NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
Est. 1978

جامعة نايف العربية
للعلوم الأمنية
تأسست ١٩٧٨

الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية

دار جامعة نايف للنشر - 2024

NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
Est. 1978

جامعة نايف العربية
للعلوم الأمنية
تأسست ١٩٧٨

الدليل الاسترشادي
للتعامل مع الأدلة الجنائية الرقمية
في الدول العربية

إعـــداد

عبدالرزاق المرجان

محمد شوقي

يوسف السبعاوي

محمد المنشاوي

مراجعة

سيوكي لي

جلال الهاشل

2024

NAIF ARAB UNIVERSITY
FOR SECURITY SCIENCES
Est. 1978

جامعة نايف العربية
للعلوم الأمنية
تأسست ١٩٧٨

The Guidance Manual for Handling Digital Forensic Evidence in Arab Countries

Prepared by

Abdulrazaq Almorjan

Mohamed Shawky

Yousif Al-Sabaawi

Mohammed Minshawy

Reviewed by

Seokhee Lee

Jalal Alhashil

2024

الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية

إعداد: د. عبدالرزاق المرجان[1]، د. محمد شوقي[2]، د.يوسف السبعاوي[3]، د. محمد المنشاوي[2].

مراجعة: د. سيوكي لي[3]، العقيد. جلال الهاشل[4].

[1] مركز الجرائم السيبرانية والأدلة الرقمية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية
[2] كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
[3] المركز العربي للبحوث القانونية والقضائية، بيروت، الجمهورية اللبنانية.
[4] إدارة فحص الجرائم المعلوماتية والأدلة الرقمية، الإدارة العامة للأدلة الجنائية، الرياض، المملكة العربية السعودية.

The Guidance Manual for Handling Digital Forensic Evidence in Arab Countries

Prepared by: Dr. Abdulrazaq Almorjan [1], Dr. Mohamed M. Shawky [2], Dr. Yousif Al-Sabaawi[3], Dr. Mohammed Minshawy[2].

Reviewed by: Dr. Seokhee Lee[3], Col. Jalal Alhashil[4]

[1]Centre of Excellence in Cybercrimes and Digital Forensics, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia

[2]College of Criminal Justice, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

[3]The Arab Center for Legal and Judicial Research, Beirut, Lebanon.

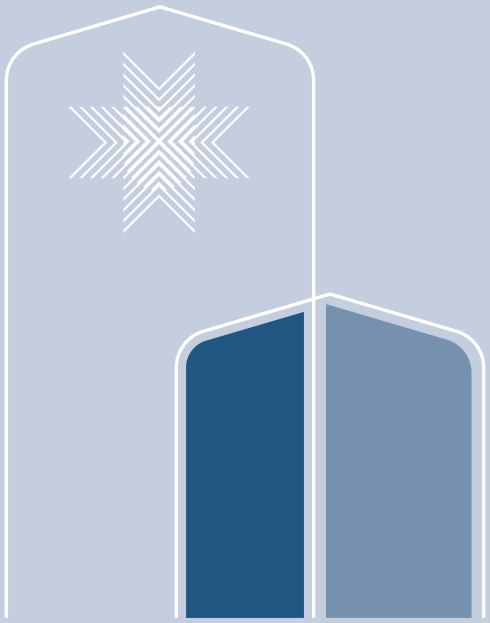
[4]The Electronic Counterfeit Examination Division, General Department of Criminal Evidence, Riyadh, Saudi Arabia.

(ردمك(ورقـــــي ISBN(PBK)978-603-8361-74-0 رقم إيداع (طباعي) pDEPOSIT 1445/19820

(ردمك (إلكتروني ISBN(EBK) 978-603-8361-78-8 رقم إيداع (إلكتروني) eDEPOSIT 1445/19833

DOI:10.26735/978-603-8361-78-8

المحتويات



الملخص التنفيذي

في خضم التطور السريع لتقنية المعلومات والاتصالات والانتشار الكبير للأجهزة الإلكترونية، تواجه الجهات الأمنية تحديًا كبيرًا ومتسارعًا في التعامل مع الأدلة الرقمية. وتؤدي هذه الأدلة التي يجري تخزينها أو نقلها عبر الأجهزة الإلكترونية دورًا أساسيًّا في عدة جرائم مختلفة كالجرائم التقليدية (القتل) أو السيبرانية (الاختراق). ويكمن التحدي في الحصول على دليل رقمي يكون مقبولًا لدى المحاكم لإثبات هذه الجرائم. فقد يكون الدليل الرقمي أحد مصادر الإثبات لجريمة ما أو المصدر الوحيد لإثبات جريمة كجرائم الاختراق أو التزييف العميق للصوت. وتزداد صعوبة التعامل مع الأدلة الرقمية نظرًا لوجودها في مسرح الجريمة التقليدي والرقمي - أجهزة إلكترونية (وعاء رقمي).

وتعتبر مشكلة التعامل مع الأدلة الرقمية من الجانب القانوني والإجرائي والفني في مسرح الجريمة التقليدي والرقمي مشكلة دولية؛ لذا جرى الاطلاع على مجموعة الأنظمة والاتفاقيات الدولية في التعامل مع هذه الأدلة كاتفاقية بودابست لمكافحة جرائم المعلوماتية (2001)، وأفضل الممارسات للاستدلال الجنائي الرقمي الصادر من مكتب الأمم المتحدة المعني بالمخدرات والجريمة، وإرشادات المنظمة الدولية للتوحيد القياسي، ونظام الإثبات السعودي الصادر حديثًا (2022). وفي الجانب الفني جرى الاطلاع على مجموعة من الإرشادات الفنية كمبادئ الإنتربول التوجيهية للمستجيب الأول في مجال الأدلة الجنائية الرقمية، وإرشادات ISO/IEC 27037 لتحديد الأدلة الرقمية وجمعها والحصول عليها والحفاظ عليها.

وجرى تطوير دليل استرشادي للدول العربية للتعامل مع الأدلة الرقمية بناء على أفضل الممارسات الدولية المتعلقة بتحريز الأدلة الرقمية وجمعها في مسرح الجريمة.

وينقسم الدليل إلى جزأين رئيسين: جزء يتعلق بالمسائل القانونية والإجرائية، وجزء يتعلق بالمسائل الفنية والتقنية.

ويقدم هذ الدليل بعض الإرشادات للمختصين والممارسين في المسائل الاستدلالية والقانونية والفنية للحصول على الأدلة الرقمية الموثوقة في المحاكم، بالإضافة إلى احتوائه على نماذج استرشادية، كتحريز الأجهزة وآلية استرشادية لترميز (تسمية) الأدلة الرقمية.

ويسعى هذا الدليل الاسترشادي إلى الإسهام في تحقيق التكامل بين الأجهزة الأمنية والعدلية بهدف خدمة العمل العربي المشترك والوصول إلى نموذج عربي يخدم التطور الحالي للتحقيق الجنائي ورفع كفاءة العمل للخبراء عبر تطوير مخرجات الدليل إلى أدلة تفصيلية وعقد دورات تدريبية للخبراء تسهم في رفع جاهزية الجهات المعنية في التعامل مع الأدلة الرقمية. في المستقبل، ستكون هناك إمكانية لتطوير هذا الدليل الاسترشادي ليسهم في توحيد الإجراءات بين الأجهزة الأمنية والعدلية في الدول العربية ليكون نواة لتبادل الأدلة الرقمية بين الدول العربية.

1. المقدمة

إنّ ثورة تكنولوجيا المعلومات والاتصالات التي شهدها العالم وجعلت منه قرية كونية قد أوجدت فضاءً سيبرانيًّا يمارَس فيه النشاط التجاري والسياسي والاجتماعي والاقتصادي... وقد سهلت الإنترنت التواصل ليس فقط بين البشر، بل تعداه إلى التواصل بين الأشياء، حيث أصبحنا نتحدث عن إنترنت الأشياء والميتافيرس. غير أنّ الفضاء السيبراني، بخدماته المتعدّدة والمتنوعة، لا يخلو من المخاطر التي تهدد المجتمع والأفراد والإدارات والأنظمة المعلوماتية، إذ إنّه شكل مكانًا لارتكاب الأفعال الجرمية، سواء من قِبل الأفراد أو الشبكات الإرهابية، وإنّ أي استخدام لتكنولوجيا المعلومات والاتصالات من قِبل الأفراد من شأنه أن يترك الآثار الرقمية أو البصمة الرقمية. وتوجد هذه الآثار الرقمية في مسرح الجريمة الرقمي. من هنا تكمن أهمية التحقيق الجنائي الرقمي في الاستدلال على الآثار الرقمية واستخراج الأدلة الرقمية من مسرح الجريمة الرقمي؛ ذلك أنّ البيئة الرقمية بما توفّره من خدمات وتقنيات جديدة لها أثر كبير في قواعد وطرق الإثبات أمام القضاء.

في ضوء ما تقدّم، تبرز أهمية وضع دليل استرشادي للتحقيق الجنائي الرقمي في الدول العربية، إذ إنّ المحققين وأجهزة إنفاذ القانون في الدول العربية لديهم أدوات وأساليب عمل وضوابط معينة مختلف بعضها عن بعض، وبالتالي فإنّ هذا الدليل الاسترشادي من شأنه أن يؤدي إلى تسهيل توحيد المعايير المتبعة في التحقيق في مسرح الجريمة الرقمي واعتماد مناهج مماثلة على المستوى العربي، مما يسهل المقارنة في العمل والإجراءات المتبعة وتعزيز التعاون.

ويهدف هذا الدليل إلى بناء القدرات في مجال الأدلة الجنائية الرقمية من خلال تقديم إرشادات للفنيين والمحققين العاملين في مجال التحقيق الجنائي الرقمي، وذلك من أجل تعزيز أساليب وعمليات الممارسات الجيدة في جمع الأدلة الجنائية الرقمية والتحقيق في مسرح الجريمة. ويهدف أيضًا إلى ضمان سلامة البيانات وموثوقيتها واحترام الحق في الخصوصية؛ فالكفاءة والنزاهة والمصداقية من المتطلبات الأساسية في التحقيق الجنائي الرقمي كي تكون الأدلة الرقمية موثوقة ومقبولة من المحاكم. ويجري اتخاذ الاعتبارات القانونية والفنية في الحسبان عند جمع الأدلة الرقمية.

1.1 الاعتبارات القانونية

يحتوي هذا الدليل على الإرشادات القانونية التي تحكم الأدلة الرقمية ويجب مراعاتها في أثناء جمع الأدلة والتحقيق في الجرائم الإلكترونية، حتى يمكن الاعتداد بمشروعيتها أمام المحاكم الجزائية.

2.1 الاعتبارات الفنية

تكمن الاعتبارات الفنية بشكلٍ أساسي في اتباع التقنيات والوسائل الفنية اللازمة للمحافظة على البيانات والأدلة الرقمية وضمان سلامتها في جميع مراحل التحقيق؛ وذلك من أجل الاعتداد بها في التحقيقات الجنائية وإمكانية قبولها أمام المحاكم.

2. المنهجية المتبعة

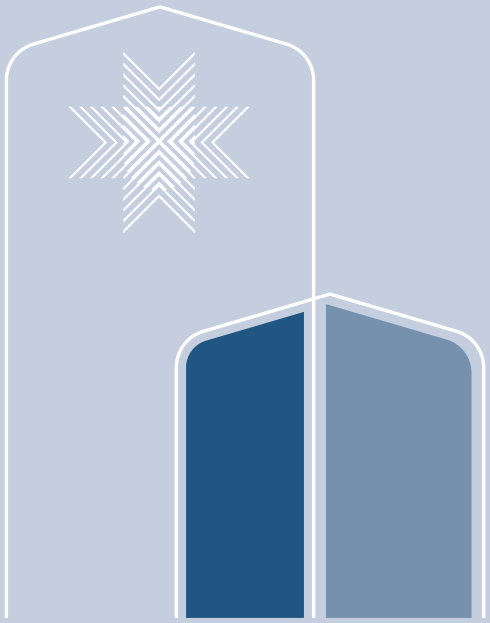
تكوّنت المنهجية المتبعة في إعداد الدليل من أربع مراحل:

المرحلة		الوصف
المرحلة الأولى	اجتماع مع الخبراء العرب	• عقد اجتماع مع الخبراء العرب لمراجعة آليات خطوات إعداد الدليل الاسترشادي.
المرحلة الثانية	جمع وحصر الأنظمة والمراجع الدولية ذات العلاقة	• تحديد ومراجعة القوانين والأنظمة العربية الخاصة بالأدلة الرقمية. • تحديد ومراجعة الأدلة الاسترشادية الدولية الخاصة بالتعامل مع الأدلة الرقمية من الجانبين الإجرائي والتقني في مسرح الجريمة الرقمي.
المرحلة الثالثة	مراجعة التعاميم المتوافرة من الجهات العربية ذات العلاقة	• مراجعة التعاميم والنماذج الخاصة المتعلقة بالأدلة الرقمية.
المرحلة الرابعة	كتابة التقرير	• كتابة الدليل الاسترشادي حسب المعايير المتبعة في جامعة نايف العربية للعلوم الأمنية.

التعريفات

الجرائم السيبرانية	مصطلح شامل يُستخدم لوصف فئتين مختلفتين من الأنشطة الإجرامية مرتبطتين ارتباطًا وثيقًا، هما: الجرائم المعتمدة على الفضاء السيبراني، والجرائم التي يتيحها الفضاء السيبراني.
الجرائم المعتمدة على الفضاء السيبراني	جرائم لا يمكن ارتكابها إلا باستخدام الحاسب أو شبكات الحاسب أو غيرها من أشكال تكنولوجيا المعلومات والاتصالات.
الجرائم التي يتيحها الفضاء السيبراني	جرائم تقليدية، يمكن توسيع نطاقها أو مدى انتشارها باستخدام أجهزة الحاسب أو شبكات الحاسب أو غيرها من أشكال تكنولوجيا المعلومات والاتصالات.
مصادر الأدلة	جهاز إلكتروني (وعاء رقمي) يحتفظ ببيانات إلكترونية كالقرص الصلب، والذاكرة الومضية (الفلاش) والشرائح الإلكترونية والكاميرات الأمنية وGPS.
سلسلة متابعة الأدلة	عملية تتتبَّع حركة الأدلة من خلال دورة حياة جمعها وحمايتها وتحليلها من خلال توثيق كل شخص تعامل مع الأدلة، وتاريخ/وقت جمعها أو نقلها، والغرض من النقل.
ISO/IEC 27037	إرشادات المنظمة الدولية للتوحيد القياسي/اللجنة الكهروتقنية الدولية.
دالة الهاش	قيم رقمية، ناتجة عن دالة التجزئة، تُستخدم لإثبات سلامة الأدلة الرقمية ولإجراء مقارنات التضمين/الاستبعاد على أساس مجموعات القيم المعروفة.

