JUSTICE ACADEMY

"التحقيق وجمع الأدلة في الجرائم الرقمية"

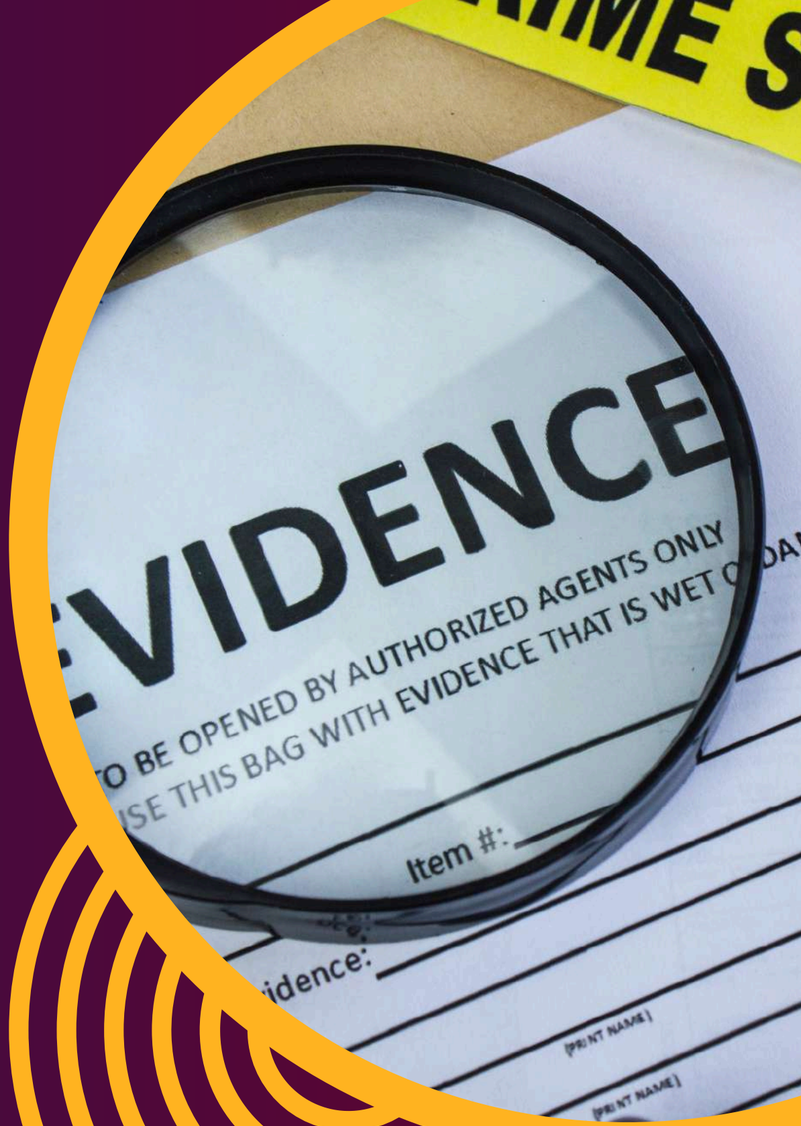
JUSTICE ACADEMY

اللواء دكتور أيمن رمضان الزيني

- أستاذ القانون باللغة الإنجليزية
- مالك ومدير مجموعة الزيني للمحاماة والاستشارات القانونية
- محكم تجاري دولي معتمد لدى العديد من المؤسسات الدولية ومحاضر وخبير صياغة العقود الدولية FIDIC & B.O.T & Franchise
- رئيس الجمعية العربية للعلوم القانونية
- عضو مجلس إدارة وأمين الصندوق DAAD Alumni verein

للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك عدة خطوات وتقنيات هامة في هذا الشأن، نجملها فيما يلي:

1. تأمين مسرح الجريمة الرقمي
2. جمع الأدلة الرقمية
3. تحليل الأدلة
4. توثيق النتائج
5. التعاون مع الجهات المختصة



للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك عدة خطوات وتقنيات هامة في هذا الشأن، نجملها فيما يلي:

1 تأمين مسرح الجريمة الرقمي

- عزل الأجهزة المتورطة وإيقاف تشغيلها بشكل صحيح.
- توثيق الحالة الأولية للأجهزة والشبكات.

JUSTICE ACADEMY

تأمين مسرح الجريمة الرقمي هو خطوة بالغة الأهمية في التحقيق بالجرائم الإلكترونية.

1. الوصول السريع والآمن:

- - الوصول إلى موقع الحادث بأسرع وقت ممكن لمنع العبث بالأدلة.
- - تأمين المنطقة المحيطة بالأجهزة الإلكترونية المعنية.

الوصول السريع والآمن إلى مسرح الجريمة الرقمي هو الخطوة الأولى والحاسمة في عملية التحقيق.\

1. الوصول السريع والآمن

أ. الاستجابة الفورية:

- - تشكيل فريق استجابة سريع يضم خبراء في الأمن السيبراني والطب الشرعي الرقمي.
- - وضع خطة عمل سريعة تحدد الأدوار والمسؤوليات لكل عضو في الفريق.

ب. تقييم المخاطر الأولي:

- - إجراء تقييم سريع للوضع لتحديد ما إذا كان هناك أي تهديدات نشطة أو مستمرة.
- - تحديد ما إذا كان المهاجم لا يزال لديه وصول نشط إلى الأنظمة.

1. الوصول السريع والآمن

ج. تأمين المكان المادي:

- - إغلاق المنطقة المحيطة بالأجهزة المتأثرة.
- - التحكم في الوصول إلى الموقع، مع السماح فقط للأفراد المصرح لهم بالدخول.

د. منع التدخل الخارجي:

- - تعطيل الاتصال بالإنترنت والشبكات الخارجية لمنع أي تدخل عن بُعد.
- - استخدام أجهزة حجب الإشارات اللاسلكية إذا لزم الأمر لمنع الاتصالات غير المصرح بها.

هـ. التوثيق الأولي:

- - البدء فورًا في توثيق الوضع كما تم العثور عليه.
- - استخدام الكاميرات وأجهزة التسجيل لتوثيق حالة الأجهزة والمكان المحيط.

1. الوصول السريع والآمن

و. الحفاظ على الأدلة المتطايرة:

- - تحديد الأجهزة التي تحتوي على بيانات متطايرة (مثل ذاكرة الوصول العشوائي) وإعطاؤها الأولوية.
- - استخدام أدوات متخصصة لجمع البيانات المتطايرة دون تغيير حالة الأجهزة.

ز. إنشاء نقطة اتصال مركزية:

- - تعيين شخص واحد ليكون نقطة الاتصال الرئيسية للتواصل مع الإدارة العليا وسلطات إنفاذ القانون.

ر. بدء سجل الأحداث:

- - إنشاء سجل زمني يوثق كل إجراء يتم اتخاذه منذ لحظة الوصول.
- - تسجيل من قام بماذا ومتى، لضمان وجود سجل دقيق لجميع الأنشطة.

1. الوصول السريع والآمن

ك. تقييم الحاجة إلى خبرات إضافية:

- - تحديد ما إذا كانت هناك حاجة إلى خبراء إضافيين (مثل محللي البرمجيات الخبيثة أو خبراء في أنظمة معينة).

ل. التنسيق مع الجهات القانونية:

- - الاتصال بالسلطات القانونية المختصة إذا كان ذلك ضروريًا.
- - التأكد من أن جميع الإجراءات تتوافق مع المتطلبات القانونية للتحقيق.

- هذه الخطوات تضمن أن يتم تأمين مسرح الجريمة الرقمي بسرعة وفعالية، مما يحافظ على سلامة الأدلة ويزيد من فرص نجاح التحقيق.

تأمين مسرح الجريمة الرقمي

2. توثيق المشهد الأولي:

- - التقاط صور فوتوغرافية وفيديو للموقع والأجهزة قبل لمسها.
- - تسجيل حالة الأجهزة (مشغلة أم مطفأة، متصلة بالإنترنت أم لا).
- توثيق المشهد الأولي هو خطوة حاسمة في التحقيق في الجرائم الإلكترونية. يساعد هذا التوثيق الدقيق في الحفاظ على سلامة الأدلة وتوفير سجل مفصل للحالة الأصلية لمسرح الجريمة.

2. توثيق المشهد الأولي:

أ. التصوير الفوتوغرافي:

- - التقاط صور واسعة للغرفة أو المكان بأكمله.
- - تصوير كل جهاز وموقعه بالنسبة للأجهزة الأخرى.
- - التقاط صور مقربة لكل جهاز، بما في ذلك الأسلاك والمنافذ المتصلة.
- - تصوير الشاشات إذا كانت الأجهزة قيد التشغيل.

ب. تصوير الفيديو:

- - تسجيل فيديو يغطي المشهد بأكمله، مع التركيز على تفاصيل الأجهزة والتوصيلات.
- - توثيق أي أنشطة مرئية على الشاشات المشغلة.

2. توثيق المشهد الأولي:

ج. رسم مخطط للموقع:

- - إنشاء رسم تخطيطي للغرفة يوضح مواقع جميع الأجهزة.
- - ترقيم كل جهاز وتحديد موقعه على المخطط.

د. توثيق حالة الأجهزة:

- - تسجيل ما إذا كانت الأجهزة مشغلة أم مطفأة.
- - توثيق أي مؤشرات ضوئية نشطة على الأجهزة.
- - تسجيل الوقت والتاريخ المعروضين على أي شاشات مرئية.

2. توثيق المشهد الأولي:

هـ. تسجيل التوصيلات الشبكية:

- - توثيق جميع الاتصالات الشبكية (سلكية ولاسلكية).
- - تسجيل أسماء الشبكات اللاسلكية المرئية.

ز. جرد الأجهزة والوسائط:

- - إنشاء قائمة تفصيلية بجميع الأجهزة الموجودة.
- - تسجيل الأرقام التسلسلية وعناوين MAC للأجهزة إن أمكن.
- - توثيق أي وسائط تخزين خارجية موجودة (أقراص صلبة، أقراص USB، بطاقات SD).

2. توثيق المشهد الأولي:

ر. ملاحظة الظروف البيئية:

- - تسجيل درجة حرارة الغرفة ومستويات الرطوبة.
- - توثيق أي أنظمة تبريد أو تهوية خاصة للأجهزة.

ك. تدوين الملاحظات الفورية:

- - كتابة أي ملاحظات عن الروائح أو الأصوات غير العادية.
- - تسجيل أي شيء يبدو غير طبيعي أو مثير للشبهة.

ل. توثيق الأشخاص الحاضرين:

- - تسجيل أسماء ومناصب جميع الأشخاص الموجودين في مسرح الجريمة.
- - توثيق وقت وصول وخروج كل شخص.

2. توثيق المشهد الأولي:

م. إنشاء سلسلة الحيازة:

- - بدء توثيق سلسلة الحيازة لكل قطعة من الأدلة.
- - تسجيل من قام بتوثيق كل جزء من المشهد.

ن. استخدام نماذج موحدة:

- - استخدام نماذج قياسية لضمان اتساق التوثيق.
- - التأكد من أن جميع النماذج تحمل التاريخ والوقت وتوقيع الشخص المسؤول.

- هذا التوثيق الشامل يساعد في إعادة بناء المشهد لاحقًا إذا لزم الأمر، ويضمن أن تكون جميع الأدلة المحتملة قد تم تسجيلها بدقة.

تأمين مسرح الجريمة الرقمي

3. عزل الأجهزة:

- - فصل الأجهزة عن شبكة الإنترنت لمنع التلاعب عن بُعد.
- - إذا كان الجهاز مشغلاً، تجنب إغلاقه فورًا وقم بتوثيق ما يظهر على الشاشة.

