الأكاديمية العربية الدولية
Arab International Academy

إسم المادة: تقنيات الأدلة الجنائية الرقمية وأدواتها

إسم المحاضر : ماهر السهلي

الأكاديمية العربية الدولية – منصة أعد

الفهرس

الفهرس

الفهرس

المقدمة

تقنيات الأدوات الجنائية الرقمية هي مجموعة من الأدوات والتقنيات التي تستخدم في مجال الجرائم الإلكترونية والتحقيقات الجنائية المتعلقة بها. تشمل هذه التقنيات استخدام الحوسبة السحابية، والتحليل الرقمي، واسترجاع البيانات، والتحقق من الهوية الرقمية، والتحليل الجنائي للشبكات والأجهزة.

تعد تقنيات الأدوات الجنائية الرقمية أدوات حاسمة في التحقيقات الجنائية الرقمية، حيث تساعد في جمع الأدلة الرقمية وتحليلها لكشف الجرائم وتحديد المشتبه بهم. تستخدم هذه التقنيات في مجموعة متنوعة من المجالات، بما في ذلك التحقيقات الجنائية، والأمن السيبراني، والتحقيقات الرقمية في المؤسسات.

الفكرة العامة

تشمل تقنيات الأدوات الجنائية الرقمية مجموعة واسعة من الأدوات والبرامج المتخصصة، مثل برامج استرجاع البيانات المحذوفة، وبرامج استعادة كلمات المرور، وبرامج تحليل الشبكات والأجهزة، وبرامج التحقق من الهوية الرقمية، وغيرها. تتطلب استخدام هذه الأدوات مهارات تقنية متقدمة وخبرة في مجال التحقيقات الجنائية الرقمية.

باستخدام تقنيات الأدوات الجنائية الرقمية، يمكن للمحققين استخلاص البيانات من الأجهزة الرقمية، مثل الهواتف الذكية والحواسيب، وتحليلها لاستخلاص المعلومات المفيدة في التحقيقات. يمكن استخدام هذه التقنيات لتحديد مصادر الهجمات السيبرانية، وتتبع الأنشطة غير المشروعة على الشبكة، واستعادة الملفات المحذوفة، والتحقق من صحة البيانات الرقمية.

تقنيات الادلة الجنائية الرقمية وادواتها

تقنيات الأدلة الجنائية الرقمية هي الأدوات والتقنيات التي تستخدم في جمع وتحليل وتقديم الأدلة الرقمية في التحقيقات الجنائية. وتشمل هذه التقنيات عدة محاور، بما في ذلك:

1. استعادة البيانات: تستخدم لاستعادة البيانات المحذوفة أو المخفية عن الأجهزة الرقمية، مثل الهواتف الذكية أو أجهزة الكمبيوتر.
2. تحليل البيانات: يتضمن تحليل البيانات المستخرجة من الأجهزة الرقمية لتحديد المعلومات المفيدة للتحقيق، مثل الصور والرسائل والسجلات.
3. استخراج الأدلة الرقمية: يتضمن استخراج الأدلة الرقمية من الأجهزة الرقمية، مثل الصور والفيديوهات والرسائل والسجلات.

محاور تقنيات الادلة الجنائية الرقمية وادواتها

4. تحليل الميتاداتا: يتضمن تحليل الميتاداتا المرتبطة بالملفات الرقمية، مثل توقيت الإنشاء والتعديل والوصول إلى الملفات.

5. التحقق الرقمي: يتضمن التحقق من صحة الأدلة الرقمية وتأكيد أصالتها وعدم تلاعبها.

أدوات تقنيات الأدلة الجنائية الرقمية

1. برامج استعادة البيانات: مثل EnCase و FTK و Recuva.

2. برامج تحليل البيانات: مثل Autopsy و Oxygen Forensic Detective و Cellebrite UFED.

3. برامج استخراج الأدلة الرقمية: مثل X-Ways Forensics و Magnet AXIOM و FTK Imager.

4. أدوات تحليل الميتاداتا: مثل ExifTool و Bulk Extractor و Metadata Analyzer.

ما علاقة تحليل البيانات بادوات الادلة الجنائية

تحليل البيانات يعتبر جزءًا أساسيًا من أدوات الأدلة الجنائية الرقمية. فعند جمع البيانات الرقمية من أجهزة الكمبيوتر والهواتف الذكية والأقراص الصلبة، يتم استخدام برامج تحليل البيانات لاستخلاص المعلومات القيمة والأدلة من هذه البيانات.

شمولية تحليل البيانات

تحليل البيانات يشمل استخلاص المعلومات المفيدة والأدلة من الملفات والمجلدات والرسائل الإلكترونية وسجلات الاتصال والوسائط المتعددة الأخرى. يتم استخدام تقنيات مختلفة في تحليل البيانات مثل تحليل النصوص، واستخلاص المعلومات، وتحليل الصور والفيديو، وتحليل البيانات المتعلقة بالتوقيت والموقع الجغرافي، وغيرها.

استخدام أدوات تحليل البيانات

يمكن للمحققين الجنائيين الرقميين تحليل البيانات المستخرجة بشكل أفضل واستخلاص المعلومات القيمة والأدلة التي يمكن استخدامها في التحقيقات الجنائية. يساعد تحليل البيانات في فهم السياق والتوجهات والعلاقات بين البيانات المستخرجة، وبالتالي يسهم في بناء حجة قوية ودقيقة في التحقيقات الجنائية.

كيف تحلل البيانات للادلة الجنائية الرقمية

تحليل البيانات للأدلة الجنائية الرقمية يتطلب استخدام أدوات وتقنيات متخصصة. فيما يلي خطوات عامة لتحليل البيانات للأدلة الجنائية الرقمية:

1. جمع البيانات: يجب جمع جميع البيانات المتاحة ذات الصلة بالتحقيق من أجهزة الكمبيوتر والهواتف الذكية والأقراص الصلبة وأي وسائط أخرى.

