التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت

الدكتور/ حسين بن سعيد الغافري

مستشار قانوني وعضو مجلس إدارة الاتحاد العربي للتحكيم الإلكتروني

hssnrg@yahoo.com

الفهرس

رقم الصفحة

تمهيد

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الإنترنت وبين التحقيق في الجرائم الأخرى فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدي المحقق، ماذا حدث ؟وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟.

تظل الجرائم المتعلقة بشبكة الإنترنت تمتاز عن غيرها من الجرائم ببعض الخصائص وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الإطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسب الآلي، ملفات تسجيل العمليات الحاسوبية، بالإضافة إلى الإطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها. كما وأن يتم في الكثير من مراحله سوف يتم في بيئة رقمية، من خلال التعامل مع الحواسيب والشبكات ووسائط التخزين ووسائل الاتصال.

وسوف نحاول من خلال هذه المحاضرة تسليط الضوء وبصورة موجزة على عملية التحقيق وجمع الأدلة في هذه النوعية المستحدثة من الجرائم من خلال أربع محاور، نبدأها بالمهارات الفنية التي ينبغي أن يكتسبها المحقق وهو بصدد التحقيق في إحدى الجرائم المتعلقة بشبكة الإنترنت، بعدها نناقش الأعمال التي يجب أن يقوم بها المحقق وهو بصدد بدء عملية التحقيق، بداء من عملية تلقي البلاغات وحتى جمع الأدلة وكيفية التعامل مع مسرح الجريمة المعلوماتية، وفي المحور الثالث سوف نتعرف على بعض الوسائل والبرمجيات المساعدة في عملية التحقيق، أما الرابع والأخير فسوف يكون عن المعوقات التي من شأنها التأثير على عملية التحقيق.

المحور الأول: المهارات الفنية اللازم توافرها لدى المحقق في الجرائم المتعلقة بشبكة الإنترنت

عند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المتعلقة بشبكة الإنترنت فإننا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها كل محق فهي مهارات أساسية يفترض بداهة توافرها في المحقق بالضرورة، فمهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق. وعليه فإن التركيز هنا سوف ينصب على تلك المهارات التي تتسم بالجدة والحداثة وتعتبر إفرازاً للتطور الإنساني في مجال تقنية الاتصالات والحوسبة وأمراً مستجداً في من يتعامل مع هذه الجرائم المستحدثة وهي:

١. التعرف على المكونات المادية للحاسب الآلي والتعامل المبدئي معها

المهم هنا أن يتمكن المحقق من معرفة الشكل المميز للحواسيب وملحقاتها ومسمى كل منها. والهدف من استخدامه وما هي احتمالات توظيفه لارتكابه أي من الجرائم الإنترنتية، حيث أن عدم تعرفه عليها قد يؤدي إلى إهمالها أو حتى إتلافها بدون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها [١]. ليس هذا فحسب بل لا بد وأن يلم المحقق بكيفية التعامل مع تلك المكونات من أجهزة وملحقات ووسائط تخزين بصفتها أدلة محتملة. واكتساب هذه المهارة يعد أحد الأهداف المرجوة من البرامج التدريبية الخاصة بالتحقيق في الجرائم الحاسوبية لدى العديد من الدول كالولايات المتحدة وكندا واستراليا [٢].

٢. معرفة أساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاتها

الكثير من الجرائم المعلوماتية يتم ارتكابها من خلال شبكة الإنترنت، وبالتالي فإن المحقق بحاجة إلى معرفة مبادئ الاتصال الشبكي وأنواعه المختلفة وكيفية انتقال البيانات من جهاز إلى آخر على شكل حزم، ومبادئ البرتوكولات الرئيسية الخاصة بالاتصال بالشبكة [٣]. وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصور كيفية ارتكاب الفعل الإجرامي في الفضاء السيبرانى من اختراق للشبكات والحواسيب واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها. كما أنها تعطي المحقق تصوراً جيداً عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات الفنية التي تحول دون ذلك [٤].

٣. تمييز أنظمة تشغيل الحاسوب المختلفة والتعامل المبدئي معها

يجب أن يكون لدى المحقق على الأقل فهم مبدئي بأنواع الأنظمة التشغيلية لأجهزة الحاسب الآلي وخصائص ومميزات كل نظام وأبجديات أنظمة الملفات التي يعتمد عليها [٥]. فمعرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية حتى يشارك في متابعة وفحص وتفتيش مسرح الجريمة. وأحياناً يجد المحقق نفسه أمام قرار فني صعب يجب أن يتخذ قرار بشأنه بالتشاور مع الخبير، وبدون توافر الحد الأدنى من المعرفة التقنية لهذا القائد فإن القرار على الأرجح سوف يكون للخبير وحده. وأكثر أنظمة التشغيل شيوعاً وشهرة والتي يجب أن تتوفر في أي برنامج تدريبي هي: أنظمة ويندوز وأنظمة يونكيس واللينكس ونظام ماكنتوش.

٤. التعرف على الصيغ المختلفة للملفات وتطبيقات الحاسوب الرئيسية التي نتعامل معها

تعد الملفات الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا المتعلقة بشبكة الإنترنت بما تحويه من معلومات [٦]، وبالتالي فإن قدرة المحقق على معرفة صيغ هذه الملفات وما يمكن أن تحويه، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو سماع أو مشاهدة محتوى هذا الملف يعد أمر في غاية الأهمية.

٥. إجادة التعامل مع خدمات الإنترنت الرئيسية

تمثل شبكة الإنترنت أداة جمع وتحريات مناسبة للمحقق، حيث أنها خلقت مجتمعاً افتراضياً شبيهاً إلى حد ما بالمجتمعات الحقيقية، ويدور في مجتمع الإنترنت هذا الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم [٧]. ومن الممكن أيضاً أن يستخدم الإنترنت كأداة تعليمية للإطلاع على مستجدات جرائم الحاسب الآلي والإنترنت وطرق التصدي لها. وكوسيلة اتصال وتبادل المعلومات فيما بين رجال نفاذ القانون.

٦. معرفة الأدوات والأساليب المستخدمة في ارتكاب جرائم الإنترنت

معرفة رجال العدالة بهذه الأساليب وكيفية استخدام هذه الأدوات أمر في غاية الأهمية خاصة لمن يتولون مناقشة الشهود واستجواب المتهمين فبدونه لن يستطيعوا طرح الأسئلة التي تتصل مباشرة بالفعل الإجرامي وأسلوب ارتكابه. كما أنها تساعد المحقق على التواصل مع خبير الحاسوب الجنائي عند شرح الأخير ما توصل إليه من أدلة أو قرائن عن الأساليب المستخدمة في ارتكاب الجريمة والأدوات التي تساعده على القيام بذلك.

٧. معرفة أهم تقنيات أمن الحاسوب والإنترنت وأدواتها وطريقة عملها

اكتساب هذه المهارة وإن كان يبدوا في الظاهر أمراً معقدا بعض الشيء، إلا أن الأمر في حقيقته ليس كذلك، حيث أن المطلوب أن يساعد معرفة هذه التقنيات المحقق استيعابها وربطها بمجريات التحقيق بشكل عام وليس أن يجعله خبيراً فيها.