عزل الأجهزة خطوة حاسمة في الحفاظ على سلامة الأدلة الرقمية.

3. عزل الأجهزة:

أ. تقييم حالة الاتصال:

- - تحديد ما إذا كانت الأجهزة متصلة بالإنترنت أو بشبكات محلية.
- - توثيق أي اتصالات نشطة قبل قطعها.

ب. قطع الاتصال بالشبكة:

- - فصل كابلات الإيثرنت بحذر.
- - إيقاف تشغيل أجهزة التوجيه والمحولات القريبة.
- - تعطيل الاتصالات اللاسلكية (WiFi, Bluetooth) على الأجهزة إن أمكن.

3. عزل الأجهزة:

ج. منع الاتصالات الخلوية:

- - وضع الهواتف المحمولة والأجهزة اللوحية في أكياس فاراداي لمنع الاتصالات الخلوية.
- - إذا لم تتوفر أكياس فاراداي، يمكن استخدام رقائق الألمنيوم كبديل مؤقت.

د. التعامل مع الأجهزة المشغلة:

- - عدم إغلاق الأجهزة المشغلة فورًا، بل توثيق ما يظهر على الشاشة أولاً.
- - استخدام أدوات الطب الشرعي الحية لجمع البيانات المتطايرة إذا لزم الأمر.

هـ. فصل مصادر الطاقة:

- - فصل الأجهزة عن مصادر الطاقة الخارجية بعد توثيق حالتها.
- - إزالة البطاريات من الأجهزة المحمولة إن أمكن لمنع أي نشاط غير مرئي.

3. عزل الأجهزة:

و. تأمين وسائط التخزين الخارجية:

- - فصل وتأمين أي أقراص صلبة خارجية أو أجهزة تخزين USB متصلة.
- - وضع علامات على هذه الأجهزة وتخزينها بشكل آمن.

ز. تعطيل ميزات الأمان عن بُعد:

- - تحديد ما إذا كانت الأجهزة تحتوي على ميزات مثل "Find My Device" وتعطيلها إن أمكن.
- - توخي الحذر لتجنب تنشيط أي آليات مسح عن بُعد.

ر. عزل الأجهزة الذكية والإنترنت الأشياء:

- - تحديد وعزل أي أجهزة ذكية متصلة بالشبكة (كاميرات المراقبة، أجهزة المنزل الذكي).
- - توثيق حالة هذه الأجهزة قبل عزلها.

تأمين مسرح الجريمة الرقمي

3. عزل الأجهزة:

ك. التعامل مع الخوادم:

- - في حالة الخوادم، استشارة خبراء النظام قبل فصل الاتصال لتجنب فقدان البيانات الحرجة.
- - توثيق أي عمليات إيقاف تشغيل للخوادم بدقة.

ل. إنشاء بيئة معزولة:

- - نقل الأجهزة المعزولة إلى منطقة آمنة بعيدة عن أي مصادر تداخل إلكتروني.
- - استخدام حاويات معزولة كهربائياً لتخزين الأجهزة الصغيرة.

م. توثيق عملية العزل:

- - تسجيل كل خطوة من عملية العزل بالتفصيل.
- - توثيق أي تغييرات في حالة الأجهزة أثناء عملية العزل.

3. عزل الأجهزة:

ن. الحفاظ على سلسلة الحيازة:

- - تحديث سجلات سلسلة الحيازة لكل جهاز تم عزله.
- - ضمان أن كل من يتعامل مع الأجهزة المعزولة يوثق تفاعله معها.
- - عزل الأجهزة بهذه الطريقة الدقيقة يضمن الحفاظ على سلامة الأدلة الرقمية ويمنع أي تلاعب أو تغيير غير مقصود في البيانات.

4. الحفاظ على البيانات المتطايرة:

- - جمع البيانات المتطايرة (مثل محتويات الذاكرة العشوائية) قبل إيقاف تشغيل الأجهزة.
- - استخدام أدوات خاصة لاستخراج هذه البيانات دون التأثير على محتوى الجهاز.

تأمين مسرح الجريمة الرقمي

4. الحفاظ على البيانات المتطايرة:

- - جمع البيانات المتطايرة (مثل محتويات الذاكرة العشوائية) قبل إيقاف تشغيل الأجهزة.
- - استخدام أدوات خاصة لاستخراج هذه البيانات دون التأثير على محتوى الجهاز.

4. الحفاظ على البيانات المتطايرة:

الحفاظ على البيانات المتطايرة هو جانب حيوي في التحقيقات الرقمية، حيث أن هذه البيانات قد تحتوي على معلومات قيمة تختفي بمجرد إيقاف تشغيل الجهاز.

أ. فهم البيانات المتطايرة:

- - تشمل محتويات الذاكرة العشوائية (RAM)، العمليات النشطة، اتصالات الشبكة المفتوحة، والبيانات المؤقتة.
- - هذه البيانات تختفي عند إيقاف تشغيل الجهاز أو فصل الطاقة.

4. الحفاظ على البيانات المتطايرة:

ب. ترتيب الأولويات:

- - البدء بالبيانات الأكثر تطايرًا (مثل محتويات RAM) ثم الانتقال إلى البيانات الأقل تطايرًا.
- - اتباع ترتيب التطاير: التسجيلات، الذاكرة، جدول التوجيه، ذاكرة التخزين المؤقت ARP، جداول العمليات، الملفات المفتوحة، اتصالات الشبكة.

ج. استخدام أدوات متخصصة:

- - توظيف أدوات الطب الشرعي الحية مثل Volatility أو Rekall.
- - استخدام أدوات تحليل الذاكرة المباشرة مثل WinPmem أو LiME.

د. التقاط صورة الذاكرة:

- - استخدام أدوات مثل FTK Imager أو Memoryze لالتقاط صورة كاملة للذاكرة.
- - تأكد من عدم تغيير حالة النظام أثناء عملية الالتقاط.

4. الحفاظ على البيانات المتطايرة:

هـ. جمع معلومات النظام:

- - تسجيل الوقت والتاريخ الحاليين للنظام.
- - جمع قائمة بالعمليات النشطة والخدمات الجارية.
- - توثيق اتصالات الشبكة المفتوحة والمنافذ النشطة.

و. استخراج المعلومات من الذاكرة:

- - تحليل محتويات الذاكرة للكشف عن البرمجيات الخبيثة أو الأنشطة المشبوهة.
- - استخراج كلمات المرور والمفاتيح التشفيرية المخزنة في الذاكرة.

ز. توثيق البيانات المستخرجة:

- - إنشاء سجل مفصل لجميع البيانات المستخرجة.
- - تسجيل الأدوات المستخدمة وإعداداتها لضمان إمكانية إعادة الإنتاج.

4. الحفاظ على البيانات المتطايرة:

ر. التعامل مع الأنظمة المشفرة:

- - في حالة الأنظمة المشفرة، جمع البيانات المتطايرة قد يكون الفرصة الوحيدة للوصول إلى المعلومات.
- - البحث عن مفاتيح التشفير في الذاكرة.

ك. تحليل الشبكة:

- - التقاط وتحليل حركة مرور الشبكة النشطة.
- - توثيق الاتصالات المشبوهة أو غير العادية.

ل. التعامل مع الأجهزة المحمولة:

- - استخدام أدوات متخصصة للأجهزة المحمولة مثل UFED أو Cellebrite.
- - جمع البيانات المتطايرة من الهواتف الذكية والأجهزة اللوحية قبل إيقاف تشغيلها.

4. الحفاظ على البيانات المتطايرة:

م. ضمان سلامة البيانات:

- - استخدام أدوات موثوقة وذات سمعة جيدة لتجنب تلوث الأدلة.
- - التحقق من صحة البيانات المجمعة باستخدام قيم التجزئة.

ن. التخزين الآمن:

- - تخزين البيانات المستخرجة على وسائط آمنة ومشفرة.
- - الحفاظ على سلسلة الحيازة لجميع البيانات المجمعة.

ي. التحليل الفوري:

- - إجراء تحليل أولي للبيانات المتطايرة على الفور، حيث قد تحتوي على معلومات حرجة للتحقيق.
- - الحفاظ على البيانات المتطايرة يتطلب سرعة ودقة في العمل. هذه العملية يمكن أن توفر أدلة قيمة لا يمكن استردادها بأي وسيلة أخرى.

4. الحفاظ على البيانات المتطايرة:

م. ضمان سلامة البيانات:

- - استخدام أدوات موثوقة وذات سمعة جيدة لتجنب تلوث الأدلة.
- - التحقق من صحة البيانات المجمعة باستخدام قيم التجزئة.

ن. التخزين الآمن:

- - تخزين البيانات المستخرجة على وسائط آمنة ومشفرة.
- - الحفاظ على سلسلة الحيازة لجميع البيانات المجمعة.

ي. التحليل الفوري:

- - إجراء تحليل أولي للبيانات المتطايرة على الفور، حيث قد تحتوي على معلومات حرجة للتحقيق.
- - الحفاظ على البيانات المتطايرة يتطلب سرعة ودقة في العمل. هذه العملية يمكن أن توفر أدلة قيمة لا يمكن استردادها بأي وسيلة أخرى.

تأمين مسرح الجريمة الرقمي

5. إيقاف تشغيل الأجهزة بشكل صحيح

- - اتباع إجراءات محددة لإيقاف تشغيل الأجهزة دون فقدان البيانات المهمة.
- - تجنب الإغلاق العادي واستخدام طرق تحافظ على محتويات الذاكرة.

- إيقاف تشغيل الأجهزة بشكل صحيح في سياق التحقيقات الرقمية هو إجراء دقيق وحساس. الهدف هو الحفاظ على أكبر قدر ممكن من الأدلة دون إتلافها أو تغييرها.

5. إيقاف تشغيل الأجهزة بشكل صحيح

أ. تقييم الحالة:

- - تحديد ما إذا كان الجهاز مشغلاً أم مطفأً.
- - توثيق حالة الجهاز قبل اتخاذ أي إجراء.

ب. جمع البيانات المتطايرة أولاً:

- - قبل إيقاف التشغيل، تأكد من جمع جميع البيانات المتطايرة الضرورية.
- - استخدم الأدوات المناسبة لاستخراج محتويات الذاكرة العشوائية (RAM).

ج. تحديد نوع الجهاز ونظام التشغيل:

- - الإجراءات تختلف بين أنظمة Windows و macOS و Linux والأجهزة المحمولة.
- - تحديد إصدار نظام التشغيل لاختيار الطريقة المناسبة.

5. إيقاف تشغيل الأجهزة بشكل صحيح

د. إيقاف التشغيل لأجهزة Windows:

- - تجنب استخدام خيار "Shut Down" العادي لأنه قد يغير البيانات.
- - استخدام أمر cmd لإيقاف التشغيل الفوري: `shutdown /s /f /t 0`
- - في حالات معينة، قد يكون من الأفضل فصل الطاقة مباشرة.

هـ. إيقاف التشغيل لأجهزة MacOS:

- - تجنب استخدام زر الطاقة أو قائمة Apple.
- - استخدام أمر Terminal: `sudo shutdown -h now`
- - في بعض الحالات، قد يُفضل فصل البطارية والطاقة معًا.

5. إيقاف تشغيل الأجهزة بشكل صحيح

و. إيقاف التشغيل لأنظمة Linux:

- - استخدام أمر `sudo shutdown -h now` :Terminal
- - في بعض الحالات، يمكن استخدام: `echo 1 > /proc/sys/kernel/sysrq` ثم `echo o > /proc/sysrq-trigger`

ز. التعامل مع الأجهزة المحمولة:

- - للهواتف الذكية والأجهزة اللوحية، غالبًا ما يُفضل عزلها عن الشبكة وتركها مشغلة.
- - إذا كان لابد من إيقاف التشغيل، استخدم وضع الطيران أولاً ثم أوقف التشغيل.