2. تنظيم البيانات: يجب تنظيم البيانات المجمعة بطريقة منظمة وهيكلية لتسهيل التحليل والاستخلاص.

3. استخلاص المعلومات: يتم استخدام تقنيات استخلاص المعلومات لتحديد المعلومات القيمة والأدلة من البيانات المجمعة. هذا يشمل استخدام تقنيات مثل تحليل النصوص والكشف عن الأنماط والتصنيف.

كيف تحلل البيانات للأدلة الجنائية الرقمية

4. تحليل البيانات: يتم استخدام تقنيات تحليل البيانات لفهم السياق والعلاقات بين البيانات المجمعة. يمكن استخدام تقنيات مثل تحليل الصور والفيديو وتحليل البيانات المتعلقة بالتوقيت والموقع الجغرافي.

5. تحليل الأدلة: يتم تحليل الأدلة المستخرجة من البيانات بشكل مفصل لتحديد قوة الأدلة وقابليتها للاستخدام في التحقيقات الجنائية. يمكن استخدام تقنيات التحقق والتحليل المتقدمة لتحديد صحة الأدلة وتوثيقها.

6. إعداد التقارير: يجب إعداد تقارير مفصلة تشرح نتائج التحليل والأدلة المستخرجة. يجب أن تكون التقارير دقيقة وشاملة وقابلة للفهم للاستخدام في التحقيقات الجنائية.

كيف تحلل البيانات للأدلة الجنائية الرقمية

7. الشهادة كشاهد: في بعض الأحيان، يمكن أن يُطلب من المحقق الجنائي الرقمي أن يشهد في المحكمة ويقدم توضيحات حول التحليل والأدلة المستخرجة.

تحليل البيانات للأدلة الجنائية الرقمية يتطلب الخبرة والمهارات الفنية في استخدام أدوات التحليل وفهم تقنيات الاستخلاص وتحليل البيانات. يجب أن يتم تنفيذ هذه العمليات بدقة وحسب المعايير والقوانين القانونية ذات الصلة.

المبادئ التوجيهية العالمية الخاصة بمختبرات الأدلة الجنائية الرقمية

تم تطوير المبادئ التوجيهية العالمية الخاصة بمختبرات الأدلة الجنائية الرقمية من قبل منظمة الشرطة الجنائية الدولية (الإنتربول) والمنظمة الدولية للشرطة الجنائية (الأيسيب). تهدف هذه المبادئ إلى توفير إرشادات عالمية لتشغيل وإدارة مختبرات الأدلة الجنائية الرقمية بطريقة موحدة ومهنية. وتشمل المبادئ التوجيهية العناصر التالية:

1. التأكد من الجودة والموثوقية: يتعين على مختبرات الأدلة الجنائية الرقمية تطبيق معايير صارمة لضمان جودة وموثوقية عملها، بما في ذلك استخدام أدوات وتقنيات معتمدة وفعالة.

2. التدريب والتأهيل: يجب أن يكون لدى فرق المختبر المهارات والمعرفة اللازمة للقيام بالتحقيقات الجنائية الرقمية بشكل فعال. يجب توفير التدريب المستمر والتأهيل المهني لأعضاء الفريق.

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

للجريمة الالكترونية تعريفات مختلفة ووصف متباين بحسب نظرة الشخص وخلفيته، فهي غالباً مرتبطة بكيان معنوي ذو قيمة مادية كبيرة، وغالبا ما تكون الاعتداءات على الكيانات المعنوية المتعلقة بقيمتها الإستراتيجية كمخازن المعلومات.

و للجرائم الالكترونية مسميات عدة منها جرائم التقنية العالية، جرائم الكمبيوتر والانترنت، جرائم أصحاب الياقات البيضاء ، وبالرغم من أن هذا المسمى يشمل طوائف متعددة من الجرائم إلا أن الجريمة الالكترونية تعتبر جزء من هذه الطوائف، كما أن لها تصنيفات عدة تختلف بحسب اختلاف معايير التصنيف.

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

نظام مكافحة جرائم المعلوماتية

يقصد بالألفاظ والعبارات الآتية ـ أينما وردت في هذا النظام ـ المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

1ـ الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.

2ـ النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

3ـ الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية /الإنترنت/ .
4ـ البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

شهد العالم تطورا تقنيا في شتى المجالات, ولعل أبرز هذه المجالات مجال الحساب الآلي والأجهزة الرقمية الذي يشهد تطورا متسارعا ومذهلا. ومع ما جلبه هذا التطور للبشرية من الخيرات والتسهيلات, إلا أنه جلب أيضا أصنافا جديدة من الجرائم لم تكن معهودة من قبل أو ساعد في حدوث بعض الجرائم. وهنا استدعت الحاجة رجال القانون إلى وجوب التعامل مع هذه المستجدات وفقا لأساليب قانونية وبطرق تقنية.

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

ثمة جمله من الصعوبات والعوائق تعترض سبيل اكتشاف جرائم الحاسب الآلي لعدة أسباب تتعلق بخصوصية هذه الجرائم العصرية فمنها ما يعود إلى قدرة الجاني في طمس معالم جريمته , وذلك بتدمير الأداة التي من الممكن أن تتخلف عنها , ومنها ما يعود إلى عدم تخلف الأدلة المادية أصلا كالتي تتخلف في الجرائم التقليدية, ومنها ما يعود إلى طبيعة المحل الذي ترد علية كونها معلومات مرمزة ومشفرة , ومنها ما يعود إلى قلة خبرة أجهزة العدالة الجنائية التي تتعامل مع هذه الجرائم أو منها ما يعود إلى طبيعة النظام الذي يعمل به الحاسب الآلي , ومنها أيضا ما يعود إلى الجهات التي تتعرض لمثل هذه الاعتداءات والتي غالبا ما تكون مؤسسات وشركات تجارية أو جهات مالية ومصرفية تؤثر الصمت على الإبلاغ عن الجريمة خوفا من أن تهز ثقة عملاءها. وسوف أقوم بتسليط الضوء على بعض هذه الصعوبات والأسباب في مقالتي هذه للتوعية بخصوصية هذا النوع من الجرائم وضرورة التوجه الجاد للتصدي لها ومكافحتها

