جامعة السودان للعلوم والتكنولوجيا

كلية الدراسات العليا

تطوير إطار شامل للتحقيق في الجرائم الإلكترونية

Developing of a Comprehensive Framework for Investigating Electronic Crimes

رسالة مقدمة لنيل درجة الدكتوراه في تقنية المعلومات

إعداد:

أزهري عبد الرحمن محمد خليل

إشراف:

أ.د. عز الدين محمد عثمان

اكتوبر 2020م

بسم الله الرحمن الرحيم

"قال هي راودتني عن نفسي وشهد شاهد من اهلها ان كان قميصه قد من قبل فصدقت وهو من الكاذبين(26) وان كان قميصه قد من دبر فكذبت وهو من الصادقين(27)"

(سورة يوسف)

اهـــداء

اهدي هذا العمل لروح زوجتي المرحومة غادة الشيخ حامد التي توفاها الله قبل اتمام هذا العمل الذي كنت اتمنى احتفائنا به معا وهي بجواري بصحبة الابناء الاعزاء شهد وعزالدين والحبيب علاء الدين ولهم اهدي هذا العمل مصحوبا بشكري وتقديري وحبي الكبير اذ بعد رحيل امهم الغالية لم ينقطعوا عن تشجيعي و تهيئة الظروف لي للاستمرار حتى اكمال هذا العمل مطوعين الظروف الصعبة التي مرت بالاسرة الصغيرة ورغم احزانهم وانشغالهم بواجباتهم الدراسية كانوا عونا وبلسما لروحي التي تاذت من فقدي امهم فاعادوا الى نفسي اليقين والصبر وساعدو في تحملنا ازمة الفقد العظيم بنفوس موقنة يملاها الرضى فجزاهم الله عني كل خير.

شكر وتقدير

الشكر للاستاذ الدكتور/ عزالدين محمد عثمان الذي لولا عونه لما رأى هذا العمل النوراذ لم يبخل علي بالتوجيه والنصح والتشجيع في تواضع العلماء الذي يميز شخصه دون تصنع عند مناقشة وتقييم الافكار والاراء وتقديم النصح والتوجيه،،،

كما اخص بالشكر الباشمهندس محمد زين العابدين عبد القادر والباشمهندس طلحة حسن طلحة والاستاذ محمد احمد علي شرف الذين وقفوا الى جانبي عونا وتشجيعا واسنادا بلا حساب سيظل دينا في عنقي ما حييت.

الشكر موصول ايضا لكل من مد يد العون لانجاز هذا البحث من محققي الشرطة وفريق الادلة الجنائية الذين ما بخلوا علي بالراي والاجابة على اسئلة المقابلات ما سهل الوصول الى نتائج هذا البحث.

المستخلص

تقدم هذه الدراسة اطارا شاملا لاستخدامه والاستعانة به في تطبيقات الكمبيوتر والوسائل الفنية لاحراز البينة وتحليلها وتقديمها امام القضاء. يقدم البحث استعراض ويوفر معلومة اساسية عن اخلاقيات السايبر وطرق مكافحة الجريمة الالكترونية من الناحية الفنية المتعلقة بتكنلوجيا السايبر و القانون، والادوات المستخدمة في جمع البينات. يتعرض البحث للدور المحتمل للفكر الانساني المتعلق بالقانون والخصوصية والاخلاق والمعايير الاجتماعية والتعاون الدولي ضد الجريمة السبرانية. استخدمت عدة مناهج للبحث للوصول للاهداف. ركز البحث على التحقيق والمكافحة والجهود العالمية والاقليمية وقدم اطارا للتحقيق ، اتصف بانه شامل و يوفر أساسا للمصطلحات الشائعة لدعم مناقشة وتبادل الخبرات. و يتمتع بالمزايا التي تم الحصول عليها من النماذج السائدة، ولكنه يوسع نطاقها ويوفر مزايا إضافية لاتصافه بالمرجعية. الإطار المرجعي يعد ضروريا لتطوير التحقيق في الجرائم الإلكترونية لأنه يسمح بالتوحيد القياسي وتناسق المصطلحات وتحديد المجالات التي تحتاج إلى البحث والتطوير .يمكن للنموزج المقترح أن يوفر أداة تدريبية وأساسا لشرح عمل المحققين لغير المتخصصين ، سواء كانوامن القائمين على تحقيق العدالة أو الإدارة. الميزة الأهم لهذا النموذج بالمقارنة مع النمازج الاخرى هي التحديد الواضح لتدفقات المعلومات في عملية التحقيق فهو يتيح تحديد تدفقات المعلومات في عملية التحقيق بجانب تحديد الأدوات وتطويرها ، والتعامل مع إدارة الحالات، وفحص الأدلة، ونشر المعلومات بتحكم .يساعد النموذج في الحصول على خبرة المحققين بهدف تطوير أدوات متقدمة. الاطار قادر على توفير دعم للمحققين، فهو يوفر اساسا للمصطلحات الشائعة لدعم وتبادل الخبرات كما ان الاطار يساعد في تطبيق المنهجيات على التقنيات الجديدة عند ظهورها بشكل فوري وسريع. يمكن استخدام النموذج بطريقة استباقية لتحديد فرص نشر التكنولوجيا لدعم عمل المحققين، وتوفير إطار لالتقاط وتحليل متطلبات أدوات التحقيق ، خاصة بالنسبة للأدوات التحليلية خلافا للاطر الاخري التي ركزت على جمع الادلة فقط. اضاف البحث نقاط قوة الاطار وعيوبه التي تم الاستعانة فيها باراء خبراء من محققي جرائم الانترنت. تعرض البحث لنشأة الانترنت ببعض التفصيل بحسبان التحقيق في جرائم

الانترنت هو موضوع البحث الى جانب تأثير الانترنت على قضايا الخصوصية واخلاقيات السايبر وتأثير تطور التكنلوجيا المستخدمة في الانترنت على تطور الجريمة الالكترونية.

Abstract

This study provides a comprehensive framework for use in computer applications and technical means to obtain evidence analyze it and present it before the court. The paper provides a review and basic information on cyber ethics and methods of combating cyber crime from a technical point of view related to cyber technology and law, and the tools used to collect evidence. The paper examines the potential role of human thought related to law, privacy, ethics, social norms and international cooperation against cybercrime. Several research methods were used to reach the goals. The research focused on investigation, control, global and regional efforts then provided a framework for investigation, which was characterized as comprehensive and provides a basis for common terminology to support discussion and exchange of experiences. It has the advantages obtained from the prevailing models, but broadens its scope and provides additional benefits not to be described as a reference. The frame of reference is essential for developing cybercrime investigation because it allows for standardization and consistency of terminology and specifies areas that need research and development. The proposed template can provide a training tool and basis for explaining the work of investigators to non-specialists, whether they are justice or administration administrators. The most important feature of this model compared to other models is the clear identification of information flows in the investigation process, as it allows identifying information flows in the investigation process as well as identifying and developing tools, dealing with case management, examining evidence, and disseminating information with control. The model helps in gaining the experience of investigators in order to develop advanced tools. The framework is able to provide support to investigators, it provides a basis for common terminology to support and exchange experiences. The framework also helps in applying methodologies to new technologies when they arise in an immediate and rapid way. The model can be used in a proactive way to identify technology deployment opportunities to support the work of investigators, and to provide a framework for capturing and analyzing requirements for investigative tools, especially for analytical tools, unlike other frameworks that focus on gathering evidence only. The research added the framework's strengths and flaws, which drew on expert opinions from cybercrime investigators. The research discusses the emergence of the Internet in some detail, according to the investigation of internet crimes as the topic of research, as well as the impact of the Internet on issues of privacy and cyber ethics and the impact of the development of technology used in the Internet on the development of electronic crime.

المحتويات

قائمة الجداول

قائمة الاشكال

جدول الاختصارات و المعاني

رقم	المختصر	المعنى
1	ICANN	Internet Corporation for Assigned Name and Number
2	DNS	Domain Name System
3	gTDL	generic Top-Level Domain
4	IANA	Internet Assigned Numbers Authority
5	ARPA	Address and routing parameter area
6	ccTDL	Country code Top-Level Domain
7	Backenc	لغات خلفية
8	Fronten	لغات العرض
9	UDRP	Uniform Domain Name Dispute Resolutior Policy
10	ASO	Address Supporting Organization
11	ALAC	At-Large Advisory Committee
12	MFT	Master File Table
13	ISPs	Internet Service Provider
14	Interpo	البوليس الدولي
15	ITU	الاتحاد العالمي للاتصالات
16	APEC	منظمة التعاون الاقتصادي لاسيا و الباسفيك
17	UN	الامم المتحدة
18	COE	المجلس الاوروبي
19	OAS	منظمة الدول الامريكية
20	MNE	جهود المنظمات متعددة الجنسيات
21	G8	مجموعة الثمانية
22	OECD	منظمة التعاون الاقتصادي
23	ASCII	مستند نصي
24	JPEG	تخزين صورة
25	P2P	نظير إلى نظير
26	ZIP	أرشيف مضغوط
27	FBI	مكتب التحقيقات الفيدرالي
28	DNS	Magnetic Force Microscopy
29	SHA-1	Secure Hash Algorithm-1
30	MD5	Massage Digest5
31	DLL	Dynamic-link Library
32	exe	Executable

I. البـــــــــاب الاول

المـــــقـدمـــــــة

(البـــاب التمهـــيدي)

1.1 المـــــقـــــدمـــــــــة

الجريمة من المنظور القانوني الوضعي هي اتيان فعل مجرم معاقب على فعله، او ترك فعل واجب معاقب على تركه، وبهذا المفهوم فهي كل ما نص القانون على تجريمه او قرر عقوبة على اتيانه" حجاج (2006). وفي اطار هذا التعريف لم يخالف اي ممن تعرض لدراسة الجريمة وتعريفها، اذ يقيد تعريف الجريمة بشكل عام المبدأ الدستوري الذي يؤكد على ان لا جريمة ولا عقوبة الا بنص وهو ما اخذت به معظم الدساتير ولم يخالف هذا المبدأ دستور جمهورية السودان 2005. (Constitution 2005)

حقق تطور التقنيات فوائد كبيرة للانسانية واسهم في رقيها وتقدمها، الا انه ايضا، مهد السبيل لظهور انماط جديدة ومهددات خطيرة لامن وسلامة البشريه، فقد برزت اشكال جديدة من انواع الجريمة، خصوصا بعد ظهور الاستخدام المكثف لشبكة الانترنت، اذ مكنت هذه التقنيات المتقدمة المجرمين من استخدام امكانات واساليب متطورة لارتكاب الكثير من الجرائم دون ان يتركوا اثرا واضحا لهذه الجرائم.

المجرم يمكنه استخدام المخترعات العلمية الالكترونية وما فيها من تقنيات متطورة لارتكاب الكثير من الجرائم مستفيدا من الامكانيات الهائلة لهذه التقنيات وتوفرها بارخص الاثمان، كما تمكنه المخترعات العلمية الالكترونية وما فيها من تقنيات متطورة من الوصول لاعداد بشرية كبيرة في نفس الوقت، لان شبكة الانترنت كما هو معلوم لا تحدها حدود ولا زمان. هذه الدراسة يتم فيها تقديم اطار شامل

مقترح للتحقيق في الجرائم الإليكترونية يمتاذ بان له القدرة على:

أ. توحيد المصطلحات.

ب. في ذات الوقت يمكن ان يسهم في دعم تطوير تقنيات وادوات جديدة للمحققين.

ج. ويشمل هذا الجهد تقديم تغطية وشرح لاكثر أدوات التحقيق في الجريمة الالكترونية استخداما. تقدم الدراسة استعراضا للاطر التي يمكن اعتمادها باعتبارها الاكثر استخداما وفائدة للتحقيق وجمع الادلة الرقمية.

د. كما تتم خلال الدراسة مقارنة النموذج المقترح الجديد ببعض النماذج المهمة الحالية وتطبيقاتها مع عرض لاوجه القصور والتفوق للنموذج المقترح.

هـ. شمل الجهد المبذول في الدراسة السعي لتحقيق التقارب بين مستلزمات تطبيق القواعد القانونية، واستخدامات تكنلوجيا السايبر (cyber technology).

و. استيعاب طبيعة الجهدين وكيفية التناغم بينهما عبر التعريف بالجريمة الالكترونية وتطورها واعتماد المعايير الدولية مع التركيزعلى الاستجابة للجريمة الالكترونية والدور الفني لاثباتها. والتحدي القانوني عند مواجهتها، في اشارة صريحة لدور الاخلاق بشكل عام واخلاق السايبر بشكل خاص.

ز. تضمنت الدراسة استعراض الجهود الدولية والتعاون الدول والاقليمي الذي استهدف الوقوف في وجه الجريمة الالكترونية ومقاومة خطرها.

ح. يتضمن جمع الادلة الجنائية الخاصة بالكمبيوتر تحديد (identification) الأدلة الرقمية المخزنة في شكل معلومات مشفرة واقتنائها (acquisition) وتحليله وعرض (presentation). (Shinder 2010) .

ط. اكدت هذه الدراسة بتقديمها اطارا شاملا للتحقيق وتبعا لتأكيدات نتائج الدراسة ان الاطار الشامل هو الاكثر قدرة على استيفاء احتياجات التحقيق في الجريمة الالكترونية وجمع الادلة الرقمية.