5. إيقاف تشغيل الأجهزة بشكل صحيح

ر. حالات خاصة:

- - في حالة الخوادم أو أنظمة قواعد البيانات، استشر الخبراء قبل إيقاف التشغيل لتجنب فقدان بيانات حرجة.
- - بعض الأنظمة المشفرة قد تتطلب إجراءات خاصة للحفاظ على إمكانية الوصول إلى البيانات.

ك. توثيق العملية:

- - سجل كل خطوة من عملية إيقاف التشغيل بالتفصيل.
- - وثق الوقت الدقيق لإيقاف التشغيل وأي ملاحظات ذات صلة.

5. إيقاف تشغيل الأجهزة بشكل صحيح

ل. فصل مصادر الطاقة:

- - بعد إيقاف التشغيل، افصل جميع مصادر الطاقة بما في ذلك البطاريات القابلة للإزالة.
- - وثق أي كابلات أو مصادر طاقة تم فصلها.

م. تأمين الجهاز:

- - ضع الجهاز في حاوية مضادة للكهرباء الساكنة.
- - ضع ملصقًا على الجهاز يحتوي على معلومات التعريف وتفاصيل إيقاف التشغيل.

5. إيقاف تشغيل الأجهزة بشكل صحيح

ن. تحديث سلسلة الحيازة:

- - سجل تفاصيل إيقاف التشغيل في وثائق سلسلة الحيازة.
- - تأكد من توقيع الشخص المسؤول عن إيقاف التشغيل على الوثائق.

- إيقاف تشغيل الأجهزة بشكل صحيح يضمن الحفاظ على سلامة الأدلة الرقمية ويمنع أي تغييرات غير مقصودة في البيانات.

تأمين مسرح الجريمة الرقمي

6. تأمين وسائط التخزين

- - إزالة الأقراص الصلبة وبطاقات الذاكرة بعناية.
- - وضع علامات على جميع الأجهزة ووسائط التخزين وتخزينها في حاويات مضادة للكهرباء الساكنة.

- تأمين وسائط التخزين هو خطوة حاسمة في الحفاظ على سلامة الأدلة الرقمية.

-هذه العملية تضمن أن البيانات المخزنة على الأجهزة تبقى سليمة وقابلة للاستخدام في التحقيق.

6. تأمين وسائط التخزين

أ. تحديد وسائط التخزين:

- - حدد جميع وسائط التخزين المتصلة بالأجهزة المضبوطة.
- - تشمل الأقراص الصلبة الداخلية والخارجية، بطاقات SD، أقراص USB، وأي وسائط تخزين أخرى.

ب. توثيق الوسائط:

- - سجل تفاصيل كل وسيط تخزين (النوع، السعة، الرقم التسلسلي).
- - التقط صورًا فوتوغرافية لكل وسيط قبل إزالته.

ج. إزالة وسائط التخزين:

- - استخدم أدوات مناسبة لإزالة الأقراص الصلبة الداخلية بعناية.
- - إفصل وسائط التخزين الخارجية بحذر.

6. تأمين وسائط التخزين

د. وضع العلامات:

- - ضع ملصقات فريدة على كل وسيط تخزين.
- - تأكد من أن الملصقات تحتوي على معرف فريد، تاريخ الضبط، واسم المحقق.

هـ. التغليف الآمن:

- - استخدم أكياس أدلة مضادة للكهرباء الساكنة لكل وسيط تخزين.
- - تأكد من إغلاق الأكياس بإحكام وختمها.

ز. حماية من المجالات المغناطيسية:

- - استخدم حاويات محمية مغناطيسيًا لنقل وتخزين الوسائط.
- - تجنب وضع الوسائط بالقرب من أجهزة إلكترونية أو مغناطيسية.

6. تأمين وسائط التخزين

ر. التخزين في بيئة محكومة:

- - احتفظ بالوسائط في بيئة ذات درجة حرارة ورطوبة مضبوطة.
- - تجنب التعرض المباشر لأشعة الشمس أو الحرارة الزائدة.

ك. إنشاء نسخ احتياطية:

- - قم بإنشاء نسخ متطابقة (bit-for-bit) من الوسائط الأصلية.
- - استخدم أدوات موثوقة مثل FTK Imager أو DD للنسخ.

ل. التحقق من سلامة النسخ:

- استخدم قيم التجزئة (Hash Values) للتأكد من تطابق النسخ مع الأصل.
- وثق قيم التجزئة لكل وسيط وكل نسخة.

6. تأمين وسائط التخزين

م. تقييد الوصول:

- - حدد الأشخاص المصرح لهم بالوصول إلى وسائط التخزين.
- - احتفظ بسجل لكل وصول أو نقل للوسائط.

ن. توثيق سلسلة الحيازة:

- - سجل كل تفاعل مع وسائط التخزين في وثائق سلسلة الحيازة.
- - تأكد من توقيع كل شخص يتعامل مع الوسائط على الوثائق.

س. التعامل مع الوسائط المشفرة:

- - حدد ما إذا كانت أي من الوسائط مشفرة.
- - حافظ على الأجهزة المشفرة في وضع التشغيل إذا أمكن لتجنب فقدان الوصول.

6. تأمين وسائط التخزين

ش. الاحتفاظ بنسخ العمل:

- - استخدم النسخ الاحتياطية للتحليل وليس الوسائط الأصلية.
- - احتفظ بالوسائط الأصلية في مكان آمن كأدلة أصلية.

ص. التحديث المستمر:

- - راجع حالة وسائط التخزين بانتظام للتأكد من عدم تدهورها.
- - قم بتحديث النسخ الاحتياطية إذا لزم الأمر.

ض. التخلص الآمن:

- عند انتهاء التحقيق، تأكد من التخلص الآمن من الوسائط وفقًا للإجراءات القانونية.
- - تأمين وسائط التخزين بهذه الطريقة الدقيقة يضمن الحفاظ على سلامة الأدلة الرقمية طوال فترة التحقيق.

تأمين مسرح الجريمة الرقمي

7. توثيق سلسلة الحيازة

- - تسجيل كل من تعامل مع الأدلة وكيف تم نقلها وتخزينها.
- - الحفاظ على سجل دقيق لضمان قبول الأدلة في المحكمة.

توثيق سلسلة الحيازة هو عملية حيوية في التحقيقات الجنائية والإجراءات القانونية. إنها تضمن إمكانية تتبع الأدلة من لحظة جمعها حتى تقديمها في المحكمة. إليك شرحًا مفصلاً لكيفية توثيق سلسلة الحيازة بشكل صحيح:

7. توثيق سلسلة الحيازة

أ. بدء السجل:

- - إنشاء سجل فور جمع الدليل.
- - تسجيل وقت وتاريخ العثور على الدليل بدقة.
- - توثيق الموقع الدقيق حيث تم العثور على الدليل.

ب. تعريف الدليل:

- - إعطاء كل دليل رقمًا تسلسليًا فريدًا.
- - وصف الدليل بدقة (الحجم، اللون، الشكل، إلخ).
- - التقاط صور للدليل في موقعه الأصلي.

ج. معلومات الجامع:

- - تسجيل اسم الشخص الذي جمع الدليل.
- - توثيق رتبته أو وظيفته.
- - تسجيل أي شهود حاضرين أثناء جمع الدليل.

7. توثيق سلسلة الحيازة

د. طريقة الجمع:

- - وصف الطريقة المستخدمة في جمع الدليل.
- - تسجيل أي أدوات أو معدات استخدمت في الجمع.
- - توثيق أي إجراءات خاصة اتخذت للحفاظ على الدليل.

ه. التغليف والتخزين الأولي:

- - تسجيل نوع الحاوية المستخدمة لتخزين الدليل.
- - توثيق أي مواد حافظة أو تبريد تم استخدامها.
- - تسجيل كيفية ختم الحاوية.

و. النقل الأولي:

- - تسجيل اسم الشخص المسؤول عن نقل الدليل.
- - توثيق وقت وتاريخ مغادرة مسرح الجريمة. - تسجيل وسيلة النقل المستخدمة.

7. توثيق سلسلة الحيازة

ز. تسليم للمختبر:

- - توثيق وقت وتاريخ وصول الدليل إلى المختبر.
- - تسجيل اسم الشخص الذي استلم الدليل في المختبر.
- - توثيق حالة الدليل عند الاستلام.

ف. الإجراءات المخبرية:

- - تسجيل كل إجراء يتم على الدليل في المختبر.
- - توثيق أسماء الفنيين الذين تعاملوا مع الدليل.
- - تسجيل تواريخ وأوقات كل إجراء.

7. توثيق سلسلة الحيازة

ق. التخزين في المختبر:

- - توثيق موقع تخزين الدليل في المختبر.
- - تسجيل أي تغييرات في ظروف التخزين.
- - توثيق أي وصول للدليل أثناء التخزين.

ك. النقل بين الأقسام:

- - تسجيل كل نقل للدليل بين الأقسام أو المختبرات.
- - توثيق أسباب النقل.
- - تسجيل حالة الدليل قبل وبعد كل نقل.

7. توثيق سلسلة الحيازة

ل. استخدام نماذج رسمية:

- - استخدام نماذج موحدة لتوثيق سلسلة الحيازة.
- - ضمان توقيع كل شخص يتعامل مع الدليل على النموذج.
- - الاحتفاظ بنسخ متعددة من النماذج.

م. التوثيق الإلكتروني:

- - استخدام أنظمة إلكترونية لتتبع الأدلة إذا كانت متاحة.
- - ضمان وجود نسخ احتياطية للسجلات الإلكترونية.
- - استخدام تواقيع إلكترونية آمنة.

7. توثيق سلسلة الحيازة

ن. المراجعة الدورية:

- - إجراء مراجعات منتظمة لسجلات سلسلة الحيازة.
- - تصحيح أي أخطاء أو نقص في التوثيق فوراً.
- - توثيق أي مراجعات تتم على السجلات.

و. التحضير للمحكمة:

- - إعداد ملخص كامل لسلسلة الحيازة.
- - التأكد من جاهزية جميع الأشخاص المذكورين في السلسلة للشهادة إذا لزم الأمر.
- - مراجعة السلسلة مع المدعي العام قبل المحاكمة.

توثيق سلسلة الحيازة بدقة يضمن سلامة الأدلة ويعزز مصداقيتها في المحكمة ، وأي انقطاع أو خلل في هذه السلسلة قد يؤدي إلى استبعاد الدليل، مما قد يؤثر بشكل كبير على نتيجة القضية.

تأمين مسرح الجريمة الرقمي

8. حماية المعلومات الحساسة

حماية المعلومات الحساسة أثناء التحقيق في الجرائم الإلكترونية هي مسؤولية أخلاقية وقانونية حاسمة ، ويمكن اتباع الخطوات التالية حماية المعلومات الحساسة :

- - التأكد من عدم الوصول إلى المعلومات الشخصية أو السرية غير المتعلقة بالتحقيق.
- - اتباع القوانين واللوائح المتعلقة بالخصوصية وحماية البيانات.
- - من المهم أن يقوم بهذه العملية متخصصون مدربون في الطب الشرعي الرقمي لضمان الحفاظ على سلامة الأدلة وقبولها قانونيًا.

8. حماية المعلومات الحساسة

أ. تحديد المعلومات الحساسة:

- - تعرّف على أنواع البيانات الحساسة مثل المعلومات الشخصية، البيانات المالية، الأسرار التجارية، والمعلومات السرية للشركات.
- - حدد المعلومات المحمية قانونيًا مثل الاتصالات بين المحامي والموكل أو السجلات الطبية.

