطالبات الابتزاز.

التواصل مع الجهات المختصة: في حالة التعرض لأي شكل من أشكال الجرائم الرقمية، اتصل بالسلطات المختصة للحصول على المساعدة والدعم القانوني.

من الضروري أن يكون التعامل مع جرائم وسائل التواصل الاجتماعي مبنيًا على الوعي والحذر، مما يساعد في تقليل المخاطر وحماية سلامتك الشخصية والرقمية.

كيفية تحديد المسؤولية القانونية

تحديد المسؤولية القانونية في حالات الجرائم المرتبطة بوسائل التواصل الاجتماعي يتطلب فهم القوانين المحلية والدولية المتعلقة بالإنترنت والاتصالات الإلكترونية. هنا بعض النقاط الرئيسية التي يمكن أن تساعد في تحديد المسؤولية القانونية:

التشريعات المحلية: يجب معرفة القوانين واللوائح التي تنظم استخدام وسائل التواصل الاجتماعي في بلدك. هذه القوانين قد تحدد المسؤولية عن الأفعال الإجرامية مثل التحرش الجنسي أو التشهير الرقمي.

سياسات وسائل التواصل الاجتماعي: كل منصة تواصل اجتماعي لديها سياسات وشروط خاصة بها لاستخدام المنصة. يتم تحديد المسؤولية والعقوبات بناءً على هذه السياسات، ويمكن الرجوع إليها في حالات النزاعات.

التحقيق القانوني: في حالة وقوع جريمة رقمية، تتم متابعة التحقيقات من قبل السلطات المختصة. يتم تحديد المسؤولية بناءً على الأدلة المتوفرة والقوانين المعمول بها.

المسؤولية المدنية والجنائية: قد تكون هناك نواحي مختلفة للمسؤولية، مثل المسؤولية المدنية (تعويضات مالية للأضرار) والمسؤولية الجنائية (عقوبات قانونية).

الحكم القضائي: يتم تحديد المسؤولية النهائية بناءً على قرارات المحاكم، حيث يتم التقييم الشامل للحالة والأدلة المقدمة.

للحصول على استشارة قانونية دقيقة، دائماً من الأفضل التواصل مع محامٍ أو خبير قانوني متخصص في القانون الرقمي والجرائم الإلكترونية. هذا يضمن تقديم المشورة القانونية المناسبة وفهم الحقوق والواجبات في الظروف القانونية المختلفة.



الوحدة السابعة

السياسات والقوانين المتعلقة بالجرائم الرقمية.

دراسة السياسات والقوانين المتعلقة بالجرائم الرقمية وكيفية تطبيقها.

دراسة القضايا القانونية المرتبطة بالجرائم الرقمية، مثل التحقق من الهوية الرقمية وإنشاء الأدلة الرقمية والحفاظ على الخصوصية الإلكترونية.

القوانين المحلية والدولية المتعلقة بالجرائم الرقمية وكيفية تطبيقها في العمل القضائي.



السياسات والقوانين المتعلقة بالجرائم الرقمية.

في العصر الرقمي الحالي، أصبح الإنترنت جزءًا لا يتجزأ من حياتنا اليومية، حيث يوفر وسيلة فعالة للتواصل، والتعليم، والتجارة، والترفيه. ومع تزايد الاعتماد على التكنولوجيا، ظهرت تحديات جديدة تتعلق بالأمن السيبراني والجرائم الرقمية. الجرائم الرقمية هي الأفعال غير القانونية التي تُرتكب باستخدام الحواسيب والشبكات الإلكترونية، وتشمل مجموعة واسعة من الأنشطة مثل القرصنة، والاحتيال الإلكتروني، وسرقة الهوية، والتشهير، والابتزاز. لمواجهة هذه التحديات، تضع الدول سياسات وقوانين تهدف إلى حماية الأفراد والمؤسسات من المخاطر الإلكترونية.