٨. الإطلاع على بعض الجوانب المتعلقة بجرائم الإنترنت

تتميز هذه الجوانب بأنه يغلب عليها الطابع النظري بحيث يمكن اكتسابها من خلال القراءة والإطلاع سواء من خلال المطبوعات أو الإنترنت، ومن أهم هذه الجوانب:

- الواقع الحالي والاتجاهات المستقبلية للجرائم المتعلقة بشبكة الإنترنت.
- الفئات المختلفة التي ينقسم إليها مرتكبو هذه الجرائم والخصائص المشتركة التي تميز كل فئة.
- معرفة وفهم التشريعات المختلفة المتعلقة بهذه الجرائم والإلمام باتجاهات القوانين والتشريعات في البلدان المختلفة.
- دراسة وتحليل بعض القضايا المشهورة للاستفادة من تجارب رجال العدالة في مواجهة هذه الجرائم.
- الوقوف على الأبعاد الدولية لهذه الجرائم وآليات التعاون المشترك بين الدول والتعرف على الاتفاقيات والمعاهدات الموجودة بهذا الخصوص.
- معرفة مصادر المعلومات المتوفرة على مواقع الإنترنت عن هذه الجرائم من خلال المواقع المتخصصة ذات المحتوى الجيد والمصداقية والاستفادة منها.

٩. معرفة الجرائم المتعلقة بالإنترنت والخصائص التي تتميز بها

الوعي الجيد بهذه الجرائم وبأنواعها المختلفة يعتبر بمثابة حجر الأساس في مواجهتها وبدونه لن تنجح السبل والوسائل الأخرى فلا يعقل أن تتم مواجهة جريمة ما إذا كان رجل العدالة المناط به هذا الأمر يجهل ماهيتها.

المحور الثاني: الأعمال التي يقوم بها المحقق في الجرائم المتعلقة بشبكة الإنترنت

أولاً. تلقي البلاغات والشكاوى

البلاغ بصورة عامة إخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع أو أن هناك اتفاقاً جنائياً على ارتكابها. والمبلغ في الجرائم المتعلقة بشبكة الإنترنت لابد وأن يكون لديه معرفة مقبولة بالجوانب الفنية للحاسب الآلي وشبكة الإنترنت حتى يتمكن من تقديم معلومات تصف الحادث بشكل جيد يمكن مع للمحقق الوقوف على طبيعة الجريمة وبشكل مقبول يمكنه من مباشرة التحقيق فيها. وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية بالجوانب الفنية للحاسب الآلي والشبكات حتى يستطيع مناقشة المبلّغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ.

ما هي المعلومات التي يجب على استيفاؤها من المبلغ؟

تتباين المعلومات التي ينبغي أن يدونها المحقق عند تلقي البلاغ بتباين فئات جرائم الحاسب الآلي والإنترنت والطبيعة الفنية التي تتميز بها كل فئة عن غيرها. وعلى الرغم من أن لكل فئة من هذه الجرائم المستحدثة معلوماتها الخاصة التي ينبغي الحرص قدر الإمكان على استيفائها عند تلقي البلاغ، إلا أن هناك معلومات تكاد تكون مشتركة بين معظم هذه الفئات، ويمكن الحصول عليها عن طريق طرح أسئلة تتناول جوانب محدد منها ما يلي [٨]:

- تاريخ ووقت تلقي البلاغ
- المعلومات الخاصة بالمبلغ
- المعلومات الخاصة بمتلقي البلاغ
- طبيعة ونوع جريمة الحاسب الآلي محل البلاغ
- الأسئلة الستة المشهورة والمتعلقة بالجريمة ماذا؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟
- المعلومات ذات العلاقة بالأنظمة الحاسوبية، مثل طبيعة العتاد ونوعية البرمجيات والمسئولين عن الأنظمة وطريقة الاتصال بهم وغيرها.

ومما يجدر التنويه عليه أن عملية تلقي البلاغ لا تعدو أن تكون محادثة قصيرة وسريعة تهدف إلى تمكين المحقق من وضع تصور مبدئي عن ظروف وملابسات الحادث قبل الانتقال إلى مسرح الجريمة. ومع ذلك فإننا نري أن دقة وتكامل المعلومات محل البلاغ على درجة كبيرة من الأهمية، حيث أنه من الممكن أن تسهم في مساعدة المحقق على:

- تحديد ما إذا كان السلوك محل البلاغ يعد سلوكاً إجرامياً يندرج ضمن جرائم الحاسب الآلي والإنترنت.
- وضع تصور مبدئي عن خطة العمل المناسبة للتحقيق في الحادث.
- تحديد نوع الخبرة الفنية التي يحتاجها في المعاينة ورفع وتحريز الأدلة من موقع الحادث، والعمل على سرعة استدعاء الخبراء القادرين على إنجاز ذلك.

وقبل أن ينهي المحقق عملية تلقي البلاغ يجب أن يحرص على التأكيد على المبلغ بضرورة القيام بالأمور التالية [٩].

١. تجهيز قائمة بأسماء العاملين في المؤسسة ممن لهم علاقة بالأجهزة المتضررة، أو علاقة بأي مشروع للأجهزة المتضررة.
٢. تجهيز النسخ الاحتياطية من بيانات الأجهزة المتضررة، لاستخدامها من قبل فريق التحقيق فور وصوله الموقع.
٣. التأكيد على عدم إبلاغ أحد بالحادث إلا من كانت الضرورة القصوى تحتم إبلاغه.

ثانياً. تحديد خطة العمل

بعد الانتهاء من جمع المعلومات اللازمة عن الحادث، يبدأ المحقق وعلى ضوء تلك المعلومات التي توافرت لديه تحديد خطة العمل المناسبة وفريق العمل اللازم للتحقيق في الحادث، وهذه الخطة يجب أن تكون قد اكتملت في ذهن المحقق بمجرد انتهائه من معاينة موقع الحادث واتضحت لديه الصورة الأولية عن الحادث [١٠].

أ. تحديد خطة العمل المناسبة

يتم التخطيط للتعامل مع حوادث الحاسب الآلي وشبكة الإنترنت على ثلاثة مستويات مختلفة، يبنى كل مستوى منها على الآخر [١١]:

١. تخطيط إستراتيجي: وهو تخطيط بعيد المدى يهتم بحماية البنية التحتية لشبكات الحاسوب الوطنية، من خلال تحديد مصادر الخطر المحتملة التي قد تمثل تهديداً لها وتحديدها، ويهتم بوضع تصورات على درجة من المرونة تكون كفيله بالتصدي لهذا النوع من الجرائم قبل وقوعها وضبطها والحد من أثارها في حال وقوعها، ويتم هذا التخطيط على مستوى واضعي السياسات الأمنية، حيث يهدف بشكل عام إلى منع هذا النوع من الجرائم من الوقوع داخل إقليم الدولة، والحد من قابلية الحواسيب والشبكات الوطنية من التعرض للهجوم، ومن ثم السيطرة على الحوادث إن وقعت وضبطها والحد من آثارها. ومن أهم ما يميز هذا النوع من التخطيط أنه يضع الخطوط الاسترشادية التي تسترشد بها الجهات المختلفة ذات العلاقة في وضع خطط التعامل مع هذا النوع من الجرائم، كما يحدد الآليات اللازمة لتنفيذ الخطة.