ب. فرز البيانات:

- - استخدم أدوات متخصصة لفرز وتصنيف البيانات حسب مستوى الحساسية.
- - قم بعملية "تنقية" (triage) أولية لتحديد المعلومات ذات الصلة بالتحقيق.

ج. تطبيق مبدأ الحد الأدنى من الامتياز:

- - قيد الوصول إلى البيانات الحساسة للأفراد الذين يحتاجون إليها فقط لأغراض التحقيق.
- - استخدم أنظمة إدارة الهوية والوصول (IAM) لتتبع وإدارة الوصول.

8. حماية المعلومات الحساسة

د. التشفير:

- - شفّر جميع البيانات الحساسة أثناء التخزين والنقل.
- - استخدم بروتوكولات تشفير قوية مثل AES-256 للتخزين و TLS 1.3 للنقل.

ه. إخفاء الهوية وإزالة البيانات الشخصية:

- - استخدم تقنيات إخفاء الهوية لإزالة المعلومات الشخصية غير الضرورية للتحقيق.
- - طبق تقنيات التعمية (obfuscation) على البيانات الحساسة التي يجب الاحتفاظ بها.

و. الفصل الفيزيقي والمنطقي:

- - احتفظ بالبيانات الحساسة على أجهزة أو شبكات منفصلة.
- - استخدم تقنيات العزل مثل الافتراضية (virtualization) لفصل بيئات العمل.

8. حماية المعلومات الحساسة

ز. التوثيق والمراقبة:

- - سجل جميع عمليات الوصول والتعامل مع المعلومات الحساسة.
- - استخدم أنظمة كشف ومنع التسلل (IDS/IPS) لمراقبة النشاط المشبوه.

ر. التدريب والتوعية:

- - درب فريق التحقيق على بروتوكولات التعامل مع المعلومات الحساسة.
- - أنشئ سياسات واضحة للتعامل مع البيانات الحساسة وتأكد من فهم الجميع لها.

س. الامتثال القانوني:

- - تأكد من الامتثال للقوانين واللوائح المتعلقة بحماية البيانات مثل GDPR أو HIPAA.
- - استشر المستشارين القانونيين عند التعامل مع معلومات حساسة قانونيًا.

8. حماية المعلومات الحساسة

ش. إدارة النسخ والتخلص:

- - تتبع جميع النسخ من البيانات الحساسة وتأكد من تأمينها.
- - استخدم تقنيات الحذف الآمن عند التخلص من البيانات غير الضرورية.

ص. التعامل مع البيانات عبر الحدود:

- - كن على دراية بقوانين نقل البيانات عبر الحدود إذا كان التحقيق يشمل عدة دول.
- - استخدم بروتوكولات آمنة لنقل البيانات دوليًا إذا لزم الأمر.

ض. استخدام التقنيات المتقدمة:

- - استخدم تقنيات مثل التشفير المتجانس للسماح بتحليل البيانات المشفرة دون فك تشفيرها.
- - استخدم أنظمة منع تسرب البيانات (DLP) لمنع الوصول غير المصرح به.

8. حماية المعلومات الحساسة

ط. التعامل مع الطلبات القانونية:

- - ضع إجراءات للتعامل مع طلبات الكشف القانونية مثل أوامر المحكمة.
- - تأكد من وجود عملية مراجعة قانونية قبل الكشف عن أي معلومات حساسة.

ظ. التقييم المستمر:

- - قم بإجراء تقييمات دورية لمخاطر البيانات وأمنها.
- - حدّث إجراءات حماية المعلومات الحساسة بناءً على التهديدات الجديدة والتكنولوجيا المتطورة.
- - حماية المعلومات الحساسة تتطلب نهجًا شاملاً ومتعدد الطبقات. يجب أن يكون هناك توازن دقيق بين متطلبات التحقيق وحقوق الخصوصية والالتزامات القانونية.

للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك عدة خطوات وتقنيات هامة في هذا الشأن:

2 جمع الأدلة الرقمية

- إنشاء نسخ متطابقة من وسائط التخزين.
- استخراج البيانات من الأجهزة والشبكات.
- جمع سجلات الإنترنت وبيانات الاتصالات.

جمع الأدلة الرقمية

جمع الأدلة الرقمية هو عملية حساسة ودقيقة في التحقيقات الجنائية الرقمية. يجب أن تتم بطريقة منهجية لضمان قبول الأدلة في المحكمة وحمايتها من التلف ، ويمكن اتباع الخطوات التالية لجمع الأدلة الرقمية:

- - نسخ محتويات الأقراص الصلبة والأجهزة.
- - استخراج البيانات من الهواتف والأجهزة المحمولة.
- - جمع سجلات الإنترنت وبيانات الاتصال.

أ. التخطيط والإعداد:

- - حدد نطاق التحقيق ونوع الأدلة المطلوبة.
- - جهز الأدوات والمعدات اللازمة (أجهزة النسخ، وسائط التخزين النظيفة، أدوات البرمجيات).

جمع الأدلة الرقمية

ب. تأمين مسرح الجريمة الرقمي:

- - اتبع إجراءات تأمين المكان كما ناقشنا سابقًا.
- - منع أي تغييرات في الأجهزة أو البيانات.

ج. التوثيق الأولي:

- - التقط صورًا للأجهزة في موقعها الأصلي.
- - سجل تفاصيل الأجهزة (الطراز، الرقم التسلسلي، حالة التشغيل).

د. جمع البيانات المتطايرة:

- - إذا كان الجهاز قيد التشغيل، قم بجمع البيانات المتطايرة أولاً.
- - استخدم أدوات مثل Volatility لاستخراج محتويات الذاكرة (RAM).

جمع الأدلة الرقمية

ه. إنشاء نسخ متطابقة (Forensic Imaging):

- - استخدم أدوات متخصصة مثل FTK Imager أو EnCase لإنشاء نسخة متطابقة.
- - تأكد من استخدام وسائط تخزين نظيفة ومعقمة للنسخ.

و. التحقق من سلامة النسخ:

- - استخدم خوارزميات التجزئة (مثل MD5 أو SHA-256) للتحقق من تطابق النسخة مع الأصل.
- - وثق قيم التجزئة لكل نسخة.

ز. جمع الأدلة المنطقية:

- - استخرج الملفات والبيانات المحددة ذات الصلة بالتحقيق.
- - جمع سجلات النظام، ملفات التكوين، وقواعد البيانات.

جمع الأدلة الرقمية

س. استرجاع البيانات المحذوفة:

- - استخدم أدوات استعادة البيانات لاسترجاع الملفات المحذوفة.
- - افحص المساحات غير المخصصة على القرص بحثًا عن بيانات متبقية.

ش. جمع البيانات من الشبكة:

- - جمع سجلات الشبكة، بيانات حركة المرور، وسجلات جدران الحماية.
- - استخرج المعلومات من أجهزة التوجيه والمحولات.

ص. التعامل مع الأجهزة المحمولة:

- - استخدم أدوات متخصصة مثل Cellebrite أو XRY لاستخراج البيانات من الهواتف الذكية والأجهزة اللوحية.
- - جمع بيانات التطبيقات، الرسائل، وسجلات المكالمات.

جمع الأدلة الرقمية

ض. جمع الأدلة السحابية:

- - حدد الخدمات السحابية المستخدمة وجمع البيانات منها وفقًا للإجراءات القانونية.
- - استخدم أدوات متخصصة لجمع البيانات من خدمات مثل Google Drive أو Dropbox.

ط. التعامل مع البيانات المشفرة:

- - حدد أي بيانات مشفرة وحاول الحصول على مفاتيح التشفير بالطرق القانونية.
- - وثق وجود التشفير وأي محاولات لفك التشفير.

ظ. توثيق عملية الجمع:

- - سجل كل خطوة من عملية جمع الأدلة بالتفصيل.
- - وثق الأدوات المستخدمة، الإعدادات، والنتائج.

جمع الأدلة الرقمية

ع. الحفاظ على سلسلة الحيازة:

- - أنشئ سجلاً لكل قطعة من الأدلة، يوثق من تعامل معها ومتى وكيف.
- - استخدم نماذج رسمية لتتبع حركة الأدلة.

غ. تخزين الأدلة:

- - خزن الأدلة الرقمية في بيئة آمنة ومحكومة.
- - تأكد من وجود نسخ احتياطية للأدلة المهمة.

ف. مراجعة وتقييم الأدلة:

- - راجع الأدلة المجمعة للتأكد من اكتمالها وصلتها بالتحقيق.
- - حدد أي فجوات في الأدلة قد تتطلب جمع المزيد.

جمع الأدلة الرقمية

- **ق. إعداد التقارير:**
- - أعد تقريرًا مفصلاً عن عملية جمع الأدلة وما تم العثور عليه.
- - تأكد من أن التقرير يتبع المعايير القانونية والمهنية.

-جمع الأدلة الرقمية هو عملية معقدة تتطلب دقة عالية والتزامًا صارمًا بالإجراءات القانونية والفنية، الهدف منها هو جمع أدلة شاملة وموثوقة يمكن استخدامها في المحكمة.

للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك عدة خطوات وتقنيات هامة في هذا الشأن، نجملها فيما يلي:

3 تحليل الأدلة

- فحص الملفات والبيانات المستخرجة.
- تحليل سجلات النظام والشبكة.
- استخدام أدوات التحليل الجنائي الرقمي.

تحليل الأدلة الرقمية

يعد تحليل الأدلة الرقمية مرحلة حاسمة في التحقيقات الجنائية الرقمية ، ويهدف لإستخراج المعلومات ذات الصلة وبناء صورة واضحة لما حدث. ، ويمكن اتباع الخطوات التالية لتحليل الأدلة الرقمية:

أ. إعداد بيئة التحليل:

- - إنشاء محطة عمل منعزلة لتجنب تلوث الأدلة.
- - تثبيت وتحديث الأدوات والبرامج اللازمة للتحليل.

ب. التحقق من سلامة الأدلة:

- - التأكد من تطابق قيم التجزئة للنسخ مع الأصل قبل البدء في التحليل.
- - توثيق أي اختلافات أو مشاكل في سلامة البيانات.

تحليل الأدلة الرقمية

ج. استعراض شامل للبيانات:

- - إجراء فحص أولي لجميع البيانات المتاحة.
- - تحديد الملفات والمجلدات الرئيسية ذات الأهمية المحتملة.

ه. تحليل نظام الملفات:

- - دراسة بنية نظام الملفات وتواريخ إنشاء وتعديل الملفات.
- - البحث عن الملفات المخفية أو المحذوفة واستردادها إن أمكن.

ز. تحليل سجلات النظام:

- فحص سجلات النظام (مثل سجل Windows) للكشف عن الأنشطة المشبوهة.
- تحليل سجلات الأمان وسجلات التطبيقات.

تحليل الأدلة الرقمية

س. تحليل الشبكات:

- - دراسة سجلات الشبكة وبيانات حركة المرور.
- - تحليل عناوين IP والاتصالات المشبوهة.

ش. تحليل البريد الإلكتروني والمراسلات:

- - فحص رسائل البريد الإلكتروني والمرفقات.
- - تحليل سجلات المراسلة الفورية وتطبيقات التواصل الاجتماعي.

ص. تحليل المتصفح:

- - دراسة سجل التصفح وملفات الكوكيز.
- - تحليل التنزيلات والمواقع التي تمت زيارتها.

تحليل الأدلة الرقمية

ض. تحليل الملفات المشبوهة:

- - فحص الملفات للكشف عن البرمجيات الخبيثة أو الأدوات المستخدمة في الجريمة.
- - استخدام أدوات تحليل البرمجيات الخبيثة مثل Volatility أو IDA Pro.