في المملكة العربية السعودية، تتصدر الحكومة جهود مكافحة الجرائم الرقمية من خلال تطوير إطار قانوني متين يحدد الجرائم ويضع العقوبات المناسبة، بالإضافة إلى تعزيز الوعي العام حول الأمان الرقمي. تهدف هذه السياسات والقوانين إلى خلق بيئة إلكترونية آمنة وموثوقة، تحمي حقوق المستخدمين وتضمن استخدام الإنترنت بشكل مسؤول.

سعت الدراسة لوضع رؤية استراتيجية نموذجية متكاملة لمكافحة الجرائم الإلكترونية من زوايا مختلفة يمكن تطبيقها على كافة المستويات، والتي من شأنها حماية المجتمع من الشائعات والأخبار المضللة المثارة على مواقع التواصل الاجتماعي، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات وتعزيز الحفاظ على الأمن القومي -من خلال استطلاع آراء الخبراء والمتخصصين- عبر ثلاث جولات مختلفة بتطبيق أسلوب دلفي، وأسلوب التخطيط الاستراتيجي، وتوصلت الدراسة إلى: تعدد أسباب وأساليب انتشار تلك الجرائم، وتنوع تهديداتها على الأصعدة الاجتماعية والسياسية والأمنية والاقتصادية، كما تعددت الآليات المقترحة ما بين الآليات القانونية والأمنية والتقنية والإعلامية والتربوية والتعليمية، والفنية والدولية للحد من مخاطر وانتشار تلك الجرائم والحفاظ على الأمن السيبراني، وسلامة المجتمع وشبكات البنية الحيوية التحتية وتدعيمها بكل وسائل الأمن والحماية.

دراسة السياسات والقوانين المتعلقة بالجرائم الرقمية وكيفية تطبيقها.

أهمية السياسات والقوانين في مكافحة الجرائم الرقمية

تشكل الجرائم الرقمية تهديدًا خطيرًا للأمن الشخصي والمؤسسي على حد سواء. فالهجمات الإلكترونية يمكن أن تتسبب في خسائر مالية فادحة، وتضر بسمعة الأفراد والشركات، وتؤدي إلى سرقة معلومات حساسة. كما أن التحرش الإلكتروني والتشهير يمكن أن يؤثران سلبًا على الصحة النفسية للأفراد. لذا، فإن وجود سياسات وقوانين واضحة وصارمة لمكافحة هذه الجرائم يعد أمرًا بالغ الأهمية.

في هذا السياق، تسعى المملكة العربية السعودية إلى وضع وتنفيذ سياسات وقوانين تتماشى مع أفضل الممارسات الدولية. تشمل هذه القوانين نظام مكافحة جرائم المعلوماتية، ونظام حماية البيانات الشخصية، ونظام حماية حقوق المؤلف، بالإضافة إلى الأنظمة التي تنظم حقوق المستهلك في المعاملات الإلكترونية.

نظام مكافحة جرائم المعلوماتية

يعد نظام مكافحة جرائم المعلوماتية من أهم التشريعات التي أصدرتها المملكة لمكافحة الجرائم الرقمية. صدر هذا النظام بمرسوم ملكي رقم م/17 وتاريخ 1428/3/8 هـ، ويهدف إلى الحد من الجرائم المعلوماتية من خلال تحديد الأفعال المحظورة والعقوبات المترتبة عليها. يتضمن النظام مواد تجرم الدخول غير المشروع إلى المواقع الإلكترونية، والتنصت أو اعتراض الاتصالات، وتزوير المستندات الإلكترونية، والابتزاز الإلكتروني، والتشهير ونشر الأكاذيب.

يحدد النظام العقوبات التي تتراوح بين الغرامات المالية والسجن لفترات تصل إلى عشر سنوات، بناءً على خطورة الجريمة والأضرار الناتجة عنها. كما يتضمن النظام إجراءات لتحقيق وحماية حقوق الضحايا، مثل التبليغ عن الجرائم وتقديم الأدلة للسلطات المختصة.