IP	البروتوكول القياسي لنقل البيانات من المصدر إلى الوجهات في شبكات الاتصالات التي تعتمد على تبديل الحزم والأنظمة المتصلة بها من هذه الشبكات.
MAC	يُعرف أيضًا باسم عنوان الجهاز أو عنوان شبكة إيثرنت، وهو معرف فريد خاص ببطاقة الشبكة داخل الحاسوب. ويتيح لخادم البروتوكول تهيئة المضيف الآلية للتأكد من السماح للحاسوب بالوصول إلى الشبكة.
RAM	يستخدم الحاسوب ذاكرة الوصول العشوائي للاحتفاظ بالتعليمات المؤقتة والبيانات اللازمة لإكمال تنفيذ المهام.
صورة (استنساخ) منطقية	تلتقط الصورة المنطقية للجهاز أو محرك الأقراص الثابتة جميع الملفات المرئية للمستخدم، ولا تقوم عادة باستعادة العناصر المحذوفة أو البيانات الموجودة في المناطق المحذوفة من الجهاز، كلك لا تقوم بجمع أجزاء الملفات.
Partition	قسم القرص هو تقسيم منطقي لمحرك الأقراص الثابتة إلى أقسام متعددة. وهو أصغر وحدة تخزين يمكن استخدامها لتخزين البيانات والملفات.
Bitlocker	هي ميزة لحماية البيانات، وهي مدمجة مع نظام التشغيل وتعالج تهديدات سرقة البيانات أو التعرض لها من قِبل أجهزة الحواسيب المفقودة أو المسروقة أو التي جرى إيقاف تشغيلها بشكل غير صحيح.



3- الأدلة الرقمية

1.3 نظرة عامة

الأدلة الرقمية هي جميع الأدلة المستمدة من البيانات المُخزّنة أو المُنتجة بواسطة أجهزة الحاسب الآلي أو الأنظمة المعلوماتية أو المنقولة بواسطتها، التي يمكن اعتمادها بوصفها وسيلة إثبات أمام المحاكم. والأدلة الرقمية هي المعلومات أو البيانات المُخزنة أو المنقولة بتنسيق ثنائي، التي يمكن الاعتماد عليها بوصفها أدلة لدى المحاكم (الإنتربول).

يمكن أن توجد هذه الأدلة على أجهزة متنوعة، مثل: الحواسيب، والهواتف المحمولة، والألواح الذكية، أو الكاميرات، وأجهزة إنترنت الأشياء. وتكون الأدلة الرقمية غالبًا متعلقة بالجرائم السيبرانية، ويُستخدم هذا المصطلح لوصف فئتين مختلفتين من الأنشطة الإجرامية، مرتبطتين ارتباطًا وثيقًا، هما: الجرائم المعتمدة على الفضاء السيبراني، والجرائم التي يتيحها الفضاء السيبراني، مثل: استغلال الأطفال في المواد الإباحية أو الاحتيال فيما يتصل ببطاقات الائتمان. كما يمكن أن تتضمن الأدلة الرقمية نصوصًا، ورسائل بريد إلكتروني، ومنشورات على وسائل التواصل الاجتماعي، وأنواعًا أخرى من البيانات.

2.3 خصائص الأدلة الرقمية

تعد الأدلة الرقمية فريدة من نوعها إذا قورنت بمعايير أدلة أخرى، مثل: بصمات الأصابع ولطخة الدم، ويرجع تفردها إلى الخصائص التالية:

- **مستترة:** لا يمكن رؤية البيانات الموجودة على الأدلة الرقمية ما دامت الأدلة الرقمية لم تكن قيد التشغيل، حيث لا يمكن الوصول إلى بيانات، مثل: سجلات المعاملات، والصفحات الشخصية لمستخدمي وسائل التواصل الاجتماعي، والصور، إلا عندما تكون الأدلة الرقمية قيد التشغيل. ففي حالات، مثل الخادم، لا يمكن الوصول إلى البيانات إلا إذا كان الخادم يعمل (قيد التشغيل). وبالتالي في حالة إيقاف تشغيل الخادم، تتلاشى إمكانية الوصول إلى البيانات، ومن ثم يتعذر أن تساعد على التحقيقات. وفي الحالات التي تكون فيها الأدلة الرقمية قيد إيقاف التشغيل، سوف يستعين مختبر الأدلة الرقمية بأدوات خاصة لتشغيل الأدلة واستخلاص البيانات منها.

- **عابرة للحدود:** يمكن نقل البيانات إلى ولاية قضائية أخرى (عابرة للحدود) بسهولة وسرعة. فعلى سبيل المثال: يمكن لمشتبه به تخزين ووضع قاعدة بيانات مالية لدى مستضيف البيانات (Data host) على الويب داخل الدولة «أ»، وفي اليوم التالي يمكن أن ينقل المشتبه به قاعدة البيانات المالية إلى أحد موفري استضافة على الويب موجود في الدولة «ب»؛ لذا، ينبغي أن يضع المحققون في اعتبارهم أن البيانات لا يُشترط أن توجد دائمًا في المكان المحدد، حيث يمكن بدلًا من ذلك استضافة البيانات في دولة أخرى، لكن يجري الوصول إليها باستخدام جهاز الحاسوب المحمول الخاص بالمشتبه به.

- **سهلة التعديل والإتلاف:** البيانات الموجودة على الأدلة الرقمية يمكن بسهولة تعديلها أو إتلافها بمجرد الضغط لمرة واحدة على أحد المفاتيح. فعلى سبيل المثال: عند قيامك بفتح ملف بتنسيق برنامج معالجة الكلمات MS Word، سوف يجري تحديث تاريخ الوصول (Access Date) إلى الطابع الزمني لآخر وصول. ويمكن أيضًا تعديل البيانات الموجودة في الأدلة الرقمية عن بُعد. بالإضافة إلى ذلك، يمكن بسهولة إتلاف البيانات من خلال استخدام أجهزة مسح البيانات؛ لذا، ينبغي للمحققين توخي الحذر الشديد عند التعامل مع الأدلة الرقمية.

- **حساسة للوقت:** تتسم الأدلة الرقمية بأنها هشة ويسهل إتلافها مع مرور الوقت. فعلى سبيل المثال: الهواتف المحمولة التي احتُفِظ بها لسنوات عديدة ولم يجرِ تشغيلها أو شحنها يمكن ألا تعمل بالصورة المناسبة عند تشغيلها بعد ذلك. وهذا يمكن أن يُعيق التحقيق في قضية ما؛ لذا، يوصى بتقديم أي أدلة رقمية موجودة في مسرح الجريمة إلى مختبر الأدلة الجنائية بأسرع وقت، بحيث يمكن للمختبر استخدام أجهزة متخصصة لإنشاء نسخة طبق الأصل من الأدلة.

- **الثبات:** بمجرد إنشائها أو تخزينها، تميل الأدلة الرقمية إلى الاستمرار مع مرور الوقت نظرًا لإمكانية عمل عدة نسخ منها ومنع الوصول إليها. تتيح هذه الخاصية للمحققين استرجاع المعلومات التي ربما جرى إنشاؤها أو الوصول إليها في الماضي وبذلك يكون الاستدلال بها مضمونًا..

- **الاستقلال المكاني:** الأدلة الرقمية ليست مرتبطة بالموقع الفعلي. يمكن تخزينها ونقلها والوصول إليها من مواقع مختلفة، مما يجعل التحقيق فيها وجمعها أكثر صعوبة ولكن أيضًا أكثر تنوعًا.

- **الموقع المنطقي للدليل:** يجري تغليف الأدلة الرقمية داخل البيئة الرقمية، مما يعني أنها موجودة داخل ملفات أو قواعد بيانات أو أجهزة محددة. إن فهم السياق والعلاقات بين هذه العناصر المغلفة أمر بالغ الأهمية لإجراء تحليل شامل.

- **البيانات الوصفية:** غالبًا ما تأتي الأدلة الرقمية مع بيانات التعريف المرتبطة بها، التي توفر معلومات مهمة حول إنشائها ومصدرها وتعديلها والوصول إليها. تساعد هذه البيانات الوصفية في إثبات صحة الأدلة وسياقها.

4- التعامل مع الأدلة الرقمية من الجانبين القانوني والإجرائي

يركز هذا الفصل على الجانبين القانوني والإجرائي في التعامل مع الأدلة الرقمية. وسيجري تقديم إرشادات في إجراءات الاستدلالات وإجراءات التحقيق وحقوق المتهم باتباع أفضل الممارسات الدولية في التعامل مع الأدلة الرقمية.

وتكمن أهمية مراعاة الإجراءات القانونية في الحصول على الأدلة ومعالجتها لضمان إمكانية قبولها من جانب المحكمة وعدم القضاء ببطلانها.

1.4 الاستدلال الجنائي الرقمي

عملية جمع الاستدلالات هي عبارة عن تقصي الجرائم، والبحث عن مرتكبيها، وجمع الأدلة والمعلومات اللازمة للتحقيق والاتهام في البيئة الرقمية، وهي من اختصاص مأموري الضبط القضائي، وتعتبر خط الدفاع الأول ضد الجرائم المرتكبة، سواء أكانت من الجرائم التقليدية أم من الجرائم السيبرانية (المعلوماتية)، (المعايير وأفضل الممارسات للاستدلال الجنائي الرقمي، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2021). وينبغي عند جمع الاستدلالات في الجرائم الإلكترونية مراعاة ما يلي:

- التأكد من دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الرقمي، وذلك بالتحقق من مدى قدرة هذه الأدوات على عرض جميع البيانات المتعلقة بالدليل الرقمي.
- الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفايتها في تقديم أفضل الممارسات بشأن الحصول على الأدلة الرقمية، مما يُسهِم في تحديد المخرجات المستمدة من تلك الأدوات (إرشادات المنظمة الدولية للتوحيد القياسي/اللجنة الكهروتقنية الدولية,2021).
- سرعة إخطار الخبراء الفنيين في مجال الحاسبات والبرامج وأنظمتها والتصوير الجنائي من قِبل مأموري الضبط الجنائي حرصًا على عدم ضياع الأدلة.
- ألا يؤدي استعمال الوسائل التقنية في البحث إلى المساس بمحتوى الأدلة الرقمية (إرشادات المنظمة الدولية للتوحيد القياسي/اللجنة الكهروتقنية الدولية).

- في مجال المعاينة في الجرائم السيبرانية، يجب إثبات وقت وتاريخ ومكان التقاط الصور في محضر يوقَّع ممَّن أجرى المعاينة.
- يجوز الطلب من طرف آخر التحفظ على بيانات مخزنة بواسطة نظام معلوماتي يقع داخل إقليم ذلك الطرف، والتي بشأنها ينوي الطالب تقديم طلب بالمساعدة المتبادلة من أجل البحث أو الدخول أو مصادرة أو تأمين أو كشف بيانات معينة متعلقة بجريمة معينة (اتفاقية بودابست، 2001).
- في حال تقديم طلب تحفظ على بيانات رقمية ذات صلة بجريمة من أجل ملاحقة جريمة، يجب أن يحدد في هذا الطلب:
  - الجهة التي تطلب التحفظ.
  - الجريمة موضوع التحقيق الجنائي أو الإجراءات الجنائية وموجز بالوقائع المتعلقة بها.
  - أي معلومات متوافرة تكشف عن شخصية المسؤول عن بيانات الكمبيوتر المخزنة أو مكان وجود النظام المعلوماتي.
  - الضرورة الموجبة للتحفظ على البيانات.
  - مع تقديم طلب المساعدة المتبادلة من أجل البحث في البيانات أو الدخول عليها أو مصادرتها أو تأمينها أو الكشف عنها (اتفاقية بودابست، 2001).
- الحفاظ على سلامة الأدلة الرقمية.
- توثيق عمليات جمع الأدلة الرقمية ومعالجتها وتحليلها بدقة مع توفير سجل شفاف للأغراض القانونية.
- ضرورة إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، بما في ذلك معلومات تتبع المستخدمين التي خزنت على تقنية معلومات، خصوصًا إذا كان هناك اعتقاد أن هذه المعلومات عرضة للفقدان أو التعديل (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، المادة 23).
- تسريع إجراءات الحصول على أمر قانوني لجمع الأدلة الرقمية أو تحليلها لخصوصية الأدلة الرقمية، مع الالتزام بالمعايير القانونية والأخلاقية، واحترام قوانين الخصوصية لضمان مقبولية الأدلة في المحكمة.
- التحقق من صحة الأدوات والمنهجيات المستخدمة في جمع الأدلة الرقمية وتحليلها. تأكَّدْ من أن التقنيات المستخدمة معتمدة من الجهات المعنية لكل دولة أو مرجعيات دولية موثوقة.
- التعامل مع الأدلة الرقمية بسرية تامة، وتقييد الوصول إلى الموظفين المصرح لهم فقط، واتخاذ التدابير اللازمة لحماية المعلومات الحساسة لمنع أي اختراق أو تسرب.

- إنشاء سلسلة متابعة الأدلة والحفاظ عليها. وثِّقْ (حدِّد) كل فرد يتعامل مع الأدلة، بالإضافة إلى تاريخ كل تفاعل ووقته والغرض منه، لضمان المساءلة.
- اتباع الإجراءات والمعايير القانونية لضمان قبول الأدلة الرقمية في المحكمة، والالتزام بقواعد الإثبات، والاستعداد لشرح وتفسير وتبرير إجراءات الفحص الجنائي الرقمي المستخدمة في أثناء التحقيق.
- يجب التعامل مع الأدلة الرقمية من قِبل مختصين وخبراء في جمع الأدلة الرقمية والحصول على شهادات مهنية في هذا المجال.
- الحفاظ على الشفافية في جميع إجراءات التحقيق الجنائي الرقمي، وتوصيل المنهجيات والنتائج والقيود بوضوح إلى أصحاب المصلحة المعنيين، بما في ذلك المهنيون القانونيون، لتسهيل عملية قانونية عادلة ومنصفة.
- ضرورة الحفاظ على سرية الإجراءات المتعلقة بالاستدلال الجنائي الرقمي طوال فترة التحقيقات (المادة. 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010).

2.4 ضوابط التحقيق الجنائي والتفتيش الرقمي.

الضوابط الشكلية في التحقيق الجنائي والتفتيش الرقمي

تهدف القواعد الشكلية إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تُتخذ لجمع الأدلة، بالإضافة إلى أن مقتضيات الإجراء تعد سياجًا يحمي الحريات الفردية. وهذه الضوابط هي:

- **ضابط الميعاد الزمني لإجراء التفتيش الرقمي:**

- يتعيَّن على الشخص القائم بالتفتيش أن يتقيد بالوقت المحدد قانونًا لمباشرة هذا الإجراء، واستثناء الجرائم الإلكترونية من شرط التفتيش في أوقات معينة، ومن ثم ينبغي النص على جواز إجراء التفتيش في الجرائم الإلكترونية في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من السلطات المختصة.
- تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكين مأموري الضبط القضائي والمحقق من كشف الجريمة، والتعرف إلى مرتكبيها بالسرعة والدقة اللازمتين.
- ينبغي استثناء التفتيش في البيئة الرقمية من شرط «إجراء التفتيش بحضور أشخاص معينين كضمانة من ضمانات التفتيش»؛ نظرًا لذاتية هذا النوع من الجرائم وما يتطلبه التحقيق بشأنها من بسط نوع من السرية في أثناء جمع الدليل الرقمي، بالإضافة إلى الإسراع في استخلاصه قبل فقدانه.