٢. تخطيط تكتيكي: ينبثق من الخطة الإستراتجية ويتم على مستوى الجهات الرسمية والغير رسمية التي لها علاقة بتقنية المعلومات ويدعم غايات وأهداف الخطة الإستراتيجية للتعامل مع جرائم الحاسوب والإنترنت. ويمتاز بأن له طابع تفصيلي أكثر من التخطيط الاستراتيجي، والخطط التكتيكية الخاصة بالتعامل مع جرائم الإنترنت يجب أن تتضمن إجراءات مسبقة التحديد على درجة عالية من التفصيل والوضوح للتحقيق في هذه الجرائم.

٣. خطة عمل: ويقصد به التخطيط الذي يقوم به المحقق لتحديد الأسلوب الأمثل في التعامل مع حادث بعينه، وذلك في الإطار العام للإجراءات الواردة في الخطة التكتيكية وبما يتناسب مع خصوصية ظروف وملابسات الحادث.

ب. مرتكزات خطة العمل

من أهم الأمور التي يجب على المحقق أخذها في الاعتبار كمرتكزات تساعده في تحديد خطة العمل المناسبة للتحقيق في أي جريمة من الجرائم الحاسوبية والإنترنت:

١. حجم ونوع الحادث التي يكون المحقق بصدد التحقيق فيه يرتبط به تحديد حجم ونـــوع فريـــق التحقيـــق، فجـــرائم الإنترنت منها الصغير ومنها الكبير ولكل جريمة مهما كان حجمها، طبيعتها الفنية الخاصة التي تفرض علـــى أعـــضاء فريق التحقيق امتلاك مهارات فنية خاصة تعتبر ضرورية للتعامل مع هذا النوع من الجرائم، وهو أمر يجب مراعاتـــه عند اختيار أعضاء الفريق [١٢].

٢. بعض الظروف المحيطة بالحادث تمثل عوامل مهمة يجب مراعاتها عند وضع خطة العمل، لما يترتب عليهـــا مـــن قرارات على درجة كبيرة من الأهمية تتعلق بالتحقيق، ومن هذه العوامل [١٣]:

- مدى أهمية الأجهزة الحاسوبية والشبكات المتضررة لعمل المنظمة أو المؤسسة.
- مدى حساسية البيانات التي قد تكون محل الجريمة الحاسوبية.
- المتهمون المحتملون.
- إطلاع الرأي العام على الجريمة أم لا.
- مستوى الاختراق الأمني الذي تسبب فيه الجاني.
- مستوى المهارة الفنية التي يتمتع بها الجاني.

٣. طبيعة مسرح الجريمة تفرض الأسلوب الأمثل للتفتيش بحثاً عن الأدلة التي تكون موجودة فيه والذي يعتبر من أهـــم خطوات عملية التحقيق وعدم نجاح المحقق في تحديد هذا الأسلوب قد يؤدي إما إلى عدم الحصول على أيـــة نتـــائج أو الحصول على كم كبير من النتائج التي لا فائدة منها [١٤]، فقائد فريق التحقيق مسئول عن تحديد حجم المهمـــة ونـــوع الأدلة التي يتم البحث عنها بحسب نوع الجريمة، وكذلك تحديد أنسب الطرق لتنفيذ عملية التفتيش وما يتبـــع ذلـــك مـــن توزيع للأدوار والواجبات على فريق التحقيق [١٥].

٤. تعين الأشخاص الذين سيتم استجوابهم، وتحديد النقاط التي يجب استيضاحهم بشأنها، وكذلك تقدير مدي الحاجة إلـــى الاستعانة ببعض الأشخاص من ذوى الاختصاصات الفنية التي يتطلبها التحقيق ولا تتوافر ضمن أفراد التحقيق.

ثالثا. تكوين فريق التحقيق

هناك محققون جنائيون ذوو خبرة طويلة، وهناك أخصائيون في الحاسب الآلي والشبكات ذوو معرفة واسعة، ولكنه من النادر أن يوجد شخص واحد يمتلك مهارات عالية في الاثنين معاً [١٦]. سيما وأن عالم الحاسوب والشبكات عالم متعدد ومتشعب وعلى درجة كبيرة من التعقيد وسرعة التطور. ولذلك كان من الضروري أن يستعين المحقق بخبراء في هذا المجال بحسب ما تفرضه ظروف كل قضية وملابساتها. كما وأن التحقيق في هذه الجرائم قد يتطلب الاستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير الذين يعتبرون من الخبراء الأساسين في معظم أنواع الجرائم. وعلى هذا الأساس يمكن تقسيم فريق التحقيق في هذا النوع من الجرائم إلى فئتين هما:

الفئة الأولى: وتمثل الأشخاص الذين يتصل عملهم مباشرة بجرائم الحاسب الآلي والإنترنت ولا يمكن التحقيق في أي جريمة تنتمي إلى هذه النوعية من الجرائم إلا بهم، ووجودهم ضروري في مسرح الجريمة ويمكن تحديد أعضاء هذه الفئة على النحو التالي:

١. قائد الفريق: يشترط فيه أن يكون له خبرة طويلة في مجال التحقيق الجنائي، ولديه معرفة بالطبيعة الخاصة بجرائم الحاسب الآلي والإنترنت يتولى السيطرة الكاملة على مسرح الجريمة، وتوزيع المهام على الفريق والإشراف على قيامهم بأعمالهم، والتنسيق مع الجهات ذات العلاقة، واتخاذ كافة القرارات المتصلة بالتحقيق [١٧].

٢. محقق جنائي: شخص أو أكثر بحسب ظروف الجريمة، لديه خبرة ومعرفة بوسائل وأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرائم الحاسوب والإنترنت وكيفية التعامل مع الأدلة الرقمية فيتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة [١٨].

٣. خبير حاسب آلي وشبكات: شخص أو أكثر بحسب الظروف يجمع بين المعرفة بعلوم الحاسوب والشبكات وبين الإلمام بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة ويكون مسئولاً عن رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض على المحكمة.

٤. خبير تدقيق حسابات: متخصص في المراجعة المحاسبية وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية والآليات المختلفة التي يتم بواسطتها تبادل النقد الإلكتروني، ويعمل مع خبير الحاسب الآلي والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة [١٩].

٥. خبير تصوير يتولى تصوير مسرح الجريمة كالمتبع في جميع الجرائم، بالتصوير الفوتوغرافي والفيديو.

٦. خبير بصمات: لرفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحواسيب والشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح والفأرة، وذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسوب.

٧. خبير رسم تخطيطي: يقوم بعمل رسم تخطيطي (كروكي) لمسرح الجريمة بطريقة فنية دقيقة مستخدماً مقياساً مناسباً للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه [٢٠].

الفئة الثانية: وهي تمثل الأشخاص الذين قد يتطلب ظروف مسرح الجريمة تواجدهم، إلا أن دورهم ليس وثيق الصلة بالطبيعة الخاصة لجرائم الحاسب الآلي، وقلما يخلوا مسرح أي جريمة مهما كان نوعها من وجودهم، مثل أفراد حماية

وتأمين المسرح وأفراد القبض وأفراد التحريات وغيرهم، وتحديد الأعضاء نوعاً وكماً متروك لتقدير المحقق على ضوء المعلومات المتوفرة لديه عن الجريمة، وحسب ما تفرضه طبيعة مسرح الجريمة وحجمها وظروفها.