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

كما أدخل الحاسوب والإنترنت خدمات وتسهيلات ومعارف بل ومصطلحات جديدة فقد أعطيا عالم الجريمة أبعاداً جديدة، فصار من الممكن ارتكاب جريمة اختلاس أو سرقة أو تزوير عن بعد، وأصبحت وسائل الأمن والحماية المحسوسة من حراسات وصناديق حفظ وأماكن تخزين لا تكفي وحدها لحماية المعلومات من اللصوص. وظهر مصطلح (((Cybercrime الذي يعني الجرائم التي ترتكب باستخدام الحاسوب وشبكة الإنترنت. وقد وصل الأمر إلى أن الحكومة الأمريكية أطلقت في فبراير 2003م مبادرة لحماية المجال المعلوماتي القومي الأمريكي أسمتها

National Strategy to Secure Cyberspace، و قد حذا عدد من الدول حذوها. ومما ينبغي ذكره في هذا المقام أن من المشروعات المقترحة في الخطة الوطنية لتقنية المعلومات في المملكة العربية السعودية مشروع إنشاء مركز وطني لأمن المعلومات، ومشروع إنشاء وحدة خاصة للمتابعة والتحقيق في المخالفات المتعلقة بأمن المعلومات

الجرائم الإلكترونية والأدلة الجنائية الإلكترونية

تساعد تقنية التصوير والتسجيل بالكاميرات الرقمية في الحد من الجرائم بشكل كبير، ويتم استخدام هذه التقنية في العديد من الدول ففي ألمانيا هناك ما يقارب مليون وستمائة ألف كاميرا، وفي بريطانيا يوجد في الأماكن العامة ما يزيد عن أربعة ملايين ومائتي ألف كاميرا بمعدل كاميرا لكل 14 مواطن، وهذا العدد يمثل 20% من الكاميرات المعدة لهذا الغرض في العالم وبذلك تكون بريطانيا من أكثر الدول استخداماً لهذه التقنية، أما بقية الدول الأوربية ففيها ما يقارب ستة ملايين وخمسمائة ألف كاميرا. وهذه التقنية تتطور بشكل سريع حيث تم تطوير جهاز ذكي يتكون من ثمان كاميرات ويقوم بمراقبة أي حركة غير طبيعية أو أي مخالفة كرمي النفايات ويلفت نظر المسئولين لها. كاميرات المراقبة في الغالب تقوم بالتسجيل لمدد طويلة ويتم الرجوع لها عند الحاجة، وفي حالات أخرى تتم للمراقبة الفورية خصوصاً في الأسواق.

كيف تعرف الأدلة الجنائية

تُعد البيانات المستقاة من الأدلة الجنائية، كبصمات الأصابع والبصمة الوراثية مثلاً، فريدة من نوعها وتعود لشخص واحد دون سواه عموماً، وهي بالتالي قادرة على تأكيد هوية شخص ما وتواجده في مسرح الجريمة. والأهم أيضاً أنها تساعد على إثبات براءة المشتبه بهم.

ويمكن كذلك استخدام البيانات المستقاة من الأدلة الجنائية على الصعيد الدولي للربط بين سلسلة من الجرائم عبر الوطنية، فيمكن مثلاً التدقيق سريعاً في بصمات الأصابع لدى عبور مشتبه به للحدود بين بلدين. كما تساعدنا هذه البيانات في تحديد هوية الضحايا في أعقاب وقوع كارثة كبرى.

كيف تعرف الأدلة الجنائية

وبات التعرف إلى الوجوه علماً بيومترياً سريع التطور يتيح لنا كماً كبيراً من الفرص الجديدة لتبيان هوية المشتبه بهم وحل الجرائم.

ونتدبر في الإنتربول قواعد البيانات الجنائية التي تتضمن ما توفره لنا البلدان الأعضاء من بصمات الأصابع وسمات البصمات الوراثية وصور عن الوجوه، بما يسمح لأجهزة الشرطة في جميع أنحاء العالم بالربط بين المجرمين ومسارح الجريمة. ونتولى كذلك تدريب الموظفين العاملين في خطوط المواجهة على تقييم الأدلة والحفاظ عليها وتشاركها مع جهات أخرى بما يتماشى مع الممارسات الفضلى المعتمَدة.

كيف تتم استعادة البيانات في الادلة الرقمية الجنائية

استعادة البيانات في الأدلة الجنائية الرقمية يتطلب استخدام أدوات استعادة البيانات المتخصصة. فيما يلي بعض الخطوات العامة لاستعادة البيانات:

1. تحديد الأجهزة: قم بتحديد الأجهزة التي قد تحتوي على البيانات المحذوفة أو المخفية المرتبطة بالجريمة. يمكن أن تشمل هذه الأجهزة أجهزة الكمبيوتر والهواتف الذكية والأقراص الصلبة والأقراص المدمجة.

2. اتخاذ التدابير اللازمة: قبل استعادة البيانات، يجب اتخاذ التدابير اللازمة لضمان سلامة الأجهزة والبيانات. يمكن استخدام تقنيات مثل صندوق التجزئة المحكم (Write Blocker) لمنع أي تغيير في البيانات أثناء عملية الاستعادة.

كيف تتم استعادة البيانات في الادلة الرقمية الجنائية

3. استخدام أدوات استعادة البيانات: قم باستخدام أدوات استعادة البيانات المتخصصة لاستعادة البيانات المحذوفة أو المخفية. هذه الأدوات تعمل على تحليل القرص الصلب واستعادة البيانات المفقودة.