تحرير محضر التفتيش الرقمي:

يجب تحرير محضر يثبت فيه كل ما حدث من إجراءات وما أسفر عن التفتيش من أدلة، ولا يشترط لصحة المحضر سوى ما تستوجبه الأسس العامة في تحرير المحاضر عمومًا، وهي:

- ضرورة أن يكون المحضر مكتوبًا باللغة الرسمية.
- أن يحمل المحضر تاريخ تحريره وتوقيع الشخص أو الجهة التي حرَّرته.
- أن يتضمن المحضر جميع البيانات المتعلقة بالتفتيش.
- إذا أُجري التفتيش من طرف سلطة التحقيق، يُشترط أن يكون مصحوبًا بكاتب يتولى تحرير المحضر وتدوين ما حدث من إجراءات والتوقيع عليه.

الإذن بالتفتيش:

- وجوب النص على منح السلطات القضائية لمأمور الضبط القضائي صلاحية تفتيش أو الدخول على:
  - » أي نظام معلوماتي أو أي جزء منه والبيانات المخزنة فيه.
  - » أي وسيط تخزين يجوز أن تكون البيانات مخزنة فيه.

وذلك للوصول إلى دليل يفيد في ارتكاب جريمة أو أي إخلال بالعدالة (اتفاقية بودابست، 2001).

- وجوب النص على الحصول على إذن بالتفتيش في البيئة الرقمية، حيث إنه طبقًا لمعيار الخصوصية التي يجب أن يحميها المشرع، فإن النظام المعلوماتي، وما يحتوي عليه من أسرار وخصوصيات الأشخاص، يخضع بالتبعية لمبدأ عدم جواز الدخول إلى هذا النظام المعلوماتي إلا بإذن (اتفاقية بودابست، 2001).

- يجب أن يشتمل الإذن بالتفتيش في البيئة الرقمية على بيان وصف الجريمة وعنوان الأماكن التي يجري زيارتها وتفتيشها، وترتيب البطلان على مخالفة ذلك، ولا شك أن صياغة الإذن بالتفتيش الخاص بالبيئة الرقمية وتنفيذه يشكِّلان تحديات كبيرة، حيث تختلط البيانات والمعلومات المطلوبة بكميات هائلة من البيانات الأخرى التي لا تتصل بالموضوع قيد التحقيق؛ لذلك فإنه لا يستقيم الأمر مع مبدأ الخصوصية أن يطلع مأمور الضبط القضائي على جميع البيانات الشخصية الموجودة بالحاسوب (اتفاقية بودابست، 2001).

- ينبغي أن يكون إذن التفتيش محددًا وأكثر تخصصًا لكي يكون مبررًا.

- في حال أمرت سلطات التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه، فإن هذا البحث يمكن

أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، وينبغي أن يجري هذا الامتداد وفقًا لضابطين:

1. إذا كان ضروريًّا لكشف الحقيقة بشأن الجريمة محل البحث.
2. إذا وُجدت مخاطر تتعلق بضياع بعض الأدلة نظرًا لسهولة محو الأدلة أو إتلاف أو نقل البيانات محل البحث. وفي هذه الحالة لا يكون تفتيش البيئة الرقمية لغير المتهم مشروعًا إلا إذا صدر الإذن من السلطات المختصة بالتفتيش؛ لأن نظام المعلومات وما يحويه من خصوصيات للأشخاص تخضع أيضًا وبالتبعية لمعيار الخصوصية من حيث عدم جواز التدخل فيها من دون إذن.

- إذا استدعى الأمر التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى، يجب النص على الحصول على إذن من سلطات تلك الدولة بذلك (المادة 32، الفقرة 2 من اتفاقية بودابست).
- يتعين تمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها إذا كان هناك اعتقاد أن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها، وكانت هذه المعلومات قابلة للوصول قانونًا (المادة. 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010).
- وفى حال قيام أسباب لدى مأموري الضبط القضائي للاعتقاد أن البيانات المخزنة أو المطلوبة موجودة داخل نظام معلوماتي آخر أو جزء منه، وأنه يمكن الدخول عليها قانونًا، يمكن لهم توسيع عملية البحث والدخول على النظام الآخر (المادة 19، الفقرة 2 من اتفاقية بودابست).

وفي كل الحالات، عند امتداد الاختصاص لخارج إقليم الدولة، يجب أن يكون الإذن بالتفتيش مكتوبًا ومسببًا لتتمكن الجهات القضائية من مراقبة مشروعيته، ويمكن تحقيقًا للسرعة أن يصدر الإذن شفهيًّا ثم يصدر فيما بعد مكتوبًا.

أن يكون الإذن بالتفتيش مسببًا

يُقصد بالتسبيب أن الأمر الصادر لا بد أن يُبنى على قرائن ودلائل تدل على أن تفتيش الحاسوب أو الشبكات أو ملحقاتها يفيد في كشف الحقيقة. وهذه بعض الإرشادات:

- لا بد أن يكون للتفتيش غاية محددة، كأن يكون قائمًا بقصد التوصل إلى ما يفيد ارتكاب جريمة إلكترونية أو عدوان إلكتروني.
- يجب أن يباشر التحقيق الجهة المختصة (النيابة العامة، أو مأمور الضبط القضائي في حالة ندبه في غير حالات التلبس بالجريمة).

- يجب الاستعانة بالخبراء الفنيين في مجال الحاسب الآلي وتقنية المعلومات وتجميع أدلتها والتحفظ عليها باعتبارها مسألة فنية لا يمكن الاعتماد فيها على معلومات سلطات التحقيق أو المحكمة (إرشادات المنظمة الدولية للتوحيد القياسي/اللجنة الكهروتقنية الدولية، 2021).

أن يكون الإذن بالتفتيش مكتوبًا:

- يجب أن يصدر الإذن بالتفتيش من سلطة التحقيق لأحد مأموري الضبط القضائي مكانيًّا ونوعيًّا، ولا يشترط أن يعين المأمور بالاسم، ويجوز أن يصرح للمأمور المأذون له بندب غيره من مأموري الضبط المختصين لتنفيذ الإذن. ويجب أن يتضمن الإذن اسم من أصدره ووظيفته وتاريخ وساعة صدوره وأسماء المقصودين بالتفتيش مع تحديد فترة معقولة وأن يذيّل الأمر بتوقيع مَن أصدره.
- ينبغي لسلطة التحقيق إصدار الأمر بالتحفظ على الأدلة الرقمية التي جرى الحصول عليها، منعًا لمحوها أو إتلافها (المادة 88 من قانون تحقيق الجنايات البلجيكي).

الضوابط الموضوعية في التحقيق الجنائي والتفتيش الرقمي:

- ضرورة وقوع جريمة من الجرائم المعلوماتية (السيبرانية) التي نص عليها المشرع طبقًا لمبدأ شرعية الجرائم والعقوبات: ينبغي النص على إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي، إما للوقاية من حدوث جرائم وإما في حالة توافر معلومات عن احتمال وقوع جرائم معينة، ويعد ذلك استثناء من القواعد العامة نظرًا لخصوصية هذه الجرائم.
- إسناد الجريمة المعلوماتية إلى شخص معين واتهامه بارتكابها أو الاشتراك فيها: لا يمكن مباشرة التفتيش لمجرد وقوع جريمة من الجرائم المعلوماتية، بل لا بد من نسبتها إلى شخص، سواء بصفته فاعلًا أصليًّا أو شريكًا فيها، وذلك بناء على توافر دلائل كافية تدعو إلى الاعتقاد أنه ارتكب أو أسهم في ارتكاب الجريمة المعلوماتية حتى يمكن انتهاك حق الخصوصية لديه وتفتيش حاسوبه الشخصي وبرامجه الخاصة.
- توافر أمارات قوية أو قرائن على وجود أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة: ينبغي أن تتوافر لدى جهات التحقيق قرائن ودلائل كافية على وجود أجهزة أو أدوات استُخدمت في ارتكاب الجريمة المعلوماتية (السيبرانية) أو أشياء متحصلة منها أو مستندات إلكترونية لها فائدة في استجلاء الحقيقة.

يُقصد بالدلائل: علامات معينة تستند إلى العقل وتستمد من ظروف أو وقائع يستنتج منها أن جريمة ما وقعت وأن شخصًا معينًا هو مرتكبها.

إنّ التفتيش لا يجري إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استُعملت في الجريمة الإلكترونية أو أشياء متحصلة منها أو أي مستندات إلكترونية

يُحتمل أن تكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره، وبالتالي فإن مجرد وقوع الجريمة لا يكفي لإصدار سلطة التحقيق الإذن بالتفتيش أو مباشرته.

إنّ المعيار لإصدار الإذن بالتفتيش أن تكون الدلائل التي تجمعت حول الجريمة تدعو إلى الاعتقاد المعقول بوقوعها، سواء أكان من تجمعت حوله هذه الدلائل فاعلًا أصليًّا أم شريكًا فيها.

وتقدير هذه الدلائل متروك لسلطة التحقيق التي تصدر الإذن بالتفتيش شريطة أن يكون تقديرها منطقيًّا ومتفقًا مع الواقع، بحيث تكشف هذه الدلائل بجدية عن وقوع جريمة معلوماتية محل الإذن وأن هناك متهمًا تُنسب إليه.

- **تحديد محل التفتيش**

يقصد بمحل التفتيش: المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، ومحل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال، والتي يدخل فيها:

- برامج التطبيق ونظم التشغيل للبيانات المستخدمة بواسطة برامج الكمبيوتر أو كيانه المنطقي.
- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات (هذا النظام اتبعته بعض الدول، مثل الولايات المتحدة الأمريكية وفرنسا، انظر قانون ولاية كاليفورنيا بخصوصية المستهلك 2020 والقانون الفرنسي رقم 17/1987 الصادر بتاريخ 6 يناير 1978 والمعدل بموجب القانون 801 لسنة 2004 الخاص بالمعالجة الآلية للبيانات والحريات).

وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة. وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونًا، لا سيما اشتراط الإذن بالتفتيش من السلطات القضائية المختصة. وهناك بعض الاعتبارات المهمة:

- يجب على المحقق الحرص على سرية جميع المعلومات التي يكشف عنها التحقيق وعدم إفشائها، رعايةً لتفادي ما يؤدي ذلك من ضرر لصالح التحقيقات وخصوصية الأفراد.

- يجب للاعتداد بحجية الدليل الإلكتروني توافر شرطين:
  - » أن تصل قيمة الدليل إلى درجة القطع من الناحية العلمية البحتة.
  - » ألا يكون في الأخذ بالدليل الرقمي مساس بالحقوق والحريات للأفراد إلا بالقدر المسموح به قانونًا.

- **مراعاة خصوصية الأفراد وعدم التمييز بينهم**

عند النظر إلى خصوصية الأفراد بناءً على النوع الاجتماعي وتجنب التمييز بين الجنسين، يجري وضع ضوابط إضافية لحماية الحقوق الفردية عند البحث على الدليل الرقمي وتفتيش الحواسيب والشبكات. وفيما يلي بعض الضوابط القانونية الواجب النظر إليها:

- حق الخصوصية

تتطلب الأنظمة القانونية عادةً وجود تصريح قانوني أو أمر قضائي لتفتيش الأدلة الرقمية. ويجري تحديد شروط هذا التصريح بناءً على مفهوم الحق في الخصوصية.

- تجنب التمييز

تمنع القوانين في كثير من البلدان التمييز بناءً على النوع الاجتماعي، ويعني ذلك أنه يجب تعامل جميع الأفراد بالمساواة أمام القانون دون أي تمييز، بناءً على الجنس أو أي عنصر آخر.

- رفع السرية

يجب على الجهات المعنية الالتزام بمبدأ رفع السرية، والكشف عن الأدلة الرقمية يكون وفقًا للقوانين المحلية وبمراعاة حقوق الأفراد.

- تشفير البيانات

قد تحتاج السلطات إلى إجراءات خاصة لكسر تشفير البيانات في حال كانت مشفرة، ويخضع هذا الإجراء للقوانين المحلية.

3.4 تقديم الدليل الرقمي لهيئة المحكمة

- يقدم الدليل الرقمي بهيئته الأصلية أو بأي وسيلة رقمية أخرى، كما يمكن للمحاكم طلب تقديم محتواه مكتوبًا متى كانت طبيعته تسمح بذلك (نظام الإثبات السعودي، 1443هـ).
- يكون للمستخرجات من الدليل الرقمي الحجية المقررة للدليل نفسه، وذلك بالقدر الذي تكون فيه المستخرجات مطابقة لسجلها الرقمي وبما لا يتعارض مع الأنظمة الوطنية (نظام الإثبات السعودي، 1443هـ).

حجية الدليل الرقمي

"اعتبارات حق المتهم في الحصول على نسخة إلكترونية طبق الأصل عن الدليل الجنائي الرقمي"

على الخصم الذي يدعي عدم صحة الدليل الرقمي عبء إثبات ادعائه (نظام الإثبات السعودي، 1443هـ).

وفق الإجراءات؛ فإن لحقِّ المتهم في الحصول على نسخة من الدليل الرقمي مكانة مهمة في النظام القانوني، وتتبع هذه الإجراءات تفصيلات محددة تختلف قليلًا من بلد إلى بلد (الإعلان السادس من الدستور الأمريكي - قانون الإجراءات الجنائية بكندا وفرنسا - قوانين الدفاع والأمان بالمملكة المتحدة)، وحتى داخل نطاق التشريعات المحلية. ومع ذلك، يمكن تلخيص الإجراءات القانونية العامة التي يمكن للمتهم اتخاذها للحصول على نسخة من الدليل الرقمي كما يلي:

- **تقديم طلب رسمي**

  يقدم المتهم أو محاميه طلبًا رسميًّا إلى الجهة القضائية المسؤولة أو الجهة الأمنية المعنية للحصول على نسخة من الدليل الرقمي.

- **تحديد الأسباب**

  يجري تحديد الأسباب التي تبرر حاجة المتهم إلى الحصول على نسخة من الدليل الرقمي، مثل استخدامها في إعداد الدفاع أو فحص الأدلة المقدمة ضده.

- **الرد الرسمي**

  تتخذ الجهة المختصة قرارًا بالموافقة أو الرفض على الطلب، وتقوم بتوجيه رد رسمي إلى المتهم أو محاميه.

- **الدعوى القضائية (إذا لزم الأمر)**

  في حال رفض الجهة المعنية منح الوصول إلى الدليل الرقمي، يمكن للمتهم أو محاميه رفع دعوى قضائية للمطالبة بحق الوصول إلى الدليل.

- **المراجعة القضائية**

  في بعض الأحيان، يمكن للمتهم أو محاميه طلب مراجعة قضائية لقرار الرفض وتقديم الأسباب التي تدعم ضرورة الحصول على الدليل الرقمي.