رابعا. جمع الأدلة

عند الشروع في جمع الأدلة من مسرح جريمة من الجرائم المتعلقة بشبكة الإنترنت ينبغي التعامل معه على أنه مسرحين هما:

١. مسرح تقليدي: ويقع خارج بيئة الحاسب الآلي والإنترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة، كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

٢. مسرح سيبراني" افتراضي": ويقع داخل بيئة الحاسب الآلي وشبكة الإنترنت، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن يتم على يد خبير متخصص في التعامل مع الأدلة الرقمية وسوف نبحث ذلك وبشيء من التفصيل في محاضرة خاصة.

أ. معاينة مسرح الجريمة المتعلقة بشبكة الإنترنت

مع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة والأولوية فيما عدا حالات استثنائية على ما عداها من الإجراءات الاستقصائية الأخرى. إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها لا ترقَ إلى نفس الدرجة من الأهمية، ومرد ذلك اعتبارين هما [٢١]:

الأول أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها آثاراً مادية، والثاني هو أن عدداً كبيراً من الأشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يفسح المجال لحدوث تغير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلالاً من الشك على الدليل المستمد من المعاينة. وحتى يكون للمعانية في الجرائم المتعلقة بشبكة الإنترنت فائدة في كشف الحقيقة عنها وعن مرتكبها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي [٢٢]:

- تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية الخاصة بالتسجيلات الإلكترونية التي تتزود بها شبكات المعلومات بموافقة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.
– وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي بالمسئولين بها ودور كل واحد منهم.
– فصل الكهرباء عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة.
– إبعاد الموظفين عن أجهزة الحاسب الآلي، وكذلك عن الأماكن الأخرى التي توجد بها أجهزة للحاسب الآلي.
– عدم نقل أي معلومة من مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من آي مجال مغناطيسي يمكن أن يتسبب في محو البيانات المسجلة.
– التحفظ عما قد يوجد بسلة المهملات [٢٣] من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة والأشرطة والأقراص الممغنطة غير السليمة، وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.
– التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد بها من بصمات.
– قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسب الآلي والشبكات ونظم المعلومات. واسترجاع المعلومات، والذين تلقوا تدريباً كافياً على التعامل مع نوعية الآثار والأدلة التي يحويها مسرح الجريمة المعلوماتية. ففي فرنسا مثلاً يقوم فريق مكون من ١٣ شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إليه وكلاء النيابة والمحققين وجميعهم تلقوا تدريب متخصص إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة. وهم يقومون بمرافقة المحققين أثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بعمل تقرير يرسل إلى القاضي الذي يتولى التحقيق. أما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعادة المعلومات من على الاسطوانة الصلبة كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة.

ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حده بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق. ولعل من أبرز الأماكن التي يحتمل وجود الأدلة الجنائية المتعلقة بجرائم الإنترنت فيها ما يلي [٢٤]:

الورق: على الرغم من إن وجود أجهزة الحاسب الآلي قلل من حجم الأوراق والملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسب الآلي، نجد الكثيرين ممن يقوموا بطابعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها في البحث عن الحقيقة.

جهاز الحاسب الآلي وملحقاته: وجود جهاز الحاسب الآلي هام جداً للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية، وإنها مرتبطة بالمكان أو الشخص الحائز على الجهاز، ولأجهزة الحاسب الآلي أشكال وأحكام وألوان مختلفة وخبير الحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة.

البرمجيات Software: إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص أو ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل [٢٥].

وسائط التخزين المتحركة: كالأقراص المدمجة "أقراص الليزر" والأقراص المرنة والأشرطة المغناطيسية والفلاش ممموري وغيرها، وتعد هذه الوسائط جزاء من الجريمة الإنترنتية متى ما كانت محتوياتها عنصر من عناصر الجريمة.

المراشد Manuals: الخاصة بالمكونات المادية والمنطقية للحاسب الآلي والتي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها [٢٦].

المودم Modem: وهو الوسيلة التي تمكّن أجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف. وفي الوقت الحالي تطورت المودم لتكون أجهزة إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.

الطابعات: والتي قد تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها.

ب. التفتيش: ويعرّف التفتيش بوجه عام بأنه عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محددة [٢٧]. وفي الجرائم المتعلقة بشبكة الإنترنت نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية. وهو إجراء جائز قانوناً ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه.

ما مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش؟

للحاسب الآلي مكونات مادية Hardware، وأخرى منطقية Software، كما أن له شبكات اتصال بعدية Networks Telecommunication سلكية ولا سلكية محلية ودولية. فما مدي قابلة تلك المكونات؟:

١. المكونات المادية للحاسب الآلي ومدى قابليتها للتفتيش

لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسب الآلي بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة [٢٨] مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب

المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب آلي أخر أو بنهاية طرفية Terminal في مكان أخر كمسكن غير المتهم مثلاً، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن [٢٩].أما لو وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطراً عليها أو حائزاً لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

٢. المكونات المنطقية للحاسب الآلي ومدي قابليتها للتفتيش

تفتيش المكونات المنطقية للحاسب الآلي أثار خلافاً كبيراً في الفقه بشأن جواز تفتيشها، فذهب رأي إلى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء" فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة [٣٠]. بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لابد أن يشمل "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي". بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب [٣١]. وفي مقابل هذين الرأيين يوجد رأي آخر نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسب الآلي أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلاً مادياً [٣٢].

ويذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكيانات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزاً مادياً في فراغ معين وأن الحيز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزاً مادياً في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معين، وإنها أيضاً تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها تعد طبقاً لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية.

٣. شبكات الحاسب الآلي ومدى خضوعها للتفتيش "التفتيش عن بعد"

إن طبيعة التكنولوجيا الرقمية قد عقَّدت من التحدي أمام أعمال التفتيش والضبط. فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش، وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها. وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر. وفي حين أن السلطات في بعض البلدان قد لا تنزعج من أن تقودها تحقيقاتها إلكترونياً إلى اختصاص قضائي سيادي آخر، إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج. وهذا يزيد من تعقيد مشاكل

الجريمة السيبرانية العابرة للحدود ويزيد من أهمية تبادل المساعدة القانونية، ونستطيع أن نميز في هذه الصورة بين ثلاثة احتمالات على النحو التالي:

– الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة:
يُثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم؟

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم ١٠٣ من قانون الإجراءات الجزائية الألماني [٣٣]. ونجد إرهاصات هذا الرأي في المادة ٨٨ من قانون تحقيق الجنايات البلجيكي التي تنص على " إذا أمر قاضي 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، ويتم هذا الامتداد وفقا لضابطين: "أ" إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث."ب" إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث [٣٤]. وذات الشيء نجده في القانون الاتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الحاسوبية تقتصر على مواقع محددة، فقد توخى قانون الجرائم السيبرنية لعام ٢٠٠١ إمكانية أن تتوزع بيانات الأدلة على شبكة حواسيب، ويسمح هذا القانون بعمليات تفتيش البيانات خارج المواقع التي يمكن اختراقها من خلال حواسيب توجد في الأبنية الجاري تفتيشها. ويشير مصطلح "البيانات المحتجزة في حاسوب ما " إلى " أية بيانات محتجزة في جهاز تخزين على شبكة حواسيب يشكِّل الحاسوب جزءاً منها". فلا توجد حدود جغرافية محددة، ولا أي اشتراط بالحصول على موافقة طرف ثالث. غير أن المادة LB٣ بقانون الجرائم لعام ١٩١٤، والتي أدرجها قانون الجرائم السيبرنية، تشترط إخطار شاغل المبنى النائي قدر الإمكان عملياً. وهذا قد يكون أكثر تعقيداً مما يبدو عليه، إذ أنه في مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكياً، فإن المرء لا يكون متأكداً دائماً من مكان وجوده [٣٥].