ط. استرداد وتحليل البيانات المحذوفة:

- - استخدام تقنيات استرداد البيانات لاستعادة الملفات المحذوفة.
- - تحليل المساحات غير المخصصة على القرص.

ظ. تحليل الصور والوسائط المتعددة:

- - فحص البيانات الوصفية للصور والفيديوهات.
- - البحث عن الصور المخفية أو المعدلة.

تحليل الأدلة الرقمية

ع. تحليل التطبيقات:

- - دراسة التطبيقات المثبتة وتواريخ تثبيتها واستخدامها.
- - تحليل بيانات التطبيقات المحددة ذات الصلة بالتحقيق.

غ. تحليل البيانات المالية:

- - فحص السجلات المالية والمعاملات المشبوهة.
- - تحليل البيانات من برامج المحاسبة أو الخدمات المصرفية عبر الإنترنت.

ف. تحليل الوقت والتسلسل الزمني:

- - إنشاء جدول زمني للأحداث الرئيسية.
- - ربط الأحداث المختلفة لبناء تسلسل زمني متماسك.

تحليل الأدلة الرقمية

ق. تحليل البيانات المشفرة:

- - محاولة فك تشفير البيانات المشفرة باستخدام الطرق القانونية المتاحة.
- - تحليل أنماط استخدام التشفير.

ك. التحليل المقارن:

- - مقارنة البيانات من مصادر مختلفة للتحقق من الاتساق.
- - البحث عن الروابط بين الأدلة المختلفة.

ل. تحليل الأنماط والسلوكيات:

- - تحديد الأنماط السلوكية والعادات من البيانات المتاحة.
- - استخدام تقنيات التحليل السلوكي لفهم دوافع وأساليب المشتبه بهم.

تحليل الأدلة الرقمية

م. استخدام تقنيات التحليل المتقدمة:

- - تطبيق تقنيات التعلم الآلي والذكاء الاصطناعي للكشف عن الأنماط المعقدة.
- - استخدام أدوات التحليل البصري للبيانات لتسهيل فهم العلاقات المعقدة.

ن. توثيق نتائج التحليل:

- - تسجيل جميع الخطوات والنتائج بدقة.
- - إعداد تقارير مفصلة تشرح منهجية التحليل والنتائج.

تحليل الأدلة الرقمية

و. مراجعة وتقييم النتائج:

- - مراجعة النتائج للتأكد من دقتها واكتمالها.
- - تحديد أي ثغرات في التحليل قد تتطلب مزيدًا من البحث.
- - استخدام برامج التحليل الجنائي لفحص الملفات والبيانات.
- - البحث عن الملفات المحذوفة واسترجاعها.
- - تحليل سجلات النظام والبرامج.

وتحليل الأدلة الرقمية عملية معقدة تتطلب مهارات متخصصة وأدوات متطورة. الهدف النهائي منها هو استخلاص معلومات ذات معنى يمكن استخدامها في التحقيق وفي المحكمة.

تحليل الأدلة الرقمية

4. تتبع مصدر الهجمات:

تتبع مصدر الهجمات في الجرائم الرقمية عملية معقدة وحساسة تتطلب مهارات تقنية عالية ومنهجية دقيقة ، ويمكن اتباع الخطوات التالية لتتبع مصادر الهجمات:

أ. جمع البيانات الأولية:

- - تحليل سجلات النظام والشبكة.
- - جمع عناوين IP المشبوهة.
- - تحديد أنماط الهجوم وتوقيتاته.

تتبع مصدر الهجمات

ب. تحليل حركة المرور الشبكية:

تحليل حركة المرور الشبكية هو عنصر أساسي في التحقيق في الجرائم الرقمية. يوفر رؤى قيمة حول طبيعة الهجمات وأساليب المهاجمين. إليك شرحًا مفصلاً لكيفية إجراء هذا التحليل:

- - استخدام أدوات تحليل الشبكة مثل Wireshark.
- - دراسة بروتوكولات الاتصال المستخدمة.
- - تحديد أي اتصالات غير عادية أو مشبوهة.

1. جمع البيانات:

- - استخدام أدوات التقاط الحزم مثل Wireshark أو tcpdump.
- - تكوين أجهزة الشبكة (مثل جدران الحماية والموجهات) لتسجيل حركة المرور.
- - جمع سجلات من أنظمة كشف/منع التسلل (IDS/IPS).

تتبع مصدر الهجمات

2. تصفية وفرز البيانات:

- - استخدام فلاتر لتحديد حركة المرور ذات الصلة.
- - فرز البيانات حسب المصدر والوجهة وأنواع البروتوكولات.

3. تحليل البروتوكولات:

- - دراسة البروتوكولات المستخدمة (مثل HTTP, HTTPS, DNS, FTP).
- - البحث عن استخدام غير عادي للبروتوكولات.

4. تحليل عناوين IP:

- - تحديد عناوين IP المشبوهة.
- - البحث عن أنماط في توزيع عناوين IP المصدر والوجهة.

تتبع مصدر الهجمات

5. دراسة أنماط حركة المرور:

- - تحليل حجم البيانات المتبادلة وتوقيتها.
- - البحث عن زيادات مفاجئة في حركة المرور.

6. فحص محتوى الحزم:

- - تحليل محتوى الحزم للبحث عن بيانات مشبوهة.
- - فك تشفير حركة المرور المشفرة إذا كان ذلك ممكنًا قانوناً.

7. تحليل الـ Payload:

- - فحص محتوى الـ Payload للبحث عن شفرات خبيثة.
- - تحليل أي ملفات تم نقلها عبر الشبكة.

تتبع مصدر الهجمات

8. دراسة سلوك التطبيقات:

- - تحليل كيفية تفاعل التطبيقات مع الشبكة.
- - البحث عن سلوك غير عادي للتطبيقات.

9. تحليل الاتصالات:

- - دراسة أنماط الاتصال بين الأجهزة.
- - تحديد أي اتصالات مع خوادم التحكم والسيطرة المعروفة.

10. تحليل الوقت:

- - دراسة توقيت الأحداث وتسلسلها.
- - البحث عن أنماط زمنية في النشاط المشبوه.

تتبع مصدر الهجمات

12. تحليل الـ DNS:

- - فحص طلبات واستجابات DNS.
- - البحث عن أسماء نطاقات مشبوهة أو غير عادية.

13. تحليل التشفير:

- - تحديد أنواع التشفير المستخدمة.
- - البحث عن استخدام غير عادي للتشفير

14. تحليل التدفق:

- - استخدام أدوات تحليل التدفق لدراسة أنماط حركة المرور على مدى فترات طويلة.
- - تحديد الاتجاهات والأنماط غير العادية.

تتبع مصدر الهجمات

15. **تحليل البروتوكولات الخاصة:**
- - البحث عن استخدام بروتوكولات غير قياسية أو معدلة.
- - تحليل أي بروتوكولات مخصصة قد يستخدمها المهاجمون.

16. **تحليل التسرب:**
- - البحث عن أدلة على تسرب البيانات.
- - تحديد أنواع البيانات التي تم نقلها خارج الشبكة.

17. **استخدام تقنيات التعلم الآلي:**
- - تطبيق خوارزميات التعلم الآلي لكشف الأنماط غير العادية.
- - استخدام أنظمة الكشف عن الشذوذ لتحديد السلوك المشبوه.

تتبع مصدر الهجمات

18. تحليل الاستجابة:

- - دراسة كيفية استجابة الشبكة للهجمات المحتملة.
- - تقييم فعالية آليات الدفاع الموجودة.

19. إعداد التقارير:

- - توثيق جميع النتائج بشكل منهجي.
- - إنشاء تمثيلات بصرية للبيانات لتسهيل الفهم.

تتبع مصدر الهجمات

20. التحليل المستمر:

- - إنشاء آليات للمراقبة المستمرة لحركة المرور.
- - تحديث أساليب التحليل باستمرار لمواكبة التهديدات الجديدة.
- - تحليل حركة المرور الشبكية يتطلب مهارات تقنية عالية وفهمًا عميقًا لبروتوكولات الشبكة وتقنيات الهجوم.
- - يجب أن يتم هذا التحليل في إطار قانوني وأخلاقي، مع احترام خصوصية المستخدمين
- وحقوقهم.
- - النتائج المستخلصة من هذا التحليل يمكن أن تكون حاسمة في كشف وفهم وتوثيق الجرائم الرقمية.

تتبع مصدر الهجمات

20. التحليل المستمر:

- - إنشاء آليات للمراقبة المستمرة لحركة المرور.
- - تحديث أساليب التحليل باستمرار لمواكبة التهديدات الجديدة.
- - تحليل حركة المرور الشبكية يتطلب مهارات تقنية عالية وفهمًا عميقًا لبروتوكولات الشبكة وتقنيات الهجوم.
- - يجب أن يتم هذا التحليل في إطار قانوني وأخلاقي، مع احترام خصوصية المستخدمين
- وحقوقهم.
- - النتائج المستخلصة من هذا التحليل يمكن أن تكون حاسمة في كشف وفهم وتوثيق الجرائم الرقمية.

تحليل الأدلة الرقمية

5. تحليل عناوين IP:

يمكن اتباع الخطوات التالية للتحقيق في الجرائم الإلكترونية باستخدام عناوين IP:

- - استخدام قواعد بيانات WHOIS لتحديد مالك العنوان.
- - تحديد الموقع الجغرافي للعنوان IP.
- - البحث عن أنماط أو روابط بين عناوين IP متعددة.
- - استخدام أدوات التحليل الجنائي الرقمي لفحص الأجهزة المرتبطة بعناوين IP المشبوهة.
- - جمع عناوين IP المرتبطة بالنشاط الإجرامي المشتبه به.
- - تحليل سجلات الاتصال وحركة المرور المرتبطة بعنوان IP المشبوه.

للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك
عدة خطوات وتقنيات هامة في هذا الشأن، نجملها فيما يلي:

4 توثيق النتائج

- إعداد تقارير مفصلة عن الأدلة المكتشفة.
- تسجيل تسلسل الأحداث وحفظ الأدلة.

توثيق النتائج

- - استخدام أدوات تحديد الموقع الجغرافي لـ IP لتحديد الموقع التقريبي للعنوان.
- - البحث عن أي استخدام لشبكات VPN أو خدمات إخفاء الهوية.
- - الاستعلام عن معلومات التسجيل من سجلات الإنترنت الإقليمية (RIRs) لمعرفة مزود خدمة الإنترنت المسؤول.
- - التواصل مع مزود الخدمة للحصول على معلومات إضافية عن العميل، مع مراعاة الإجراءات القانونية.
- - توثيق جميع الخطوات والنتائج بدقة لاستخدامها كأدلة محتملة.

6. تحليل البرمجيات الخبيثة:

تحليل البرمجيات الخبيثة أجراء هام في مجال التحقيق في الجرائم الإلكترونية، يمكن اتباع الخطوات التالية لتحليل البرمجيات الخبيثة:

العزل الآمن:

- - إنشاء بيئة افتراضية معزولة لتحليل البرمجيات الخبيثة بأمان.
- - استخدام أدوات مثل VMware أو VirtualBox لإنشاء أجهزة افتراضية.
- - عزل وتحليل أي برمجيات خبيثة مستخدمة في الهجوم.
- - تحديد "بصمة" البرمجية الخبيثة ومقارنتها مع قواعد البيانات المعروفة.
- - تحليل شفرة البرمجية للبحث عن أدلة على مصدرها.

6. تحليل البرمجيات الخبيثة:

التحليل الثابت:

- - فحص شفرة البرمجية الخبيثة دون تشغيلها.
- - استخدام أدوات مثل IDA Pro أو Ghidra لتفكيك الكود والتحليل.