4. التحليل والتصنيف: بمجرد استعادة البيانات، قم بتحليلها وتصنيفها وتنظيمها وفقًا للمعلومات المهمة للقضية. يمكن استخدام برامج التحليل الرقمي لفحص البيانات وتحديد المعلومات ذات الصلة.

5. التحقق من صحة البيانات: قم بالتحقق من صحة البيانات المستعادة والتأكد من أنها غير مزورة أو معدلة. يمكن استخدام تقنيات التوقيع الرقمي والتحليل المتقدم للتأكد من صحة البيانات.

كيف تتم استعادة البيانات في الادلة الرقمية الجنائية

6. توثيق العملية: قم بتوثيق جميع الخطوات التي تم اتخاذها لاستعادة البيانات، بما في ذلك الأدوات المستخدمة والنتائج المحققة. يجب أن يكون هناك سلاسل سلسلة من الحوادث لتحديد من يدير ويتحكم في البيانات.

7. تقديم التقارير: قم بإعداد تقارير تفصيلية تشرح عملية استعادة البيانات والنتائج التي تم الوصول إليها. يجب أن تكون التقارير مفهومة وشاملة وتوضح المعلومات المستعادة وطريقة الاستعادة.

تذكر أن استعادة البيانات في الأدلة الجنائية الرقمية يتطلب خبرة ومهارات تحليلية قوية لضمان استعادة البيانات بدقة وامتثال

كيف يتم التحقق من صحة البيانات في الأدلة الرقمية الجنائية

في السياق الجنائي، يشير مصطلح "الدل" إلى الأدلة الرقمية أو الإلكترونية التي يتم جمعها واستخدامها في التحقيقات الجنائية. وتشمل هذه الأدلة الرسائل الإلكترونية، وسجلات المكالمات، والصور والفيديوهات الرقمية، والتسجيلات الصوتية، والبيانات المستخرجة من أجهزة الكمبيوتر والهواتف الذكية، وغيرها.

للتحقق من صحة البيانات في الأدلة الرقمية، تعتمد العديد من الطرق والتقنيات، بما في ذلك

1. التحقق من صحة البيانات المستخرجة: يتم استخراج البيانات الرقمية من الأجهزة المحجوزة بواسطة أدوات خاصة مثل برامج استرداد الملفات أو تقنيات الاستعادة المتقدمة. يجب على المحققين التحقق من صحة هذه البيانات والتأكد من أنها لم تتعرض للتلاعب أو التغيير.

كيف يتم التحقق من صحة البيانات في الأدلة الرقمية الجنائية

2. التحقق من الأصالة: يجب التحقق من أن الأدلة الرقمية لم تتعرض للتزوير أو التلاعب. يتم ذلك من خلال فحص البيانات المستخرجة للتأكد من أنها تمثل الحالة الأصلية وأنها لم تتعرض لأي تغييرات غير مشروعة.

3. التحقق من توقيت البيانات: يجب التحقق من صحة ودقة توقيت البيانات الرقمية، مثل توقيت إنشاء الملفات أو إرسال الرسائل الإلكترونية. يمكن استخدام التوقيعات الرقمية والسجلات الزمنية وغيرها من التقنيات للتحقق من ذلك.

4. التحقق من مصدر البيانات: يجب التحقق من مصدر البيانات الرقمية ومصداقيته. يتم ذلك عن طريق فحص سجلات النشاط والمعلومات المتاحة حول المستخدمين والأجهزة المستخدمة.

كيف يتم التحقق من صحة البيانات في الأدلة الرقمية الجنائية

5. التحقق من سلامة البيانات: يجب التحقق من أن البيانات الرقمية لم تتعرض لأي تلف أو فقدان أثناء جمعها أو نقلها أو تخزينها. يتم ذلك من خلال فحص البيانات للتأكد من عدم وجود أخطاء أو تلاشي فيها.

تتطلب عملية التحقق من صحة البيانات الرقمية مهارات فنية وتقنية متخصصة، وعادة ما يتم تنفيذها بواسطة خبراء الأدلة الرقمية أو المحققين الجنائيين المتخصصين.

كيف تقدم التقارير للأدلة الجنائية الرقمية

تقديم التقارير للأدلة الجنائية الرقمية يتطلب اتباع إجراءات محددة واستخدام تنسيقات معينة. فيما يلي بعض الخطوات التي يمكن اتباعها:

1. جمع الأدلة: يجب جمع جميع الأدلة الرقمية ذات الصلة بالجريمة المحتملة. قد تشمل هذه الأدلة نسخًا من الملفات، وسجلات الإنترنت، وصور الشاشة، والبريد الإلكتروني، والرسائل النصية، وغيرها.

2. توثيق الأدلة: يجب توثيق جميع الأدلة المجمعة بدقة. يجب تسجيل التواريخ والأوقات، والمصادر، وأي تغييرات أو تلاعب في الأدلة.

3. تحليل الأدلة: يتم تحليل الأدلة الرقمية لاستخلاص المعلومات المفيدة والحصول على فهم أفضل للجريمة المحتملة. يمكن استخدام برامج تحليل الأدلة الرقمية لتسهيل هذه العملية.

كيف تقدم التقارير للأدلة الجنائية الرقمية

4. كتابة التقارير: بعد تحليل الأدلة، يجب كتابة تقارير مفصلة تشرح النتائج والاستنتاجات. يجب أن تكون التقارير مدعمة بالأدلة المستخدمة وتوضح الطرق المستخدمة في التحليل.

5. توثيق السلسلة القانونية: يجب توثيق سلسلة الحفاظ على الأدلة منذ جمعها حتى تقديمها كدليل قانوني. يجب أن يكون هناك سجل دقيق لكل خطوة وتغيير تم على الأدلة

6. التدقيق والتحقق: يجب أن يتم التدقيق والتحقق من التقارير والأدلة المقدمة لضمان صحتها وصلاحيتها كدليل قانوني

يجب أن يتم اتباع إرشادات وإجراءات الادلة الجنائية الرقمية المعتمدة في الدولة أو المنظمة المعنية لضمان تقديم التقارير بشكل صحيح وقانوني.