نظام حماية البيانات الشخصية

مع تزايد الاعتماد على التكنولوجيا الرقمية، أصبحت حماية البيانات الشخصية ضرورة ملحة. يهدف نظام حماية البيانات الشخصية إلى ضمان عدم استخدام البيانات بطرق غير مشروعة، ويحمي خصوصية الأفراد من خلال تحديد الشروط والضوابط اللازمة لمعالجة البيانات الشخصية.

يشمل النظام متطلبات مثل الحصول على موافقة صريحة من الأفراد قبل جمع بياناتهم، وتوفير خيارات للمستخدمين للتحكم في كيفية استخدام بياناتهم، وضمان أمان البيانات من خلال تدابير تقنية وتنظيمية مناسبة. يعتبر هذا النظام خطوة مهمة نحو تعزيز الثقة في استخدام الخدمات الرقمية وحماية الحقوق الرقمية للأفراد.

نظام حماية حقوق المؤلف

يعد نظام حماية حقوق المؤلف جزءاً أساسياً من الإطار القانوني لحماية الإبداع والملكية الفكرية في العصر الرقمي. يحمي هذا النظام حقوق المؤلفين والمبدعين في أعمالهم الرقمية، ويشمل حماية الأعمال المنشورة على الإنترنت والنشر الإلكتروني.

يهدف النظام إلى تشجيع الإبداع والابتكار من خلال ضمان حقوق المبدعين ومنع الاستخدام غير المصرح به لأعمالهم. تشمل العقوبات المفروضة على المخالفين الغرامات المالية والسجن، بالإضافة إلى إمكانية المطالبة بتعويضات مالية عن الأضرار الناتجة عن انتهاك حقوق المؤلف.

نظام حماية المستهلك

مع انتشار التجارة الإلكترونية، أصبح حماية حقوق المستهلكين في المعاملات الإلكترونية أمراً بالغ الأهمية. ينظم نظام حماية المستهلك حقوق المستهلكين في المعاملات عبر الإنترنت، ويحدد مسؤولية التجار ومزودي الخدمات لضمان تقديم خدمات موثوقة وآمنة.

يهدف النظام إلى حماية المستهلكين من الاحتيال والتلاعب الإلكتروني، ويشمل إجراءات مثل توفير معلومات واضحة ودقيقة عن المنتجات والخدمات، وضمان حقوق الاسترجاع والاستبدال، وحماية البيانات الشخصية للمستهلكين.

الهيئة الوطنية للأمن السيبراني

تلعب الهيئة الوطنية للأمن السيبراني دوراً حيوياً في تعزيز الأمن السيبراني في المملكة العربية السعودية. تقوم الهيئة بوضع السياسات والإجراءات والتوجيهات اللازمة لحماية البنية التحتية الرقمية والمعلومات، وتعمل على تعزيز الوعي بالأمن السيبراني بين المواطنين والمؤسسات.

التحديات والحلول

تواجه مكافحة الجرائم الرقمية في المملكة تحديات عديدة، منها التطور السريع للتكنولوجيا الذي يتطلب تحديثاً مستمراً للقوانين والسياسات، بالإضافة إلى الحاجة لزيادة الوعي بين المواطنين حول مخاطر الجرائم الرقمية وكيفية الوقاية منها. لتجاوز هذه التحديات، تسعى المملكة إلى تطوير التشريعات بصفة دورية لتواكب التغيرات التكنولوجية، وتعزيز التعاون الدولي لمكافحة الجرائم العابرة للحدود، وتبادل المعلومات والخبرات مع الجهات الدولية. كما تنظم الحكومة حملات توعية وبرامج تدريبية لتثقيف المواطنين حول الأمان الرقمي وكيفية حماية أنفسهم من الجرائم الإلكترونية.

دراسة القضايا القانونية المرتبطة بالجرائم الرقمية، مثل التحقق من الهوية الرقمية وإنشاء الأدلة الرقمية والحفاظ على الخصوصية الإلكترونية.