الالتماس الاستئنافي

إذا كان هناك رفض نهائي لتوفير الدليل الرقمي، يمكن للمتهم أو محاميه تقديم الالتماس الاستئنافي إلى المحكمة العليا أو هيئة قضائية أعلى للنظر في القرار.

ملحوظة: يجب على المتهم أو محاميه أن يتبعا الإجراءات المحددة في نظام القانون المعمول به في البلد المعني، حيث يمكن أن تختلف هذه الإجراءات بناءً على التشريعات والنظم القانونية المحلية.

5- التعامل مع الأدلة الرقمية من الجانب الفني

يركز هذا الفصل على الجانب الفني في التعامل مع الأدلة الرقمية في مسرح الجريمة التقليدي والرقمي. وسيجري تقديم إرشادات في تحديد والبحث عن الأدلة ذات الصلة والتعرُّف إليها وتوثيقها، وجمع الأجهزة الإلكترونية التي يمكن أن تحتوي على أدلة رقمية تكون ذات قيمة في الإثبات، واتباع أفضل الممارسات الدولية في التعامل مع الأدلة الرقمية.

وتكمن أهمية هذه الإرشادات في الحصول على الأدلة ومعالجتها لضمان إمكانية قبولها من جانب المحكمة وعدم القضاء ببطلانها.

ويتضمن التعامل مع الأجهزة الإلكترونية في مسرح الجريمة التي يُعتقد احتواؤها على دليل رقمي خمس عمليات رئيسة، هي: التجهيز، والتعرّف، والجمع، والتحليل، وإعداد التقرير. وهذه العمليات موضحة في (الجدول 1).

تُرسي عملية التجهيز أساس التحقيق الناجح، وتتضمن جميع الأنشطة الضرورية لضمان إجراء التحقيق بفعالية، بما يراعي الجوانب الأخلاقية ويتوافق مع المتطلبات القانونية.

وتتضمن عملية التعرف: التعرف إلى مصادر الأدلة وتحديد الأدلة الرقمية المحتملة التي قد تكون ذات صلة بالتحقيق، وتوثيقها.

بعد ذلك، تتضمن عملية الجمع الحصول على الأجهزة الإلكترونية الذي يُعتقد احتواؤها على دليل رقمي وتحريزها. وخلال هذه العملية، سيجري إنشاء سلسلة متابعة الأدلة والمحافظة عليها دائمًا.

وأخيرًا، تتضمن عملية إعداد التقرير توثيق جميع العمليات والخطوات التي جرى اتخاذها على الأدلة الرقمية في مسرح الجريمة بغرض استعادة وتوضيح وتقديم الأدلة الرقمية إلى المحكمة أو الإدارة العليا.

الجدول 1: العمليات الخاصة بالتعامل مع الأدلة الرقمية

الرقم	العمليات
1	التجهيز للتحقيق
2	التعرّف إلى مصادر الأدلة الرقمية
3	جمع الأدلة
4	التعبئة والنقل والتخزين
5	إعداد التقرير

1.5 التجهيز للتحقيق

قبل البدء في التحقيق في مسرح الجريمة، يجب تجهيز عناصر متنوعة من أجل ضمان سلاسة العمليات في الموقع. وتتمثل الجوانب الرئيسة لمرحلة التجهيز الموضحة في الجدول 2 .

الجدول 2: القائمة المرجعية لعملية التجهيز

الرقم	القائمة المرجعية	الوصف
1	السلطة القانونية	• **التراخيص أو التفويض** ضمان الحصول على التراخيص القانونية المناسبة، مثل: تراخيص البحث أو خطابات التفويض، قبل الشروع في أي أنشطة خاصة بالأدلة الجنائية. • **الامتثال للقوانين واللوائح** فهم القوانين واللوائح ذات الصلة، المتعلقة بجمع الأدلة الرقمية والتعامل معها، والامتثال لها.
2	التوثيق	• **توثيق القضية** البيان الواضح لمدى التحقيق وأهدافه. وتوثيق أي معلومات أولية حول الحادث، بما فيها تاريخ ووقت اكتشافه، والأفراد المتورطون فيه، ووصف مختصر له. • **سلسلة متابعة الأدلة** عملية تتبَّع حركة الأدلة من خلال دورة حياة جمعها وحمايتها وتحليلها بتوثيق كل شخص تعامل مع الأدلة، وتاريخ/وقت جمعها أو نقلها، والغرض من النقل.

3	تخطيط الموارد	• **المورد البشري** تحديد وتخصيص الموظفين الضروريين للتحقيق، مع ضمان تمتع أفراد فريق التحقيق بالمهارات والخبرات اللازمة. • **الأجهزة والأدوات** التأكد من أن الأجهزة والبرامج والأدوات اللازمة للتحقيق متاحة لفريق التحقيق والأدلة الجنائية. يجب اختبار الأدوات على فترات زمنية مخططة للتأكد من أنها تعمل جيدًا.
4	خطة التواصل	• **التواصل مع أصحاب المصلحة** وضع خطة تواصل لإطْلاع أصحاب المصلحة على مدى التقدم في التحقيق. ويمكن أن يكون من بين أصحاب المصلحة المدّعون العامّون والإدارة العليا. • **التواصل الداخلي على مستوى الفريق** إعداد خمس قنوات تواصُل فعالة على مستوى فريق الأدلة الجنائية لمشاركة المعلومات والمستجدات.
5	تقييم المخاطر	• **تحديد المخاطر** تحديد المخاطر والتحديات المحتملة التي يمكن مواجهتها في أثناء التحقيق. وهذا يمكن أن يشمل التحديات التقنية، أو العقبات القانونية، أو المسائل المتعلقة بالموظفين. • **وضع خطة للحد من المخاطر** وضع خطة مع أعضاء الفريق للحد من المخاطر. فعلى سبيل المثال: هل يصبح التصوير من خلال قرص ثابت في مسرح الجريمة أمرًا ضروريًّا إذا أبدى أحد المشتبه بهم سلوكًا عدائيًّا؟ أو هل ينبغي لنا الحصول على القرص الثابت؟

6	التعرف إلى الأدلة	• **التعرف إلى مصادر الأدلة المحتملة** تحديد مصادر الأدلة الرقمية المحتملة المتعلقة بالتحقيق. ويمكن أن تتضمن هذه المصادر خوادم الويب والتخزين السحابي، وخوادم قواعد البيانات، ومزودي خدمات الإنترنت، وشركات الاتصالات الهاتفية.
7	خطة الحصول على بيانات الأدلة الجنائية	• **تحديد إجراءات الحصول على البيانات** إعداد إجراءات للحصول على البيانات الموجودة على الحاسوب، والبيانات الموجودة على السحابة، والبيانات المتطايرة، وخلافه. وهذا يتضمن تحديد الأدوات والتقنيات المطلوب استخدامها.
8	الجوانب اللوجستية والجدولة	• **وضع إطار زمني للتحقيق** إن إجراء تحقيق أمر شبيه بإدارة مشروع، ومن ثم يُفضَّل وضع أُطر زمنية وتحديد مراحل للتحقيق. فعلى سبيل المثال: ما التاريخ المتوقع والمدة المتوقعة لعملية جمع الأدلة وتحليلها؟ وما النتيجة المتوقعة من عملية جمع الأدلة وتحليلها؟ • **التنسيق مع أعضاء الفريق** تنسيق الأنشطة مع أقسام أو منظمات أخرى مشاركة في التحقيق. من بين الأمور التي ينبغي التنسيق فيها: الجوانب اللوجستية الخاصة بأعضاء الفريق والأدلة التي جرى تحريزها.

عند إجراء تحقيق في مسرح الجريمة، يمكن أن توجد بعض الاختلافات في أنواع الأدلة الرقمية التي ربما يكتشفها المحقق. وفيما يلي بعض الاعتبارات العامة لعدة مواقع مختلفة:

- **المنـزل**

قد تتمثل الأدلة الرقمية العادية الموجودة في هذا الموقع في حواسيب شخصية، وهواتف ذكية، وأقراص ثابتة خارجية، وأجهزة لوحية. ويمكن أن تكون لدى المشتبه بهم حسابات على وسائل التواصل الاجتماعي أو تطبيقات للمراسلة جرى تسجيل الدخول إليها على الأجهزة.

- **الشركة**

في أغلب الأحوال، سوف يكتشف المحققون أجهزة حواسيب محمولة بالشركة يستخدمها الموظفون بالإضافة إلى بعض أجهزة الخوادم. كما يمكن أن يحتوي الموقع على دوائر تلفزيونية مغلقة وأجهزة تحكم في الوصول من خلال القياسات الحيوية. ومن ثم ربما يحتاج المحققون إلى فهم البنية الأساسية للشبكة من أجل تضييق مدى التحقيق.

- **السيارة**

تحتوي السيارات غالبًا على أنظمة تحديد الموقع (GPS)، وأنظمة معلومات وترفيه، وأجهزة تسجيل بيانات الأحداث التي تتعرض لها السيارة، والتي يمكن أن توفر بدورها معلومات قيّمة. وربما يحتاج المحققون أيضًا إلى فحص أجهزة محمولة أو أدوات ذكية أخرى موجودة في السيارة.

- **مراكز البيانات**

تعد مراكز البيانات مرافق آمنة بشكل كبير تُخزَّن فيها الخوادم والبنية الأساسية الحرجة الأخرى. ونظرًا لأن مراكز البيانات تستضيف بيانات من عدة شركات، فينبغي للمحققين سؤال مسؤول النظام عن المساحة الدقيقة للتخزين التي تخزن البيانات المتعلقة بالقضية.

2.5 التعرف على مصادر الأدلة الرقمية

تحدث عملية التعرف إلى مصادر الأدلة في مسرح الجريمة، وبالتالي فمن اللازم إعطاء أولوية لسلامة جميع العاملين الموجودين في مسرح الجريمة من خلال اتخاذ الاحتياطات الضرورية للحيلولة دون تعرضهم لأي أضرار محتملة. ويجري بيان العملية في الأقسام التالية:

التعرف إلى مسرح الجريمة

يعد تحديد مسرح الجريمة الرقمي بالصورة السليمة أمرًا لا غنى عنه لنجاح أي تحقيق رقمي. حيث يضع الأساس للخطوات اللاحقة، بما في ذلك جمع الأدلة والمحافظة عليها وتحليلها.

يتضمن التعرف إلى مسرح الجريمة في ضوء التحقيق الرقمي التعرف إلى البيئة الرقمية، التي يمكن أن توجد فيها أدلة محتملة، وفهم تلك البيئة. فربما يكون مسرحُ الجريمةِ مكتبَ المشتبهِ به أو منزله أو مركز البيانات الذي جرت فيه استضافة موقع الويب وقاعدة البيانات، أو غرفة تحكم لدوائر تلفزيونية مغلقة، وغيرها. بالإضافة إلى ذلك، محاولة اكتشاف تخطيط الشبكة لمسرح الجريمة، بما في ذلك المواقع المحتملة لأجهزة التوجيه وأجهزة التبديل وجدران الحماية.

تأمين مسرح الجريمة

يعد تأمين مسرح الجريمة خطوة مهمة في أي تحقيق، سواء أكان مسرح الجريمة تقليديًّا أم رقميًّا (الأجهزة الإلكترونية)، حيث يساعد تأمين مسرح الجريمة بالصورة المناسبة في المحافظة على الأدلة، وصون نزاهة التحقيق، وضمان سلامة المحققين.

عند الدخول إلى مسرح الجريمة التقليدي، عَرِّف نفسك للموجودين في المكان ووَضِّح الغرض من التحقيق، وتعرَّف إلى جميع الأشخاص في المكان وأبعدهم عن الأجهزة الإلكترونية ومصدر التيار الكهربائي، وافحص كل غرفة موجودة بالمكان، وحَدِّد أماكن الأجهزة الإلكترونية (مسرح الجريمة الرقمي) التي قد توجد بها أدلة رقمية محتملة.

اجْعَلِ الوصول إلى مسرح الجريمة الرقمي مقتصرًا على الأشخاص المصرح لهم فقط. وقَيِّد الأذون التي تُمنح لمستخدمي الأدلة الرقمية للحيلولة دون إجراء تعديلات عليها، سواء أكان ذلك مقصودًا أم غير مقصود.

التعرف إلى الأدلة الرقمية المحتملة

تتضمن عملية التعرف إلى الأدلة المحتملة البحث بانتظام عن مصادر الأدلة الرقمية التي ربما تكون ذات صلة بالتحقيق والتعرف إليها. ويمكن أن تشمل هذه العملية ما يأتي:

- أجهزة الحواسيب وأجهزة الحواسيب المحمولة.
- الأجهزة المحمولة (الهواتف والأجهزة اللوحية).
- أجهزة الخوادم والشبكات.
- وسائط التخزين الخارجية (محركات أقراص USB - محركات أقراص ثابتة خارجية).
- حسابات تخزين سحابي.
- البريد الإلكتروني ومنصات التواصل.
- حسابات على وسائل التواصل الاجتماعي.
- السجلات وسجلات النظام.

توثيق مسرح الجريمة

في مسرح الجريمة الرقمي، يعد التوثيق الدقيق أمرًا ضروريًّا لنجاح أي تحقيق، حيث يساعد المحققين على إعادة تشكيل الأحداث على نحو دقيق وتكوين أساس لتقديم نتائج من خلال إجراءات قانونية.

حَدِّد مواضع الأجهزة الإلكترونية (مصادر الأدلة الرقمية) ووثِّق مكان اكتشافها. وقد يجري توثيق مسرح الجريمة باستخدام كاميرا رقمية، من خلال لقطات فيديو أو باستخدام مخططات ورسومات. وينبغي توثيق الرؤى العامة والتفصيلية للأدلة الرقمية توثيقًا مناسبًا، حيث يعد من الضروري التقاط صور لأي جوانب قصور موجودة في الأجهزة، مثل: جهاز حاسوب محمول، لوحة مفاتيحه غير موجود بها بعض المفاتيح.

إجراء مقابلة قصيرة

يحصل المحقق على معلومات متعلقة بالأدلة الرقمية من المالك ويؤكدها؛ وذلك للانتفاع منها. وربما توفر هذه البيانات تلميحات عمَّا ينبغي فعله لاحقًا، مثل: وجود هاتف محمول آخر يحتفظ به المشتبه به في مواقع مختلفة. وتتمثل المعلومات المهمة، التي ينبغي البحث للحصول عليها من المالك أو من الشخص المسؤول عن الأدلة الرقمية، في الغرض من الجهاز، ومستخدم الجهاز، ووجود أي تخزين خارج الموقع، مثل: سحابة وخوادم، وبيانات الاعتماد الخاصة بالجهاز.

يمكن أن يساعد ذلك على التحقيق والادعاء في القضية في مرحلة لاحقة في حالة معرفة الدافع من وجود الجهاز وتحديد المالك في أثناء التحقيق في مسرح الجريمة.

3.5 جمع الأدلة

ينبغي للمحققين اتخاذ قرار بالحصول على الأدلة الرقمية أو تحريزها أو كلا الأمرين عندما تكون موجودة في مسرح الجريمة.