ي. تؤكد الدراسة ان النموذج الشامل للتحقيقات المقترح للتحقيق في الجرائم الإليكترونية يستمد اهميته من قدرته على توحيد المصطلحات وتحديد المتطلبات ودعم تطوير تقنيات وأدوات جديدة للمحققين.

ك. نموذج التحقيقات الذي يقدم في هذه الدراسة ، يجمع بين النماذج الحالية ، ويعممها ، ويمددها عن طريق معالجة بعض الأنشطة غير المدرجة فيها صراحة ، وعلى عكس النماذج السابقة ، يمثل هذا النموذج بشكل صريح تدفقات المعلومات في التحقيق ويلتقط النطاق الكامل للتحقيق، وليس فقط معالجة الأدلة.

ل. يتم عرض نتائج تقييم النموذج من خلال الممارسة الافتراضية لمحققي الجرائم الالكترونية وسد النقص الذي تكمله الحلول التي هي من صميم مقاصد الاطار المقترح.

م. تحتاج اجراءات جمع الادلة الجنائية الرقمية (Digital Forensics) لمراعاة دراسات الادلة

الجنائية المتعلقة بالكمبيوتر والذاكرة المحمولة، والحصول على الادلة الجنائية الخاصة بالشبكات واستعادة البيانات. (Fatah 1999)

ن. يمكن لأدوات جمع الادلة الرقمية المختلفة أن تجعل عملية البحث أسهل واكثر دقة، اذ يمكن أن تكون الأدوات عبارة عن برنامج أو جهاز أو مجموعة من كليهما، بحيث انه يمكن استخدامها في التحقيق لجمع المعلومات وتحليلها، وإعداد التقارير وإعطاء التوجيهات للتحقيق، في الجوانب المعينة واجبة الاستخدام لاكمال المهمة بنجاح .

س. يمكن أن تكون الأدوات المستخدمة في التحقيق مفتوحة المصدر أو مملوكة للقائمين على التحقيق. (Johansen 2020)

ع. تأتي ادوات التحقيق على اشكال قد تختلف عن بعضها فبينما تأتي بعض الأدوات مع جهاز مصحوب بحزمة برامج نجد أن بعضها قد يكون مجرد تطبيق.

ف. قد تتطلب بعض اجراءات جمع الادلة الرقمية اتصالا نشطا بالإنترنت بينما يمكن في حالات آخرى العمل في وضع عدم الاتصال (GROUP 2020)

يمكن في كثير من الاحيان تحديد نوع الجريمة التي وقعت والأداة المناسبة لمباشرة التحقيق فيها ويمكن لهذه الأدوات المستخدمة بشكل فردي أو مع أدوات أخرى أن تساعد في تحليل منهجي وفعال للأدلة الامر الذي يبشر بالوصول الى ما يؤدي إلى الاستنتاجات المناسبة. (Kanellis 2006)

2.1 انبثاق فكرة الدراسة:

انبثقت فكرة هذه الدراسة من ان المسائل المتعلقة بمثل واخلاقيات السايبر (Cyber Ethics) ذادت اهميتها بسبب تعلقها بجوانب عديدة و معقدة، حيث يشمل هذا التعلق علوم الحاسوب ، وتقنية المعلومات، و كافة تكنلوجيا السايبر (Cyber Technology)، والكثير من العلوم الانسانية (Humanitarian Sciences)، و اهمها العلوم القانونية ، فبعد ظهور وتطور الانترنت ، برزت مسائل عديدة اصبحت تشكل اسئلة لا نهائية تتزامن وتزداد تعقيدا مع كل تطور تكنلوجي(Casey 2009)، مع ملاحظة ان هذا التطور مازال يمضي بلا توقف، وعليه حاولنا الاستفاده من اسهامات الفكر الانساني ، وفتح باب نحسبه جديدا، لذا فان هذه الدراسة في جانب منها، تهتم بما يمكن ان يكون عليه اسهام علوم الكبيوتر و التكنلوجيا كأدوات و كمؤثر على الفكر القانوني، وذلك لايجاد ما هو ممكن من الحلول الغائبة سيما و ان الجهد ما زال في بداياته (Maravic &Bosnjak 2014)) لذا اهتمت الدراسة باطر التحقيق (Investigation Framework) وادواته (Investigation Tools) وفي الجانب الاخر فالدراسة تسعى للفت النظر الى ما يمكن ان يقاس عليه بالنسبة لقضايا المستقبل، مثل تدريب القانونيين وعلى الاخص تجهيز القضاة فنيا بما يكفي من المعرفة المتعلقة بتكنلوجيا السايبر وذلك في محاولة لتوحيد النظر الى ماسيكون عليه الحال في مستقبل هذه التكنلوجيا، جنبا الى جنب التطور المضطرد لتكنلوجيا الاثبات (Evidence Technology)، والتحقيق في الجريمة الإليكترونية. (Kanellis 2006) وذلك عبر دراسة تفصيلية وتقصي عميق لسبر غور مستقبل العلاقة الحالية والمنتظرة فيما بين تطبيقات

القانون (Law Enforcement) واختراق التكنلوجيا لعالم ارتكاب الجريمة وتكنلوجيا التحقيق واثبات الجريمة ايا كان تعلقها.

3.1 أهمية الدراسة

يكتسب هذا البحث أهميته من ان مسألة توسيع فكرة سيادة القانون (Rule of Law) في فضاء السايبر قد صارت ذات اهمية حتمتها زيادة الحاجة للثقة المنشود توفرها لدى القطاعات المتعاملة مع تكنلوجيا السايبر (Cybertechnology) ، سواءا تمثل ذلك في قطاع الاعمال (Business Sector) حكوميا أو خاصا اوقطاع الافراد، مع الوضع في الاعتبار أن هذا التوسع والتمدد مازال في بداياته.

الجريمة الإليكترونية حتى الان تقع عمليا تبعة مقاومتها على المتضررين منها، وبالتالي فانه تقع على المنظمات والمؤسسات أعباء الدفاع عن النظم الخاصة بها، وأيضا حماية معلوماتها من التعديات (Trespasses) والهجوم (Attacks) الذي قد يقع عليها من غير محسوبيها أو من محسوبيها الذين يتبعون لها، أي من الخارج أو من الداخل Marshell) (2008، اذ أن الردع القانوني ما زال بلا فاعلية تذكر او بلا فاعلية يمكن الاعتداد بها، وبالتالي فان جل المنظمات والقطاعات المعنية تعكف باجتهاد واضح علي تفعيل منظوماتها وخططها الامنية الإليكترونية بقدراتها الذاتية. (Cyber Security Plans)

4.1 تفعيل خطط الدفاع

تفعيل الخطط الامنية وتفعيل مسألة التكنلوجيا المتعلقة بالامن السبراني يتطلب ابتداءا توفير موارد تثقيف العاملين لادراك اهداف الخطوات الامنية (Security Practices) ومن ثم وضع الخطط الشاملة للتعامل مع درجات الاهمية المتفاوتة للمعلومات ، والبيانات الحساسة (Sensitive Data) ، والسجلات (Records) ، والمعاملات (Transactions) ، واستخدام تكنلوجيا امنية فعالة (Marshell (2008، كبرامج مكافحة الفيروسات (Anti-Virus Software)، والجدران النارية (Firewalls) ، وأدوات كشف التسلل (Detection Tools) ، وخدمات التوثيق (Authentication Services)، والتشفير (Encryption)، بالنسبة لكافة مناشط المنظمة او المؤسسة، وما تعلق منها بالصناعة (Manufacturing)، والتشغيل (Operating)، والبرمجة (Programming) . (Sammons 2012)

على وجه العموم نلاحظ أن اجهزة الدفاع و توفير الامن ، دائما ما تعتمد على وسائل مكلفة و معقدة لانتاجها ، واستمرار تشغيلها (Complex and Expensive)، للدرجة التي نجد أنه وفي كثير من الاحايين، ان مستخدميها و تجنبا لمتاعب التشغيل وعلو نفقاته، يعمدون الى التنازل عن بعض أسباب الامان، بعدم تفعيل اجهزة الدفاع و الامن بوجه كاف، أو فعال، فضلا عن تعطيل اليات الامن ، الامر الذى ادي لاهتمام اكبر بمسألة الحماية القانونية، وما يتبعها من فنيات، خصوصا في مجال جمع الادلة الشرعية الرقمية ومراحل التحقيق بوجه عام، لذا تحتم النظر لهذه الفنيات (Technicalities)، من زاوية اوسع،

تشمل الرؤية التقنية وعلى وجه الخصوص كل ما يدخل او يتعلق بمحاور تكنلوجيا السايبر (Cyber Technology)، و جمع الأدلة الشرعية الرقمية (Digital Forensic)، وهو حقل جديد وسريع النمو، ولاينطوي فقط على العناية بجمع وفحص الأدلة الإلكترونية، او تقييم الأضرار التي لحقت بالكمبيوتر، نتيجة للهجمات الإلكترونية فقط ، ولكن أيضا ينطوي العمل به على سعي لاستعادة المعلومات المفقودة. (Casey 2009)

مع تزايد أهمية أمن الكمبيوتر اليوم، وخطورة الجريمة الالكترونية، اصبح من الضروري لمحترفي الكمبيوتر التمتع بالفهم القانوني، و فهم التكنولوجيا التي تستخدم في جمع الادلة الشرعية الرقمية (Digital Evidence)، وكل ما هو دائر حول المعلومات الأساسية المتعلقة بالتقنيات المستخدمة في هذا الاطار. ويشمل ذلك استرداد البيانات، والاستجابة الأساسية لاي متسلل (System Intruder) على النظام، وكل ما يتعلق بتكنولوجيا البرمجيات الرئيسية (Technology of Key Logging Software)، و الأجهزة ، والجوانب القانونية ، والأخلاقية ، وكل ما تعلق بتكنلوجيا جمع الادلة الشرعية الرقمية (Digital Forensic) .

شهدت الحقبة الراهنة تطورا ملحوظا في استخدام البينة الرقمية (Digital Evidence) ويرجع ذلك التطور بشكل مباشر الى أسباب متعددة ومتنوعة.

ابرز اسباب تطور استخدام البينة الرقمية ان المحاكم بحكم الواقع، اصبحت تقبل تقديم البينة الرقمية للفصل في القضايا المعروضة امامها وقد حتم

هذا القبول توفر قوانين قادرة على معالجة قضايا السايبر الحالية (Current Issues)، والمتوقعة (Anticipated). كما حتم ايضا وابتداءا التعاون البناء بين اهل الفكر القانوني، ومحترفي الكمبيوتر، و تقانة المعلومات.

5.1 كفاية التحقيق: Investigation Sufficiency

. قبل تطوير إجراءات وتقنيات جمع الادلة الجنائية للكمبيوتر ، تم ترك العديد من حالات جرائم الكمبيوتر دون حل، ثم ان هناك العديد من الأسباب التي تجعل التحقيق كافي لتأسيس محاكمة ناجحة ، ولكن كان ان الغالب هو عدم الاستعداد للقيام بالتحقيق بصورة كافية تساهم في تحقيق محاكمة او محاسبة عادلة. (Lee 2001)

المنظمة التي تحقق في الافعال المشبوهة غالبا ما يفتقر استشراف التحقيق المقصود منها وفيها إلى الأدوات والمهارات اللازمة لجمع الأدلة بنجاح. (GROUP 2020)

قد يفتقر الأفراد الذين يحاولون التحقيق في النشاط المشبوه إلى الموارد المالية أو الموارد الفنية أو الأدوات اللازمة لإجراء مثل هذا التحقيق بشكل كاف والتأكد من أن الأدلة لا جدال فيها في جميع الظروف، وان التحقيق قد تم وفق الاطار المناسب لمباشرته. (J Khakurel 2016)

لما كان الردع القانوني ما زال بلا فاعلية تذكر او بلا فاعلية يمكن الاعتداد بها، فان جل المنظمات والقطاعات المعنية تعكف باجتهاد واضح علي تفعيل منظوماتها وخططها الامنية الإليكترونية بقدراتها

الذاتية دفاعا عن النظم الخاصة بها وأيضا لحماية معلوماتها من التعديات (Cyber Security Plans). (Sammons 2012)

6.1 مشكلة الدراسة

اثر التطور التكنلوجي بصورة مرعبة على أساليب ارتكاب الجرائم بشكل عام وبشكل اكثر خصوصية على اساليب ارتكاب الجرائم الالكترونية، (Casey 2009) ومن ثم فقد أصبح مطلوبا من سلطات إنفاذ وتطبيق القانون أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات بشقيه الجنائي أو المدني لذلك تكمن مشكلة البحث في تقديم دليل رقمي مقبول لدي المحاكم وفق اطار محكم، يكون له حجية في النظم الإثباتية المختلفة، من خلال الدراسة المقارنة لاستخدامات الدليل الرقمي حول العالم، او في مختلف الدول بمختلف انظمتها التشريعية، وامكانية التعاون الفني والتشريعي بينها، ويشمل ذلك مدي التعامل مع مسألة اقليمية القوانين. (Maravic &Bosnjak 2014))

تتلخص مشكلة هذه الدراسة في النقاط التالية:

في الوقت الحالي ، هناك نقص في النماذج العامة الموجهة بالتحديد إلى تحقيقات جرائم الإنترنت . (Fortinet 2009)

تركز النماذج المتاحة على جزء من عملية التحقيق المتمثل في التعامل مع جمع الأدلة وتحليلها وتقديمها بينما يجدر أن يشتمل النموذج العام بالكامل على جوانب أخرى إذا أريد له أن يكون شاملا. (Hawthorne 2014)

اكد البحث ان مثل هذا النموذج مفيد ليس فقط لتطبيق القانون، بل يمكن أن يفيد مديري تكنولوجيا المعلومات وممارسي الأمن والمدققين.