في العالم الرقمي اليوم، أصبحت الجرائم الإلكترونية مصدر قلق كبير، حيث تطورت وتنوعت أشكالها مع التقدم التكنولوجي. تطرح هذه الجرائم تحديات قانونية معقدة تتطلب استجابة شاملة من الناحية القانونية والتقنية. في هذا السياق، تتناول هذه الدراسة القضايا القانونية المرتبطة بالجرائم الرقمية، بما في ذلك التحقق من الهوية الرقمية، وإنشاء الأدلة الرقمية، والحفاظ على الخصوصية الإلكترونية.

1. التحقق من الهوية الرقمية

التحديات:

سرقة الهوية: تُعد واحدة من الجرائم الرقمية الأكثر شيوعاً، حيث يمكن للمجرمين استخدام معلومات شخصية مسروقة للوصول إلى الحسابات المالية أو ارتكاب جرائم أخرى.

انتحال الهوية: يشمل انتحال شخصية الأفراد عبر الإنترنت لتحقيق مكاسب غير مشروعة أو للتشهير.

القوانين والسياسات:

نظام مكافحة جرائم المعلوماتية: يجرم استخدام المعلومات الشخصية بطرق غير مشروعة، ويحدد عقوبات صارمة على جرائم سرقة وانتحال الهوية.

أنظمة التحقق الإلكتروني: تتطلب اللوائح من المؤسسات المالية والتجارية استخدام تقنيات متقدمة للتحقق من هوية العملاء، مثل المصادقة الثنائية (2FA) والبصمات البيومترية.

الإجراءات:

استخدام تقنيات التشفير: لحماية البيانات الحساسة والتأكد من صحة الهوية الرقمية.

تعزيز الوعي: تثقيف الجمهور حول كيفية حماية معلوماتهم الشخصية وكيفية التعرف على محاولات سرقة الهوية.

2. إنشاء الأدلة الرقمية

التحديات:

قابلية التزوير: يمكن بسهولة تزوير الأدلة الرقمية مثل رسائل البريد الإلكتروني، والصور، والملفات الرقمية.

سلامة الأدلة: تتطلب الأدلة الرقمية إجراءات دقيقة لضمان عدم التلاعب بها أو فقدانها أثناء جمعها أو تخزينها أو نقلها. القوانين والسياسات:

نظام الإجراءات الجزائية: يحدد الإجراءات الواجب اتباعها لجمع الأدلة الرقمية وضمان سلامتها.

معايير الأدلة الرقمية: تُستخدم معايير دولية لضمان قبول الأدلة الرقمية في المحاكم، مثل معايير **ISO/IEC 27037** المتعلقة بإرشادات التعرف على الأدلة الرقمية وجمعها.

الإجراءات:

تدريب المحققين: توفير تدريب متخصص للمحققين في الجرائم الرقمية على كيفية جمع وتحليل الأدلة الرقمية بشكل صحيح. استخدام أدوات متقدمة: الاستعانة بأدوات وبرامج متخصصة لتحليل الأدلة الرقمية وتوثيقها.

3. الحفاظ على الخصوصية الإلكترونية

التحديات:

انتهاك الخصوصية: يشمل جمع البيانات الشخصية دون موافقة، واستخدامها بطرق غير مصرح بها. تسريب البيانات: يمكن أن يؤدي إلى أضرار كبيرة للأفراد والمؤسسات إذا لم يتم حماية البيانات بشكل كافٍ. القوانين والسياسات:

نظام حماية البيانات الشخصية: ينص على حقوق الأفراد في حماية بياناتهم الشخصية ويفرض واجبات على الجهات التي تجمع وتعالج هذه البيانات.

تشريعات الخصوصية: تتضمن قوانين محددة لحماية خصوصية الأفراد على الإنترنت، بما في ذلك الحصول على موافقة صريحة قبل جمع البيانات.