خلال عملية جمع الأدلة، في حالة وجود أنشطة عن بُعد مشتبه بها تُجرَى على الأدلة الرقمية، يجب على المحققين المختصين تحريز الأجهزة الإلكترونية بالشكل الصحيح وتعطيل وعزل الاتصال بالشبكة للجهاز (اتصال واي فاي "WiFi"، وبلوتوث "Buletooth"، واتصال المدى القريب "NFC")، فورًا، وذلك إما عن طريق إعدادات الجهاز وإما وضعه في حقيبة خاصة عازلة للإشارة. ويهدف هذا الإجراء إلى الحيلولة دون حدوث أي تلاعب بالأدلة، مثل: حذف أو تعديل البيانات الموجودة على الأدلة الرقمية أو تدمير الجهاز.

وتختلف عملية جمع الأدلة تبعًا لاختلاف نوع الجهاز. وسيجري توضيح مسار العملية التفصيلية لأجهزة الحواسيب، والهواتف المحمولة، والخوادم، وكاميرات المراقبة والبيانات المتاحة عبر الإنترنت الموجودة في مسارح الجريمة.

خلال عملية جمع الأدلة، ينبغي للمحققين تحديد الأدلة الرقمية المحتمل وجودها في مسرح الجريمة. بعدها ينبغي للمحققين اتخاذ قرار له مبرراته بشأن ما سيجري فعله مع الأدلة الرقمية المكتشَفة بناء على هذه الأسئلة:

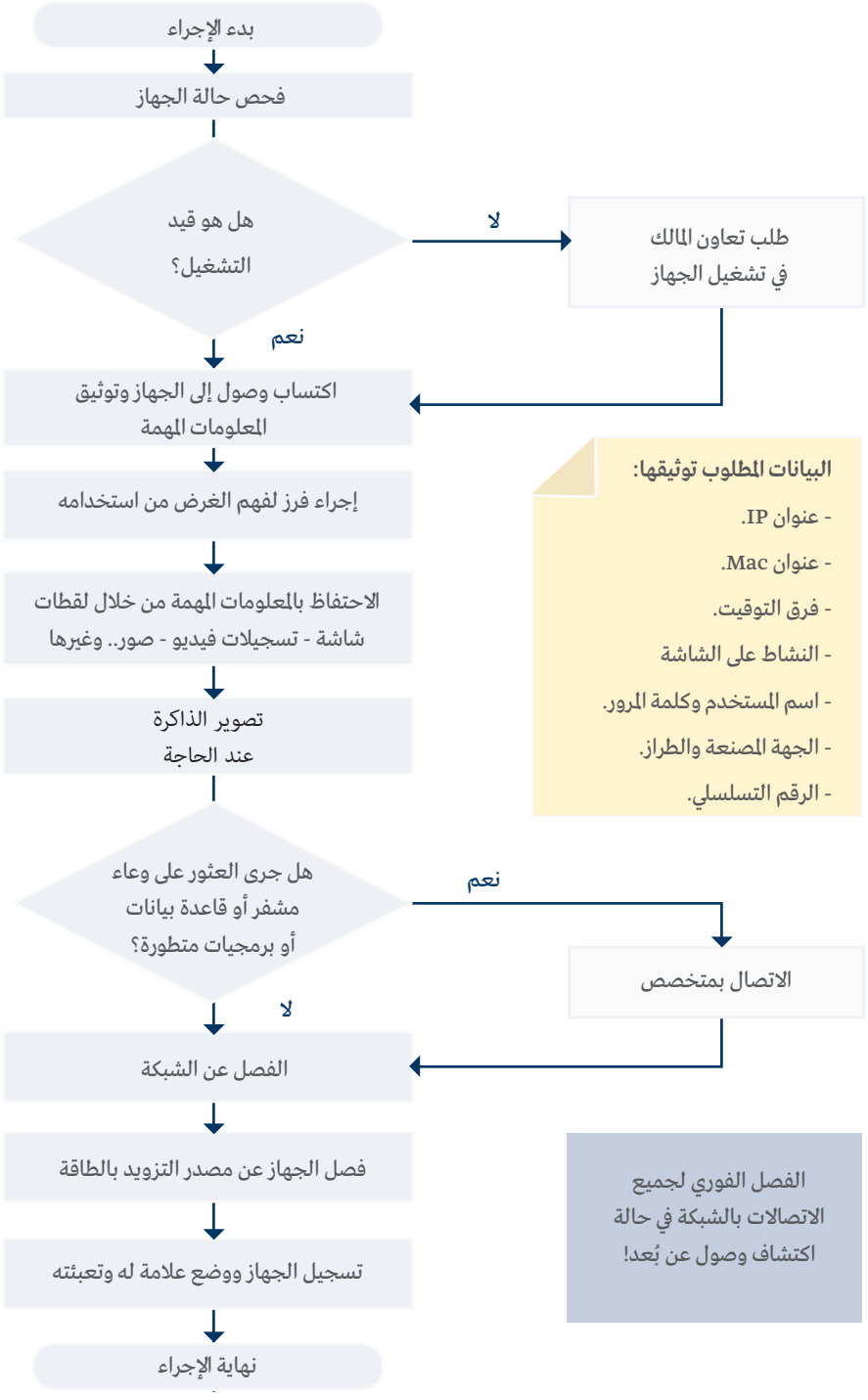
- هل يجري جمع كل الأدلة الرقمية أم فقط الأدلة الرقمية المتعلقة بالقضية (بناء على الفرز)؟
- هل يجري جمع الوحدة المادية التي تحتوي على البيانات، أم فقط الحصول على بياناتها؟
- ما الطريقة المستخدمة في الحصول على الأدلة؟ أهي النسخ، أم التنزيل، أم التصوير؟
- هل جهاز التخزين الخاص بجهة التحقيق والأدلة الجنائية ضخم بشكلٍ يكفي لتخزين جميع البيانات المطلوبة؟

هناك نقطة أخرى يجب التفكير فيها، هي ما إذا كانت هناك حاجة إلى إجراء تحقيقات الأدلة الجنائية التقليدية، مثل الحصول على بصمات الأصابع أو الحمض النووي على الأجهزة الإلكترونية. إذا كان ذلك مطلوبًا، فتأكد من وجود متخصص، وقم بإجراء تحقيقات الأدلة الجنائية التقليدية أولًا، قبل الانتقال إلى القسم الفرعي التالي في هذه الوثيقة. ويمكن جمع الأدلة الرقمية من الأجهزة الإلكترونية.

1.3.5 جمع الأدلة الرقمية من الحاسوب

في حالة اكتشاف جهاز حاسوب في مسرح الجريمة، يمكن اتباع الإرشادات التالية للحصول على الأدلة الرقمية:

- قم أولًا بفحص حالته.
- إذا كان قيد إيقاف التشغيل، ففكر في أن تطلب تعاون المالك لتشغيل جهاز الحاسوب. وإذا كان المشتبه به على مستوى عالٍ من الدراية التقنية، فلا تقُم بتشغيله.
- إذا كان جهاز الحاسوب قيد التشغيل، اطلب تعاون المشتبه به في الحصول على كلمة المرور.
- توثيق المعلومات المهمة، مثل: عنوان IP، وعنوان MAC، وفرق التوقيت، والنشاط على الشاشة، وأي أسماء مستخدمين وكلمات مرور، والجهة المصنعة، والطراز، والرقم التسلسلي.
- قم بعدها بإجراء فرز (تقييم أولي) باستخدام أدوات متخصصة وموثوقة لتصفح الحاسوب وفهم الغرض منه ومدى صلته بالقضية. احتفظ بالمعلومات المهمة من خلال توثيق المحتويات على الشاشة، أو تسجيلات فيديو، أو صور.
- قم باستنساخ منطقي لذاكرة الوصول العشوائي إذا كان ذلك ضروريًّا، وذلك يجري عادة لحالات، مثل: قضايا اختراق أمن البيانات وبرامج الفدية الضارة.
- في حالة وجود وعاء مشفر أو قاعدة بيانات أو برمجيات متطورة، حينئذ يمكن للمحققين طلب المساعدة من متخصصين بشأن ما ينبغي فعله.
- افصل جهاز الحاسوب عن الشبكة وعن مصادر التزويد بالطاقة من خلال فصل الكابل عن الجزء الخلفي من جهاز الحاسوب، أو بالضغط على زر إيقاف التشغيل لمدة تزيد على 5 ثوان. ويوضح الشكل 1 هذه الخطوات.
- في النهاية، سجِّل الأدلة في نموذج تحريز الأدلة (Evidence Seizure Form) وفقًا لما هو موضح في الملحق 4، وميزها بالعلامات تبعًا لما هو موضح في الملحق 6، وقم بتعبئة وختم الأدلة.



الشكل 1: جمع الأدلة الرقمية من الحاسوب

استنساخ ذاكرة الوصول العشوائي (البيانات غير المستدامة)

تتضمن هذه العملية استنساخًا منطقيًّا لمحتويات ذاكرة الوصول العشوائي (RAM)، للحصول على البيانات غير المستدامة (البيانات المتطايرة) التي تختفي بعد إيقاف تشغيل الجهاز. وتحتوي هذه البيانات على العمليات الجارية، واتصالات الشبكة المفتوحة، ومفاتيح التشفير، وغيرها من البيانات غير المستدامة التي يمكن أن تكون ذات قيمة في التحقيق. وتأتي أهمية استنساخ ذاكرة الوصول العشوائي (RAM) خصوصًا في الحالات التي قد تكون فيها البيانات غير المستدامة ذات صلة بالتحقيق، مثل استنساخ البرامج الضارة النشطة أو استعادة مفاتيح التشفير من الذاكرة؛ فهو يسمح للمختصين في الأدلة الجنائية الرقمية بتحليل بيانات ذاكرة الوصول العشوائي (RAM) المستخرجة بحثًا عن أدلة محتملة دون تغيير الحالة الأصلية.

لإنشاء نسخة جنائية من ذاكرة الوصول العشوائي(RAM) ، يُنصح باتباع الآتي:

- تحديد الأجهزة ذات العلاقة في التحقيق لاستنساخ البيانات غير المستدامة الموجودة في ذاكرة الوصول العشوائي.
- استخدام أقراص التخزين المحمولة (portable disk) لتنفيذ برنامج يقوم بجمع البيانات غير المستدامة الموجودة في ذاكرة الوصول العشوائي لهذه الأجهزة والتي تتناسب مع نظام التشغيل الخاصة بهذه الأجهزة.
- حفظ البيانات غير المستدامة في أقراص التخزين المحمولة وليس في الأجهزة ذات العلاقة بالتحقيق.
- إذا كانت هناك أي تطبيقات مشفرة مثل:bitlocker encryption ، يجري استنساخ منطقي (Logical Image) لملفات معينة أو partition.
- إغلاق الجهاز، ونقله إلى المعامل.
- توثيق الإجراءات في سلسلة متابعة الأدلة.

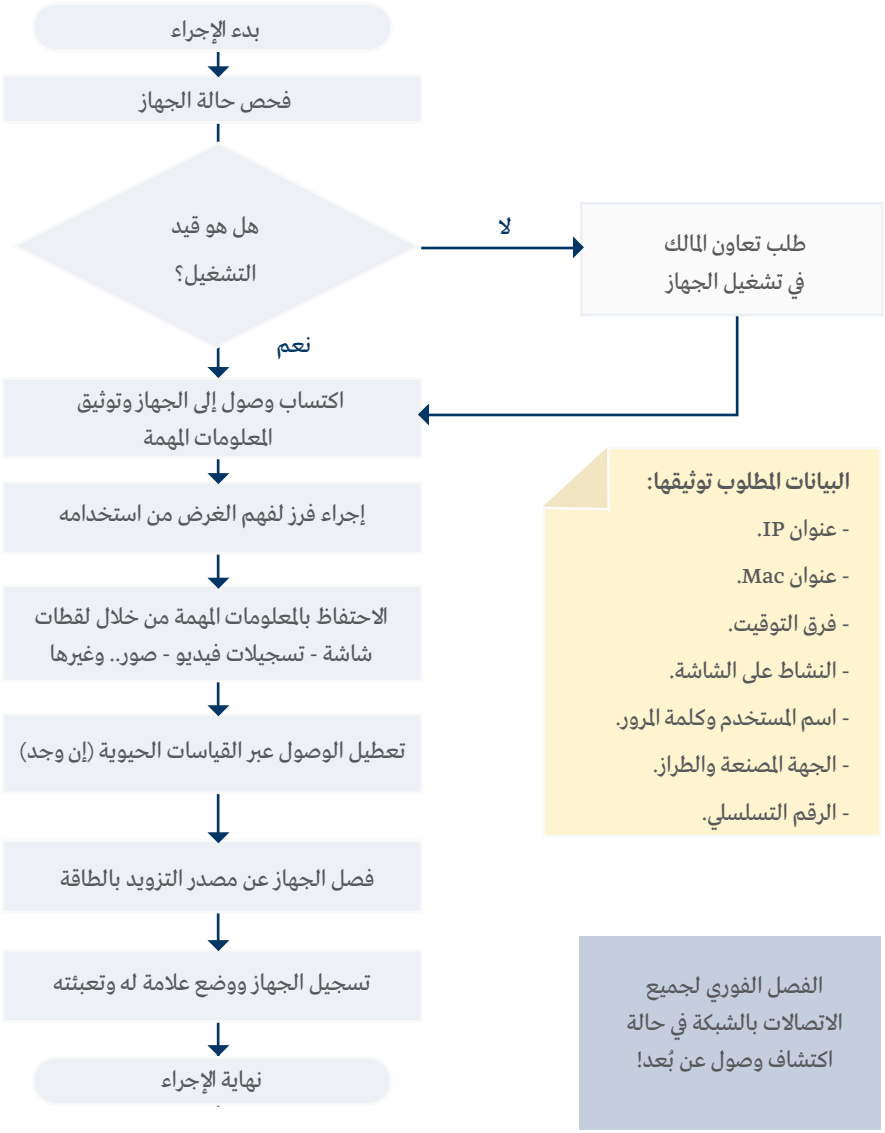
2.3.5 جمع الأدلة الرقمية من هواتف محمولة وأجهزة لوحية (أجهزة محمولة)

يجري التعامل مع الهواتف المحمولة واللوحية في مسرح الجريمة إذا استدعى الأمر ذلك بناءً على بعض المعطيات المهمة، على سبيل المثال:

- نوع الجريمة: احتواء الهواتف المحمولة على معلومات حساسة لضبط المجرمين المتورطين في قضايا أمن دولة أو تهريب مخدرات أو جرائم منظمة.
- تحديد الأجهزة المحرزة: إذا كانت هناك أجهزة كثيرة موجودة في مسرح الجريمة فلا بد من تحديد الأجهزة المحمولة ذات الصلة بالجريمة.