ممارسي الأمن والمدققين أصبحوا في وضع يسمح لهم بإجراء التحقيقات بسبب تزايد حالات الجريمة الالكترونية ، وأيضا بسبب انتهاكات سياسات المؤسسة وإرشاداتها (مثل إساءة استخدام اتصالات الإنترنت في مكان العمل (GROUP 2020).

الدراسة تقدم هنا نموذجا موسعا للتحقيقات في الجرائم الالكترونية التي تحدد أنشطة عملية التحقيق والتدفقات الرئيسية للمعلومات في تلك العملية ، وهو جانب مهم في تطوير الأدوات الداعمة.

يتم في هذا البحث وصف لاهم النماذج المتوفرة حاليا واكثرها استخداما في التحقيق ومقارنتها بالنموذج الجديد المقترح، ليتبين أن النموذج المقترح هنا أوسع من النماذج التي تتعامل فقط مع معالجة الأدلة الرقمية .

هذا النموذج يحاول ، الاستيلاء على أكبر قدر ممكن من عملية التحقيق في الجرائم الإلكترونية بأكملها بما في ذلك أنشطة معالجة الأدلة الرقمية.

i الجهود البحثية المبذولة للحصول على البينة الرقميةومعالجتها (processing)وتقديمها وقبولها (acceptance) ما زالت مبعثرة تحتاج جهدا كبيرا لجمع اجزائها. (Adams 2013)

ii القواعد القانونية التي تحكم الجريمة الالكترونية حتى الان لا تقوى على التعميم بسبب انها متفرقة ومختلفة. (Shinder 2010).

iii مازالت الكثير من الادلة التي تقدم ضد مرتكبي الجرائم الالكترونية تعاني عدم القبول لدى المحاكم لاسباب فنية واجرائية. (Carrier and 2003).

iv تكنلوجيا التحقيق تواجهها مشاكل كثيرة تحتاج توحيد فهم شامل و ممنهج ومتفق عليه كاطار للتحقيق يغطي كل معينات وجزئيات جمع الادلة الرقمية (digital evidence) في اطار ما يتطلبه الحصول على البينات وفق القانون ومعالجتها وتقديمها بالكيفية المقبولة قانونا. (Investigation Framework)

v ومن هنا جاء دافع هذه الدراسة لتقديم مقترح اطار للتحقيق في الجريمة الالكترونية في المجال الاكثر شيوعا من اطرها وهو اطار للتحقيق في جرائم الانترنت.

7.1 أهمية المشكلة

تبدو أهمية مشكلة الدراسة في أنها محاولة يمكن ان تضاف الى جهود البحث العلمي في مجال تحقيقات جرائم الإنترنت ، لانها تقصد المقارة بين تطبيق القواعد القانونية، واستخدامات تكنلوجيا السايبر.

وهي ايضا محاولة لتقديم أسلوب علمي، وقانوني، يمكن الاستعانة به فيما يخص الحصول على الاطار (framework) المناسب للحصول على البينات والتحقيق وإثبات الجريمة التي تتم عبر أجهزة الكمبيوتر، بما يساعد على بلورة فهم الدليل الرقمي المقدم لأجهزة إنفاذ وتطبيق القانون، بما يدعم حجية المخرجات الكمبيوترية في المواد الجنائية والمدنية.

يعد النموذج الجيد لتحقيقات جرائم الإنترنت أمرا مهما ، لأنه يوفر إطارا مرجعيا مجردا، بغض النظر عن

أي تكنولوجيا أو بيئة تنظيمية معينة ، لمناقشة التقنيات والتكنولوجيا لدعم عمل المحققين.(Mohay 2003)

8.1 اطـــــار التحـــقـــيـــق الشـــامـــل:

الاطار المقترح في هذه الدراسة والذي اخذ اسم (اطار التحقيق الشامل) قصد منه أن يوفر أساسا للمصطلحات الشائعة التي تدعم مناقشة وتبادل الخبرات.

يمكن استخدام الاطـــــار للمساعدة في تطوير وتطبيق المنهجيات على التقنيات الجديدة فور ظهورها لتصبح موضع تحقيقات.

علاوة على كل ذلك ، يمكن استخدام النموذج بطريقة استباقية لتحديد فرص تطوير ونشر التكنولوجيا لدعم عمل المحققين ، وتوفير إطار لالتقاط وتحليل متطلبات أدوات التحقيق ، خاصة بالنسبة للأدوات التحليلية الآلية المتقدمة.

9.1 أسئلة الدراسة والفرضيات

فرضيات الدراسة كانت هي العوامل المفتاحية التي اتخذتها الدراسة موجها انبنت عليه مراحلها التي تأرجحت بين القانون والتكنلوجيا والعوامل الاجتماعية والاجتهادات الفردية والتعاون الدولي والممارسات البوليسية المتعلقة بالتحقيق.

الحصول على الدليل الالكتروني يتطلب استخدام اطار التحقيق الذي يستوفي المتطلبات التكنلوجية والقانونية ،وهذا يحتم ان تعمد العملية البحثية الى تجزءة عناصر البحث وترتيب الفرضيات التي بموجبها يمكن تقرير مواكبة المخرجات لطبيعة الحلول التي يمكن الوصول اليها بتوافر عوامل

مفتاحية Key Factors اقتضتها الدراسة وعليه فقد اعتمد البحث ما يلى من فرضيات كموجهات لسير البحث:

الفرضية الاولى: الجريمة الإليكترونية جريمة حديثة نسبيا وتتميز بانها عابرة لحدود الدول مما ادي لبروز عوامل مؤثرة على عملية كشفها والتحقيق فيها .

تعرض الدراسة العوامل المفتاحية وتستعرضها في شكل دراسة مقارنة للجوانب القانونية اولا والتي تستصحب فيها الجهود الدولية والمحلية في مكافحة الجريمة الالكترونيه، اذ تستعرض الدراسة الجهود التكنلوجية وما تم استخدامه من ادوات.

الفرضية الثانية: ليس هناك اطار تحقيق واحد متفق عليه ولكن تعددت اطر التحقيق مما يفتح المجال واسعا لطرق هذا المجال بحثا عن الاطار الشامل.

الفرضية الثالثة: لا زالت هناك هوة بين الفكر القانوني والفكر التقني تحتاج ان يتم سدها للوصول الى تلاقح الفكرين والحصول على ما يخدم التحقيق المثمر في الجريمة الإليكترونية.

اهتمت الدراسة بالناحية التكنلوجية في محاولة للمقاربة بين التكنلوجيا وما عليه الفكر المتعلق باخلاق السايبر و بتكنلوجيا السايبر مربوطا بالفكر القانوني من خلال الجهود المبذولة اقليميا وعالميا للاجابة على السؤال المتعلق بكيفية المقاربة بين هذه الافكار على ارض الواقع.

الفرضية الرابعة: دراسة الخصوصية في المجال القانوني وما طرأ عليها من تغيرات بسبب تكنلوجيا المعلومات وتحتم استعراض اثر التكنلوجيا على

الخصوصية من حيث كمية المعلومات Information Quantity والسرعة في التداول وطريقة الحفظ ونوع التداول واستعراض الماضي و الحاضر والانواع ودور الاديان مقارنا بالاختراقات التكنلوجية وتوافر الوسائل المحسنة- نظم تعزيز الخصوصية (Privacy Enhancing) الى جانب ان كل الاعراف والنظم المختلفة، قد اسهمت في وضع حماية للخصوصية (Privacy)، الا ان الخصوصية في مجال السايبر (Cyberspace) اصبح امرها اكثر تعقيدا، لاسباب تتعلق بالتجدد المستمر لامكانية الاختراق وانواعه، اضافة لاسباب أخرى كثيرة، منها زيادة الاعتماد في اكثر الامور خصوصية على التكنلوجيا.

الفرضية الخامسة: ادي التطور التكنلوجي الى تنامي مهددات النظم و امن المعلومات وفقا لتنامي القدرات التكنلوجية

تعرض البحث في هذه المرحلة لمهددات النظم (وامن المعلومات، من جانبها التكنلوجي والاقتصادي فقد اضحت المسائل المتعلقة بامن النظم في ذاتها تجارة تدر الملايين، وتستوعب الاعداد الغفيرة من اهل التكنلوجيا والادارة و المفكرين والعلماء من شتى التخصصات، والمعارف.

صار هناك من يصنع المهددات (Threats Producer) ، وهناك من يتولي توفير اسلحة مكافحتها (Defensive Arms) وربما يكون الاسمين لمسمى واحد وقد كثر الحديث عن هذا الجانب. فان امن النظم وامن المعلومات يتقدم موازيا للتطور التكنلوجي، بل ويشكل دائرة خاصة للتنافس المعرفي، وهوتنافس يشبه كثيرا التكتيكات العسكرية كما ان الجريمة

الالكترونية فتحت بابا لا يتصور احد انغلاقه قريبا. (Zoltanszabodfw 2012)

الفرضية السادسة: الجدل حول طبيعة الجريمة الاكترونية وتعريفها مازال في مبتداه والاتفاق على العناصر المكونة لها وكذلك هو حال الحديث عن العقوبة وجدواها ومدى توافقها مع مبادئ الاصلاح والتقويم ومسائل اخري كثيرة (Casey 2009)، ستشمل الدراسة اجدرها بالتناول. والاهم في هذه المرحلة هو ما تعلق بعلوم القانون (Law) والحاسوب وبعض ما يخص تقنية المعلومات ووسائل الاثبات المتعلقة بالجريمة الالكترونية في القوانين الوضعية وطرق جمع البينات والتطور البرمجي والفني والجنائ ومتطلبات قبول البينة أمام المحاكم من الناحية الفنية والقانونية وقد اولى البحث في هذا الاطار المشكلات التي تعترض التحقيق اهتماما جاء ختاما للدراسة المقارنة التي شملت تجارب ، الدول الاكثر تقدما وتسير في طريق التعاون والاجتهاد المستمر مع عرض المجهودات المختلفة، لبعض الدول والمنظمات الدولية المهتمة بموضوع الجريمة الإليكترونية.

10.1 أهداف الدراسة :

هدف هذا البحث الى الاسهام في حل بعض قضايا السايبر الهامة والمؤثرة والتي مازالت تنتظر الدراسة والاسهام الفكري والعملي وتحديدا وسائل جمع الادلة الشرعية واطر مباشرة التحقيق الذي اختصه البحث بـــ:

1) تقديم اطار للتحقيق في جرائم الانترنت يمكن على خلاف الاطر المعروفه استخدامه حسب المقترح وتعميمه على كافة التحقيقات المتعلقة بالحصول

على الادلة الالكترونية والاستعانة به مع الكثير من تطبيقات الكمبيوتر والوسائل الفنية لاحراز البينة وتحليلها وتقديمها امام القضاء بصورة فاعلة تقضي على الفشل الذي قد يلازم مقاضاة مجرمي الجرائم الإليكترونية وما تعلق منها بالانترنت نظرا الى ان تقديم مرتكبي المخالفات المستخدم في اتيانها امكانيات التكنلوجيا بكل تعقيداتها وتقديمها للمحاكمة الجنائية وغيرها ما زالت تحفه صعوبات عديدة تصل في كثير من الاحايين الى صعوبة هي اشبه بالاستحالة (Shinder 2010).

2) من ناحية اخرى هدف البحث لاستعراض و توفير المعلومة الاساسية عن وضع الجريمة الإليكترونية وطرق مكافحتها من الناحية الفنية المتعلقة بتكنلوجيا السايبر و القانون، والادوات المستخدمة في جمع البينات الان وفي الماضي وكيفية استشراف المستقبل.
3) هدف البحث ايضا لاستعراض الدور المحتمل للفكر الانساني المتعلق بالقانون والاخلاق والمعايير الاجتماعية وغيرها من ضوابط السلوك والتعرض لموقف التشريعات العالمية والتعاون الدولي وموقفه من الجريمة الإليكترونية.
4) ايضاح الموقف العام لمسألة التحقيق والاثبات بصورة عامة تجاه الجريمة الإليكترونية من الجانب القانوني والتكنلوجي.