الإجراءات:

تدابير أمنية صارمة: تطبيق تدابير مثل التشفير، وجدران الحماية، وأنظمة كشف التسلل لحماية البيانات الحساسة. إدارة الوصول: التحكم في من يمكنه الوصول إلى البيانات الشخصية وضمان أنه مقتصر على الأشخاص المصرح لهم فقط. الحالات الدراسية في السعودية:

مثال 1: قضية اختراق وسرقة بيانات مصرفية

في إحدى القضايا الشهيرة في السعودية، تعرضت مؤسسة مالية لهجوم سيبراني أدى إلى سرقة بيانات حساسة للعملاء. تم القبض على الجناة باستخدام تقنيات تتبع رقمية متقدمة، وقدموا للمحاكمة بتهمة تشتمل خرق نظام مكافحة جرائم المعلوماتية.

مثال 2: قضية ابتزاز إلكتروني

تلقي أحد الأفراد تهديدات عبر البريد الإلكتروني من قبل مجهول يطالب بفدية مقابل عدم نشر صور شخصية. تم التعرف على الجاني من خلال تعقب البريد الإلكتروني المستخدم، وتقديمه للمحاكمة بموجب قانون الابتزاز الإلكتروني. التوصيات:

تعزيز الإطار القانوني:

تحديث التشريعات: بما يتماشى مع التطورات التقنية لضمان شموليتها وقدرتها على التعامل مع التهديدات الجديدة. التعاون الدولي: تعزيز التعاون مع الدول الأخرى لتبادل المعلومات والخبرات في مكافحة الجرائم الرقمية. تحسين الوعي والتدريب:

برامج التوعية: تنظيم حملات توعية لتثقيف المواطنين حول الجرائم الرقمية وكيفية حماية أنفسهم.

تدريب مستمر: توفير تدريب دوري للمحققين والقضاة على التعامل مع الأدلة الرقمية والتحقيق في الجرائم الإلكترونية. استخدام التكنولوجيا المتقدمة:

أدوات التحليل المتقدمة: استخدام أدوات تحليل البيانات الكبيرة والذكاء الاصطناعي للكشف عن الأنشطة المشبوهة ومنع الجرائم الرقمية.

تطوير الأنظمة الأمنية: الاستثمار في تطوير أنظمة أمان سببراني متقدمة لحماية البيانات والشبكات.

إن دراسة القضايا القانونية المرتبطة بالجرائم الرقمية تبرز أهمية وجود إطار قانوني متين وشامل يواكب التطورات التكنولوجية. تتطلب مكافحة الجرائم الرقمية التعاون بين الجهات القانونية والتقنية، وتعزيز الوعي العام، واستخدام التكنولوجيا المتقدمة لضمان بيئة إلكترونية آمنة وموثوقة. المملكة العربية السعودية تسعى بجدية لتعزيز قوانينها وسياساتها في هذا المجال، مما يجعلها نموذجاً يحتذى به في المنطقة.

القوانين المحلية والدولية المتعلقة بالجرائم الرقمية وكيفية تطبيقها في العمل القضائي.

في العصر الرقمي، أصبحت الجرائم الإلكترونية تهديداً عالمياً يتطلب تعاوناً دولياً وإطاراً قانونياً محلياً ودولياً لمواجهته. تتناول هذه الدراسة القوانين المحلية والدولية المتعلقة بالجرائم الرقمية وكيفية تطبيقها في العمل القضائي، مع التركيز على المملكة العربية السعودية كدراسة حالة سوف نتعرف عنها بالتفصيل.

القوانين المحلية

1. نظام مكافحة جرائم المعلوماتية

صدر بمرسوم ملكي رقم م/17 وتاريخ 1428/3/8هـ، ويهدف إلى الحد من الجرائم المعلوماتية من خلال تجريم الأفعال المحظورة وتحديد العقوبات المترتبة عليها. يشمل النظام:

الدخول غير المشروع إلى الأنظمة الإلكترونية.

التنصت واعتراض الاتصالات.

تزوير المستندات الإلكترونية.

الابتزاز والتشهير الإلكتروني.

نشر البرمجيات الضارة.