ويمكن اتباع بعض الإرشادات للحصول على الأدلة الرقمية في مسرح الجريمة، وهي:

- للمحققين أولًا فحص حالة الجهاز، وإذا كان قيد إيقاف التشغيل، فيطلب تعاون المالك لتشغيل الجهاز، وذلك مثلًا بطلب الرمز السري للجهاز، مع مراعاة الإجراءات اللازمة لحفظه من التلف أو التدمير، ويجب عدم تشغيله إلا من خلال خبير الأدلة الرقمية. الشكل 2 يوضح إجراءات جمع الأدلة من الهواتف المحمولة والأجهزة اللوحية.
- إذا كان الجهاز المحمول قيد التشغيل، يجري الدخول إلى الجهاز بطلب تعاون المشتبه به للحصول على كلمة المرور.
- توثيق المعلومات المهمة، مثل: عنوان بروتوكول الإنترنت (IP)، وعنوان التحكم بالنفاذ للوسط MAC (إذا كان الهاتف المحمول مرتبطًا بالخادم)، وفرق التوقيت، والنشاط على الشاشة، وكلمة المرور الخاصة بالجهاز، وكلمات المرور الأخرى ذات الصلة، مثل: كلمة مرور وضع المطوّر وكلمة مرور القفل الزمني للشاشة، والجهة المصنعة، والطراز، والهوية الدولية للأجهزة المتنقلة (IMEI) أو الرقم التسلسلي له.
- قم بعدها بإجراء فرز من خلال تصفح الجهاز لفهم الغرض منه ومدى صلته بالقضية. واحتفِظ بالمعلومات المهمة من خلال لقطات شاشة، أو تسجيلات فيديو، أو صور.
- بعدها قم بتعطيل أي وصول عبر القياسات الحيوية من خلال الانتقال إلى إعدادات الجهاز. وافصل الجهاز عن الشبكة، بما في ذلك اتصال بلوتوث (Bluetooth)، وNFC، والأشعة تحت الحمراء، وواي فاي (WiFi).
- قم في النهاية بتسجيل الأدلة في نموذج تحريز الأدلة وفقًا لما هو موضح في الملحق 4، وميزها بالعلامات تبعًا لما هو موضح في الملحق 6، وقم بتعبئة الأدلة وختمها.



الشكل 2: جمع الأدلة الرقمية من الهواتف المحمولة والأجهزة اللوحية

اعتبارات إضافية للهواتف المحمولة والأجهزة اللوحية

تعد معالجة هذه الأجهزة صعبة جدًّا، وتستخدم الهواتف المحمولة العديد من أنظمة التشغيل؛ مثل: iOS وAndroid وWindows وBlackberry وColorOS وغيرها كثير. كل نظام تشغيل له طريقته الخاصة في التشغيل.. ومع ذلك، ستوفر هذه التعليمات أفضل الممارسات العامة للتعامل مع الأجهزة ومعالجتها.

عند جمع الهواتف المحمولة، يجب مراعاة النقاط التالية لضمان النجاح:

- **قطع الاتصال بالشبكة**

يجب حظر أي إشارات شبكة تدخل أو تخرج من الأجهزة، لمنع الأطراف المشتبه بهم من الوصول عن بعد، ما يمكن استخدامه لتعديل البيانات والتلاعب بها، وكذلك لمنع الأجهزة من تشغيل العمليات التلقائية.

أسهل طريقة هي الانتقال إلى إعدادات الجهاز وتشغيل وضع الطيران، والتأكد من إيقاف تشغيل اتصالات الشبكة الأخرى، مثل البلوتوث، وNFC، خاصية الاتصال بالمدى القريب، وبيانات الهاتف وأي ميزة مشاركة قريبة.

الطريقة الأخرى هي استخدامFaraday Bag : يمكن وضع الأجهزة في حقيبة Faraday Bag لمنع أي إشارة شبكة واردة وصادرة.

- **الكابلات والمحولات الفريدة**

في مسرح الجريمة، لا يلزم ضبط الكابلات والمحولات المتوافرة بشكل شائع مثل كابلات C-type micro-USB cables، ومع ذلك، فإذا عثر المحققون على أنواع فريدة من الكابلات التي لا يمكن رؤيتها بشكل شائع في أي مكان، فمن المستحسَن جمع تلك الكابلات والمحولات، وذلك لأن محللي الأدلة الرقمية قد يحتاجون إلى هذه الكابلات لتشغيل الجهاز في أثناء عملية التحليل في مختبر الأدلة الرقمية في مرحلة لاحقة.

- **فقدان الطاقة**

عند الإمكان، تأكد من الحفاظ على طاقة الجهاز حتى يجري تسليمه إلى المختبر الجنائي. يُرجى ملاحظة أنه بمجرد أن تنفد الطاقة، قد تصبح بعض البيانات غير متاحة، مثل بيانات اعتماد المستخدم. عندما يحدث ذلك، قد لا تتمكن الأدوات الجنائية من استرداد مزيد من البيانات من الجهاز، وبخاصة البيانات الموجودة في السحابة.

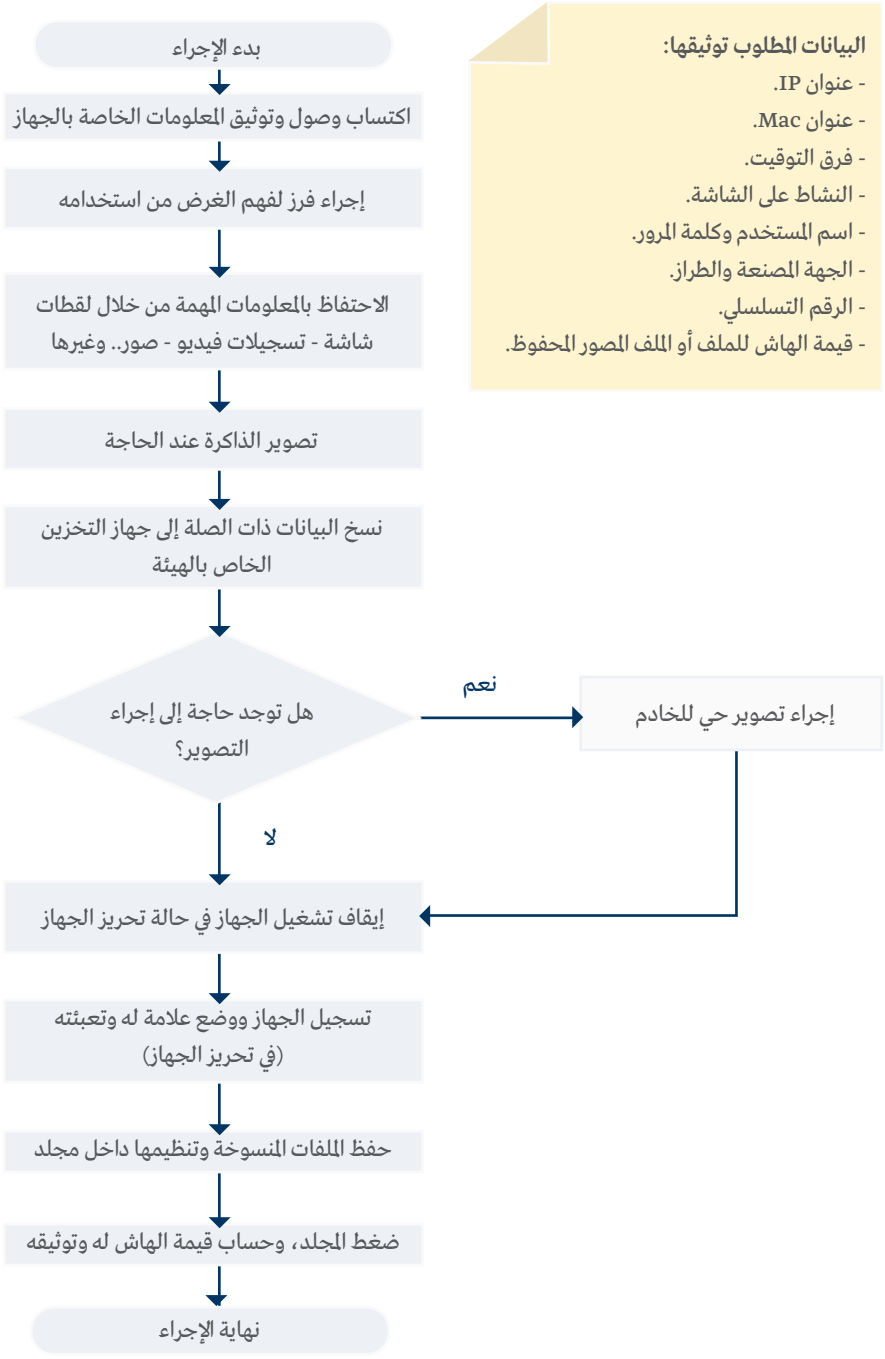
- **الحصول على كلمة المرور وبيانات الاعتماد**

يحتاج المحققون في مسرح الجريمة إلى التعاون مع المشتبه به في توفير كلمة المرور وبيانات الاعتماد. لا تحاول كسر أو تخمين كلمة المرور؛ هذا لأنه عند عدة محاولات فشل، سيقوم الجهاز بتشغيل عمليات آلية مثل تدمير البيانات.

3.3.5 جمع الأدلة الرقمية من الخادم

في حالة اكتشاف خادم، يمكن اتباع بعض الإرشادات، وهي:

- اكتسب وصولًا إلى الجهاز ووثّق المعلومات المهمة من خلال: عنوان IP، وعنوان MAC، وفرق التوقيت، والنشاط على الشاشة، واسم المستخدم وكلمة المرور، والجهة المصنعة، والطراز، والرقم التسلسلي.
- قُمْ بعدها بإجراء فرز من خلال تصفح الجهاز لفهم الغرض منه ومدى صلته بالقضية. احتفظ بالمعلومات المهمة من خلال لقطات شاشة، أو تسجيلات فيديو، أو صور.
- قُمْ باستنساخ ذاكرة الجهاز إذا كان ذلك ضروريًّا، ويحدث هذا الإجراء عادة في بعض الحالات، مثل: قضايا اختراق أمن البيانات وبرامج الفدية الضارة. وفي حالة الحاجة إلى إجراء استنساخ لغرض استعادة بيانات محذوفة، قم بإجراء تصوير حي.
- إذا كان من الضروري تحريز الجهاز، قم بإيقاف تشغيله بالصورة المناسبة. وسَجِّلْه في نموذج تحريز الأدلة وفقًا لما هو موضح في الملحق 4، ومَيِّزْهُ بالعلامات تبعًا لما هو موضح في الملحق 6، وقم بتعبئة الأدلة وختمها.
- قُمْ في النهاية بحفظ وتنظيم جميع الملفات المنسوخة داخل مجلد واضغطه واحسب قيمة الهاش له. ووثّق قيم الهاش للمجلد المضغوط والملف الذي جرى تصويره (إن وُجد). (الشكل 3 يوضح إجراءات جمع الأدلة من الخادم).

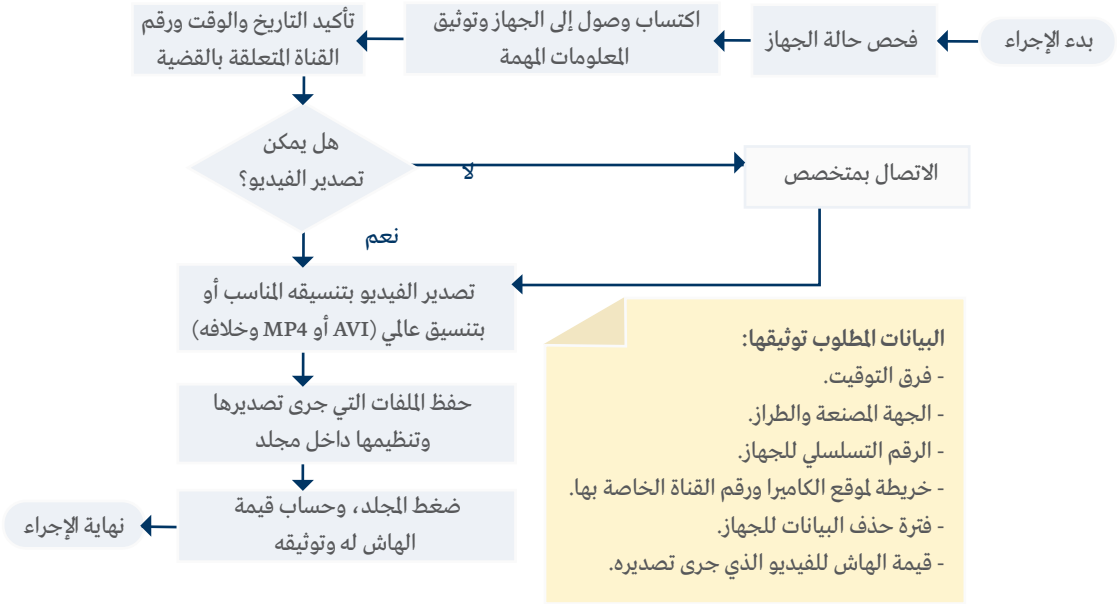


الشكل 3: جمع الأدلة الرقمية من الخادم

4.3.5 جمع الأدلة الرقمية من نظام مراقبة

في حالة اكتشاف أدلة رقمية متاحة عبر نظام مراقبة، يمكن اتباع بعض الإرشادات، وهي:

- افحص حالة نظام المراقبة عند اكتشافه، واكتسب وصولًا إلى الجهاز بأن تطلب تعاون أحد التقنيين/المشتبه به في إدخال كلمة المرور.
- وثّق المعلومات المهمة، مثل: فرق التوقيت، والجهة المصنعة، والطراز، والرقم التسلسلي، وخريطة موقع الكاميرا، وفترة حذف البيانات للجهاز.
- بعدها قم بتأكيد التاريخ والوقت ورقم القناة التي يكون خلالها تسجيل الكاميرا متعلقًا بالقضية. وقم بتصدير الفيديو بتنسيقه الأصلي للمحافظة على جودته. وإذا كان ذلك غير ممكن، فاستخدم تنسيقًا عالميًّا مثل AVI وMP4.
- في حالة تعذر تصدير ملفات الفيديو، فاطلب حينئذ مساعدة المتخصصين، كأشخاص أكثر خبرة في المجال أو موردين.
- قم في النهاية بحفظ وتنظيم جميع الملفات المنسوخة داخل مجلد واضغطه واحسب قيمة الهاش له.
- وثّق قيم الهاش للملف المضغوط في نموذج تحريز الأدلة وفقًا لما هو موضح في الملحق 4. (الشكل 4 يوضح إجراءات جمع الأدلة الرقمية من نظام المراقبة).



الشكل 4: جمع الأدلة الرقمية من نظام المراقبة

5.3.5 جمع الأدلة الرقمية من السحابة وتطبيقات المراسلة الفورية

خلال عملية الفرز التي تُجرى على أجهزة حواسيب أو هواتف محمولة أو أجهزة لوحية، ربما يُصادف المحققون بيانات جرى الوصول إليها من حسابات عبر الإنترنت، مثل: المحافظ الإلكترونية، وحسابات على تطبيقات Facebook وGoogle Drive وGoogle Maps وWhatsApp وTelegram.