التحليل الديناميكي:

- - تشغيل البرمجية الخبيثة في بيئة محكومة لمراقبة سلوكها.
- - استخدام أدوات مثل Process Monitor وWiresharkg لتتبع النشاط.

تحليل الشبكة:

- - مراقبة اتصالات الشبكة التي تقوم بها البرمجية الخبيثة.
- - تحديد عناوين IP وبروتوكولات الاتصال المستخدمة.

6. تحليل البرمجيات الخبيثة:

- استخراج المعلومات:

- - البحث عن مؤشرات الاختراق (IoCs) مثل التواقيع وعناوين IP.
- - تحديد وظائف البرمجية الخبيثة وأهدافها.

- تحليل التشفير:

- - الكشف عن أي تقنيات تشفير مستخدمة لإخفاء النشاط.
- - محاولة فك التشفير لاستخراج المزيد من المعلومات.

- تحليل البيانات المستخرجة:

- - دراسة أي بيانات تم جمعها أو سرقتها بواسطة البرمجية الخبيثة.

- إعداد التقارير:

- - توثيق جميع النتائج بشكل شامل لاستخدامها في التحقيقات.

توثيق النتائج

7. تحليل التكتيكات والتقنيات والإجراءات (TTPs):

تحليل التكتيكات والتقنيات والإجراءات (TTPs) في الجرائم الإلكترونية هو نهج استراتيجي مهم لفهم أساليب المهاجمين وطرق عملهم ،ويمكن اتباع الخطوات التالية لتحليل التكتيكات والتقنيات والإجراءات:-

أ. تعريف TTPs:

1. - **التكتيكات**: الأهداف العامة للمهاجم.
2. - **التقنيات**: الطرق المستخدمة لتحقيق هذه الأهداف.
3. - **الإجراءات**: الخطوات التفصيلية المتبعة في الهجوم.

توثيق النتائج

ه. تحليل الأدوات:

- - دراسة الأدوات والبرامج المستخدمة في الهجوم.
- - تحديد ما إذا كانت أدوات مخصصة أو متاحة للعموم.

و. فهم الدوافع:

- - تحليل الأهداف المحتملة للمهاجمين (مالية، سياسية، إلخ).
- - ربط الدوافع بالتكتيكات المستخدمة.

توثيق النتائج

ز. تحديد البنية التحتية للهجوم:

- - تحليل عناوين IP وأسماء النطاقات المستخدمة.
- - دراسة البنية التحتية للقيادة والتحكم (C2).
- - دراسة أساليب الهجوم المستخدمة.
- - مقارنة الأساليب مع هجمات سابقة معروفة
- - تحديد أي "توقيع" فريد للمهاجم

ر. تحليل التطور:

- - مقارنة TTPs الحالية مع الهجمات السابقة.
- - تحديد كيفية تطور أساليب المهاجمين مع مرور الوقت.

توثيق النتائج

ك. إنشاء ملف تعريف للمهاجم:

- - جمع كل المعلومات لإنشاء صورة شاملة عن المهاجم وأساليبه.

ل. تطوير استراتيجيات الدفاع:

- - استخدام فهم TTPs لتحسين الأمن وإجراءات الاستجابة للحوادث.

ن. مشاركة المعلومات:

- - التعاون مع المجتمع الأمني لمشاركة المعلومات حول TTPs الجديدة.

8. تحليل البريد الإلكتروني:

تحليل البريد الإلكتروني يعد جزءًا حيويًا في التحقيقات المتعلقة بالجرائم الإلكترونية ، ويمكن اتباع الخطوات التالية لتحليل تحليل التكتيكات والتقنيات والإجراءات:-

أ. استخراج البيانات:

- - جمع رسائل البريد الإلكتروني ذات الصلة من الخوادم أو أجهزة المستخدمين.
- - الحفاظ على سلامة البيانات باستخدام أدوات الطب الشرعي الرقمي.

ب. تحليل الرأس (Header):

- - فحص معلومات الرأس لتحديد المرسل الحقيقي والمسار الذي سلكته الرسالة.
- - التحقق من عناوين IP وأوقات الإرسال.

8. تحليل البريد الإلكتروني:

ج. تحليل المحتوى:

- - دراسة نص الرسالة بحثًا عن أدلة أو كلمات مفتاحية.
- - تحليل اللغة المستخدمة وأسلوب الكتابة.

د. فحص المرفقات:

- - تحليل أي ملفات مرفقة بحثًا عن برمجيات خبيثة.
- - استخدام أدوات مثل VirusTotal لفحص المرفقات.

ه. تحليل الروابط:

- - فحص أي روابط واردة في الرسالة.
- - تحليل الوجهة الحقيقية للروابط المختصرة.

8. تحليل البريد الإلكتروني:

و. تحليل البنية التحتية:

- - تتبع مصدر الرسائل الإلكترونية إلى خوادم البريد المستخدمة.
- - تحديد ما إذا كانت الرسائل جزءًا من حملة أوسع.

ز. تحليل النمط:

- - البحث عن أنماط في الرسائل المتعددة.
- - ربط الرسائل بحملات تصيد أو هجمات معروفة.

ك. استخراج المعلومات الجغرافية:

- - استخدام معلومات IP لتحديد الموقع المحتمل للمرسل.

ل. تحليل التوقيع الرقمي:

- - التحقق من صحة التوقيعات الرقمية إن وجدت.
- - تحديد ما إذا كانت الرسائل قد تم التلاعب بها.

8. تحليل البريد الإلكتروني:

م. تحليل الصور:

- - فحص البيانات الوصفية للصور المضمنة.
- - البحث عن معلومات مخفية في الصور (Steganography).

ن. ربط الحسابات:

- - تحديد الحسابات المرتبطة بعناوين البريد الإلكتروني المشبوهة.

ي. إعداد التقارير:

- - توثيق جميع النتائج بشكل منهجي.
- - إنشاء تسلسل زمني للأحداث المرتبطة بالرسائل.

9. استخدام مصائد العسل (Honeypots):

استخدام مصائد العسل (Honeypots) هو أسلوب فعال في مكافحة الجرائم الإلكترونية ودراسة سلوك المهاجمين، ويمكن اتباع الخطوات التالية لاستخدام مصائد العسل (Honeypots):

أ. تعريف مصائد العسل:

- - أنظمة أو موارد مصممة لتبدو جذابة للمهاجمين، ولكنها في الواقع مراقبة ومعزولة.

ب. أنواع مصائد العسل:

- - منخفضة التفاعل: تحاكي خدمات بسيطة.
- - عالية التفاعل: أنظمة كاملة تسمح بتفاعل أكبر مع المهاجمين.

مصائد العسل (Honeypots):

ج. أهداف استخدام مصائد العسل:

- - جمع معلومات عن تكتيكات المهاجمين.
- - اكتشاف تهديدات جديدة وبرمجيات خبيثة.
- - تحويل انتباه المهاجمين عن الأنظمة الحقيقية.

د. تنفيذ مصائد العسل:

- - إعداد بنية تحتية منفصلة لمصائد العسل.
- - تكوين أنظمة تبدو جذابة ولكنها آمنة.
- - إعداد أدوات المراقبة والتسجيل.

مصائد العسل (Honeypots):

ه. جمع البيانات:

- - تسجيل جميع الأنشطة على مصائد العسل.
- - جمع عينات من البرمجيات الخبيثة المستخدمة.
- - تحليل أنماط الهجوم وتقنيات الاختراق.

و. تحليل السلوك:

- - دراسة كيفية تفاعل المهاجمين مع النظام.
- - تحديد الأهداف والدوافع المحتملة للمهاجمين.

ز. تحديد مصدر الهجمات:

- - تتبع عناوين IP ومصادر الهجمات.
- - محاولة تحديد هوية أو مجموعة المهاجمين.

مصائد العسل (Honeypots):

ر. اكتشاف التهديدات الجديدة:

- - تحليل أي تقنيات أو برمجيات خبيثة جديدة.
- - تحديث أنظمة الأمان بناءً على المعلومات المكتشفة.

ك. التعاون مع جهات إنفاذ القانون:

- - مشاركة المعلومات المجمعة مع السلطات المختصة.
- - استخدام البيانات كأدلة في التحقيقات الجنائية.

ل. تحسين الدفاعات:

- - استخدام المعرفة المكتسبة لتعزيز أمن الأنظمة الحقيقية.
- - تطوير استراتيجيات دفاعية جديدة بناءً على سلوك المهاجمين.

مصائد العسل (Honeypots):

م. الاعتبارات القانونية والأخلاقية:

- - ضمان الامتثال للقوانين المحلية والدولية.
- - مراعاة الجوانب الأخلاقية في جمع وتحليل البيانات.

ن. تطوير شبكات مصائد العسل:

- - إنشاء شبكات واسعة من مصائد العسل لتغطية نطاق أوسع من التهديدات.

للتحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، هناك عدة خطوات وتقنيات هامة في هذا الشأن، نجملها فيما يلي:

5 التعاون مع الجهات المختصة

- التنسيق مع سلطات إنفاذ القانون.
- الاستعانة بخبراء في مجالات محددة إذا لزم الأمر.

التعاون مع الجهات المختصة

10. تحليل وسائل التواصل الاجتماعي:

تحليل وسائل التواصل الاجتماعي يعد جزءًا هماً في التحقيقات المتعلقة بالجرائم الإلكترونية ، ويمكن اتباع الخطوات التالية لتحليل وسائل التواصل الاجتماعي:

أ. جمع البيانات:

- - استخراج المعلومات المتاحة للعموم من منصات التواصل الاجتماعي.
- - الحصول على أوامر قضائية للوصول إلى البيانات المحمية إذا لزم الأمر.

ب. تحليل الملف الشخصي:

- - دراسة معلومات الملف الشخصي والصور.
- - تحليل تاريخ إنشاء الحساب ونشاطه.

تحليل الأدلة الرقمية

ج. تحليل الشبكات الاجتماعية:

- - رسم خريطة للعلاقات بين الحسابات.
- - تحديد الروابط بين الأشخاص والمجموعات ذات الصلة.

د. تحليل المحتوى:

- - دراسة المنشورات والتعليقات بحثًا عن أدلة أو معلومات ذات صلة.
- - تحليل الصور ومقاطع الفيديو المشاركة.

ه. تحليل البيانات الوصفية:

- - فحص البيانات الوصفية للمنشورات والصور (مثل الموقع الجغرافي وتوقيت النشر).

و. تحليل الأنماط السلوكية:

- - دراسة أنماط النشاط وأوقات النشر.

- تحديد السلوكيات غير العادية أو المشبوهة.

تحليل الأدلة الرقمية

ز. تحليل اللغة:

- - دراسة أسلوب الكتابة واللهجات المستخدمة.
- - استخدام تقنيات تحليل النص لاكتشاف الأنماط أو الكلمات المفتاحية.

ر. تتبع الحركة عبر الإنترنت:

- - تحليل الروابط المشاركة والمواقع التي يتم الوصول إليها.
- - تتبع استخدام العملات المشفرة إذا كان ذلك مرتبطًا بالجريمة.

س. تحليل التفاعلات:

- - دراسة التفاعلات مع المنشورات (الإعجابات، التعليقات، المشاركات).
- - تحديد الحسابات الوهمية أو الآلية.

تحليل الأدلة الرقمية

ك. استخدام أدوات التحليل المتخصصة:

- - استخدام برامج مثل Maltego أو IBM i2 لتحليل العلاقات والبيانات.

ل. تحليل الاتجاهات والهاشتاجات:

- - دراسة استخدام الهاشتاجات والمواضيع الشائعة.
- - تحديد الحملات المنسقة أو التأثير على الرأي العام.