11.1 مناهج البحث Methodologies:

وصولا لتحقيق اهداف البحث انتهج البحث عدة طرق من حيث تعلقه بالاهداف، فكان اساسيا (Basic Research) في مراحله الاولي، وتطبيقيا (Applied Research) في

المراحل الاكثر تقدما، و تقويميا (Evaluation Research) بعد توفر المعلومة الكافية لاتخاذ القرار، بعد الوصول وبعد المناقشة الى النتائج، واجرائيا (Action Research)، بان هدف الى طرح الحلول العملية للمشكلات الفعلية، التي تعانيها مسألة التحقيق فيما يتعلق باحراز البينة ثم تحليلها، لاستخدامها بصورة فاعلة امام القضاء، وتقديم مرتكبي الجريمة الالكترونية للعدالة بشكل يمكن من الاقتصاص منهم ونولهم لما يستحقونه من العقاب. (Library. 2017)

انتهجنا في هذا البحث ايضا المنهج الكمي (Quantitative Research)، الذي عني بجمع بيانات رقمية وتحليلها، وقد استصحبنا في ذلك ايضا تقارير المنظمات التي عنيت بموضوع الجريمة الالكترونية والدوريات المختصة والمؤلفات ذات الصلة لمعرفة اثر المتغيرات او العلاقات بينها من خلال المنهج الوصفي (Descriptive Research) احيانا و الارتباطي (Co-relational Research) في احيان اخرى. كما استعنا ايضا بالمنهج النوعي الذي استخدمنا فيه اساليبا غيركمية رقمية لجمع البيانات و تحليلها للوصول الى مقترحات أوردناها ضمن مخرجات البحث. (Library. 2017)

12.1 تقسيم البحث:

هذه الدراسة مقدمة في قسمين رئيسيين مفصلة في ست ابواب على النحو التالي :

أ) **القسم الاول** من الدراسة يختص بالجانب القانوني او النظري من الدراسة و يضم ثلاثة ابواب من البحث يتعرض فيها لمدخل الدراسة تليها الابواب التي يعرض فيها للدراسات

السابقة المتعلقة ب القانون و التعريف والتطور التأريخي للجريمة الإليكترونية. ثم يتناول البحث الجريمة الإليكترونية والانترنت في استعراض لنشأة الانترنت واثره على تطور قضية الجريمة الإليكترونية مستعرضا الدراسات السابقة (Literature review) الخاصة بالجريمة الإليكترونية والانترنت ثم يتعرض البحث في شكل تفصيلي للدراسات السابقة الخاصة بالتحقيق في الجريمة الإليكترونية في بعض دول العالم ثم تطور تكنلوجيا السايبروالتعاون الدولي لمكافحة الجريمة الإليكترونية.

ب) **القسم الثاني** من الدراسة ويقع في ثلاثة ابواب، يختص بالجزء التقني من الدراسة والخاص بالدراسات السابقة (Literature review) الخاصة بطرق وادوات وخطوات استخدام تكنلوجيا حماية الانظمة واسترجاع المعلومات وادوات التحقيق المتوفرة ثم اطر التحقيق وتقديم وشرح الاطار المقترح وتقييمه ومن ثم نتائج اومخرجات البحث والتوصيات مصحوبة بالصعوبات التي واجهت البحث وما يمكن انجازه مستقبلا، ومن ثم قوائم المراجع وقوائم النشر واسئلة المقابلات.

13.1 ابواب البحث:

الباب الاول : المقدمة -(الباب التمهيدي)

وهو مدخل الدراسة الذي يطرح محتويات البحث التي تشمل مشكلة الدراسةوالفرضيات اهداف البحث، مناهج البحث، ثم تقسيم البحث.

الباب الثاني: التعريف والتطور التأريخي للجريمة الإليكترونية

وهذا الباب يتعلق بالدراسات السابقة والدور الفني لاثبات الجريمة الإليكترونية ودور الاخلاق اعتماد والمعايير الدولية، و الاستجابة التأريخية للجريمة والتحديات

الباب الثالث : أثر تطور الانترنت و قضايا الخصوصية

في هذا الباب يتم استعراض تأريخ الانترنت ، وقضية الخصوصية في فضاء السايبر و القانون، ثم ولادة، وملكية الانترنت، مع التعرض لأهم صور الاعتداء وقرصنة الفضاء الإلكتروني.

ويتناول الوضع العملي للتحقيق في الجريمة الإليكترونية والتعاون الدولي لمكافحة الجريمة الإليكترونية ، و الجهود الاحترافية والاقليمية، والعالمية وجهود الامم المتحدة وتنسيق التشريعات والتعاون الشرطي.

الباب الرابع : التحقيق في جرائم الانترنت والجرائم الإليكترونية :

يشمل هذا الباب تعريف التحقيق في جرائم الإنترنت، و الادلة الشرعية الرقمية، وأهم أدوات جمع الادلة الشرعية، مع التعرض لبعض افضل ادوات التحقيق المعروفة ثم تناول البحث تحليل الادلة الجنائية عموما و في نظامي وندوز و نظام يونكس..

الباب الخامس : مشاكل الاختراق والتداخل القانوني والالكتروني

يشمل هذا الباب التعرض للمشاكل التي تعترض التحقيق من حيث طبيعة الجريمة الالكترونية وعبورها للحدود ثم الموجهات القانونية العامة الخاصة واطر التحقيق واكثرها شيوعا التي مهدت الطريق لطرحنا الاطار المقترح في هذا البحث.

الباب السادس: اطار التحقيق الشامل (الاطار المقترح)

في هذا الباب، يتم تقديم نموذج او اطار التحقيق المقترح ، ثم طريقة عمل الاطار ، ومزايا وعيوب ، وتقييم الاطار ثم نعرض لاستجابة المحققين للنموزج المقترح، مع تقديم وصف التحقيق، و النتائج وتطبيق النموذج.

الخاتمة والتوصيات والدروس المستفادة

يشمل هذا الباب العناوين المتعلقة بما تم تحقيقه من الاهداف ثم معوقات البحث والدروس المستفادة واخيرا التوصيات.

الملحقات

يشمل هذا الباب قائمة المراجع ثم الملحقات التي تشمل الاوراق المنشورة واسئلة المقابلات.

II. الـــــبـــــاب الـــــثـــانـــــي

التعريف و التطور التأريخي للجريمة الإليكترونية

1.2 المـــــــقـــــدمـــــــــة :

تعريف الجريمة الإليكترونية

توصلت الجهود التي بذلت في سبيل الوصول الى تعريف واحد للجريمة الإليكترونية الى انه من الصعب الوصول إلى تعريف واحد للجريمة الإليكترونية (مصري 2005).

يعتبر التطور السريع في وسائل تقنية المعلومات، و تنوع واختلاف أساليب ارتكاب الجريمة الإليكترونية، وظهور أشكال جديدة و مستحدثة، وكذلك اختلاف الزاوية التي ينظر من خلالها من يحاول أن يعرف الجريمة الإليكترونية، من الاسباب القوية التي اكدت صعوبة الوصول الى تعريف واحد للجريمة الإليكترونية (Svedman 2020).

الجريمة الالكترونية ، أو الجريمة الموجهة نحو الكمبيوتر ، هي جريمة تنطوي على كمبيوتر وشبكة ويشمل ذلك تكنلوجيا الهاتف المحمول. (Moore 2005)

التعريف الذي نال ما يقارب الاجماع هو الذي عرفها بان الجريمة الالكترونية هي الجريمة التي تم استخدام الكمبيوتر في ارتكابها ، أو قد يكون الكمبيوتر هو الهدف من ارتكابها اساسا (Warren G. Kruse 2002).

قد تكون الجرائم الإليكترونية هي التي ترتكب ضد أفراد أو مجموعات من الأفراد بدافع إجرامي لإلحاق الأذى المتعمد بسمعة الضحية أو التسبب في ضرر بدني أو عقلي ، أو خسارة ، للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات اتصالات حديثة (شبكات غرف الدردشة ورسائل البريد الإلكتروني ولوحات الإعلانات والمجموعات) والهواتف المحمولة (Halder D 2011) .

قد تهدد الجرائم الإليكترونية أمن الانسان أو أمنه المالي وصحته. أصبحت القضايا المحيطة بهذه الأنواع من الجرائم عالية المستوى ، لا سيما تلك المتعلقة بالقرصنة وانتهاك حقوق النشر والمراقبة الجماعية غير المبررة، استغلال الأطفال في المواد الإباحية (sextortion)، وتربية الأطفال والجرائم ضد الاموال. (Morgan 2016)

برزت الجرائم الالكترونية كتحدي قانوني كبير، وقد مال المعرفون إلى اصباغ صفة العمومية على معظم تعريفات الجريمة الإليكترونية، دون تحديد او الولوج في التفاصيل تحسبا للتطور التقني والعلمي (scientific evolution) في المستقبل، فضلا عن حداثة الجهود العلمية المتعلقة بدراسة الجريمة الإليكترونية على وجه العموم (Carrier 2006).

جريمة الإنترنت، أو الجريمة الالكترونية ، هي جريمة تنطوي على جهاز كمبيوتر وشبكة، كما انه قد يتم استخدام الكمبيوتر في ارتكاب الجريمة، أو قد يكون جهاز الكمبيوتر هو الهدف.

يعرف البعض الجرائم الالكترونية وفقا لاهدافها بأنها: الجرائم التي ترتكب بدافع إجرامي لإلحاق الأذى بالسمعة أو التسبب في ضرر مادي او نفسي اويمس مصالح عامة او خاصة وذلك باستخدام شبكات الاتصالات الحديثة مثل (غرف الدردشة ورسائل البريد الإلكتروني ولوحات الإعلانات والهواتف المحمولة (-SMS / MMS-) (Jaishankar 2011).

الجرائم الالكترونية قد تهدد أمن البلاد او اوضاعها المالية والاقتصادية. (Hauck2002)
للوصول كما سبقت الاشارة فان تعريف الجريمة بشكل عام، هي كل فعل أو نشاط يتم بطريقة غير مشروعة،

بمعنى كل نشاط مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها في مختلف دول العالم و منصوص على عقوبة لها (حجاج 2006) .

ذهب البعض الى انه إذا ما استخدمت الوسائط التقنية او التكنلوجية لارتكاب النشاط الاجرامي ، أصبح الفعل جريمة الكترونية.

كما ذهب البعض ايضا لتعريفالجريمة الالكترونية بانها كل سلوك غير مشروع قانونا اوغير مصرح به ويتعلق بالمعالجة الآلية للبيانات اونقلها (مصري 2005) ويضيف مورقان ان التقنية قد تكون إما وسيلة تستخدم في ارتكاب الفعل أو هي البيئة والوسط الذي يحدث فيه الجرم أو يكون هو الهدف أو الغاية من ارتكاب الفعل المجرم، او غايته المرجوة (Morgan 2016) أي أن الوسيط يكون آلة تقنية كجهاز الحاسوب ، الذي يكون دوما وسيلة للفعل الإجرامي الإلكتروني دون إهمال بعض الأجهزة التقنية الأخرى كالهواتف المحمولة، ولا سيما مع الانتشار الواسع لاستخدامات الانترنت باعتباره وسيلة اتصالات عالمية تعتمد على البرامج المعلوماتية الحديثة في ضبط مختلف البيانات والمعطيات المعلوماتية الدقيقة.

في كثير من الاحيان يشار إلى المجرمين الذين يقومون بالأنشطة غير القانونية على أنهم متسللون webster). 2020)

الجريمة الإليكترونية قد تصلح كأسم للأنشطة غير القانونية التي تتم بوساطة الإنترنت والتي تحدث غالبا في الشبكات الإلكترونية العالمية (Chang 2003).

غالبا ما تتحدى جرائم الإنترنت الدولية فعالية القانون وإنفاذ القانون على الصعيدين المحلي والدولي، نظرا لأن القوانين الحالية في العديد من البلدان ليست مصممة للتعامل مع الجرائم الالكترونية ، فإن المجرمين يقومون بسلوكيات صارمة على الإنترنت من أجل الاستفادة من العقوبات أو الصعوبات الأقل في تعقبهم .

الجريمة الالكترونية بطبعها دولية أو عابرة للحدود الوطنية والسبب الرئيس هو انه لا توجد حدود إلكترونية بين الدول (Fortinet 2009).

تعاني كلاهما البلدان النامية و كذلك البلدان المتقدمة على حد السواء من تحديات الجريمة الإليكترونية ، كما ان الحكومات والصناعات قد أدركت تدريجيا التهديدات الهائلة لجرائم الإنترنت على الأمن الاقتصادي والسياسي والمصالح العامة .

يزداد التعقيد في أنواع الجريمة الإليكترونية وأشكالها مع الوقت مصحوبا نتيجة لذلك باذدياد صعوبة الوقوف في وجه تحدياتها .

2.2 القانون والتطور التأريخي للجريمة الإليكترونية :

بذلت العديد من المنظمات والحكومات جهودا مشتركة لوضع معايير عالمية للتشريع وإنفاذ القانون على الصعيدين الإقليمي والدولي.

التعاون بين الصين والولايات المتحدة الذي يعد واحدا من أكثر انواع التعاون الدولي إثارة للانتباه ، لفت الانظار في الآونة الأخيرة لأن كلا الدولتين في وضع يضعهما في خانة أكبر الدول المصدرة للجرائم الإليكترونية . (Fortinet 2009)

جرائم الانترنت والقانون وفقا لاستطلاع أجرته شركة ماكونيل الدولية (GROUP 2020) حول قوانين الإنترنت في 52 دولة ، اسفرت نتائجه عن النقاط التالية:

نظرا لتجاهل احتمال التوقيف، يتربص مجرموا الإنترنت في جميع أنحاء العالم بشبكة الإنترنت ويبذلون جهودا متواصلة لتهديد الصحة المالية للشركات واضعاف ثقة العملاء في ذات الوقت الذي يشكلون فيه تهديدا لأمن الدول. (ITU 2009)

ذهبت التقديرات المتحفظة الى ان تكلفة الجريمة الإلكترونية قد تصل الى نحو حوالي 50 مليار دولار سنويا. مع وجود أكثر من 60 مليون شخص في أمريكا الشمالية لديهم تسهيلات مصرفية عبر الإنترنت.