– الاحتمال الثاني: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة من المشاكل التي تواجه سلطة الادعاء في جمع الأدلة قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية مستهدفين عرقلة الادعاء في جمع الأدلة والتحقيقات [٣٦]. وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي للدولة أخرى وهو ما يسمي بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها. لذا فإن جانب من الفقه يرى بأن التفتيش الإلكتروني العابر للحدود لا بد وأن يتم في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد تعقد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك اتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني [٣٧].

وكتطبيق لهذا الإجراء الأخير: فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، فقد تبين وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها. وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين [٣٨]. ومع ذلك أجازت المادة ٣٢ من الاتفاقية الأوربية بشأن الجرائم المعلوماتية والتي أعدها المجلس الأوربي وتم التوقيع عليها في بودابست في ٢٠٠١/١١/٢٣ م إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور. والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

– الاحتمال الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي

التنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريباً. فالقانون الفرنسي الصادر في ١٩٩١/٧/١٠ م يجيز اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات [٣٩]. وفي هولندا أجاز المشرع لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات [٤٠]. وفي اليابان أقرت محكمة مقاطعة KOFU سنة ١٩٩١ م شرعية التنصت على شبكات الحاسب للبحث عن دليل [٤١].

وتفتيش نظم الحاسب الآلي يمكن أن يتم بطرق عدة، فمثلاً المرشد الفيدرالي الأمريكي [٤٢] جاء بأربع طرق أساسية للتفتيش ممكنة التحقيق هي [٤٣]:

١. تفتيش الحاسب الآلي وطبع نسخة ورقية من ملفات معينة في ذات الوقت.

٢. تفتيش الحاسب الآلي وعمل نسخة إلكترونية من ملفات معينة في ذات الوقت.

٣.عمل نسخة إلكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع، وبعد ذلك يتم إعادة عمل نسخة تعمل من جهاز التخزين خارج الموقع للمراجعة.

٤. ضبط الجهاز وإزالة ملحقاته ومراجعة محتوياته خارج الموقع.

المحور الثالث: الوسائل والبرمجيات المساعدة في التحقيق في الجرائم المتعلقة بالإنترنت

عند القيام بالتحقيق في جريمة ما، فإنه يجب على المحقق الالتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني. وحيث أن للجرائم المتعلقة بالإنترنت طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة وبالتالي حل لغزها والوصول إلى الجاني. وتوجد ثمة وسائل تساعد على تلك أهمها:

الوسائل المادية

وهي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها [٤٤]:

أ. عناوين IP، والبريد الإلكتروني، وبرامج المحادثة: عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة. وهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، كل جزء يتكون من أربع خانات، فيكون المجموع اثنا عشر خانة كحد أقصى، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه [٤٥]. وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية. ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضاً إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسب الآلي في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل WINDOWS حيث يتم كتابة WINPCFG في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان IP، مع ملاحظة أن عنوان الإنترنت قد يتغير مع كل اتصال بشبكة الإنترنت. أما في حالة استخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة [٤٦].

ب. البروكسي PROXY: يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memory . وتقوم فكرة البروكسي على تلقى مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية. أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة

العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP. ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوى في الإثبات عن طريق فحص تلك العلميات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة [٤٧].

ج. برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم وتقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى [٤٨].

د. نظام كشف الاختراق Intrusion Detection System: ويرمز له اختصاراً بالأحرف IDS وهذه الفئة من البرامج تتولي مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة [٤٩]. ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عده ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة [٥٠] والتي يمكن أن تقدم معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.

هـ. نظام جرة العسل Honey Pot: وهو نظام حاسوبي مصمم خصيصاً لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعاً خاطئاً بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها وبالتالي اتخاذ إجراء وقائي فعال [٥١] وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها ويهتم فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.

و. أدوات تدقيق ومراجعة العمليات الحاسوبية Auditing Tools:

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها Logs والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل المختلفة، وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل، وكل ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يمكن أن تقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها [٥٢]. ومن الأمثلة على هذه الأدوات أداة Event Viewer لبيئة النوافذ، وأداة Syslogd لبيئة يونيكس [٥٣].

ح. أدوات الضبط: هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية، منها على سبيل المثال برامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التنصت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي [٥٤]، والتسجيل وغيرها من الأدوات مثل [٥٥] IDS,MNM4,CONTENT MANGEMENT .

ط. الوسائل المساعدة للتحقيق: من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب، وبرامج نسخ البيانات، أيضاً من الأدوات المهمة والتي تساعد جداً في عملية التحقيق في برامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة مما يساعد في المحافظة على مسرح الجريمة، وهناك البرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني إلى حذفها نهائياً من الحاسب الآلي [٥٦].

وهناك أيضا برمجيات تحرير الملفات الست عشرية Hexadecimal Editors وهي برامج تمكن المحقق من الإطلاع على محتوى كل ملف حاسوبي بشكله الثنائي، متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خاصة وأن بعض الأنظمة قد لا تستطيع تحديد إلى أية فئة من الملفات ينتمي هذا الملف، وقد يتطلب الأمر استخدام هذا النوع من برامج التحرير التي تعتمد على أن الكثير من الملفات تحتوى على مجموعة من الرموز ذات الدلالة تتواجد في بداية الملف، ويستطيع الخبير الحاسوبي من خلالها تحديد نوع الملف بدقة [٥٧]. وهناك برمجيات البحث عن المفردات النصية والتي تستخدم في البحث عبر البيانات عن تلك الملفات التي تحتوى على مفردات معينة عادة ما تكون لها علاقة بالقضية [٥٨].

كذلك توجد برمجيات استعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز وبالتالي فهي تقدم خدمة جيدة للمحقق من خلال تمكينه من مشاهدة واستعراض الصور الرقمية المخزنة داخل أجهزة الحاسب الآلي أو وسائط التخزين الخارجية، حيث تبرز الحاجة لهذه البرمجيات في الجرائم الإباحية "نشر مواد ذات طابع إباحي".

ي. أدوات فحص ومراقبة الشبكات [٥٩]: هذه الأدوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها، ومن هذه الأدوات:

١. أداة ARP: ووظيفتها تحديد مكان الحاسب الآلي فيزيائياً على الشبكة.

٢. برنامج Visual Route 5.2a: وهو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

٣. أداة TRACER: تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الخيار Time To Live TTL)) التي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات. ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة. وهذه الأداة تستخدم

في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضاً من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.

٤. أداة NET STAT: هي أداة لفحص حالة الاتصال الحالي للبرتوكول TCP/IP، ولها عدد من المهام من أهمها عرض جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه.

الوسائل الإجرائية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها [٦٠]:

١. اقتفاء الأثر: من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح آثارك Cover Your Tracks، فلو لم يقم المخترق بمسح آثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم. ويمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

٢.الإطلاع على عمليات النظام المعلوماتي وأسلوب حمايته: ينبغي على المحقق وهو بصدد التحقيق في إحدى الجرائم المعلوماتية كالجرائم المتعلقة بشبكة الإنترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي عليه الإطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي. والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها، والاستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية [٦١].