يمكن للمحققين اللجوء إلى طرف ثالث للحصول على بيانات بناء على تراخيص البحث، لكن يمكن أن يستغرق هذا الإجراء بعض الوقت، وهناك احتمال متمثل في عدم استجابة الطرف الثالث. ونظرًا لوجود المالك في مسرح الجريمة، فبالتالي يُفضل جمع البيانات عندما لا تزال هناك قدرة على عرضها على الشاشة أو في حالة إمكانية الوصول إلى حساب عبر الإنترنت.

في حالة اكتشاف أدلة متاحة عبر الإنترنت، يمكن اتباع بعض الإرشادات، وهي:

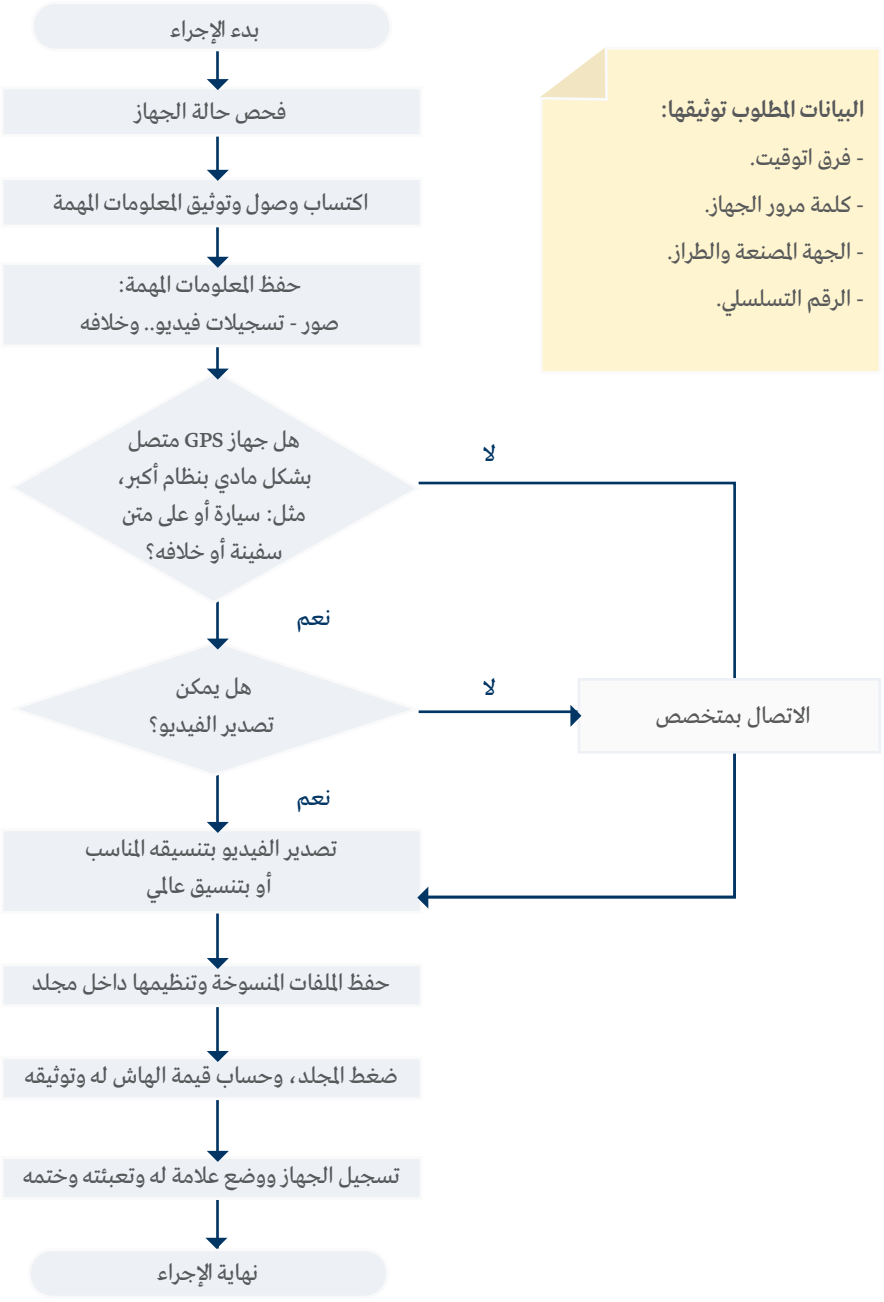
- اكتسِب وصولًا إلى الحساب المتاح عبر الإنترنت، ووثق المعلومات المهمة، مثل: اسم مستخدم الحساب، وتاريخ الوصول ووقته.
- قم بعدها بإجراء فرز لجمع معلومات أولية من خلال تصفح الحساب لفهم الغرض منه ومدى صلته بالقضية.
- قم بعد ذلك بحفظ البيانات المهمة من خلال استخدام طريقة واحدة أو أكثر من الطرق التالية:
  - حفظ الصفحات بتنسيق PDF.
  - لقطة شاشة للصفحات.
  - تسجيل شاشة للصفحات.
  - تنزيل البيانات.
  - استخدام برامج انعكاس الشاشة (screen mirroring) إذا كان الجهاز هاتفًا محمولًا أو جهازًا لوحيًّا.
- قُمْ في النهاية بحفظ وتنظيم جميع الملفات المنسوخة داخل مجلد واضغطه واحسب قيمة الهاش له. وقم بتوثيق قيم الهاش للملف المضغوط في نموذج تحريز الأدلة وفقًا لما هو موضح في الملحق 4. (الشكل 5 يوضح إجراءات جمع الأدلة الرقمية من السحابة وتطبيقات المراسلة الفورية).

الشكل 5: جمع الأدلة الرقمية من السحابة وتطبيقات المراسلة الفورية

6.3.5 جمع الأدلة الرقمية من جهاز نظام تحديد المواقع العالمي (GPS)

عند وجود جهاز GPS في مسرح الجريمة، يمكن اتباع الإرشادات التالية:

- قم بفحص حالة وحدة GPS عند اكتشافها، واكتسب وصولًا إلى الجهاز بأن تطلب تعاون المالك في إدخال كلمة المرور.
- وثِّق المعلومات المهمة، مثل: فرق التوقيت، وكلمة المرور الخاصة بالجهاز، والجهة المصنعة، والطراز، والرقم التسلسلي للجهاز.
- قم بإجراء فرز من خلال تصفح الجهاز لفهم الغرض منه ومدى صلته بالقضية. واحتفظ بالمعلومات المهمة في شكل تسجيلات فيديو أو صور.
- إذا كان الجهاز قائمًا بذاته ويمكن فصله عن النظام (سيارة أو على متن سفينة)، قُم بتحريزه.
- وثِّق الأدلة في نموذج تحريز الأدلة وفقًا لما هو موضح في الملحق 4، وميزه بالعلامات تبعًا لما هو موضح في الملحق 6، وقم بتعبئة الأدلة وختمها.
- إذا كان الجهاز متصلًا بالنظام، يجب على المحقق تصدير ملفات الفيديو إلى جهاز التخزين الخاص بجهة التحقيق والأدلة الجنائية.
- قم بتصدير ملفات الفيديو بتنسيقها الأصلي للحفاظ على جودتها. وفي حالة عدم إمكانية ذلك، استخدِم تنسيقًا عالميًا.
- إذا تعذر تصدير ملفات الفيديو، فاطلب حينئذ مساعدة المتخصصين، مثل: أشخاص أكثر خبرة في المجال أو موردين. الشكل 6 يوضح إجراءات جمع الأدلة الرقمية من جهاز مزود بتقنية GPS.



الشكل 6: إجراءات جمع الأدلة الرقمية من جهاز مزود بتقنية GPS

4.5 التعبئة والنقل والتخزين

يمكن تقسيم هذه العملية الرئيسة إلى ثلاث عمليات فرعية، هي:

تعبئة الأدلة

تتميز الأدلة الرقمية بأنها حساسة بشكل كبير تجاه الكهرباء الساكنة والمجالات المغناطيسية ودرجات الحرارة المفرطة والرطوبة والصدمات المادية. وبالتالي يجب تعبئة الأدلة الرقمية بالصورة المناسبة للحيلولة دون تعرضها للتلف خلال عملية النقل. كما ينبغي ختمها من أجل منع العبث بها. ويجب أن يتميز الختم بأن له القدرة على توضيح أي محاولات للوصول إلى الأدلة. ومواد العبوات والأختام تتمثل في المظاريف محكمة الغلق، والحقائب البلاستيكية المقاومة للعبث بها، والمواد اللاصقة المقاومة للعبث بها عند فتح العبوة، ووسائل الختم الساخنة التي توضع على فتحة العبوة.

يجب أن يوضح الختم المعلومات التالية لبيان الشخص المسؤول عن الأدلة الرقمية؛ حيث تبدأ سلسلة متابعة الأدلة عند هذه النقطة:

- العلامة أو الوسم الخاص بالأدلة.
- الأحرف الأولى من اسم المحقق (من قام بتعبئة الأدلة وختمها).
- تاريخ الختم ووقته.

نقل الأدلة

يجب توفير الحماية الكافية للأدلة الرقمية من المخاطر المحتملة، مثل: الصدمات، والإشعاع الكهرومغناطيسي، والحرارة، والرطوبة في أثناء عملية النقل. كما يجب وضعها على سطح مستوٍ وآمن. علاوة على ذلك، لا تترك الأدلة دون الإشراف عليها في أثناء النقل، وتأكد من خضوعها لإشراف شخص مسؤول واحد على الأقل في أثناء عملية النقل.

تخزين الأدلة

يمكن تخزين الأجهزة الإلكترونية داخل غرفةِ تخزينٍ عادية مملوكةٍ للهيئة للحفاظ على الأدلة الرقمية الموجودة داخل هذه الأجهزة. ومن ناحية أخرى، تأكد من أن الغرفة محمية من درجات الحرارة المفرطة والرطوبة، وأن بيئة الغرفة يمكن التحكم في مناخها. وعند تخزين الأجهزة، ينبغي للمحقق اتباع السياسات الخاصة بجهة التحقيق والأدلة الجنائية. وعند تسليم هذه الأجهزة إلى الشخص المسؤول عن غرفة تخزين الأدلة، تأكد من تحديث سلسلة متابعة الأدلة، حيث من الطبيعي في تلك الحالة قيام الشخص المسؤول بعمل قائمة جرد المخزون للأدلة المقدمة.

5.5 إعداد التقرير

في نهاية التعامل مع الأدلة الرقمية، يجب على المحقق إعداد تقرير مختصر للتحقيق في الموقع متعلق بالأدلة الرقمية. فبعد أن جرى جمع تلك الأدلة الرقمية من مسرح الجريمة، ينبغي للمحققين إعداد ملخص للأنشطة التفصيلية في صورة تقرير. ويتمثل الهدف من عملية إعداد التقرير في تقديم بيان واضح ودقيق وشامل للتحقيق، بما يضمن القدرة على استيعاب النتائج والاستفادة منها من جانب المدّعين العامّين للقضية أو من جانب الإدارة العليا.

- وتجري عادة كتابة التقرير من جانب المحقق الذي يتعامل مع الأدلة الرقمية. ومن بين العناصر التي ينبغي إدراجها في التقرير، ما يأتي:
- طلب التحقيق في قضية: هو الإرشادات التي جرى تلقيها من الإدارة، والهدف منها هو إجراء تحقيق في مسرح جريمة.
- المعلومات الأساسية عن القضية: وصف مختصر لنظرة عامة إلى القضية، وأعضاء الفريق، والقانون المتبع، وأي معلومات أخرى مهمة.
- ملخص للتحقيق في مسرح الجريمة: وصف لموقع مسرح الجريمة، وبيان التاريخ والوقت، وأعضاء الفريق الموجودين في مسرح الجريمة، والنتائج التي جرى التوصل إليها من العمل، مثل: إجمالي الأدلة التي جرى تحريزها.
- قائمة تحريز الأجهزة: هذه القائمة أحد أنواع النماذج المستخدمة لتوثيق جميع الأجهزة الإلكترونية التي جرى تحريزها والتي قد تتضمن أدلة رقمية. وتحتوي القائمة على معلومات تفصيلية عن هذه الأجهزة. وتتوافر عينة لمثل هذا النموذج في الملحق 4.
- سلسلة متابعة الأدلة: يعد هذا نوعًا آخر من أنواع النماذج التي توثّق قائمة بجميع الأشخاص المسؤولين عن الأدلة.

بعد أن جرى جمع الأدلة، ينبغي تحليلها لاستخلاص البيانات المحذوفة واستعادة أي بيانات مخفية وإعادة صياغة جميع البيانات لتصبح معلومات ووقائع ذات معنى. وبعد عملية إعداد التقرير، يقدم المحققون الأدلة الإلكترونية والرقمية إلى مختبر الأدلة الرقمية بغرض تحليلها. وهذا الإجراء موضح في القسم رقم 5.

- **تقديم الأدلة الرقمية للتحقيق**

بعد جمع الأدلة الإلكترونية الموجودة في مسرح الجريمة، ينبغي تقديمها إلى مختبر الأدلة الرقمية من أجل تحليلها. والهدف من إرسال الأدلة الإلكترونية إلى مختبر الأدلة الجنائية هو استعادة الأدلة الرقمية وإعادة بنائها ومعرفة الارتباط بينها.

وينبغي تزويد مختبر الأدلة الجنائية بما يلي عند طلب تحليل أدلة رقمية:

- الأجهزة الإلكترونية - لكي يُجرَى تحليل جنائي رقمي، يجب أن تكون الأدلة موجودة.
- الهدف من القضية - نطاق واضح للتحليل.
- المعلومات الناتجة عن الفرز - البيانات التي جرى جمعها في مسرح الجريمة.

عند تقديم الأدلة الرقمية إلى مختبر الأدلة الجنائية، يجب على المحقق التأكد من قيام محلل الأدلة الجنائية بتعبئة نموذج سلسلة متابعة الأدلة.

سوف يقوم المختبر بإعداد تقرير أدلة جنائية في نهاية عملية التحليل. ويمكن تقديم هذا التقرير إلى المدعي العام لاستعراض القضية، كما يمكن تقديمه إلى المحكمة لدعم التحقيق في القضية.