لا تقدر التكلفة المترتبة على جرائم الإنترنت في الولايات المتحدة وحدها بالمليون ، ولكن بالمليارات (تشير التقديرات إلى أن هذه التكلفة تصل إلى 5 مليارات دولار سنويا) (GROUP 2020).

مع وجود نشاط إجرامي واسع النطاق على هذا المستوى الضخم ، لا يمكن تصور عدم تدخل القانون و التماس التعويض الا ان العكس تماما هو الذي حدث اذ انه قد تم الإبلاغ عن حوالي 10% بالمائة فقط من جميع الجرائم الإلكترونية . (GROUP 2020)

الجرائم التي يتم الإبلاغ عنها فعليا ، نجد ان 2% في المائة فقط منها وصل الحكم فيها الى شكل من أشكال الإدانة لمجرم الإنترنت. (Johansen 2020)

نسبة للخوف من خطر فقدان ثقة العملاء في شبكتهم ، فقد اختارت الشركات الكبرى التي وقعت ضحية لجرائم الإنترنت في الماضي عدم الإبلاغ عن الجرائم التي تتعرض لها الانظمة الخاصة بها (ITU 2009).

عندما يكون الضحايا قد طلبوا الانصاف والرد في إطار نظام الدفاع الجنائي ، كان الإجماع العام بين الضحايا هو أن القانون سوف يقدم مساعدة ضئيلة أو معدومة لقضيتهم .

هناك بعض الحالات التي لا يكون فيها متاحا لضحايا العصابات الإجرامية التي تحرض على جرائم الإنترنت اللجوء إلى إجراءات الدفاع الجنائي التي من شأنها حماية حقوقهم وحرياتهم الفردية ، ويمكن التمثيل لذلك بالعصابات الإجرامية التي كانت تعمل في السابق في دول بعينها والتي كانت تبيع الصور الإباحية للأطفال عبر الإنترنت لعملاء في الغرب بينما يكون العملاء بدورهم يعتقدون أنهم في مأمن من المقاضاة في منازلهم . (GROUP 2020)

بغض النظر عن عامل اللجؤ للقانون، ومع وجود 90 في المائة من الشركات الأمريكية التي شملتها الدراسة الاستقصائية ظهر ان هذه الشركات واجهت انتهاكات أمنية متعلقة بالكمبيوتر في عام 2001 ، فمن الواضح أن الجرائم الإلكترونية قد وصلت إلى أبعاد متوطنة. (Lee 2001)

معالجة مشكلة الانتهاكات الامنية المتعلقة بالكمبيوتر اصبحت ضرورة. كما ان نظام الدفاع الجنائي لا بد من ان يصبح احد وسائل مقاومة جريمة الإنترنت بوضعها المتطور مع مر الايام تبعا للتطور التكنلوجي الذي لا يتوقف (GROUP 2020)

أمام الفراغات التشريعية التي أصبحت عبء علي كاهل الدول بعد انتشار الجرائم الالكترونية ، خاصة مع استخدام الإنترنت ''الشبكة العنكبوتية www'' ونظرا لخصوصيتها المميزة، بات من الضروري إيجاد إطار فعال يضمن استحداث آليات للتعاون

الدولي في مجال مكافحة هذا النوع من الجرائم من خلال التشجيع على تبادل الخبرات من أجل الضبط الجنائي لها، باعتبارها جرائم افتراضية، مع تكوين مختصين في المجال سواء الضبطية القضائية أو القضاء بوجه عام،(Heiser 2001) وإيجاد تشريع دولي خاص لمواجهة هذا الخطر، وتبني منظومة معلوماتية موحدة تعتمد على إنشاء مكتب عالمي أو إقليمي للتوثيق الإلكتروني، مع تسجيل كافة البرامج المعلوماتية وحفظها واعتماد الدلائل أو القرائن الرقمية كدلائل إثبات الجريمة ومن ثمة إدانة مقترفيها والحرص على إدراج مثل هذه الجرائم ضمن اختصاصات المحكمة الجنائية الدولية نظرا لطابعها العالمي، فالتشريع الدولي المنشود يجب أن يبنى على أطر قانونية موحدة يتم فيها عولمة القوانين وصلاحيات الاختصاص المفتوحة والمشتركة بين جميع دول العالم.(Reed 2004)

3.2 اعتماد المعايير الدولية:

تلعب تكنولوجيا المعلومات والاتصالات (ICT) دورا مهما في المساعدة على ضمان التشغيل البيني والأمني استنادا إلى المعايير العالمية.(Patel 2000)

تم اتخاذ تدابير مضادة عامة في مكافحة الجريمة الإليكترونية ، مثل التدابير القانونية في التدقيق في التشريعات والتدابير التقنية في تتبع الجرائم على الشبكة العنكبوتية ، وكذلك مراقبة محتوى الإنترنت ، واستخدام الادلة الجنائية الخاصة بالكمبيوتر ، والتشفير، إلخ...(Harrison 2002).

ادى تطور جرائم الكمبيوتر والجرائم الإليكترونية الى اعتبار التعديات الجنائية على تكنولوجيا المعلومات والاستجابة القانونية اللازمة عند حدوث اي اختراق او اساءة هما القضيتان الواجب مناقشتهما بالتزامن مع تقديم اي تطور تكنولوجي(Kerr 2005).

4.2 الاستجابة التأريخة للجريمة الالكترونية:

على مدار اكثر من خمسين عاما مضت ، تم تنفيذ العديد من الحلول ضد الجريمة الالكترونية على الاصعدة الوطنية والإقليمية والدولية. الا ان أحد الأسباب في انها لا تزال خطرا ماثلا ويمثل تحديا هو التطور التقني المستمر، فضلا عن الأساليب والظروف المتغيرة التي ترتكب فيها الجرائم الالكترونية (GROUP 2020).

i. **في الستينيات** من القرن العشرين ، أدى إدخال أنظمة الكمبيوتر التي تعتمد على الترانزستور ، والتي كانت أصغر وأقل تكلفة من الأجهزة القائمة على الأنابيب المفرغة ، إلى زيادة في استخدام تكنولوجيا الكمبيوتر.

في هذه المرحلة المبكرة ، تركزت الجرائم على الأضرار المادية لأنظمة الكمبيوتر والبيانات المخزنة. على سبيل المثال ، في كندا ، حيث تسببت أعمال شغب الطلاب في عام 1969 في حريق دمر بيانات الكمبيوتر المستضافة في الجامعة. (Harrison 2002)

في منتصف الستينيات ، بدأت الولايات المتحدة مناقشة حول إنشاء سلطة مركزية لتخزين البيانات لجميع الوزارات. في هذا السياق ،

تمت مناقشة التعديات الجنائية المحتملة لقواعد البيانات. (Palmer 2002)

ii. في **السبعينيات** من القرن العشرين ، زاد استخدام أنظمة الكمبيوتر وبيانات الكمبيوتر.

في نهاية العقد ، كان هناك ما يقدر بنحو 100000 حاسوب مركزي يعمل في الولايات المتحدة. (Ó Ciardhuáin 2002)

مع انخفاض الأسعار ، اصبحت تكنولوجيا الكمبيوتر تستخدم على نطاق واسع في الإدارة والأعمال ، ومن قبل الجمهور. (Venema 1999) اتسمت السبعينيات بالتحول من جرائم الملكية التقليدية ضد أنظمة الكمبيوتر التي هيمنت على الستينيات إلى أشكال جديدة من الجريمة. بينما لا يزال الضرر المادي شكلا ذا صلة من أشكال التعديات الجنائية ضد أنظمة الكمبيوتر ، فقد تم الاعتراف بـ 123 شكلا جديدا من جرائم الكمبيوتر. وشملت الاستخدام غير القانوني لأنظمة الكمبيوتر والتلاعب بالبيانات الإلكترونية. (Saferstein 2000)

أدى التحول من المعاملات اليدوية إلى المعاملات التي يديرها الكمبيوتر إلى شكل جديد آخر من أشكال الجريمة يتمثل في الاحتيال المتصل بالحاسوب.

في هذه الحقبة ، كانت الخسائر المقدرة بملايين الدولارات ناجمة عن الاحتيال المتصل بالحاسوب.

كان الاحتيال المرتبط بالحاسوب ، على وجه الخصوص ، يمثل تحديا حقيقيا ، وكانت وكالات إنفاذ القانون تحقق في عدد متزايد من الحالات. (UN 2000)

نظرا لأن تطبيق التشريعات الحالية في قضايا جرائم الكمبيوتر أدى إلى صعوبات، فقد بدأت مناقشة الحلول القانونية في أنحاء مختلفة من العالم (Hauck 2002)

ناقشت الولايات المتحدة مشروع قانون مصمم خصيصا للتصدي للجريمة الإلكترونية وكانت هي الاسبق في ذلك.

كما ناقش الإنتربول ظواهر وإمكانيات الاستجابة القانونية. (DictHer 2000)

iii. في **ثمانينات** القرن العشرين ، أصبحت أجهزة الكمبيوتر الشخصية أكثر شعبية.

ومع التطور التقني ، زاد عدد أنظمة الكمبيوتر وبالتالي عدد الأهداف المحتملة للمجرمين مرة أخرى. لأول مرة ، شملت الأهداف مجموعة واسعة من البنيات التحتية الحيوية. وكان أحد الآثار الجانبية لانتشار أنظمة الكمبيوتر زيادة الاهتمام بالبرمجيات ، مما أدى إلى ظهور الأشكال الأولى من قرصنة البرمجيات والجرائم المتعلقة بالبراءات. (TWG 2001)

ربطت أنظمة الكمبيوتر واضافت أنواع جديدة من الجرائم ،كما ادي انتشار الشبكات الى تمكين المخالفين من الدخول إلى نظام الكمبيوتر دون التواجد في مسرح الجريمة. (Rynearson 2002)

التقنية الجديدة التي اتاحت إمكانية توزيع البرامج عبر الشبكات مكنت المجرمين من نشر البرامج الضارة ، واكتشاف الاكثر اضرارا والمزيد من فيروسات الكمبيوتر.

بدأت 138 دولة عملية تحديث تشريعاتها لتلبية متطلبات البيئة الجنائية المتغيرة. فكان تبعا لذلك ان شاركت المنظمات الدولية أيضا في هذه العملية. (UN 2000)

أنشأت منظمة التنمية و التعاون الاقتصادي OECD (The Organization for Economic Cooperation and Development) ومجلس أوروبا مجموعات دراسة لتحليل الظواهر وتقييم إمكانيات الاستجابة القانونية.

iv. **مع بداية التسعينات** من القرن الماضي أدى إدخال الواجهة الرسومية "WWW" الى نمو سريع في عدد مستخدمي الإنترنت إلذي نجمت عنه تحديات جديدة.

ادت زيادة مستخدمي الانترنت الى ان تصبح المعلومات التي يتم توفيرها بشكل قانوني في اي بلد متاحة على المستوى العالمي حتى في البلدان التي يتم فيها تجريم نشر ذات المعلومات ويظهر ذلك بصورة اوضح من زاوية عدم اتساق القوانين فما قد يعد جريمة في دولة، قد لا يعد كذلك في دولة اخرى ومثلما هو حال ما قد يكون مسموحا به للكبار و لا يكون مسموحا به للصغار كجزء من مشكلة المستمع الخفي في الانترنت (Invisible Audience). (عثمان 2013)

وكذلك الحال بالنسبة لبرتكولات الانترنت وعدم فرضها اي قيود على الاستخدام للمستفيدين من خدمات الانترنت بل على العكس تماما يتمتعون بكامل الحرية التي لم يتدخل فيها اي ملاك للانترنت باي كوابح تمثل خاصية من خواص الانترنت. (Venema 1999)

مع التطور التقني برزت الشواغل الأخرى المرتبطة بالخدمات عبر الإنترنت والتي تبين أنها تمثل تحديا كبيرا في التحقيق في الجريمة العابرة للحدود الوطنية وسرعة تبادل المعلومات. (Mohay 2003)

انتقل توزيع الصور الإباحية للأطفال من التبادل المادي (hardcopy) للكتب والأشرطة إلى التوزيع عبر الإنترنت (softcopy) من خلال المواقع الإلكترونية وخدمات الإنترنت فبينما كانت جرائم الكمبيوتر جرائم محلية عامة .(Local) حول الإنترنت الجرائم الإلكترونية إلى جريمة عابرة للحدود الوطنية (boarder-cross) ، ونتيجة لذلك ، عالج المجتمع الدولي هذه القضية بشكل مكثف. المثال على التدخل الدولي قرار الجمعية العامة للأمم المتحدة رقم 121/45 الذي تم تبنيه عام 1990 (UN 1990) ودليل منع ومكافحة الجرائم المتعلقة بالحاسوب الصادر في عام 1994.