٣. الاستعانة بالذكاء الصناعي: أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج صممت خصيصا لهذا الغرض.

المحور الرابع: معوقات التحقيق في الجرائم المتعلقة بالإنترنت

يتسم التحقيق في الجرائم المتعلقة بالإنترنت وملاحقة مرتكبيها جنائياً بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق، بل يمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضاً على المجرم نفسه، حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه، الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشد ضرراً على المجتمع المحلي أو المجتمعات الأخرى [٦٢]. ومن أهم المعوقات التي قد تواجه القائمين على مكافحة الجرائم المعلوماتية والتحقيق فيها:

١. عوائق تتعلق بالجريمة

- خفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه.
- افتقاد أكثر الآثار التقليدية.
- صعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها.
- سهولة محو الدليل أو تدميره في زمن قصير جداً فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، وبالتالي تنصله من مسئولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة [٦٣].
- الضخامة البالغة لكم المعلومات والبيانات المتعين فحصها، وإمكانية خروجها عن نطاق إقليم الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية [٦٤]. بالإضافة إلى عدم المعرفة بمكونات الجريمة المتعلقة بالإنترنت من قبل بعض الأطراف المعينة.
- عدم المعرفة بمكونات الجريمة المتعلقة بشبكة الإنترنت من قبل بعض الأطراف المعنية [٦٥].

٢. عوائق تتعلق بالجهات المتضررة

- عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معوقات التحقيق.
- إغفال الجانب التوعوى لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بشبكة الإنترنت [٦٦].
- تسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، على سبيل المثال مستخدمو شبكة الإنترنت عبر مزودي الخدمة أو بطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم"عملية ربط رقم المستخدم مع هويته" عند الاشتراك في خدمة الإنترنت، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة [٦٧].
- الإحجام عن الإبلاغ: من أهم وأخطر المشكلات التي تتعلق بعملية الإبلاغ عن جرائم الإنترنت، حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم، خاصة المؤسسات والشركات التجارية، حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم. ففي دراسة للمعهد الوطني للعدالة التابع

لوزارة العدل الأمريكية شملت ١٢٧ من العاملين في مجال التحقيق في جرائم الحاسوب والإنترنت يمثلون ١١٤ وكالة رسمية، كان غالبية المشاركين في الدراسة يعتقدون أن معظم جرائم الحاسوب والإنترنت التي يتم اكتشافها لا يبلغ عنها للشرطة. كما توصلت دراسة أخري أجراها معهد أمن الحاسوبCSI بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي ٧٠%من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها لسلطات إنفاذ العدالة.

ويمكن أن يعزي إحجام البعض عن الإبلاغ لعدة أسباب.

– عدم إدراك الأفراد أو مدراء الأنظمة الحاسوبية ومسئولي الشركات أن مثل هذه الأفعال والهجمات تعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دولياً.

– خوف الجهات التي وقعت عليها الجرائم، خاصة المؤسسات والشركات المالية من أن يؤثر انتشار خبر الحادث على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعاً بإهمالها أو قلة خبرتها أو عدم وعيها الأمني [٦٨]، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي قد ينعكس سلباً على أرباحها وقيمة أسهمها [٦٩].

– خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق إلي احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، عطفا على ما قد تسببت الجريمة خسارتها أصلا.

– بعض الضحايا قد تساوره الشكوك حول مقدرة رجال إنفاذ القانون على التعامل مع هذا النوع المستحدث من الجرائم.

– الرغبة في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليده من الآخرين مستقبلاً [٧٠].

– قد تكون بعض هذه الجرائم محدودة الأثر، مما يدفع بعدم الإبلاغ عنها، فقد يقوم مخترق ما للنظام بإظهار رسالة تفيد بقيامه بهذه العملية، أو يقوم مجرم آخر بإرسال فيروس حاسب آلي إلى جهاز المستفيد ويكون هذا الفيروس محدود الأثر، أو تقوم برامج الحماية من الفيروسات بالقضاء عليه.

– قد يكون الإفصاح عن التعرض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتى. فقد يحرم الموظف في الجهة من خدمات معينة على الإنترنت أو قد يحرم من خدمات الإنترنت عموماً حين يتعرض لجريمة معلوماتية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها.

– عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة إنها ممكن أن تحدث في مؤسسته.

٣. عوائق تتعلق بجهات التحقيق "عدم توفر الكفاءة البشرية المؤهلة للتحقيق"

– معوقات ترجع إلى شخصية المحقق، مثل التهيب من استخدام الحاسب الآلي والتهيب من استخدام شبكة الإنترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

– تتعلق بالنواحي الفنية، كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، ونقص المهارة في استخدام الحاسب الآلي والإنترنت، وعدم توفر المعرفة بأساليب ارتكاب جرائم الحاسب الآلي والإنترنت، وقلة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت والمعرفة باللغة الإنجليزية [٧١]. سيما وإن للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، وليس هذا فحسب بل أختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة متطورة ومتجددة.

ومن أجل ذلك فإنه لابد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم أسلوب يجمع بين الخبرة الفنيـــة والكفـــاءة المهنية ومن الممكن حيال ذلك إتباع الخطوات التالية [٧٢]:

أ. تبادل المعلومات بين المحقق وخبير الحاسب الآلي وذلك قبل البدء في التحقيق وأخذ أقوال الشهود والمشتبه فـــيهم أو استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم [٧٣] ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلائها من الأشخاص. وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معانيها ليتم الاستفادة منها عند الضرورة.

ب. يتم حصر النقاط المطلوب استجلائها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيـــب تلك النقاط.

جـــ. يتم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي تتم الاتفاق عليها مسبقاً قبل بدء التحقيق.

د. التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاتـــه الخاصـــة بالـــشاهد أو المتهم الذي تم التحقيق معه. مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه.

ولضمان نجاح التحقيق في الجرائم المعلوماتية فهناك بعض القواعد التي ينبغي مراعاتها أهمها:

أ. تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها أو أن الأدلة اللازمة لاكتشافها واثبات التهمة قد قضي عليها.

ب. ضرورة مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها.

جـــ. مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البرد الإلكتروني وغيرها من الحقوق.

د. العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها.

هـــ. مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدا، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.

و.الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية، ولا سيما وأن هذا التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق.

المراجع

[١]

USSS United States Secret Service (2002). Best Practices for Seizing Electronic Evidence .on line: www.secretservice.gov/electronic_evidence.shtml.

[٢]

Thompson, David (1990) .Computer Crime The Improvement Of Investigative Skills: Final Report: Part Tow, www.acpr.gov.au/pdf/ACPR101.pdf 21/10/2003.

[٣] محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت "دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤ م ص ٩٥- ٩٦.

[٤]

Shindre, Debra (2000). Scene Of The Cyber crime: Computer Forensics Hand Book. Rockland, MA: Syngress Publishing.

[٥]

ISTS, Institute for security Technology Studies (2002). Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment.available On line at 4/6/2003:
www.ists.dartmouth.eud/TAG/need/ISTS_NA.pdf

[٦] غالباً ما يتم حفظ البيانات الرقمية داخل جهاز الحاسب الآلي على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمي ملفات، حيث يتميز كل ملف ببيئة وصيغة خاصة تسمى Format تميزه عن غيره وغالباً ما ترتبط كل صيغة بنوع محدد من المحتوى. كأن يحتوى الملف على بيانات تمثل صورة أو صوت أو فيديو أو مستند خطي أو غير ذلك. أنظر. محمد بن نصير محمد السرحاني: المرجع السابق ص ٩٧.