تعريف الجرائم ذات الدليل الجنائي الرقمي

الجرائم ذات الدليل الجنائي الرقمي هي الجرائم التي يتم استخدام أو تنفيذها باستخدام التكنولوجيا الرقمية، وبالتالي يترك الجاني أو المشتبه به أدلة رقمية تشير إلى ارتكابه للجريمة. تشمل هذه الجرائم على سبيل المثال لا الحصر:

- اختراق الأجهزة الإلكترونية وسرقة المعلومات الشخصية أو المالية.
- توزيع وتبادل المواد الإباحية عبر الإنترنت.
- احتيال الهوية الرقمية وسرقة معلومات الدخول إلى حسابات المستخدمين.
- التلاعب بالبيانات وتغييرها للإضرار بالأفراد أو المؤسسات.
- انتحال شخصية أو إنشاء حسابات وهمية على وسائل التواصل الاجتماعي لأغراض احتيالية أو ضارة.

تحقيق هذه الجرائم يتطلب استخدام الأدلة الجنائية الرقمية لتحديد هوية المشتبه به وتقديم الأدلة المؤكدة على ارتكابه للجريمة.

اساسيات الجرائم الإلكترونية

الجرائم الإلكترونية هي أعمال غير قانونية تتم باستخدام التكنولوجيا الرقمية. وتشمل بعض أساسيات الجرائم الإلكترونية ما يلي:

1. الاحتيال عبر الإنترنت: يشمل استخدام الأدوات والتقنيات الرقمية للقيام بأنشطة احتيالية، مثل سرقة المعلومات الشخصية أو المالية للأفراد أو الشركات.

2. الاختراق الإلكتروني: يتعلق بالدخول غير المشروع إلى أنظمة الكمبيوتر أو الشبكات الإلكترونية دون إذن، وسرقة المعلومات أو تعطيل الخدمات.

3. التجسس: يشمل جمع المعلومات السرية أو الحساسة من خلال استخدام برامج التجسس أو التلاعب في أنظمة الكمبيوتر.

اساسيات الجرائم الإلكترونية

4. الابتزاز: يتضمن تهديد الأفراد أو المؤسسات بنشر معلومات حساسة أو محرجة على الإنترنت ما لم يتم دفع فدية.

5. توزيع المواد الإباحية غير القانونية: يتعلق بتوزيع أو نشر المواد الإباحية غير القانونية عبر الإنترنت، بما في ذلك الأفلام أو الصور التي تتضمن الأطفال.

6. التحرش عبر الإنترنت: يشمل إرسال رسائل مزعجة أو تهديدات أو مضايقات عبر الإنترنت للأفراد.

تعد هذه مجرد أمثلة على بعض أساسيات الجرائم الإلكترونية، وهناك العديد من الأشكال والأنواع الأخرى لهذه الجرائم.

ما نظرية ادوات الجرائم الإلكترونية اتجاه الاختراق الالكتروني

نظرية أدوات الجرائم الإلكترونية تشير إلى الأدوات والتقنيات التي يستخدمها المجرمون الإلكترونيون للقيام بأعمالهم الغير قانونية، ومن بين هذه الأدوات تتواجد أدوات الاختراق الإلكتروني. تعتبر الاختراقات الإلكترونية أحد أشكال الجرائم الإلكترونية الشائعة والخطيرة، حيث يستخدم المجرمون تقنيات متقدمة لاختراق أنظمة الكمبيوتر أو الشبكات الإلكترونية دون إذن.

تشمل أدوات الاختراق الإلكتروني مجموعة متنوعة من التقنيات والبرامج، مثل برامج التجسس وبرامج الفدية وبرامج الاختراق وبرامج التصيد وغيرها. يستخدم المجرمون هذه الأدوات للوصول إلى المعلومات السرية أو لسرقة المعلومات الشخصية أو لتعطيل الخدمات أو للقيام بأعمال تخريبية.

تتطور أدوات الاختراق الإلكتروني باستمرار، حيث يعمل المجرمون الإلكترونيون على ابتكار تقنيات جديدة وتحديث الأدوات الحالية للتغلب على إجراءات الأمان والحماية التي تتخذها المؤسسات والأفراد. وبالتالي، فإن مكافحة الاختراق الإلكتروني يتطلب تحديث وتطوير استراتيجيات الأمان والحماية للتصدي لهذه الأدوات المتطورة.

من هم المجرمون الالكترونيون

المجرمون الإلكترونيون هم الأفراد أو المجموعات الذين يستخدمون التكنولوجيا الحديثة والأدوات الإلكترونية لارتكاب جرائم. قد يشمل ذلك الاختراق الإلكتروني، وسرقة المعلومات، والتصيد الاحتيالي، والاحتيال الإلكتروني، والقرصنة، والتجسس، والتعدي على الخصوصية، وغيرها من الأنشطة غير القانونية التي تتعلق بالتكنولوجيا. يمكن أن يكون لدى المجرمين الإلكترونيين دوافع مختلفة وأهداف مختلفة، بما في ذلك تحقيق مكاسب مالية غير قانونية أو التسبب في أضرار للأفراد أو المؤسسات أو الحكومات.

كيف تتطور الجرائم الإلكترونية

تطورت الجرائم الإلكترونية بشكل كبير على مر السنين نتيجة للتقدم التكنولوجي وانتشار استخدام الإنترنت والأجهزة الذكية. وفيما يلي بعض الطرق التي تطورت بها الجرائم الإلكترونية:

1. زيادة في أنواع الجرائم: تطورت الجرائم الإلكترونية لتشمل مجموعة واسعة من الأنشطة غير القانونية، مثل اختراق الحسابات المصرفية، والاحتيال عبر الإنترنت، والتجسس، والابتزاز الإلكتروني، والتحرش عبر الإنترنت، والقرصنة، والتلاعب في البيانات، وغيرها.