العقوبات تتراوح بين الغرامات المالية والسجن لفترات تصل إلى عشر سنوات.

2. نظام حماية البيانات الشخصية

يهدف إلى حماية بيانات الأفراد وضمان عدم استخدامها بطرق غير مشروعة. يشمل النظام متطلبات مثل:

الحصول على موافقة الأفراد قبل جمع البيانات.

توفير خيارات للمستخدمين للتحكم في بياناتهم.

ضمان أمان البيانات من خلال تدابير تقنية وتنظيمية.

3. نظام مكافحة الجرائم الإلكترونية

يحدد هذا النظام الأحكام والعقوبات المتعلقة بالجرائم الإلكترونية، بما في ذلك:

الغرامات المالية.

السجن.

4. الهيئة الوطنية للأمن السيبراني

تعمل على وضع السياسات والإجراءات لحماية البنية التحتية الرقمية والمعلومات.

القوانين الدولية

1. اتفاقية بودابست (اتفاقية الجرائم الإلكترونية)

وهي المعاهدة الدولية الوحيدة التي تسعى إلى معالجة الجرائم الإلكترونية بشكل شامل. تهدف إلى:

توحيد التشريعات الوطنية.

تعزيز التعاون الدولي.

تسهيل تبادل المعلومات.

2. لائحة حماية البيانات العامة للاتحاد الأوروبي (GDPR)

تهدف إلى حماية البيانات الشخصية لمواطني الاتحاد الأوروبي، وتشمل: قواعد صارمة لجمع ومعالجة البيانات الشخصية.

حقوق الأفراد في الوصول إلى بياناتهم وتصحيحها وحذفها.

3. مبادئ الأمم المتحدة للتعاون في مكافحة الجرائم الإلكترونية

تضع إطارًا للتعاون الدولي في مكافحة الجرائم الإلكترونية، وتدعو الدول إلى: تعزيز التعاون بين الأجهزة الأمنية.

تبادل المعلومات والخبرات.

التنسيق في التحقيقات والملاحقات القضائية.

كيفية تطبيق القوانين في العمل القضائي

1. الإجراءات القضائية في المملكة العربية السعودية

التبليغ والتحقيق: يمكن للمواطنين التبليغ عن الجرائم الرقمية عبر تطبيق "كلنا أمن". تقوم الجهات المختصة بالتحقيق وجمع الأدلة الرقمية.

المحاكمة والعقوبات: تقدم الأدلة الرقمية في المحاكم، وتصدر الأحكام بناءً على الأدلة المقدمة. تتراوح العقوبات بين الغرامات المالية والسجن.

التعاون الدولي: تستفيد المملكة من اتفاقيات التعاون الدولي لتبادل المعلومات وملاحقة الجناة عبر الحدود.

2. إجراءات جمع وتحليل الأدلة الرقمية

حفظ الأدلة الرقمية: يجب جمع الأدلة الرقمية بطريقة تحفظ سلامتها وتمنع التلاعب بها.

استخدام تقنيات متقدمة: تعتمد الجهات المختصة على تقنيات حديثة لتحليل البيانات الرقمية وتتبع الأنشطة غير المشروعة. شهادة الخبراء: يمكن الاستعانة بخبراء في الجرائم الرقمية لتقديم الشهادات الفنية في المحاكم.

3. حماية الخصوصية

التوازن بين إنفاذ القانون وحماية الخصوصية: يجب أن توازن الإجراءات القضائية بين مكافحة الجرائم الرقمية وحماية خصوصية الأفراد.

الامتثال للمعايير الدولية: تلتزم الجهات القضائية بالمعايير الدولية لحماية البيانات أثناء جمع وتحليل الأدلة.


التحديات والحلول

➤ التحديات

التطور السريع للتكنولوجيا: يصعب على القوانين مواكبة التطورات التكنولوجية المستمرة.
التعاون الدولي: قد تكون هناك عقبات في التعاون الدولي نتيجة اختلاف القوانين والثقافات.
التوازن بين الأمن والخصوصية: الحفاظ على توازن بين إنفاذ القانون وحماية حقوق الأفراد يمثل تحديًا كبيرًا.