م. تحليل الإعلانات:

- - دراسة الإعلانات المستهدفة وكيفية استخدامها في الأنشطة الإجرامية.

تحليل الأدلة الرقمية

ن. التحقق من الهوية:

- - محاولة التحقق من هوية المستخدمين الحقيقية خلف الحسابات.

و. تحليل المجموعات المغلقة:

- - دراسة المجموعات الخاصة والمغلقة المرتبطة بالأنشطة الإجرامية.

ي. إعداد التقارير:

- - توثيق جميع النتائج بشكل منهجي ومفصل.
- - إنشاء تسلسل زمني للأحداث والأنشطة ذات الصلة.

11- التعاون مع الجهات المختصة:

التعاون مع الجهات المختصة في الجرائم الرقمية هو أمر بالغ الأهمية لضمان تحقيق فعال وشامل. هذا التعاون يشمل العديد من الأطراف ويتطلب تنسيقًا دقيقاً ، ويمكن اتباع الخطوات التالية للتعاون الفعال بين الجهات ذات الصلة:

أ. تحديد الجهات ذات الصلة:

- - وحدات الجرائم الإلكترونية في الشرطة.
- - هيئات الأمن السيبراني الوطنية .
- - وكالات الاستخبارات.
- - مكاتب المدعين العامين المتخصصين في الجرائم الإلكترونية.
- - فرق الاستجابة للحوادث الأمنية (CERTs).

ب. إنشاء قنوات اتصال آمنة:

- - استخدام منصات اتصال مشفرة.
- - تحديد نقاط اتصال رئيسية في كل جهة.
- - وضع بروتوكولات لتبادل المعلومات الحساسة.

ج. تبادل المعلومات:

- - مشاركة التقارير الأولية عن الحوادث.
- - تبادل المعلومات الاستخباراتية عن التهديدات الناشئة.
- - إنشاء قاعدة بيانات مشتركة للتهديدات والمهاجمين المعروفين.

د. تنسيق الجهود التحقيقية:

- - عقد اجتماعات منتظمة لتنسيق الاستراتيجيات.
- - تحديد أدوار ومسؤوليات واضحة لكل جهة.
- - تجنب ازدواجية الجهود وتداخل التحقيقات.

ه. التعاون في جمع الأدلة:

- - تنسيق عمليات المداهمة وضبط الأجهزة الإلكترونية.
- - تبادل الخبرات في تقنيات التحليل الجنائي الرقمي.
- - مشاركة الموارد التقنية والمعملية.

و. التعاون القانوني:

- - العمل مع المدعين العامين لضمان قانونية الإجراءات.
- - الحصول على أوامر قضائية وإذن للتفتيش عند الضرورة.
- - تقديم المساعدة في صياغة لوائح الاتهام.

ز. التعاون الدولي:

- - التنسيق مع الإنتربول ووكالات إنفاذ القانون الدولية.
- - استخدام اتفاقيات المساعدة القانونية المتبادلة (MLATs).
- - تبادل المعلومات مع الشركاء الدوليين حول التهديدات العابرة للحدود.

ر. التعاون مع القطاع الخاص:

- - العمل مع شركات الأمن السيبراني لتحليل التهديدات.
- - التنسيق مع مزودي خدمات الإنترنت للحصول على معلومات حول حركة المرور.
- - التعاون مع الشركات التكنولوجية الكبرى لمكافحة الجرائم على منصاتهم.

س. تدريب وبناء القدرات:

- - تنظيم دورات تدريبية مشتركة لتحسين المهارات التقنية.
- - تبادل أفضل الممارسات والدروس المستفادة.
- - إجراء تمارين محاكاة لتحسين الاستجابة للحوادث.

ك. إنشاء فرق عمل مشتركة:

- - تشكيل فرق متعددة التخصصات للتعامل مع قضايا معقدة.
- - دمج خبراء من مختلف الوكالات في فريق واحد.

ل. التعاون في مجال البحث والتطوير:

- - العمل مع الجامعات ومراكز البحوث لتطوير تقنيات جديدة.
- - المشاركة في مشاريع بحثية مشتركة حول التهديدات الناشئة.

م. التوعية العامة:

- - تنسيق حملات التوعية حول الأمن السيبراني.
- - نشر معلومات موحدة عن التهديدات الحالية والوقاية منها.

ن. التعامل مع وسائل الإعلام:

- - تنسيق البيانات الصحفية والتصريحات العامة.
- - ضمان توافق الرسائل الإعلامية بين مختلف الجهات.

و. إدارة الأزمات:

- - إنشاء مركز عمليات مشترك للتعامل مع الحوادث الكبرى.
- - تطوير خطط استجابة موحدة للهجمات واسعة النطاق.

ي. المراجعة والتقييم:

- - إجراء تقييمات دورية لفعالية التعاون.
- - تحديد مجالات التحسين وتنفيذ التغييرات اللازمة.

والتعاون الفعال بين الجهات المختصة يعزز القدرة على مكافحة الجرائم الرقمية بشكل أكثر كفاءة وشمولية ، كما يساعد هذا التعاون في سد الثغرات التي قد يستغلها المجرمون، ويضمن استجابة أسرع وأكثر فعالية للتهديدات السيبرانية المتطورة باستمرار.

من المهم أن يتم إجراء التحقيق من قبل خبراء متخصصين في الأمن السيبراني والتحقيق الرقمي، مع الالتزام بالإجراءات القانونية لضمان صحة الأدلة وقبولها في المحكمة.

12. التعاون الدولي:

التعاون الدولي يعد عنصراً حاسماً في مكافحة الجرائم الإلكترونية ، نظراً لطبيعتها العابرة للحدود، ويمكن اتباع الخطوات التالية للتعاون الفعال علي الصعيد الدولي:

أ. الاتفاقيات الدولية:

- - اتفاقية بودابست للجريمة السيبرانية: أول معاهدة دولية تعالج الجرائم الإلكترونية.
- - اتفاقيات ثنائية ومتعددة الأطراف بين الدول لتسهيل التعاون.
- ب. تبادل المعلومات:
- - إنشاء قنوات آمنة لتبادل المعلومات الاستخباراتية.
- - مشاركة البيانات حول التهديدات الناشئة والتقنيات الجديدة.

ج. التعاون في إنفاذ القانون:

- - تنسيق العمليات عبر الحدود.
- - تبادل الأدلة الرقمية وفقًا للإجراءات القانونية.

د. المساعدة القانونية المتبادلة:

- - إجراءات رسمية لطلب المساعدة في التحقيقات والملاحقات القضائية.
- - تسريع عمليات تسليم المجرمين في قضايا الجرائم الإلكترونية.

ه. بناء القدرات:

- - تدريب مشترك للمحققين وخبراء الأمن السيبراني.
- - نقل المعرفة والخبرات بين الدول المتقدمة والنامية.

ز. توحيد المعايير:

- - العمل على توحيد التشريعات المتعلقة بالجرائم الإلكترونية.
- - تطوير معايير مشتركة لجمع الأدلة الرقمية وتحليلها.

ر. التعاون مع القطاع الخاص:

- - إشراك شركات التكنولوجيا الكبرى في جهود مكافحة الجريمة.
- - التعاون مع مزودي خدمات الإنترنت لتتبع الأنشطة الإجرامية.

د. المنظمات الدولية:

- - دور الإنتربول في تنسيق العمليات الدولية.
- - مبادرات الأمم المتحدة والاتحاد الأوروبي في مجال الأمن السيبراني.

ك. فرق الاستجابة للطوارئ الحاسوبية (CERT):

- - التعاون بين فرق CERT الوطنية لمواجهة التهديدات العالمية.

ل. البحث والتطوير المشترك:

- - مشاريع بحثية دولية لتطوير تقنيات جديدة لمكافحة الجرائم الإلكترونية.

م. التصدي للتحديات القانونية:

- - معالجة قضايا الولاية القضائية في الفضاء السيبراني.
- - تطوير آليات لحل النزاعات في القضايا العابرة للحدود.

ن. حماية البيانات والخصوصية:

- - ضمان التوازن بين التعاون الدولي وحماية حقوق الأفراد.

و. الدبلوماسية السيبرانية:

- - تطوير قنوات دبلوماسية للتعامل مع قضايا الأمن السيبراني الدولية.

ي. التعاون في مجال الأدلة الرقمية:

- - تطوير بروتوكولات موحدة لجمع وتحليل وتبادل الأدلة الرقمية.

13. تحليل الدلائل اللغوية:

تحليل الدلائل اللغوية في الجرائم الإلكترونية، المعروف أيضًا باسم علم اللغويات الجنائية الرقمية، هو مجال مهم في التحقيقات الجنائية الرقمية ، ويمكن اتباع الخطوات التالية في مجال تحليل الدلائل اللغوية:

أ. تعريف التحليل اللغوي الجنائي:

- - دراسة اللغة المستخدمة في الاتصالات الإلكترونية لغرض التحقيق الجنائي.

ب. مجالات التطبيق:

- - تحديد هوية المؤلف في الرسائل المجهولة.
- - كشف الاحتيال والتهديدات عبر الإنترنت.
- - تحليل محتوى وسائل التواصل الاجتماعي والمنتديات.

ج. تقنيات التحليل:

- - تحليل الأسلوب: دراسة الخصائص الفريدة لأسلوب الكتابة.
- - تحليل المفردات: فحص اختيار الكلمات واستخدامها.
- - تحليل النحو والتركيب: دراسة بنية الجمل والقواعد اللغوية.

د. استخدام الذكاء الاصطناعي:

- - توظيف خوارزميات معالجة اللغة الطبيعية (NLP).
- - استخدام تقنيات التعلم الآلي لتحديد الأنماط اللغوية.

ه. تحليل اللهجات والتنوعات اللغوية:

- - تحديد الخلفية الجغرافية أو الثقافية للمؤلف.
- - دراسة استخدام اللغة العامية أو المصطلحات الخاصة.

و. تحليل الأخطاء اللغوية:

- - دراسة الأخطاء الإملائية والنحوية المميزة.
- - تحليل الأخطاء الناتجة عن استخدام لغة غير أصلية.

ز. تحليل السياق:

- - فهم السياق الثقافي والاجتماعي للغة المستخدمة.
- - تحليل الإشارات الضمنية والتلميحات في النص.

ك. مقارنة النصوص:

- - مقارنة النصوص المشتبه بها مع نماذج معروفة.
- - استخدام تقنيات القياس الكمي لتحديد التشابهات.

ل. تحليل العواطف والنوايا:

- - تقييم النبرة العاطفية في النص.
- - تحديد النوايا المحتملة وراء الرسائل.

م. التعامل مع اللغات المتعددة:

- - تحليل النصوص في حالات استخدام لغات متعددة أو مختلطة.
- - دراسة أنماط التبديل اللغوي.

ن. تحليل الرموز والاختصارات:

- - فهم الرموز واللغة المشفرة المستخدمة في المجتمعات الإلكترونية.
- - تحليل استخدام الإيموجي والرموز التعبيرية.

ه. إعداد التقارير الخبيرة:

- - صياغة تقارير تحليلية مفصلة للاستخدام في المحاكم.
- - تقديم شهادات الخبراء في القضايا الجنائية.

و. التحديات والاعتبارات الأخلاقية:

- - مراعاة حدود دقة التحليل اللغوي.
- - الالتزام بالمعايير الأخلاقية في جمع وتحليل البيانات اللغوية.

ي. التطور المستمر:

- - مواكبة التغيرات في اللغة المستخدمة عبر الإنترنت.
- - تطوير أدوات وتقنيات جديدة لمواجهة التحديات المتغيرة.