2. تقنيات أكثر تطورًا: استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي والحوسبة السحابية والبلوكشين قد أدى إلى تطور تقنيات الجرائم الإلكترونية. فعلى سبيل المثال، يمكن للمجرمين استخدام هذه التقنيات لاختراق الأنظمة وسرقة المعلومات الحساسة بطرق أكثر تطورًا وصعوبة في اكتشافها.

كيف تتطور الجرائم الإلكترونية

3. الهجمات الجماعية: تطورت الهجمات الجماعية أو ما يُعرف بـ "الهجمات الموزعة للخدمة" حيث يستخدم المجرمون شبكة من الأجهزة المخترقة لتوجيه حركة مرور ضخمة نحو موقع أو خدمة معينة، مما يؤدي إلى تعطيلها وعدم توفرها للمستخدمين.

4. الاحتيال عبر الهواتف المحمولة: مع انتشار استخدام الهواتف المحمولة، أصبحت الجرائم الإلكترونية تستهدف هذه الأجهزة بشكل أكبر. وتشمل هذه الجرائم الاحتيال عبر الرسائل النصية، والبرامج الخبيثة المستهدفة لأنظمة التشغيل المحمولة، والتصيد الاحتيالي عبر التطبيقات.

5. انتشار الجرائم الإلكترونية المنظمة: أصبحت الجرائم الإلكترونية تُنفَّذ بواسطة مجموعات منظمة وقوية، حيث يعمل المجرمون على تكوين شبكات واسعة تتخذ إجراءات متطورة للتخفي وتجنب الكشف.

كيف تتطور الجرائم الإلكترونية

6. تزايد التهديدات للأفراد والمؤسسات: نتيجة لتطور الجرائم الإلكترونية، أصبحت الأفراد والمؤسسات أكثر عرضة للتهديدات الإلكترونية. فقد زادت حالات اختراق الحسابات الشخصية وسرقة المعلومات الشخصية والمالية، واستهداف الشركات والحكومات بأنواع مختلفة من الهجمات.

على الرغم من التطور التكنولوجي السريع، فإن جهود مكافحة الجرائم الإلكترونية أيضًا تتطور بشكل مستمر للتصدي لهذه التهديدات.

شمولية الأدلة الجنائية الرقمية وأدواتها

الأدلة الجنائية الرقمية هي الأدلة التي تتعلق بالجرائم الإلكترونية والتي يتم استخلاصها من الأجهزة الإلكترونية مثل الحواسيب والهواتف الذكية والأجهزة اللوحية وغيرها. تعد هذه الأدلة أحد المكونات الرئيسية في عملية التحقيق في الجرائم الإلكترونية وتلعب دورًا حاسمًا في تقديم الأدلة التي يمكن استخدامها في المحاكمات.

تشمل الأدلة الجنائية الرقمية مجموعة متنوعة من المعلومات والبيانات التي يتم استخلاصها من الأجهزة الإلكترونية. يمكن أن تشمل هذه الأدلة سجلات المكالمات، والرسائل النصية، والبريد الإلكتروني، والصور والفيديوهات، وسجلات التصفح على الإنترنت، والملفات المخزنة على الأجهزة، وغيرها من المعلومات ذات الصلة.

تعد استخلاص الأدلة الجنائية الرقمية عملية معقدة وتحتاج إلى مهارات تحليلية وتقنية متخصصة. يتطلب ذلك فهمًا عميقًا للتكنولوجيا الرقمية والأنظمة المستخدمة في الأجهزة الإلكترونية، بالإضافة إلى معرفة بالأدوات والتقنيات المستخدمة في استخلاص الأدلة.

شمولية الأدلة الجنائية الرقمية وأدواتها

بعد استخلاص الأدلة، يجب أن يتم تحليلها وتفسيرها بشكل صحيح لتحديد قيمتها القانونية والجنائية. يعتمد ذلك على قدرة المحققين على تحليل البيانات والبحث عن أدلة قوية وذات صلة بالجريمة المرتكبة.

تعد الأدلة الجنائية الرقمية أداة قوية في مكافحة الجرائم الإلكترونية وتقديم العدالة. تساهم في تحديد هوية المشتبه بهم، وتثبت وجود الجريمة، وتقدم الأدلة التي يمكن استخدامها في المحاكمات. ومع تزايد استخدام التكنولوجيا الرقمية في حياتنا اليومية، من المتوقع أن تزداد أهمية الأدلة الجنائية الرقمية في المستقبل.

محللي البحث الرقمي

محللو البحث الرقمي هم المحققون والخبراء الذين يتخصصون في استخلاص وتحليل الأدلة الجنائية الرقمية. يعملون على فحص الأجهزة الإلكترونية واستخلاص المعلومات والبيانات ذات الصلة بالجرائم الإلكترونية. يستخدمون الأدوات والتقنيات المتخصصة لاستعادة المعلومات المحذوفة أو المخفية وتحليلها بشكل صحيح.

يجب أن يكون لدى محللي البحث الرقمي مهارات تقنية قوية وفهم عميق للتكنولوجيا الرقمية والأنظمة المستخدمة في الأجهزة الإلكترونية. يجب أن يكونوا قادرين على تحليل البيانات والبحث عن أدلة قوية وذات صلة بالجرائم المرتكبة. كما يجب أن يكون لديهم معرفة بالقوانين والإجراءات المتعلقة بالتحقيقات يعمل محللو البحث الرقمي في مختلف المؤسسات والوكالات الحكومية، مثل الشرطة والأجهزة الأمنية، والشركات الأمنية والاستشارية، والمختبرات الجنائية الرقمية. يمكن أن يكونوا أيضًا شهودًا خبراء في المحاكم لتقديم الأدلة الجنائية الرقمية وشهادتها.