➤ الحلول

تحديث التشريعات بانتظام: يجب تحديث القوانين بشكل دوري لمواكبة التطورات التكنولوجية.
تعزيز التعاون الدولي: ضرورة تعزيز التعاون بين الدول من خلال الاتفاقيات الدولية وتبادل المعلومات والخبرات.
التوعية والتدريب: تنظيم حملات توعية وتدريب للقضاة والمحققين على التعامل مع الجرائم الرقمية والأدلة الإلكترونية.
تعد القوانين والسياسات المتعلقة بالجرائم الرقمية جزءًا أساسيًا من الجهود المبذولة لمكافحة التهديدات الإلكترونية وحماية المجتمع. في المملكة العربية السعودية، يتم تطبيق إطار قانوني شامل يتضمن نظام مكافحة جرائم المعلوماتية، ونظام حماية البيانات الشخصية، ونظام حماية حقوق المؤلف، بالإضافة إلى التعاون الدولي من خلال الاتفاقيات العالمية مثل اتفاقية بودابست. من خلال تحديث التشريعات وتعزيز التعاون الدولي والتوعية العامة، تسعى المملكة إلى خلق بيئة رقمية آمنة وموثوقة تحمي حقوق الأفراد والمؤسسات وتضمن استخدام الإنترنت بشكل مسؤول.



الوحدة الثامنة

مراجعة شاملة لمادة الجرائم الرقمية



مراجعة شاملة لمادة الجرائم الرقمية

الجرائم الرقمية أصبحت واحدة من أبرز التحديات في العصر الحديث، حيث يتزايد اعتماد الأفراد والمؤسسات على التكنولوجيا والإنترنت. تتنوع الجرائم الرقمية وتشمل الاحتيال الإلكتروني، التسلل إلى الأنظمة، التجسس، التزييف الإلكتروني، والابتزاز الرقمي. تمثل هذه الجرائم تهديدًا كبيرًا للأمن السيبراني، وتتطلب استجابة قانونية وتقنية شاملة. هذه المراجعة تغطي التعرف على الجرائم الرقمية، التحقيق فيها، الأمن السيبراني، الحماية، الجرائم المرتبطة بوسائل التواصل الاجتماعي، والسياسات والقوانين المتعلقة بالجرائم الرقمية.

تعرفنا على الجرائم الرقمية هي أنشطة غير قانونية تُرتكب باستخدام التكنولوجيا الرقمية، وتستهدف الأنظمة الإلكترونية والمعلومات الشخصية. تشمل الأنواع الشائعة من الجرائم الرقمية الاحتيال عبر الإنترنت، التسلل إلى الأنظمة، التجسس الإلكتروني، التزييف، والابتزاز الرقمي. لكل نوع من هذه الجرائم تأثيرات مختلفة على الأفراد والمؤسسات، تتراوح من الخسائر المالية إلى الأضرار بسمعة الشركات.

التحقيق في الجرائم الرقمية يتطلب مهارات ومعرفة تقنية متقدمة. يبدأ التحقيق بجمع الأدلة الرقمية من أجهزة الحاسوب، الهواتف الذكية، والشبكات. يتبع ذلك تحليل الأدلة باستخدام أدوات وتقنيات متخصصة لتحديد مصدر الجريمة وكيفية ارتكابها. المحققون يواجهون تحديات متعددة مثل التشفير، إخفاء الهوية، وتعدد المواقع الجغرافية للمجرمين.

الأمن السيبراني والحماية يمثل خط الدفاع الأول ضد الجرائم الرقمية. يشمل الأمن السيبراني حماية الأنظمة والشبكات من التهديدات الإلكترونية من خلال استخدام تقنيات مثل التشفير، الجدران النارية، وأنظمة كشف التسلل. استراتيجيات الأمن السيبراني تشمل الوقاية، الكشف، الاستجابة، والتعافي من الهجمات السيبرانية. الحماية الشخصية تتطلب من الأفراد اتباع ممارسات أمان جيدة مثل استخدام كلمات مرور قوية، تحديث البرمجيات بانتظام، وتجنب الروابط المشبوهة.