كما هو الحال في كل العقود السابقة ، استمر اكتشاف اتجاهات جديدة في جرائم الكمبيوتر والجرائم الإليكترونية في القرن الحادي والعشرين. (TWG 2001)

v. سيطر العقد الأول من الألفية الجديدة من خلال أساليب جديدة ومتطورة للغاية من ارتكاب الجرائم ، مثل "التصيد" ، و "هجمات الروبوتات"، واستخدام الناشئة من التكنولوجيا التي هي أكثر صعوبة في عملية إنفاذ القانون للتعامل والتحقيق في الجريمة الإليكترونية ، مثل "الصوت عبر بروتوكول الإنترنت. (Adams 2013)

5.2 تطور تكنلوجيا السايبرو الدور الفني لاثبات الجريمة الإليكترونية :

تكنلوجيا السايبر اصبحت هي المسيطر على غالبية الانشطة الانسانية .الا انه وبرغم ذلك يمكن القول بان هذه التكنلوجيا مازالت تتلمس طريقها الى كل المجالات. فهذه التكنلوجيا حتى الان لم تكمل رحلتها الى كل ما يمكنها الوصول اليه، اذ ما زال الدرب امامها طويلا خلافا لبقية العلوم التي تكاد تكون قد وصلت مرحلة النضج، سيما فيما يتعلق بتناول المسائل الاخلاقية والقانونية والامنية وقضايا الخصوصية وقضايا الملكية الفكرية (Intellectual Property) فضلا عن مشكلة سرعة التطور الذي يحدث وباستمرار مدهش في المجال التكنلوجي.

خلال حقبة الثمانينات ، كانت معظم التحقيقات الجنائية الرقمية تتألف من تحليل حي ، حيث تفحص الوسائط الرقمية مباشرة باستخدام أدوات غير متخصصة .

في حقبة التسعينيات ، تم إنشاء العديد من الأدوات المجانية وغيرها من أدوات الملكية (كل من الأجهزة والبرامج) للسماح بإجراء التحقيقات دون تعديل الوسائط. (David Icove 2001)

ركزت هذه المجموعة الأولى من الأدوات بشكل أساسي على الادلة الشرعية للكمبيوتر ، على الرغم من أن أدوات مماثلة تطورت في السنوات الأخيرة في مجال الادلة الشرعية للأجهزة المحمولة تتضمن هذه القائمة أمثلة بارزة لأدوات الادلة الشرعية الرقمية .

6.2 دور الشكاوي في الاهتمام بمكافحة الجريمة الإليكترونية :

المفاهيم المتعلقة باخلاقيات المهنة بالنسبة لقضايا السايبر لم تقترب من التوحد حتى في المجال الواحد. بدون النظر والبحث عن توحد المبادئ العامة يمكن ملاحظة نسبية المعايير واختلافها من مؤسسة الى اخرى، حتى ان البعض يرى ان ظروف كل مؤسسة هي التي تحدد المعايير التي تنظر بها كل مؤسسة للقضايا المتعلقة بالقضايا موضوع البحث.

دون سائر انواع العلوم فان تكنلوجيا السايبر ما زالت تتمدد افقيا ورأسيا و في كل الاتجاهات بشكل يجعل التأريخ لها او رصد تطورها امرا في غاية الصعوبة والتعقيد، فضلا عن التأسيس باستخدام ما يصلح لعملية الضبط الاخلاقي والقانوني في عموم مستجدات المسائل المستقبلية الخاصة بالجانب الفني في قضايا الاثبات والتحقيق وجمع البينات.(Reith 2002)

بسبب الانتشار المخيف للجرائم الإلكترونية كظاهرة عالمية، والتهديد المستمر لكل النشاط الانساني، وللمصالح المرتبطة بالتقنيات الجديدة، اصبح من الضروري البحث عن كيفية إيجاد حلول فعالة، واتخاذ تدابير وقائية، وردعية لوقف التهديد المتصاعد للجريمة الالكترونية، التي باتت تهدد اقتصاديات وأمن واستقرار الدول، بعد تطور الجريمة الإلكترونية من إطارها الكلاسيكي المعروف، إلى التقنية العلمية الحديثة.

هددت الجريمة الإليكترونية التجارة إلاكترونية، التي اصبحت رائجة وسادت كل التعاملات بين الافراد

والشركات والدول، وهو ما اصطلح على تسميته بالاقتصاد الرقمي. (UN 2013)

اثارت الشكاوى الرسمية التي اعتمدها المركز العالمي لشكاوى الانترنت منذ بدايتها كثيرا من الرعب، فقد بلغت تكلفتها في العام 2000 خسارة مادية قدرت بـــ12 بليون دولار جراء النتائج التدميرية التي تسببت فيها فيروسات إتلاف برامج المعلوماتية.

قدرت مجمل الشكاوى الرسمية التي قدمها الضحايا للمركز بـــ 275284 شكوى في ذلك العام وحده.

في كثير من الدول خصصت وسائل مختلفة للتبليغ عن جرائم الانترنت ولهذا ومن أجل حماية فعالة لبرامج المعلوماتية وقاعدة البيانات كان لابد من اعتماد السبل القانونية الوقائية من خلال الدخول لقواعد البيانات عن طريق كلمات المرور و تجنب استخدام كلمات السر المكونة من كلمات يمكن حزرها مع الحرص على تغييرها دوريا كل مرة إن تطلب الأمر ذلك. (Ó Ciardhuáin 2002)

تشمل الجوانب الوقائية، تكثيف برامج الرقابة على نوادي ومقاهي الانترنيت، والعمل على ترصد وحجب المواقع الإباحية كما هو الحال في كثير من الدول وخصوصا الاسلامية منها وضمنها السودان، مع اعتماد برامج خاصة مضادة للفيروسات التدميرية واستعمالها بشكل مستمر. (Morgan 2016)

7.2 الجريمة الالكترونية ودور الاخلاق و اخلاقيات السايبر:

من الصعب جدا تحديد ماهية "الأخلاق" ، لان آراء كثير من الناس عن الأخلاق تميل الى الهشاشة فكثير من الناس يميلون إلى مساواة الأخلاق مع مشاعرهم.

واقع الحال ان يكون الشخص اخلاقيا، كما نعتقد، ليست مسألة اتباع الشخص لمشاعره فالشخص وفقا لمشاعره قد ينكص عن القيام بما هو صحيح أو اخلاقي، والمشاعر كثيرا ما تنحرف عن ما هو أخلاقي. ولا ينبغي لأحد تحديد الأخلاق بالنظر الى الدين، فان معظم الديانات، بطبيعة الحال، تضع معايير أخلاقية عالية. كما لا يمكن ان تكون الأخلاق محصورة بالدين، ولا يتمتع بها غير المتدينين، لان الأخلاق تنطبق بنفس القدر على سلوك الملحد مثله مثل الشخص الورع المتدين. كما ان الدين يمكن، أن يضع معايير أخلاقية عالية، ويمكن أن يوفر الدوافع المكثفة للسلوك الأخلاقي، ومع ذلك، لا يمكن أن يقتصر مفهوم الاخلاق على الدين ولا هو نفس الدين. (Bicchieri 2006)

المعايير الأخلاقية أيضا ليست هي القانون لان القانون غالبا ما يتضمن المعايير الأخلاقية التي يؤمن بها معظم المواطنين، بينما ان القوانين، مثل المشاعر، يمكن أن تحيد عن ما هو أخلاقي. ويبقى السؤال عن ما هي الأخلاق؟

وللاجابة شقان:

أولا، الأخلاق هي عبارة عن معايير (Standards) لتحديد الصواب والخطأ وتعنى بتحديد ما يجب ان يقوم به البشرعادة، من حيث الحقوق والواجبات، والفوائد للمجتمع والإنصاف (Equity)،

أو فضائل (Virtues) معينة ، على سبيل المثال، فالاخلاق هي من يشير إلى تلك المعايير التي تفرض التزامات معقولة (Rational) مثل الامتناع عن الاغتصاب والسرقة والقتل والاعتداء والافتراء والتزوير الخ.... (Tracy Cross 2009)

تشمل المعايير الأخلاقية تلك التي تأمر بفضائل الصدق، الرحمة ، والولاء.

وتشمل المعايير الأخلاقية المعايير المتعلقة بالحقوق، مثل الحق في الحياة والحق في عدم التعرض للإصابة ، والحق في الخصوصية. هذه المعايير هي معايير كافية للأخلاق لأنها معتمدة Accredited لأسباب ثابتة ومتبعة من افراد المجتمع (Spinello 2010).

ثانيا ، الأخلاق تتطلب وتدعو الشخص إلى دراسة وتطوير المعايير الأخلاقية لديه. وكما سبق ذكره، فانه من الممكن للمشاعر والقوانين والأعراف الاجتماعية ان تحيد Deviate عن ما هو أخلاقي. ولذلك فمن الضروري ان يتم فحص و باستمرار المعايير الاخلاقية لضمان أن تكون معقولة ومبرره اجتماعيا أيضا ، ثم يتوالى الجهد المتواصل لدراسة المعتقدات الأخلاقية الخاصة والسلوك الأخلاقي، والسعي لضمان أن المؤسسات التي تساعد على تشكيل المبادئ العامة، قادرة على ان ترقى إلى معايير معقولة وتستند على أساس متين (Ó Ciardhuáin 2002).

هناك ميل من جانب العديد من المتدينين الى أن عبء الإثبات بالضرورة يقع على عاتق غير المؤمنين (Non-theist) عندما يتعلق الأمر بمسألة الأخلاق. وبالتالي، يطلب من الفرد الذي يعمل دون وجود قاعدة دينية لتبرير افعاله بافتراض من المؤمن انه ليس ممكنا

وجود أخلاق في غياب شكل من أشكال القانون الاعلي " الدين". (Tracy Cross 2009)

في الثقافة الغربية، نجد ان الناس قد اعتادوا على فكرة ان كل قانون يقتضي اصداره وجود نائب منتخب للقيام بهذا الدور، ولكل قاعدة لابد من وجود المنفذ، ولكل مؤسسة لابد من وجود شخص ما في السلطة، وهكذا دواليك، بمعني ان القواعد التي تضبط السلوك تحتاج في الغالب الاعم لوجود السلطة النهائية المسؤلة عن تنفيذها وهو امر يتفاوت بدرجات كبيرة او باعتبارات ضعيفة تجعل معني الاخلاق ودورها ثانويا في ضبط سلوك افراد المجتمع (Tracy Cross 2009) .

8.2 المعايير الاجتماعية :

المعايير الاجتماعية، مثل العديد من الظواهر الاجتماعية الأخرى، هي، نتيجة غيرمخطط لها، أو متوقعة كنتيجة من تفاعلات الأفراد.

وقد قيل أن الأعراف الاجتماعية يجب أن تفهم على أنها تلعب الدور النحوي او القاعدي لتفسير وفهم نتائج التفاعلات الاجتماعية . فهو مثل النحو أو هو نظام قواعد تحدد ما هو مقبول وما هو غير مقبول في اي مجتمع أو مجموعة (Posner 2009) .

مسألة هامة أخرى، وهي في كثير من الأحيان غير واضحة عن المعايير الاجتماعية و هي العلاقة بين المعتقدات المعيارية والسلوك. لما كانت القواعد المثيرة للاهتمام و الدراسة هي تلك التي تنشأ من دون تخطيط أو تصميم من تفاعلات الأفراد فان النظرية الهامة هى تحليل الظروف التي ابرزت تلك القواعد إلى حيز الوجود .

دراسة المعايير الاجتماعية يمكن أن تساعدنا على فهم طائفة واسعة من السلوك البشري الذي على ما يبدو محيرا.

وجود القاعدة والامتثال لها يمكن أن يكون أفضل فهم من حيث التفضيلات المشروطة لاتباع قواعد السلوك التي تنطبق على فئات من التفاعل الاجتماعي.

التفضيلات المشروطة نوعان مختلفان من التوقعات:

النوع الاول هوالتوقعات التجريبية وتعني وجود عدد كاف من الناس ينضم إلى القاعدة السلوكية،

والنوع الثاني هي التوقعات المعيارية وهي أن الآخرين يتوقعون انضمام الاخر لمتابعة القاعدة السلوكية أيضا، وربما يتم فرض عقوبات لمخالفة القاعدة او العدوان.

المعايير الاجتماعية، لا تزال تترك الكثير ليتم التحقيق فيه، في حين أن هناك العديد من النماذج المتاحة كما القول بانه لا يوجد هناك من يفترض وجود قواعد مسبقة او قواعد مقرونة بعدد السكان. (Posner 2009).

9.2 اخلاقيات السايبر

نخلص مما سبق الى ان اخلاقيات السايبر (Cyber Ethics) هي الدراسة الفلسفية الأخلاقية المتعلقة بأجهزة الكمبيوتر، وتشمل سلوك المستخدم وما هو مبرمج لأجهزة الكمبيوتر القيام به، وكيف يؤثر هذا على الفرد والمجتمع.

ادى اختراع الكاميرات في أواخر القرن ال19، الى المناقشات الأخلاقية بصورة تشبه تماما ألمناقشات الاخلاقية التي صاحبت ظهور شبكة الانترنت اليوم.

الخصوصية هي أيضا لا غنى عنها للشعور الذاتي وهو "شعور بأن هناك منطقة من حياة الفرد التي هي تماما تحت سيطرته، وهي منطقة خالية من التدخل الخارجي". سنت الحكومات المختلفة لوائح في حين أن المنظمات قد حددت سياسات حول أخلاقيات الإنترنت. (Volonino 2008)

10.2 الأخلاق في الأمن الالكتروني :

الأخلاقيات - المبادئ الأخلاقية التي تحكم سلوك الشخص - هي جزء مهم من أي استراتيجية دفاع سليمة للأمن السيبراني.