مختبر جرائم الحاسوب

مختبر جرائم الحاسوب هو مكان يتم فيه تحليل وتحقيق في الجرائم الإلكترونية والأدلة الرقمية المتعلقة بها. يتضمن المختبر عادة مجموعة من المحللين الرقميين والخبراء الذين يستخدمون التقنيات والأدوات المتخصصة لفحص واستخلاص الأدلة من الأجهزة الإلكترونية.

يشمل عمل المختبر جمع الأجهزة المشتبه فيها وتحليلها بحثًا عن أدلة رقمية قوية. يتم استخدام تقنيات مثل استعادة الملفات المحذوفة، وتحليل البيانات، واستخلاص المعلومات المخفية لاستعادة الأدلة المحذوفة أو المخفية.

بالإضافة إلى ذلك، يتضمن مختبر جرائم الحاسوب تحليل البيانات والأدلة المستخرجة لفهم سياق الجريمة وتوفير التقارير والشهادات الفنية المطلوبة في التحقيقات الجنائية.

متطلبات مختبر جرائم الأدلة الرقمية

متطلبات مختبر جرائم الأدلة الرقمية تختلف بناءً على البلد والمنظمة التي تدير المختبر. ومع ذلك، هناك بعض المتطلبات العامة التي قد تشمل:

1. التجهيزات المادية: يحتاج مختبر جرائم الأدلة الرقمية إلى تجهيزات مادية مثل أجهزة الكمبيوتر المتخصصة، والأجهزة الإلكترونية الأخرى مثل الهواتف الذكية والأجهزة اللوحية، وأدوات استخراج البيانات، وأدوات التحليل والتحقق.

2. البرامج والأدوات: يجب أن يكون لدى المختبر برامج وأدوات خاصة لاستخلاص وتحليل البيانات الرقمية. قد تشمل هذه الأدوات برامج استعادة الملفات المحذوفة، وبرامج تحليل الصور والفيديو، وبرامج استعادة كلمات المرور، وغيرها.

متطلبات مختبر جرائم الأدلة الرقمية

3. الخبرة والمهارات: يجب أن يكون لدى فريق المختبر خبرة ومهارات في مجال جرائم الأدلة الرقمية. يجب أن يكونوا قادرين على استخدام الأدوات والبرامج بفعالية، وتحليل البيانات المستخرجة، وتوثيق الأدلة بطريقة صحيحة.

4. السلامة والأمان: يجب أن تتوفر إجراءات سلامة وأمان صارمة في المختبر لحماية الأدلة الرقمية وضمان سلامتها. يجب أن يتم تأمين المختبر بشكل جيد وتنفيذ سياسات الوصول والحفاظ على سرية البيانات.

5. التعاون والتعاون: قد يتطلب عمل مختبر جرائم الأدلة الرقمية التعاون مع الجهات الأخرى مثل الشرطة والنيابة العامة والخبراء القانونيين. يجب أن يكون لدى المختبر قدرة على التعاون والتواصل بفعالية مع هذه الجهات.

برنامج إذن التفتيش

برنامج إذن التفتيش هو برنامج يستخدم في مختبر جرائم الحاسوب للحصول على إذن قانوني لتفتيش واستخلاص البيانات من أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى. يساعد هذا البرنامج في ضمان الامتثال للقوانين وحقوق الأفراد أثناء عملية التحقيق في الجرائم الإلكترونية. يتضمن برنامج إذن التفتيش عادة إجراءات وإرشادات للحصول على الموافقة القانونية والإشراف على عملية التفتيش وتوثيق الأدلة المستخرجة.

تقنيات التحليل الرقمي في التحقيقات الجنائية

تقنيات التحليل الرقمي في التحقيقات الجنائية تشمل مجموعة متنوعة من الأدوات والتقنيات التي تستخدم لاستخراج وتحليل البيانات الرقمية. وتشمل بعض هذه التقنيات:

1. استعادة الملفات المحذوفة: تستخدم هذه التقنية لاستعادة الملفات التي تم حذفها عن طريق الخطأ أو عن طريق التلاعب العمد. يتم استخدام برامج خاصة لاستعادة هذه الملفات من وسائط التخزين المختلفة مثل الأقراص الصلبة والهواتف الذكية.

2. تحليل الصور والفيديو: يستخدم التحليل الرقمي لتحليل الصور والفيديو المستخرجة من أجهزة الكمبيوتر والهواتف الذكية وغيرها من وسائط التخزين. يمكن استخدام هذه التقنية لتحديد مصدر الصورة أو الفيديو، واستخلاص المعلومات الخفية منها، وتحليل البيانات الزمنية والمكانية المرتبطة بها.

تقنيات التحليل الرقمي في التحقيقات الجنائية

3. استعادة كلمات المرور: تستخدم هذه التقنية لاستعادة كلمات المرور المفقودة أو المنسية للوصول إلى حسابات المستخدمين. يتم استخدام برامج خاصة لتجريب مجموعة من الكلمات المرور المحتملة حتى يتم العثور على الكلمة المرور الصحيحة.

4. تحليل البيانات الشبكية: يستخدم التحليل الرقمي لتحليل بيانات الشبكة المستخرجة من أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى. يمكن استخدام هذه التقنية لتحديد نشاطات المستخدم على الشبكة، وتحليل سجلات الاتصال، وتحديد مصادر الهجمات الإلكترونية.

5. تحليل البيانات المشفرة: يستخدم التحليل الرقمي لفك تشفير البيانات المشفرة المستخرجة من أجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى. يمكن استخدام هذه التقنية لاستعادة المعلومات المخفية أو المحذوفة من البيانات المشفرة.