[٧]

Davis, David (1998) Internet Detective: An Investigator's Guide. West Midland, UK: Police Research Group.

[٨]

Sterneckert, Alan (2004). Critical Incident Management. Boca Raton, Florida: CRC Press.

[٩]

Middleton, Bruce (2002). Cyber Crime Investigator's Field Guid.Boca Raton, Florida: Auerbach Publications.

[١٠]

Icove, D, Segar.K & Vonstorch,W (1995). Computer Crime: A Crimefighter's Handbook. .Sebastopol.California: O'Reilly & Associates.

[١١] محمد بن نصير محمد السرحاني: المرجع السابق ص ٧٠.

[١٢]

Icove, D, Segar.K & Vonstorch,W (1995). Computer Crime: A Crimefighter's Handbook Sebastopol.California: O'Reilly & Associates.

[١٣]

Mandia&, K.& Prosise, C. (2001) . Incident response: Investigating Computer .Crime .Berkeley, California: McGraw-Hill.

[١٤]

Schultz, E & Shumway, R. (2002) Incident Response: A Strategic Guide to Handling System and Network Secueity Breaches. Indianapolis, Indian: New Riders Publishing.

[١٥]

Wright, Timothy (2000)(d). The Field Guide for Investigating Computer Crime: Search and (Seizure Planning (on line) www.securityfocus.com/infocus/1247 (05-09-2003.

[١٦]

Groover, Richard (1996). Overcoming Obstacles: Preparing for Computer – related Crime. (online): www.fbi.gov/publications/leb/1996/aug962.txt (06/06/2003.

[١٧]

Icove, D, Segar.K& Vonstorch ,W et al,1999&Wright, 2000d.

[١٨]

Icove et al,1995.

[١٩]

Icove et al,1995 &Stephenson Peter (2000) . Investigating Computer- Related Crime.Boca .Raton Florida: CRC Press.

[٢٠]

Wright, Timothy (2000)(d). The Field Guide for Investigating Computer Crime: Search and Seizure Planning (on line) www.securityfocus.com/infocus/1247 (05-09-2003).

[٢١] الدكتور:هشام محمد فريد رستم:الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص ٥٩ & الدكتور: عبد الله حسين على محمود:إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، إمارة دبي بدولة الإمارات العربية المتحدة – ٢٦-٢٠٠٣/٤/٢٨ م، المجلد الأول، ص ٥٩٨.

[٢٢] أنظر في ذلك:

– الدكتور محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، سابق الإشارة إليه، ص ٣٠-٣١

– الدكتور: هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص ٦٠

– الدكتور: عبد الله حسن علي محمود: إجراءات جمع الأدلة في مجال سرقة المعلومات، مرجع سابق ص ٥٥٩-٥٦٠.

[٢٣] من فحص بعض البطاقات المثقبة المعثور عليها بسلة المهملات في المكان الموجود به جهاز الحاسب الآلي أمكن كشف غموض جريمة شهيرة لسرقة البرمجيات عن بعد وقعت أحداثها بسانتا كلارا بالولايات المتحدة الأمريكية. حول التفاصيل الفنية لارتكاب هذه الجريمة أنظر: الدكتور: هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط ١٩٩٢ م ص ١٢٦-١٢٧.

[٢٤] أنظر في ذلك:

- الدكتور: عبد الله حسين علي محمود: إجراءات جمع الأدلة في مجال جرائم سرقة المعلومات، المرجع السابق ص ٦٢٤-٦٢٧

- الدكتور: محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من ١-٣/٥/٢٠٠٠ م، المجلد الثالث ص ١٠٢٥-١٠٢٥٩.

[٢٥]

Sammes T & Jenkinson B, (2000). Forensic Computing: Apratitioner's Guide London: Springer.

[٢٦] محمد بن نصير محمد السرحاني: المرجع السابق ص ٨١.

[٢٧] الدكتور: هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى "ط١"، دار النهضة العربية، القاهرة ١٩٩٧ ص ٤٧.

[٢٨] الدكتور: هلالي عبد اللاه أحمد، المرجع السابق ص ٧٣.

[٢٩] الدكتور: عبد الله حسين علي محمود: سرقة المعلومات المخزنة في الحاسب الآلي، مرجع سابق- ص ٣٧٠.

[٣٠]

Vassilaki (Irini): Computer crimes and other crimes against inforation technology in Greece. .Rev. Intern De. Dr. Pen. P.371.

[٣١]

Piragoff (Donald K): Computer crimes and other crimes against information technology in Canda: Rev. Intern. De. Dr. Pen. 1993P. 241.

[٣٢] أشار إلى هذا الرأي د. هلالي عبد الله، تفتيش نظم الحاسب الآلي، مرجع سابق.

[٣٣]

Kaspersen (W.K.Henrik) :"computer crime and other crime against Information Technology In Netherlands" R.I.D.P 1993, p479.

[٣٤] الدكتور: محمد أبو العلاء عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المرجع السابق ص ٣٤-٣٥.

[٣٥] مقتضيات تعامل أجهزة النيابة العامة مع الجريمة السيبرنيَة (الحاسوبية)، ورقة عمل قدمت إلى مؤتمر القمة العالمي لأعضاء ورؤساء النيابة العامة، المنعقد بالعاصمة القطرية الدوحة في الفترة من ١٤-١٦ /١١/٢٠٠٥، ص ١٥.

[٣٦]

Sieber(Ulrich):"computer crime and other crime against Information Technology – Commentary and Preparatory question for The colloquium of the A.I.D.P In Wurzburg" R.I.D.P 1993, p77.

[٣٧] الدكتور: محمد أبو العلاء عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المرجع السابق- ص ٣٥٠.

[٣٨]

Mohrenschlager "Manfred": Op., Cit., P. 351.

[٣٩]

Francillon (Jacques):"" les crimes in formatiques et d'aulres crimes dans le domain de technologies informatique en France" R.I.D.P 1993, p309

[٤٠]

Kaspersen (W.K.Henrik): op-cit.p500-501.

[٤١]

Yamaguchi (Atsushi):"computer crime and other crime against Information Technology In Japan" R.I.D.P 1993,p443 Yamaguchi (Atsushi) :"computer crime and other crime against Information Technology In Japan" R.I.D.P 1993, p443.

[٤٢] تم وضع هذا المرشد عام ١٩٩٤ م، وصدر له ملحقان في عامي ١٩٩٧، ١٩٩٩، ولقد قام بإعداده مجموعة عمل في قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف أستاذ القانون الجنائي Orin Kerr، ولقد صدرت له عدة تعديلات أخرها كان تعديل ٢٠٠٢ الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في ٢٠٠١/١٠/٢٦.

[٤٣] المرشد الأمريكي، مرجع سابق م ١٦٢.

[٤٤] سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٣ م ص ٩٨.

[٤٥]

Arabiat 2000 ON Line available at www.arabiat.com.

[٤٦] حول ذلك أنظر:

– سليمان بن مهجع العنزي: المرجع السابق ص ٩٩

NOR2000(2002) . ON Line available at www.non2000.com/netwrk/htm at 19/6/2002.