الجرائم المرتبطة بوسائل التواصل الاجتماعي أصبحت ساحة جديدة للجرائم الرقمية. تشمل الجرائم الشائعة التحرش الجنسي، التشهير، والابتزاز عبر وسائل التواصل الاجتماعي. يمكن أن تتسبب هذه الجرائم في أضرار نفسية واجتماعية كبيرة للضحايا. لمكافحة هذه الجرائم، يجب تعزيز التوعية حول أمان الإنترنت وتشجيع الإبلاغ عن أي أنشطة مشبوهة.

السياسات والقوانين المتعلقة بالجرائم الرقمية و تنقسم لقوانين محلية ودولية وتمثلان دورًا حاسمًا في مكافحة الجرائم الرقمية. في المملكة العربية السعودية، يشمل نظام مكافحة جرائم المعلوماتية، ونظام حماية البيانات الشخصية، واللوائح المتعلقة بحماية المستهلك. دولياً، تتضمن التشريعات اتفاقية بودابست، ولائحة حماية البيانات العامة للاتحاد الأوروبي (GDPR)، ومبادئ الأمم المتحدة للتعاون في مكافحة الجرائم الإلكترونية. تطبيق هذه القوانين يتطلب تعاونًا دوليًا وتحديثًا مستمرًا للتشريعات لمواكبة التطورات التكنولوجية.

دراسة القضايا القانونية المرتبطة بالجرائم الرقمية والتحقق من الهوية الرقمية، إنشاء الأدلة الرقمية، والحفاظ على الخصوصية الإلكترونية. يجب على المحققين ضمان جمع الأدلة بشكل قانوني وسليم لحمايتها من التلاعب. الخصوصية الإلكترونية تمثل تحديًا آخر، حيث يجب تحقيق توازن بين حماية البيانات الشخصية وإنفاذ القانون.

كيفية جمع الأدلة الرقمية وتحليلها وتقييمها: جمع الأدلة الرقمية يتطلب استخدام تقنيات متقدمة للحفاظ على سلامة الأدلة. الأدوات المستخدمة تشمل برامج استعادة البيانات، تحليل الشبكات، وتقنيات التعقب الرقمي. يجب أن يتم تحليل الأدلة وتقييمها بدقة لتقديمها في المحاكم، وضمان أنها تتماشى مع المعايير القانونية.

كيفية تطبيق الأساليب القانونية في مكافحة الجرائم الرقمية

تطبيق الأساليب القانونية يشمل التحقيق، جمع الأدلة، والتعاون الدولي. يجب على الجهات القضائية العمل مع خبراء التقنية لضمان جمع الأدلة وتحليلها بشكل صحيح. التعاون مع الدول الأخرى عبر الاتفاقيات الدولية يساهم في ملاحقة المجرمين عبر الحدود.

الجرائم الرقمية تتطلب استجابة شاملة من الناحية القانونية والتقنية. القوانين والسياسات المحلية والدولية تلعب دورًا حيويًا في مكافحة هذه الجرائم. يجب تعزيز التوعية والتدريب المستمر للمحققين والمدعين العامين، وتحديث التشريعات بانتظام لمواكبة التطورات التكنولوجية. من خلال التعاون الدولي واستخدام التقنيات المتقدمة، يمكن مواجهة التحديات المتعلقة بالجرائم الرقمية وحماية الأفراد والمؤسسات من التهديدات الإلكترونية.

Adam M. Bossler و Thomas J. Holt "Cybercrime and Digital Forensics: An Introduction"	١-	المراجع
Marjie T. Britz "Computer Forensics and Cyber Crime: An Introduction.	٢-	
Majid Yar "Cybercrime and Society.	٣-	