6- التوصيات

- تعميم الدليل الاسترشادي على أعضاء مجلسي وزراء الداخلية ووزراء العدل العرب للاستفادة منه في التعامل مع الأدلة الرقمية.
- تشكيل فريق عربي متخصص في الأدلة الرقمية للتواصل مع الشركات العالمية (ميتا - منصة إكس - تيك توك - شركة أبل) للاتفاق على آلية لتبادل الأدلة الرقمية الموجودة في الحوسبة السحابية في حالة وقوع جرائم.
- ضرورة مواءمة المنظمين في الدول العربية للقوانين الوطنية مع التطور التقني، لا سيما فيما يتعلق بضبط الأدلة الرقمية واستخراجها؛ ذلك أن التطور السريع للجريمة الإلكترونية يشكل حقيقة مدهشة يمكن تفسيرها، خصوصًا، من خلال انتشار أنظمة الحواسيب وشبكات الاتصالات السلكية واللاسلكية. وإذا كانت بعض الدول العربية قد منحت لنفسها اعتماد قوانين متخصصة بوصفها أدوات لمحاربة هذه الجريمة، فإن هذا ليس في كل الدول، ويعود ذلك إلى الأساليب المختلفة المستخدمة في معالجة المشكلة. ومن هذا المنظور، لا يزال التباين في القوانين الوطنية مهمًّا بشكل خاص، حيث إن العديد من الدول لم تعتمد تشريعات مُخصَّصة في هذا المجال، لا سيما فيما يتعلق بالضبط والتفتيش للأدلة الرقمية.
- أهمية التعاون الدولي بين الدول العربية فيما يتعلق باستخراج أذون تفتيش الحواسيب والشبكات والتحفظ على الأدلة الرقمية.
- من المهم تعزيز التعاون المتزايد بين القطاع الخاص والجهات الحكومية فيما يتعلق بالأدلة الرقمية. وبالتالي يمكن للقطاع الخاص أن يضمن نقل المعرفة إلى منسوبيه، لا سيما بالنظر إلى التعقيد التقني للتحقيقات في الجرائم الإلكترونية.
- في الملاحقة الجنائية، ينبغي زيادة استخدام الوحدات المتخصصة والمتعددة الأغراض والمتعددة التخصصات.

- هناك حاجة إلى توطيد التعاون بين سلطات الملاحقة الجنائيَّة ومزودي الخدمات؛ فالهدف الرئيس هو حل مشكلة مسؤولية متعهدي الخدمة بالنسبة لتقديم أدلة رقمية تفيد في إدانة متهم.
- تقديم برامج تدريبية للنيابات العامة وجهات الضبط والاستدلال لاستخدام الدليل الاسترشادي للتحقيق الجنائي الرقمي.
- **تطوير الدليل الاسترشادي باستمرار ليتضمن الآتي:**
  - إرشادات للتحقيق خاصة بأجهزة إنترنت الأشياء.
  - إرشادات للتحقيق خاصة بالمنزل الذكي والأجهزة الذكية (ساعة ذكية، تلفاز).
  - إرشادات للتحقيق خاصة بأجهزة الألعاب (Gaming Console).
  - إرشادات للتحقيق خاصة بالعملات المشفرة.
  - إرشادات للتحقيق خاصة بالطائرات المُسَيَّرة.
  - إرشادات للتحقيق خاصة بالمركبات.
  - إرشادات للتحقيق خاصة بالأجهزة الموجودة على متن السفن.
  - إرشادات للتحقيق خاصة بالميتافيرس.

7- المراجع

المراجع العربية

اللجنة الكهروتقنية الدولية (2021). إرشادات المنظمة الدولية للتوحيد القياسي.

- جامعة الدول العربية (2010). الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

- مجلس أوروب (2001). اتفاقية بودابست للجرائم المعلوماتية.

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (2021). المعايير وأفضل الممارسات للاستدلال الجنائي الرقمي.

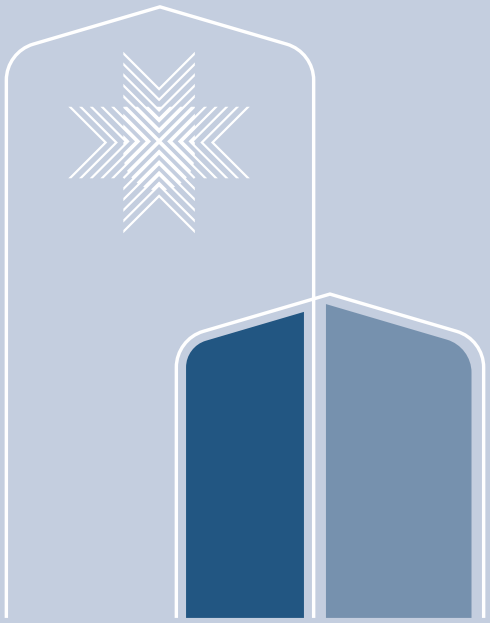
- القانون السعودي للإثبات (2021). النشر: 04 / 06 / 1443 هـ (07 / 10 / 2022م).

- القانون الفرنسي رقم 17 / 1978 (1978). حماية البيانات الشخصية.

- قانون ولاية كاليفورنيا الخاص بخصوصية المستهلك (California Consumer Privacy Act 2020).

المصادر الإلكترونية

- Interpol. (n.d.). Guidelines to Digital Forensics First Responders (Version 7). Retrieved from https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20RespondersV7.pdf?inLanguage=eng-GB.
- International Organization for Standardization (ISO). (n.d.). ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from https://www.iso.org/standard/44381.html.
- Scientific Working Group on Digital Evidence (SWGDE). (n.d.). Best Practices for Portable GPS Device Examinations. Retrieved from https://drive.google.com/file/d/1CUVojNZPBomLl7PDLS8o8AA3nQNBuqL2/view.



8- الملاحق

1.8 الملحق 1: قائمة المهارات الأساسية اللازمة للتعامل مع الأدلة الرقمية

الرقم	المهارة	الوصف
1	الإلمام بالمهارات الأساسية الخاصة بالحاسوب	نظام الملفات، وكيفية قيام الحاسوب بتخزين بيانات، وتطور التكنولوجيا الرقمية.
2	معرفة أساسيات التحقيق	الهدف من التحقيق الجنائي، ومنهجية التحقيق، وأسلوب التقصي، والاستنتاج الاستقرائي والاستدلالي.
3	معرفة أساسيات التعامل مع الأدلة الرقمية	مقدمة لعلوم الأدلة الجنائية، والأدلة الرقمية وطبيعتها ومنهجيتها والمصطلحات المستخدمة في مجال الأدلة الجنائية.
4	جمع المعلومات	المعلومات مفتوحة المصدر، وحفظ المعلومات التي جرى جمعها، وإدارة معلومات القضية.
5	الحصول على البيانات	إجراء تصوير غير حي، وتصوير حي، وقيمة الهاش، واستخلاص البيانات.
6	الالتزام بمدونة الأخلاقيات	مدونة الأخلاقيات المهنية، ومدونة قواعد السلوك الأخلاقي وغير الأخلاقي، وحماية سرية معلومات القضية.
7	الإلمام بالقوانين واللوائح	القوانين المتعلقة بالقضايا، والقانون الدولي، والتعاون الدولي، والإدلاء بشهادة الخبراء في المحكمة، والمعرفة بهيكل المحكمة، وتقديم الأدلة الرقمية إلى المحكمة.

2.8 الملحق 2: قائمة الأجهزة الرئيسة اللازمة للتحقيق في الموقع

الرقم	الجهاز	الوصف
1	أجهزة الحصول على البيانات	أحد أنواع الأجهزة، التي هي عادة أجهزة تجارية، يمكن استخدامها لتصوير أجهزة التخزين الخاصة بالهدف، مثل: الأقراص الثابتة ومحركات أقراص الفلاش. كما يمكن استخدامها لمسح قرص ثابت وتهيئته. * أجهزة التخزين الخاصة بالهدف هي أجهزة تخص المشتبه به.
2	جهاز التخزين للوجهة	جهاز التخزين للوجهة هو جهاز يُستخدم لتخزين ملفات الصور أو البيانات التي جرى تنزيلها من جهاز تخزين خاص بالهدف. يمكن أن يتمثل جهاز التخزين للوجهة في قرص ثابت خارجي أو محرك أقراص USB.
3	جهاز الحاسوب المحمول	جهاز حاسوب محمول يُستخدم لمهام إدارية في الموقع، مثل: إجراء بحث أو تسجيل دخول إلى أحد الحسابات أو لكتابة نماذج.
4	الكاميرا	يجري استخدام الكاميرا لتوثيق مسرح الجريمة.
5	مجموعة الأدوات الخاصة بالحاسوب الشخصي	يجري استخدام مجموعة الأدوات الخاصة بالحاسوب الشخصي عندما تكون هناك حاجة إلى جمع أدلة رقمية موجودة في الموقع. على سبيل المثال: إذا كان الدليل جهاز حاسوب مكتبي، فربما يحتاج محلل الأدلة الرقمية إلى إخراج القرص الثابت من وحدة النظام (system unit) باستخدام مجموعة الأدوات الخاصة بالحاسوب الشخصي وإجراء تصوير للقرص الثابت.

6	توصيلة كابل الطاقة	في الحالات التي يحتاج فيها محلل الأدلة الرقمية إلى تشغيل أي جهاز، ويكون مصدر التزويد بالطاقة محدودًا أو موجودًا في مكان بعيد، حينها يمكن استخدام توصيلة كابل الطاقة للحصول على الطاقة اللازمة.
7	اتصال مستقر بالإنترنت	يُستخدم الاتصال بالإنترنت من جانب محلل الأدلة الرقمية من أجل الدخول إلى حساب على الإنترنت أو لتنزيل بيانات مخزنة على خادم مستهدف أو لإجراء عمليات بحث على الإنترنت. ويمكن لمحلل الأدلة الرقمية استخدام الهاتف المحمول الخاص به وتشغيل وظيفة نقطة الاتصال (hotspot)، أو أن يتوافر لديه جهاز محمول مخصص للاتصال بالإنترنت.
8	المحوّلات	أنواع مختلفة من المحولات لتوصيل أجهزة الهدف بأجهزة أو برامج الأدلة الجنائية.
9	حقيبة/صندوق تعبئة الأدلة	حقيبة أو صندوق من البلاستيك لتعبئة الأدلة الرقمية. وسوف يجري ختم الحقيبة أو الصندوق قبل نقله إلى مختبر الأدلة الرقمية بغرض تخزينه.
10	العلامة الخاصة بالأدلة	مادة لتمييز الأدلة. ويمكن أن تكون علامة أو مادة لاصقة مقاومة للعبث.

3.8 الملحق 3: نموذج طلب التحقيق في قضية

نموذج طلب التحقيق في قضية			
رقم القضية:			
رقم طالب التحقيق في القضية:			
نوع الطلب:		◊ دعم في الموقع ◊ حصول على بيانات ◊ فحص ◊ أخرى:	
اسم طالب التحقيق:			
عنوان طالب التحقيق:			
البريد الإلكتروني لطالب التحقيق:			
رقم هاتف طالب التحقيق:			
نوع القضية:			
وصف القضية:		متلقي الطلب:	
مقدم الطلب:		التوقيع هنا:	
الاسم:		الاسم:	
رقم الهوية:		رقم الهوية:	
التاريخ:		التاريخ:	

4.8 الملحق 4: نموذج تحريز الأدلة

نموذج تحريز الأدلة					
الرقم	علامة الأدلة	الرقم التسلسلي	الجهة المصنعة	الطراز	الحالة & الملاحظة

تفاصيل التسليم	
معلومات المالك	معلومات المحقق
نوع القضية:	متلقي الطلب:
التوقيع هنا:	التوقيع هنا:
الاسم:	الاسم:
رقم الهوية:	رقم الهوية:
التاريخ:	التاريخ:

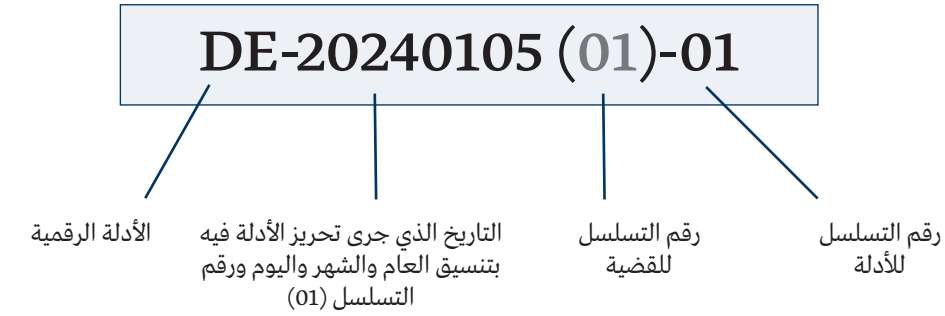
5.8 الملحق 5: نموذج سلسلة متابعة الأدلة

نموذج سلسلة متابعة الأدلة				
علامة الأدلة (الرقم)	التاريخ/الوقت	مُسلَّمة من جانب التوقيع واسم/وحدة يمكن قراءتها	متسلَّمة من جانب التوقيع واسم/وحدة يمكن قراءتها	موقع التخزين الجديد

تفاصيل التسليم	
العناصر التالية لم تعُد هناك حاجة إليها بوصفها أدلة، ومصرح بالتخلص منها عن طريق (اختر طريقة التخلص المناسبة): ◊ إعادتها إلى المالك. ◊ بيع بالمزاد العلني/الإتلاف/التحويل.	
معلومات المحقق	معلومات المالك
التوقيع هنا	التوقيع هنا
الاسم:	الاسم:
رقم الهوية:	رقم الهوية:
التاريخ والوقت:	التاريخ والوقت:

6.8 الملحق 6: وضع العلامات (الوسم) للأدلة الرقمية

مثال توضيحي لوضع العلامات:



- **DE-20240501(01)-MP01**

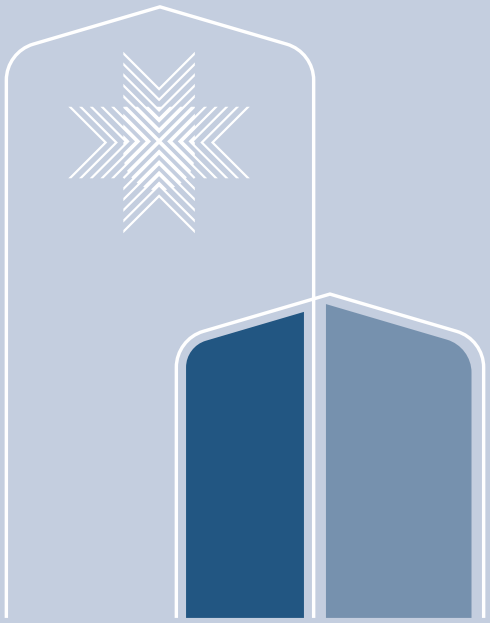
توضح هذه العلامة أن الدليل عبارة عن هاتف ذكي (MP01)، جرى تحريزه بتاريخ الخامس من يناير 2024، وهذا الدليل يخص القضية رقم 20240501(01).

- **DE-20240501(01)- MP01-SIM01**

توضح هذه العلامة أن الدليل عبارة عن بطاقة (SIM01) SIM موجودة داخل هاتف ذكي MP01، جرى تحريزه بتاريخ الخامس من يناير 2024، وهذا الدليل يخص القضية رقم 20240501(01).

- **DE-20240501(01)-HD01**

توضح هذه العلامة أن الدليل عبارة عن حاسوب محمول (HD01) جرى تحريزه بتاريخ الخامس من يناير 2024، وهذا الدليل يخص القضية رقم 20240501(01).



nauss.edu.sa » nauss.sa » +966 11 246 3444

info@nauss.edu.sa » nauss_sa » +966 11 245 0222