تحليل البيانات المشفرة في تقنيات الأدلة الجنائية الرقمية

تحليل البيانات المشفرة في تقنيات الأدلة الجنائية الرقمية يتطلب استخدام أدوات وتقنيات متخصصة. هناك عدة طرق يمكن استخدامها لتحليل البيانات المشفرة، ومن بينها:

1. تجريب الكلمات المرور: يمكن استخدام برامج خاصة لتجريب مجموعة من الكلمات المرور المحتملة لفك تشفير البيانات المشفرة. يتم تجريب هذه الكلمات المرور باستخدام قوائم من الكلمات المشهورة أو المعروفة للمستخدم، أو يتم إنشاء قوائم خاصة بالكلمات المحتملة بناءً على معلومات المستخدم.

2. استخدام الهجمات القوية: تستخدم هذه الطريقة لاستخلاص المفاتيح المستخدمة في عملية التشفير. تعتمد هذه الطريقة على استخدام قوة الحوسبة لاختبار كل المفاتيح المحتملة حتى يتم العثور على المفتاح الصحيح. يتطلب استخدام هذه الطريقة وقتًا طويلاً وموارد حوسبة كبيرة

تحلل البيانات المشفرة في تقنيات الأدلة الجنائية الرقمية

3. استخدام الهجمات الجانبية: تستخدم هذه الطريقة لاستخلاص المفاتيح المستخدمة في عملية التشفير من خلال تحليل السلوك الجانبي للجهاز المشفر. يمكن أن تشمل هذه الطريقة تحليل استهلاك الطاقة أو التوقيت أثناء عملية التشفير.

4. استخدام الهجمات على ثغرات البرمجيات: تستخدم هذه الطريقة للاستفادة من ثغرات في برامج التشفير أو أنظمة التشفير لاستخلاص المفاتيح المستخدمة في عملية التشفير. يعتمد استخدام هذه الطريقة على اكتشاف واستغلال ثغرات الأمان في البرمجيات أو أنظمة التشفير.

5. استخدام التعاون مع الشركات المصنعة: في بعض الحالات، يمكن الاستعانة بالشركات المصنعة للأجهزة أو البرمجيات المشفرة للحصول على المفاتيح المستخدمة في التشفير. تعتمد هذه الطريقة على التعاون مع الشركات المصنعة للحصول على المفاتيح أو الأدوات اللازمة لفك تشفير البيانات.

الانتربول وعلاقته بتقنيات الأدلة الجنائية الرقمية

الانتربول الدولي هو منظمة دولية تعمل على تعزيز التعاون الدولي في مكافحة الجريمة. تتعاون الانتربول مع الـ FBI والعديد من الجهات الأخرى في مجال تقنيات الأدلة الجنائية الرقمية.

تتضمن علاقة الانتربول بتقنيات الأدلة الجنائية الرقمية تبادل المعلومات والخبرات بين الدول الأعضاء، وتنسيق التحقيقات المشتركة في حالات الجرائم التي تتطلب التحليل الرقمي.

وبشكل عام، يعمل الانتربول على تطوير قدراته في مجال تقنيات الأدلة الجنائية الرقمية وتوفير التدريب والدعم التقني للدول الأعضاء، بهدف تحسين قدراتها في مكافحة الجريمة الرقمية وتحليل الأدلة الجنائية ذات الصلة.

أبعاد الانتربول الدولي بتقنيات الأدلة الرقمية

تشمل أبعاد الانتربول الدولي بتقنيات الأدلة الرقمية ما يلي:

1. تبادل المعلومات: يقوم الانتربول بتبادل المعلومات الرقمية بين الدول الأعضاء لتعزيز التحقيقات وتقديم المساعدة في الكشف عن الجرائم وملاحقة المجرمين.
2. التحليل الرقمي: يساعد الانتربول في تنسيق التحليل الرقمي للأدلة والمعلومات الجنائية، مما يسهم في تحديد هوية المشتبه بهم وجمع الأدلة اللازمة لإثبات الجرائم.
3. التدريب والتطوير: يقدم الانتربول التدريب والدعم التقني للدول الأعضاء في مجال تقنيات الأدلة الجنائية الرقمية، بهدف تعزيز قدراتها في مكافحة الجريمة الرقمية وتحليل الأدلة ذات الصلة.

الشرطة الفيدرالية الأمريكية وتقنيات الأدلة الجنائية الرقمية

الشرطة الفيدرالية الأمريكية هي إحدى الجهات الرئيسية في مجال تقنيات الأدلة الجنائية الرقمية. تعمل الـ FBI على تطوير وتحسين قدراتها في تحليل البيانات المشفرة وجمع الأدلة الرقمية لمكافحة الجريمة والإرهاب. تعمل الوكالة على تطوير أدوات وبرامج خاصة بها لاستخلاص المعلومات من الأجهزة الإلكترونية وفك شفرات التشفير.

تعمل الـ FBI أيضًا على التعاون مع جهات دولية أخرى، مثل Interpol ، في تبادل المعلومات والتجارب والتقنيات المتعلقة بتحليل الأدلة الجنائية الرقمية. يتم تنسيق هذه الجهود المشتركة من خلال تبادل المعلومات والتدريب والتعاون في التحقيقات.

بصفة عامة، يتطلب تحليل الأدلة الجنائية الرقمية تعاونًا وتنسيقًا بين العديد من الجهات المعنية، سواء كانت محلية أو دولية، حيث يتم تبادل المعلومات والخبرات لتحسين القدرات وزيادة الفعالية

مثال عام عن الأدلة الجنائية الرقمية وأدواتها

استخدام تحليل البيانات الرقمية لتحديد موقع المشتبه به في جريمة. يمكن للشرطة الفيدرالية استخدام أدوات مثل تحليل سجلات الهاتف المحمول والبيانات الجغرافية لتتبع حركة المشتبه به وتحديد موقعه في وقت معين. يمكن أيضًا استخدام بيانات المواقع الإلكترونية وسجلات الدخول لتحديد الأشخاص الذين قاموا بزيارة موقع معين أو قاموا بإجراءات معينة على الإنترنت.

الأكاديمية العربية الدولية
Arab International Academy

شكراً لكم