بدون وجود معايير وقواعد أخلاقية واضحة ، لا يمكن تمييز محترفي الأمن السيبراني تقريبا عن مجرمي القبعة السوداء الذين يسعون ضدهم لحماية الأنظمة والبيانات. (عثمان 2013).

11.2 أهمية أخلاقيات السايبر:

يجب أن نتأكد من أن المستخدمين يفهمون مسؤولياتهم عن إدارة أنفسهم عبر الإنترنت. أخلاقيات الإنترنت عنصر مهم في فهم المستخدمين لمسؤولياتهم وقدرتهم على ادارة انفسهم عبر الانترنت.

تشير اخلاقيات الانترنت (Cyber Ethics) إلى مدونة السلوك المسؤول عن الإنترنت.

يجب على الجميع استخدام جميع المبادئ الأساسية لأخلاقيات الإنترنت حتى ينعم الجميع بخدمة سيبرانية جيدة. (العنزي 2019).

12.2 أختلاف أخلاقيات السايبر:

هناك اعتقاد بان اخلاقيات السايبر ليست مثل غيرها مما يثير السؤال الحتمي القائل: هل قضايا أخلاقيات السايبر فريدة من نوعها؟ للاجابة عى ذلك لا بد من النظر للامر من جانبين هما كيفية وصف اخلاقيات السايبر والناحية الاخرى هي الحجج التي تبرر وجود الاختلاف واقعيا.

اخلاقيات السايبرتوصف بأنها مجال جديد للأخلاقيات ونوع فريد من الاخلاقيات بشكل عام.

تستند الحجج الخاصة بمثل هذه الاراء إلى القابلية للتوسع المنطقي لأجهزة الكمبيوتر وتأثير الكمبيوتر على المجتمع وكون ان الجريمة الإليكترونية يبدو ان العنصر المادي فيها يصعب تمييزه لانه يميل اكثر للخفية. (Tracy Cross 2009).

13.2 تعريف أخلاقيات السايبر :

الأخلاق هي منظومة قيم يعتبرها الناس بشكل عام جالبة للخير وطاردة للشر وفقا للفلسفة الليبرالية وهي ما يتميز به الإنسان عن غيره. وقد قيل عن الاخلاق إنها شكل من أشكال الوعي الإنساني كما تعتبر مجموعة من القيم والمبادئ التي تحرك الأشخاص والشعوب كالعدل والحرية والمساواة بحيث ترتقي إلى درجة أن تصبح مرجعية ثقافية لتلك الشعوب لتكون سندا قانونيا تستقي منه الدول الأنظمة والقوانين (Spinello 2010).

وهي السجايا والطباع والأحوال الباطنة التي تدرك بالبصيرة والغريزة، وبالعكس يمكن اعتبار الخلق الحسن من أعمال القلوب وصفاته. فأعمال القلوب

تختص بعمل القلب بينما الخلق يكون قلبيا ويكون ظاهرا أيضا.

والأخلاق هي دراسة، حيث يقيم السلوك الإنساني على ضوء القواعد الأخلاقية التي تضع معايير للسلوك، التي يضعها الإنسان لنفسه أو يعتبرها التزامات ومبادئ يمشي عليها وأيضا واجبات تتم بداخلها أعماله أو هي محاولة لإزالة البعد المعنوي لعلم الأخلاق، وجعله عنصرا مكيفا، أي أن الأخلاق هي محاولة التطبيق العلمي، والواقعي للمعاني التي يديرها علم الأخلاق بصفة نظرية، ومجردة.

الكلمة الإنجليزية للأخلاق «Ethic» مستخلصة من الأبجدية اليونانية «ἦθεα» (إيثيه) أي «عادة». وتكون الأخلاق طاقما من المعتقدات، أو المثاليات الموجهة، والتي تتخلل الفرد أو مجموعة من الناس في المجتمع. (الركابي 2009)

نكتفي في هذا المقام بالتعريف الذي نعتقده لاخلاقيات السايبرفهي الدراسة الفلسفية للأخلاقيات المتعلقة بأجهزة الكمبيوتر، بما في ذلك سلوك المستخدم وما تقوم به أجهزة الكمبيوتر، وكيف يؤثر ذلك على الأفراد والمجتمع.

خالفت الحكومات المنظمات المختلفة باعتمادها اللوائح والقوانين التي تحكم السلوك المتعلق بتكنلوجيا السابير، في حين أن المنظمات اعتمدت سياسات متعلقة بأخلاقيات السايبر واهتمت اكثر بالتكنلوجيا المتعلقة بالإنترنت.

مما سبق يمكن ان نخلص الى تعلق الأخلاق بالسلوك الصحيح و الخاطئ، وايضا تشير الأخلاق إلى القواعد

التي يوفرها مصدر خارجي، مثل ، قواعد السلوك في أماكن العمل أو المبادئ في الأديان.

ايضا تشير الأخلاق إلى مبادئ الفرد على المستوي الشخصي فيما يتعلق بالصواب والخطأ.

الأخلاقيات هي معايير خارجية توفرها المؤسسات أو المجموعات أو الثقافة التي ينتمي إليها الفرد. على سبيل المثال ، يتعين على المحامين ورجال الشرطة والأطباء اتباع مدونة أخلاقية وتخص مهنتهم ، بغض النظر عن مشاعرهم أو تفضيلاتهم.

يمكن أيضا اعتبار الأخلاقيات نظاما اجتماعيا أو إطارا لسلوك مقبول.

تتأثر الأخلاق أيضا بالثقافة أو المجتمع ، لكنها مبادئ شخصية غالبا ما يتم إنشاؤها ودعمها بواسطة الأفراد أنفسهم.

14.2 مبادئ الأخلاق المهنية للمحترفين:

يمكن ترتيب المبادي التي تحكم الاخلاق المهنية القائمة على الاحترف عموما على النحو البالي:

أ. النزاهة. يجب أن يكون المحترف مباشرا وصادقا في جميع العلاقات المهنية والمتعلقة بمهن.
ب. لموضوعية.
ت. الكفاءة المهنية والعناية الواجبة.
ث. السرية.
ج. السلوك المهني.

ذهب الفكر القانوني الى صعوبة تكييف الجريمة الإليكترونية بسبب التطور السريع في وسائل تقنية المعلومات بالإضافة إلى تنوع واختلاف أساليب ارتكابها وظهور أشكال جديدة و مستحدثة وكذلك

اختلاف الزاوية التي ينظر من خلالها من يحاول أن يعرفها لذلك ظهرت الجرائم الإليكترونية كتحدي قانوني كبير وقد آثر المعرفون وضع تعريف للجريمة الالكترونية يمكن الحكم عليه بانه قد مال الي ان يتصف بالعمومية دون تحديد للتفاصيل تحسبا للتطور التقني والعلمي في المستقبل (ITU 2009) اضافة الى حداثة دراسة الجريمة الالكترونية عموما. (حجاج2006).

فلما كانت الجريمة " هي كل فعل أو نشاط يتم بطريقة غير مشروعة"، بمعنى كل نشاط مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها عبر مختلف دول العالم و منصوص على عقوبتها.(حجاج 2006).

فان النشاط غير المشروع إذا ما استخدمت فيه وسائط تقنية علمية، أصبح الفعل جريمة سيبرانية، لانه وطبقا لخلاصة ما ورد من تعريفات للجريمة الإليكترونية فهي كل سلوك غير مشروع قانونا اوغير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها تكون التقنية فيه إما وسيلة تستخدم في ارتكاب الفعل أو هي البيئة والوسط الذي يحدث فيه الجرم أو يكون الهدف أو الغاية لارتكاب الفعل المجرم،(Hayes 2013) أي أن الوسيط يكون آلة تقنية كجهاز الحاسوب ، الذي يكون دوما وسيلة للفعل الإجرامي السيبراني دون إهمال لبعض الأجهزة التقنية الأخرى كالهواتف المحمولة، ولا سيما مع الانتشار الواسع لاستخدامات الانترنت باعتباره وسيلة اتصالات عالمية تعتمد على البرامج المعلوماتية الحديثة في ضبط البيانات والمعطيات المعلوماتية الدقيقة.

فالجريمة الإليكترونية يمكن وصفها بأنها كل فعل يستهدف الفضاء الالكتروني أو استخدمت التكنولوجيا الحديثة في ارتكابه او ارتكب عبر الوسائط الالكترونية.

15.2 تحديات المكافحة و التحقيق في الجريمة الالكترونية:

برزت عدة تحديات امام القائمين على مكافحة الجريمة الالكترونية بشكل عام كتحديات عامة تلخصت في ستة اسباب تفاعل فيها دور التكنلوجيا الخاصة بالاتصال مع الاعداد المتزايدة لمستخدمي الانترنت اضافة لسهولة الحصول على الاجهزة وخدمة الانترنت وتوافر المعلومة التي تخدم شتى احتياجات من لديهم الاستعداد لارتكاب الجريمة فضلا عن غياب القدرة على التحكم في الانترنت، بمعنى انه متاح لكل من يرغب في الحصول على خدماته واخيرا فان الجريمة يمكن ان يكون لها بعدا دوليا يمكن مرتكبيها ويجعل الفرصة سانحة لهم للافلات بجرائمهم. (عثمان 2013)

فيما يلي سنتعرض في هذا البحث للتحديات العامة التي تواجه مسألة التحقيق في الجريمة الالكترونية وتقديم مرتكبيها للمحاكمة وذلك على النحو التالي:

اولا: الاعتماد على تكنلوجيا الاتصال Reliance on ICTs

تعتمد العديد من الاتصالات اليومية على تكنولوجيا المعلومات والاتصالات (ICT) والخدمات المستندة إلى الإنترنت، بما في ذلك المكالمات والاتصالات عبر بروتوكول الإنترنت (TCP/IP) أو البريد الالكتروني (Email) في كل المجالات الخاصة بالاتصال. (communication)

تكنولوجيا المعلومات والاتصالات الان هي المسؤولة عن وظائف التحكم والإدارة في المباني ، السيارات والطيران، وإمدادات الطاقة، والمياه وخدمات الاتصالات، كلها تعتمد على تكنولوجيا المعلومات والاتصالات. ومن المرجح أن تزايد الاعتماد على تحقيق مزيد من التكامل والاعتمادية على تكنولوجيا المعلومات والاتصالات في الحياة يجعل النظم والخدمات أكثرعرضة لهجمات خطيرة على اهداف استراتيجية (Svedman 2020).

البنيات التحتية التقنية الحالية تعاني من نقاط ضعف عديدة ويتمثل ذلك كمثال في الاحادية (monoculture) وتجانس نظم التشغيل (Homogeneity of Operating systems) ويتجلى في ان غالبية المستخدمين يستخدمون المايكروسوف (Microsoft operating system) الامر الذي يجعل مهمة المجرمين اكثر سهولة فان الهدف قد اصبح اكثر تحديدا وواحدا وتصميم خطة الهجوم في مثل هذه الحالة لابد من ان تكون اكثر سهولة ويسرا .

اعتماد المجتمعات على تكنلوجيا الاتصالات ليس مقصورا على المجتمعات الغربية وحدها. كثير من الدول النامية تواجه خطر الهجمات ضد بنياتها التحتية، وضد المستخدمين.

ادى تطوير التكنلوجيا الرخيصة مثل (WiMAX) لتمكين الدول النامية من تقديم خدمات الانترنيت لاعداد اكبر من مواطنيها . برغم ان هذا التوسع في نشر خدمات الانترنت قد عرض الدول النامية لمخاطر عديدة الا ان الفرصة ما زالت مواتية بالنسبة للدول النامية لتفادي الاخطاء التي وقعت فيها الدول المتقدمة التي اهتمت بنشر خدمات الانترت على اكبر

نطاق دون الاعتناء بمسائل الامان، بشكل كاف. الاعتناء بمسائل الامان في البدايات قد يكون مكلفا الا ان تأخر الالتفات لهذا الجانب قطعا سيكون اكثر تكلفة مستقبلا. الاستراتيجيات والخطط الدفاعية لابد من الاهتمام بها ابتداءا مثل ما هو الحال فيما يتعلق بسن القوانين وتطوير سلطة انفاذ القانون والقائمين على مكافحة الجريمة الالكترونية (TWG 2001) .

ثانيا : اعداد المستخدمين Number of Users

مع الايام تذداد اعداد مستخدمي خدمات الانترنت. وبالرغم من انه من غير المعروف ما هي اعداد مستخدمي الانترنت لاغراض الجريمة، الا ان التصور الاقل لهذه الاعداد لن ينقص عن المليون شخص اذا جاز لنا استخلاص هذا التصور من معلومة ان 40% من سكان الكرة الارضية يتمتعون بمدخل لخدمات الانترنت. وقد سبب تذايد اعداد مسنخدمي الانترنت مصاعب عديدة لجهات انفاذ القانون (Bace 2003) .

ثالثا : توفر الاجهزة ومداخل الانترنت

ارتكاب الجريمة الإليكترونية يحتاج فقط توفر الجهاز (hardware) والبرنامج (software) والمدخل للانترنت (internet access) لارتكاب الجريمة بنجاح ودون تعقيد.

هناك الكثير من المغريات التي تمكن الناس في الدول الاقل نموا من ارتكاب اخطر الجرائم، باستخدام اجهزة رخيصة او مستعملة لارتكاب الجريمة الالكترونية اذ ان معرفة كيفية ارتكاب الجريمة هي المحفذ وليس نوع وتقدم الجهاز .