[٤٧] سليمان بن مهجع العنزي: المرجع السابق ص ٩٩.

[٤٨] من الأمثلة على هذه البرامج: برنامج Hack Tracer v1,2 وهو يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق التي تعرض لها جهازه، يحتوى على اسم وتاريخ الواقعة وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الدولة التي تمت منها محاولة الاختراق واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، ورقم المنفذ والبوابة الخاصة، وبيانات الشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام هواتفها والفاكسات الخاصة بها وآخر تحديث قامت به في أجهزة الخدمة الخاصة بها، وغيرها من المعلومات لمزيد من التفاصيل حول هذا البرنامج أنظر: سليمان بن مهجع العنزي: المرجع السابق ص ١٠٠.

[٤٩]

Bace, Rebecca (2000) Interusion Detection, Indianapolis , Indiaina : Macmillah Techniccat Publishing.

[٥٠] محمد بن نصير محمد: المرجع السابق ص ٨٤.

[٥١]

Spitzner , Lance (2003) . Honeypots: Tracking Hackers Boston: Addison- wesley.

[٥٢]

Champlain, Jack (2003) . Auditing Information Systems. Hoboken, New jersey, John wiley of sons.

[٥٣] محمد بن نصير محمد السرحاني: المرجع السابق ص ٨٤.

[٥٤] تستخدم لعمل نسخة مطابقة تماما للأقراص الصلبة الموجودة في الحواسيب محل التحقيق وعلى مستوى البت Bitstream Backup، بغرض عمل الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغير في البيانات الموجودة.

ومن أشهر هذه البرمجيات برنامج Safeback وبرنامج Encase وتعمل في بيئة ونـدوز، وكذلك أداةDD لبيئة يونيكس.

[٥٥] سليمان بن مهجع العنزي: المرجع السابق ص ١٠١.

[٥٦] ومن أشهرها على سبيل المثال، برنامج Get Free لبيئة النوافذ، وبرنامج Extractor لبيئة يونيكس: أنظر سليمان بن مهجع العنزي: المرجع السابق ص ١٠١-١٠٢ & محمد بن نصير محمد السرحاني: المرجع السابق ص٨٥.

[٥٧] ومن أشهر هذه البرمجيات برنامج Gander وبرنامج win Hex..أنظر محمد بن نصير محمد السرحاني: المرجع السابق ص ٨٥.

[٥٨] من الأمثلة عليها برنامجEt search وبرنامجString Search. أنظر محمد بن نصير محمد السرحاني: المرجع السابق ص ٨٥.

[٥٩] حول هذا الموضوع أنظر:

- سليمان بن مهجع العنزي: المرجع السابق ص ١٠٤ -١٠٥

- عبد القادر الفنتوخ: المسرح الإلكتروني بحث منشور على شبكة الإنترنت http://writers.alriyadh.com.sa/kpage.asp?art=7753 الرياض ١٤٢٣ هـ ص ١٨

- محمد أمين البشري: التحقيق في جرائم الحاسب الآلي والإنترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد ٣٠، جامعة نايف العربية للعلوم الأمنية، الرياض ١٤٢١ هـ ص ١٨٦.

[٦١] يراعي هنا ضرورة أن يتأكد قائد فريق التحقيق من حرص جميع أعضاء فريق التحقيق على الأمور التالية أثناء تعاملهم مع الأدلة الرقمية على وجه الخصوص:

- عدم القيام بأي عمل من شأنه إحداث تعديل أو تغير أي دليل.

- عدم تنفيذ أية برامج على الحواسيب الموجودة في موقع الجريمة خصوصا البرامج ذات الصلة بأنظمة التشغيل.

- ضرورة عمل نسخة مطابقة للأقراص الصلبة، ومن ثم عمل الفحوصات الجنائية على هذه النسخة فقط، سواء تم ذلك داخل مسرح الجريمة أو خارجها. وهنا يجب التأكيد على أنه لا تكفي نسخة احتياطية من البيانات المراد فحصها، وإنما يجب عمل نسخة مطابقة تماما لكامل القرص الصلب، وعلى مستوى البت bit وهي أصغر وحدة لقياس كم البيانات الرقمية، وهذه الطريقة تعرف باسم "Bit Stream Back - UP". بل إنه من الأفضل عمل نسخة احتياطية ثانية من النسخة الاحتياطية الأولي وعلى مستوى البت أيضا ومن ثم إجراء الفحوصات الجنائية على النسخة الثانية، بحيث تظل النسخة الأولى دون أن تطالها أية تعديلات.

أنظر. محمد نصير بن محمد السرحاني: المرجع السابق ص ٧٩.

[٦٢] عبد الرحمن بحر: معوقات التحقيق في جرائم الإنترنت "دراسة مسحيه على ضباط الشرطة بدولة البحرين: رسالة ماجستير: جامعة نايف العربية للعلوم الأمنية، الرياض ١٩٩٩ م ص ٥١؛ سليمان بن مهجع العنزي: المرجع السابق ص ١١٣.

[٦٣] من الأمثلة على ذلك قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة. لمزيد من التفاصيل أنظر الدكتور هشام محمد فريد رستم: الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"، المرجع السابق ص ٤٣٠. & وفي واقعة مماثلة حدثت وقائعها بدولة الإمارات العربية المتحدة تتمثل في قيام مشغل حاسب آلي بتهديد المؤسسة التي يعمل بها لتنفيذ مجموعة من المطالب وذلك بعد أن قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة. وإزاء رفض المؤسسة الاستجابة لمطالبه أقدم على الانتحار مما سبب صعوبة بالغة في استرجاع البيانات التي كان قد حذفها. أنظر. خالد الستاني – أمن المعلومات وتحليل المخاطر، ورقة عمل مقدمة إلى ندوة فيروسات الحاسب التي عقدها معهد التنمية الإدارية بالمجمع الثقافي بإمارة أبو ظبي بدولة الإمارات العربية المتحدة في ١٩٩٦/٩/٢٣ م.

[٦٤] عبد الرحمن بحر: المرجع السابق ص ٤٦.

[٦٥] أنظر:

– سليمان بن مهجع العنزي: المرجع السابق ص ١١٤

John Eaton and Jeremy Smithers , This is it a Managers Guide to Information Technology. London , Philip Allan , 1982 , p263.

[٦٦] باسم الحمادي: إثبات جرائم الإنترنت صعب، بحث منشور على شبكة الإنترنت بتاريخ ٧ محرم ١٤٢٣ هـ على موقع: www.alrivadh.com.sa، الرياض ص ١٤.

[٦٧] باسم الحمادي: المرجع السابق ص ١٤.

[٦٨] طارق عبد الله الشدي: آلية البناء لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض ١٤٢٣ هـ ص ٢١٠.

[٦٩] باسم الحمادي: المرجع السابق ص ٢٣.

[٧٠] الدكتور: زكي أمين حسونة: جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، مرجع سابق ص ٤٧٦.

[٧١] سليمان بن مهجع العنزي: المرجع السابق ص ١١٩.

[٧٢] الدكتور: محمد الأمين البشرى: التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة ١-٢٠٠٠/٥/٣ م الطبعة الثالثة ٢٠٠٤ م ص ١٠٧٣.

[٧٣]

United Nation . United Nation Manual on the Prevention and control of Computer – Related crime: Vienna 1999.