14. تتبع التحويلات المالية:

تتبع التحويلات المالية يعد عنصراً حاسماً في التحقيق في الجرائم الإلكترونية، خاصة في قضايا غسل الأموال والاحتيال المالي، ويمكن اتباع الخطوات التالية في مجال تتبع التحويلات المالية:

أ. تحديد مصادر الأموال:

- - تتبع الأموال إلى مصدرها الأصلي.
- - تحليل الحسابات المصرفية والمعاملات الأولية.

ب. تحليل أنماط التحويل:

- - دراسة تكرار وحجم وتوقيت التحويلات.
- - تحديد الأنماط غير العادية أو المشبوهة.

ج. تتبع العملات المشفرة:

- - استخدام أدوات تحليل البلوكتشين لتتبع المعاملات.
- - تحديد محافظ العملات المشفرة المرتبطة بالأنشطة الإجرامية.

د. التعاون مع المؤسسات المالية:

- - الحصول على سجلات المعاملات من البنوك وشركات التحويل.
- - استخدام آليات الإبلاغ عن المعاملات المشبوهة.

ه. تحليل الشبكات المالية:

- - رسم خرائط للعلاقات بين الحسابات والكيانات المالية.
- - تحديد الشبكات المعقدة المستخدمة في غسل الأموال.

و. استخدام تقنيات التحليل المتقدمة:

- - توظيف الذكاء الاصطناعي وتعلم الآلة لكشف الأنماط المعقدة.
- - استخدام تحليل البيانات الضخمة لمعالجة كميات هائلة من المعلومات المالية.

ز. تتبع التحويلات عبر الحدود:

- - التعاون مع السلطات الدولية لتتبع الأموال عبر الدول.
- - تحليل استخدام الحوالات والتحويلات غير الرسمية.

س. دراسة الشركات الوهمية والواجهات:

- - تحليل الهياكل التنظيمية للشركات المشبوهة.
- - كشف استخدام الشركات الوهمية في إخفاء مصادر الأموال.

ش. تحليل المعاملات النقدية:

- - تتبع عمليات السحب والإيداع النقدي.
- - تحديد محاولات تجزئة المعاملات لتجنب حدود الإبلاغ.

ص. استخدام تقنيات التحليل المالي:

- - تطبيق أساليب المحاسبة الجنائية.
- - تحليل التدفقات النقدية والميزانيات العمومية.

ض. تتبع الأصول الرقمية:

- - تحليل شراء وبيع الأصول الرقمية مثل NFTs.
- - تتبع استخدام منصات التداول الإلكترونية.

ط. تحليل أنظمة الدفع البديلة:

- - دراسة استخدام خدمات الدفع الإلكترونية مثل PayPal وVenmo.
- - تتبع المعاملات عبر تطبيقات التحويل المالي المشفرة.

ظ. التعامل مع البيانات المشفرة:

- - استخدام تقنيات فك التشفير لتحليل المعلومات المالية المحمية.
- - التعاون مع خبراء الأمن السيبراني لفك شفرات الاتصالات المالية.

ع. إعداد التقارير المالية الجنائية:

- - توثيق مسارات الأموال بشكل دقيق ومفصل.
- - إعداد تقارير قابلة للاستخدام في المحاكم.

15. استخدام تقنيات التحليل المتقدمة:

استخدام تقنيات التحليل المتقدمة من الأمور الهامة في مجال التحقيق في جرائم الإلكترونية ، ويمكن اتباع الخطوات التالية في مجال أستخدام تقنيات التحليل المتقدمة:

أ. تحليل البيانات الضخمة:

- - استخدام خوارزميات متطورة لتحليل كميات هائلة من البيانات الرقمية.
- - الكشف عن الأنماط والعلاقات غير الواضحة بين مجموعات البيانات المختلفة.

ب. الذكاء الاصطناعي وتعلم الآلة:

- - استخدام نماذج التعلم الآلي للتنبؤ بالسلوك الإجرامي المحتمل.
- - تطوير أنظمة ذكية قادرة على التعرف التلقائي على الأنشطة المشبوهة.

ج. تحليل الشبكات الاجتماعية:

- - دراسة العلاقات والتفاعلات بين الأفراد والمجموعات عبر منصات التواصل الاجتماعي.
- - تحديد الشبكات الإجرامية المحتملة وقنوات الاتصال المستخدمة.

د. التحليل الجنائي الرقمي:

- - استرجاع وتحليل البيانات من الأجهزة الإلكترونية المصادرة.
- - استخدام أدوات متخصصة لاستعادة البيانات المحذوفة أو المشفرة.

ه. تحليل السلوك على الإنترنت:

- - تتبع وتحليل أنماط التصفح وسجلات الاتصال.
- - الكشف عن الأنشطة المشبوهة أو غير العادية.

و. تحليل العملات المشفرة:

- - تتبع المعاملات المالية المشبوهة باستخدام العملات الرقمية.
- - تحليل سلاسل الكتل (blockchain) للكشف عن الأنشطة غير القانونية.

ز. التحليل اللغوي الحاسوبي:

- - تحليل المحتوى النصي للرسائل والمنشورات للكشف عن التهديدات أو الأنشطة الإجرامية
- - استخدام تقنيات معالجة اللغة الطبيعية لفهم السياق والنوايا

16. إعادة بناء الهجوم:

أسلوب إعادة بناء الهجوم في مجال الجرائم الإلكترونية يعد تقنية هامة في مجال التحقيقات الرقمية ، وهذه العملية تساعد المحققين على فهم كيفية حدوث الهجوم الإلكتروني وتحديد نقاط الضعف في الأنظمة ، ويمكن اتباع الخطوات التالية في مجال أستخدام أسلوب إعادة بناء الهجوم في الجرائم الإلكترونية:

أ. جمع الأدلة الرقمية:

- - تجميع السجلات والبيانات من الأنظمة المتأثرة.
- - استخراج المعلومات من الأجهزة والشبكات المستهدفة.

ب. تحليل البيانات:

- - فحص السجلات والبيانات المجمعة بدقة.
- - البحث عن أنماط وعلامات مميزة للهجوم.

ج. تحديد نقطة الدخول:

- - تعيين الطريقة التي استخدمها المهاجم للوصول إلى النظام.
- - تحليل الثغرات الأمنية التي تم استغلالها.

د. تتبع مسار الهجوم:

- - إعادة بناء الخطوات التي اتخذها المهاجم داخل النظام.
- - تحديد الأنشطة الضارة التي تم تنفيذها.

ه. تحديد الأدوات والتقنيات المستخدمة:

- - التعرف على البرمجيات الخبيثة أو الأدوات المستخدمة في الهجوم.
- - تحليل أساليب التشفير أو التمويه المستخدمة.

و. تقييم الأضرار:

- - تحديد مدى تأثير الهجوم على النظام والبيانات.
- - تقييم البيانات التي تم الوصول إليها أو سرقتها.

ز. تحديد هوية المهاجم (إن أمكن):

- - البحث عن أدلة قد تشير إلى هوية المهاجم أو موقعه.
- - تحليل أسلوب الهجوم للمقارنة مع هجمات معروفة سابقة.

ك. توثيق النتائج:

- - إعداد تقرير مفصل يصف عملية إعادة بناء الهجوم.
- - تقديم توصيات لتحسين الأمن ومنع الهجمات المستقبلية.

ل. التعلم واستخلاص الدروس:

- - استخدام المعلومات المكتسبة لتحسين الأنظمة الدفاعية.
- - تطوير استراتيجيات جديدة لمواجهة التهديدات المماثلة.

وهذه العملية يجب أن تتم بشكل قانوني وأخلاقي، مع احترام الخصوصية وحقوق الأفراد.

كما أن التعاون بين مختلف الجهات المعنية (مثل فرق الأمن السيبراني وجهات إنفاذ القانون) يكون ضرورياً لنجاح هذه العملية.

17. توثيق النتائج:

توثيق النتائج في الجرائم الرقمية خطوة حاسمة في التحقيقات الجنائية الرقمية. والتوثيق الدقيق والشامل للنتائج في الجرائم الرقمية يعزز مصداقية التحقيق ويسهل فهم القضية سواء من قبل المحققين الآخرين أو المحامين أو القضاة ، كما يضمن قانونية جميع الإجراءات المتخذة، مما يزيد من احتمالية قبول الأدلة في المحكمة.

ويجب أن يكون التوثيق شاملاً ودقيقاً لضمان قبوله في المحكمة وفعاليته في التحقيق ، ويمكن اتباع الخطوات التالية لتحقي توثيق نتائج فعال:

أ. إنشاء ملف القضية:

- - تخصيص رقم فريد للقضية.
- - تسجيل التفاصيل الأساسية (التاريخ، الوقت، الموقع، الأطراف المعنية).
- - إنشاء فهرس لجميع الوثائق والأدلة المجمعة.

ب. وصف منهجية التحقيق:

- - توثيق جميع الخطوات المتخذة في التحقيق بالتفصيل.
- - شرح الأدوات والتقنيات المستخدمة.
- - تبرير اختيار طرق التحقيق المحددة

ج. توثيق الأدلة الرقمية:

- - تسجيل تفاصيل كل قطعة من الأدلة الرقمية (نوع الملف، الحجم، التاريخ).
- - توثيق القيم الهاشية (hash values) للملفات لإثبات سلامتها.
- - وصف مكان وكيفية استخراج كل دليل.

د. سجلات سلسلة الحيازة:

- - تتبع حركة كل دليل رقمي منذ جمعه حتى تقديمه.
- - توثيق كل شخص تعامل مع الدليل وسبب تعامله معه.
- - تسجيل أي نسخ أو نقل للبيانات.

ه. تحليل البيانات:

- - شرح عملية تحليل البيانات بالتفصيل.
- - توثيق النتائج الرئيسية والاكتشافات.
- - تضمين الرسوم البيانية والمخططات لتوضيح النتائج.

و. تقارير الأدوات المستخدمة:

- - إرفاق تقارير مفصلة من أدوات التحليل الجنائي الرقمي.
- - شرح معنى النتائج التقنية بلغة مفهومة.

ر. تحليل الأنماط والعلاقات:

- - توثيق أي أنماط أو علاقات ملحوظة في البيانات.
- - شرح كيفية ارتباط مختلف الأدلة ببعضها البعض.

س. توثيق المقابلات:

- - تسجيل تفاصيل أي مقابلات أجريت خلال التحقيق.
- - تضمين نصوص المقابلات أو ملخصات دقيقة.

ش. تقييم موثوقية الأدلة:

- - مناقشة أي قيود أو شكوك في الأدلة المجمعة.
- - تقييم مدى موثوقية مصادر المعلومات.

ص. الاستنتاجات والتوصيات:

- - تقديم استنتاجات مبنية على الأدلة.
- - تقديم توصيات للإجراءات المستقبلية أو التحقيقات الإضافية.

ض. الملاحق:

- - إرفاق أي وثائق داعمة أو بيانات خام.
- - تضمين قائمة بالمصطلحات التقنية وشرحها.

ط. مراجعة النظراء:

- - توثيق أي مراجعة للتقرير من قبل محققين آخرين.
- - تضمين أي تعليقات أو تصحيحات من المراجعة.

ظ. التوقيع والتصديق:

- - توقيع التقرير من قبل المحقق الرئيسي.
- - تصديق التقرير من قبل السلطة المختصة.

ف. تأمين التقرير:

- - ضمان تخزين التقرير بشكل آمن.
- - إنشاء نسخ احتياطية مشفرة.

ق. تحديثات التقرير:

- - توثيق أي تحديثات أو إضافات لاحقة للتقرير.
- - تبرير سبب التحديثات وتاريخها.

JUSTICE
ACADEMY

THANK YOU

FOR YOUR ATTENTION