ارتكاب الجريمة الالكترونية يصبح اسهل من خلال استخدام البرامج المتخصصة كما انه في الامكان

الحصول على الادوات البرامجية من الانترنت التي تمكن من الوصول للمنصات المفتوحة او اختراق كلمات المرور. نسبة لانتشار تقنيات التواصل واحد لواحد (peer to-peer) وتقنيات المطابقة (mirroring techniques) فان انتشار هذا النوع من التكنلوجيا يصعب احتواؤه (Mohay 2003) .برغم ارتفاع تكلفة الانترنت الا ان وتيرة تذايد مستخدمي الانترنت ظلت على الدوام مرتفعة في الدول المتقدمة واخذة في الارتفاع في الدول الاقل نموا. تسعى جهات انفاذ القانون دائما لوضع الضوابط لاستخدامات الانترنت الا ان المهتمين بحقوق الانسان والحريات الخاصة دائما ما يقفون عائقا امام هذه الضوابط، برغم ان هذه الضوابط تساعد على مكافحة الجريمة وتسريع اجراءات التحقيق. استقر الرأي على ان ضوابط استخدام الانترنت فيها انتهاك لحقوق الانسان وقد حكمت المحكمة الاوروبية في عدد من قضايا الاعلام ان مبدأ حرية التعبير لا ينطبق فقط على محتوى المعلومات وانما يشمل ذلك وسائل تبادل المعلومات .

رابعا : توافر المعلومات:

اتاح الانترنت ملايين الصفحات التي توفر احدث المعلومات عن شتى الامور.

اصبح اي فرد قادرا على المشاركة ويملك صفحة او يمكنه النشر. تتعدد الامثلة التي تؤكد هذا القول وأشهر الامثلة وكيبيديا (Wikipedia) (تتيح النشر لكل من يستطيع المشاركة بالنشر فهي موسوعة متاح فيها النشر لكل شخص.)

حققت محركات البحث القوية نجاحات شكلت الجزء الاكبر من نجاحات الانترنت، كما انها مكنت مستخدمي الانترنت من الوصول الى ملايين الصفحات في اوقات قياسية. التكنلوجيا المتقدمة التي جاءت مع الانترنت تم استخدامها لاغراض مشروعة وغير مشروعة .

وفر الانترنت المعلومات في شتى ضروب المعرفة وهو امر اصبح متاحا للاستخدام لكل الناس دون شروط، مثل ان ينوي المجرم القيام باي نوع من الهجوم، فنجده متمتعا بكل المعلومات التي يحتاجها لصنع القنبلة من المواد العادية المتوفرة في اقرب المحال المجاورة لمكان اقامته (Reed 2004) .

خامسا : وسائل التحكم في الانترنت:

تحتاج كل شبكات الاتصال، مثل الهواتف النقالة وغيرها الى ادارة مركزية ومقاييس فنية تتحكم في تشغيلها. اصبح يتردد الان نوع من النقاش حول العالم ان الانترنت لا يختلف عن بقية وسائل الاتصال. وهو بدوره مثلها يحتاج الضوابط التشغيلية. بدأت جهود ملحوظة في هذا الخصوص تمثلت في المواصفات التي يتطلبها القانون فيما يتعلق بمركزية التحكم في الانترنت.

صمم الانترنت في الاساس كشبكة عسكرية، قائمة على لامركزية شبكته. يسعى الانترنت للحفاظ على الوظائف الرئيسية التى قام لانجازها سليمة حتى لو تعرض لاي هجوم، وهو امر يجعل انه من الصعوبة بمكان التفكير او انجاز تحكم مركزي فيه. لان الانترنت صمم في الاساس لاغراض لا علاقة لها بالتحقيق الجنائي (UN 2000).

ازدادت استخدامات الانترنت المدنية، واصبح واضحا تحول الاستخدامات من العسكرية، الى الاستخدامات

المدنية، الا ان المشكلة تكمن في ان الشبكة الخاصة بالانترنت، قد انشئت على اساس عسكري ولاغراض عسكرية، لذا فان ادوات التحكم المركزي غير متوفرة من الاساس ، ولا مجال لتنفيذها بأثر رجعي (retrospective) لاعادة تصميم شبكة الانترنت (redesign of network).

غياب اجهزة التحكم المركزي في الانترنت جعل مهمة التحقيق في الجريمة الإليكترونية امرا في غاية الصعوبة.

من ابرز امثلة مشكلة غياب اجهزة التحكم المركزي هي قدرة مستخدمي الانترنت على استخدام خدمات (filter technology) اتصالات مشفرة (encrypted) .

بعض الحلول التي يمكن تصورها لمنع دخول مستخدمي خدمة الانترنت تتمثل في قدرة مقدمي الخدمة (service providers) على منع المستخدمين من الدخول الى المواقع التي تحوي المواد غير القانونية باغلاق المواقع الا ان هذا الاغلاق يمكن تفاديه ايضا باستخدام مواقع غير مسماة (anonymous) توفر اتصالا مشفرا بين الموقع ومركز الخدمة (Service Center)، وهذا بدوره يقود الى عدم القدرة على منع دخول هذه المواقع لان طلبات الدخول لهذه المواقع ترد مشفرة الامر الذي يمنع القدرة علي فتحها بواسطة مقدم الخدمة.

سادسا : الابعاد الدولية

غالبا ما تتأثر اكثر من دولة بعملية نقل المعلومات عبر الانترنت. فاذا ما تم استخدام التوجيه الامثل (optimal routing)لاغلاق الروابط المباشرة مع الدولة بشكل مؤقت فان المستخدمين يمكنهم عند محدودية نقل المعلومة في دولة المصدر فيمكن خروج

المعلومات وعودتها للدولة مرة اخرى بموجهات من خارج اقليم الدولة .

يستدعي التحقيق في الجريمة الالكترونية سرعة التحرك، وسرعة بدء التحقيق لان ازالة اثار الجريمة لا تحتاج وقتا طويلا. وفي ذات الاطار فان سلطة التحقيق تكون محدودة بقوانين الدول. كما ان الكثير من خدمات الانترنت تعتمد على اجهزة تعمل في دولة اخرى هي بالطبع خارج حدود الدولة التي وقعت الجريمة الالكترونية في اقليمها.

وهذه الحقائق تجعل قضية التعاون بين الدول قضية محورية لمكافحة الجريمة الإليكترونية (Howard 2004).

يسعى مرتكبي الجريمة الإليكترونية لتفادي ارتكاب الجريمة في الدول التي تملك تشريعات قوية لمكافحتها، اي السعي كأمر طبيعي لتفادي الوقوع في براثن القانون وبالتالي ارتكاب الجريمة حيث تكون نصوص وقواعد التجريم اقل شدة واضعف احكاما (Kerr 2005).

جنوح مرتكبي الجريمة الإليكترونية الى هذا المنحى يقود على الدوام الى ارتكاب الجريمة الإليكترونية بصورة اكثر اضرارا، بينما يجد مرتكبيها الفرصة سانحة للافلات بجرائمهم، ويرجع ذلك لصعوبة التحدي الذي يواجه القائمين على فرض القانون، وابتداءا جهة التحقيق ثم من بعدها والاكثر خطورة القضاء .فان موقف القضاة من تكنلوجيا السايبر اكثر سلبية لعدم تلقيهم التدريب الكافي للتعامل مع الدليل الالكتروني (Punja 2008). فضلا عن ان الاداء الاوتماتيكي) للانترنت يساعد جهات تقديم خدمة الانترنت على توفير الخدمة بقيمة اقل.

16.2 الملخص و المناقشة :

خلص البحث الى انه لا يوجد تعريف واحد متفق عليه بشكل شائع للجريمة الالكترونية ، الا انه من خلال الاستعراض السابق فنحن نتفق مع القول بان التعريف الجامع هو ان الجريمة الالكترونية هي أي نوع من النشاط غير القانوني الذي يحدث عبر الوسائل الرقمية وتعد سرقة البيانات ، واحدة من أكثر أنواع الجرائم الالكترونية شيوعا ، ولكن الجريمة الالكترونية يمكن ان تشمل أيضا مجموعة واسعة من الأنشطة الضارة ، مثل البلطجة الإلكترونية أو زرع الديدان أو الفيروسات .(Iovation 2020)

من حيث الوسيلة فان الجريمة الالكترونية تعرف بأنها جريمة يكون فيها الكمبيوتر هو موضوع الجريمة (القرصنة أو التصيد أو البريد العشوائي) أو يتم فيها استخدام الكمبيوتر كأداة لارتكاب الجريمة (استغلال الأطفال و جرائم الكراهية والإباحية). (UNODC 2013)

الجهود التي بذلت في سبيل الوصول الى تعريف واحد للجريمة الإليكترونية خلصت الى انه من الصعب الوصول إلى تعريف واحد للجريمة الإليكترونية.

فضل المعرفون وضع تعريف للجريمة الالكترونية يمكن الحكم عليه بانه قد مال الي الاتصاف بالعمومية دون تحديد للتفاصيل تحسبا للتطور التقني والعلمي في المستقبل اضافة الى حداثة دراسة الجريمة الالكترونية عموما. وفقا لذلك رجح القول بان الجريمة الالكترونية هي كل فعل يستهدف الفضاء الالكتروني أو استخدمت التكنولوجيا الحديثة في ارتكابه او ارتكب عبر الوسائط الالكترونية.

تم اتخاذ تدابير مضادة عامة في مكافحة الجريمة الالكترونية ، مثل التدابير القانونية في التدقيق في التشريعات والتدابير التقنية في تتبع الجرائم على الشبكة العنكبوتية ، ومراقبة محتوى ما هو متوفر على الإنترنت ، واستخدام الادلة الجنائية الخاصة بالكمبيوتر، والتشفير، إلخ. نظرا لعدم تجانس تطبيق القانون والإجراءات التقنية المضادة للبلدان المختلفة ، ستركز هذه الدراسة عند منافشة الجهود التشريعية بشكل أساسي على المبادرات التشريعية والتنظيمية للتعاون الدولي.

حدد البحث التحديات العامة التي تواجه مسألة التحقيق في الجريمة الالكترونية وتقديم مرتكبيها للمحاكمة وذلك على النحو التالي:

اولا: الاعتماد على تكنلوجيا الاتصال Reliance on ICTs

ثانيا : اعداد المستخدمين Number of Users

ثالثا : توفر الاجهزة ومداخل الانترنت Devices& access to the internet

رابعا : توافر المعلومات Availability of Information

خامسا : غياب وسائل التحكم في الانترنت Missing mechanisms of control

سادسا : الابعاد الدولية International Dimensions

يسعى مرتكبي الجريمة الالكترونية لتفادي ارتكاب الجريمة في الدول التي تملك تشريعات قوية لمكافحتها ، اي السعي كأمر طبيعي لتفادي الوقوع في براثن القانون وبالتالي ارتكاب الجريمة حيث تكون نصوص وقواعد التجريم اقل شدة واضعف احكاما .

جنوح مرتكبي الجريمة الالكترونية الى هذا المنحى يقود على الدوام الى ارتكاب الجريمة الالكترونية بصورة اكثر اضرارا، بينما يجد مرتكبيها الفرصة سانحة للافلات بجرائمهم، ويرجع ذلك لصعوبة التحدي الذي يواجه القائمين على فرض القانون، وابتداءا جهة التحقيق ثم من بعدها والاكثر خطورة القضاء .

يساعد الاداء الاتوماتيكي (automation) للانترنت جهات تقديم خدمة الانترنت على توفير الخدمة بقيمة اقل.

تسعى جهات انفاذ القانون دائما لوضع الضوابط لاستخدامات الانترنت الا ان المهتمين بحقوق الانسان والحريات الخاصة دائما ما يقفون عائقا امام هذه الضوابط.

لا تشجع إجراءات الدفاع الجنائي ضد الأعمال والسلوك من قبل مجرمي الإنترنت الضحايا على الإبلاغ عن الحالات بل على العكس من ذلك فان الحجة تذهب في الاتجاه الآخر.

III. الباب الثالث

أثر تطور الانترنت وقضايا الخصوصية

1.3 الـــمـــــقد مـــــة :

2.3 الجريمة الالكترونية وقضية الخصوصية :

هناك العديد من مخاوف الخصوصية المحيطة بالجرائم الإليكترونية ، و يبدو ذلك اكثر وضوحا عندما يتم اعتراض المعلومات السرية أو الكشف عنها بشكل قانوني أو غير ذلك. (Gavison 1984)

في كل الاحوال يمكن تحديد مزيد من الجرائم الالكترونية المتعلقة بالخصوصية اذ انه و من المنظور الاجتماعي وتعريف الجرائم الإليكترونية ضد المرأة يبدو انتهاك الخصوصية واضحا في الجرائم الموجهة ضد النساء على وجه الخصوص مع وجود دافع تعمد تسبيب ضرر للضحية نفسيا وجسديا ، وذلك باستخدام شبكات الاتصالات الحديثة عبر الانترنت والهواتف المحمولة (Morgan 2016)

على الصعيد الدولي ، تشارك كثير من الجهات الفاعلة الحكومية وغير الحكومية في جرائم الإنترنت، و المثال الاوضح لذلك التجسس والسرقة المالية والجرائم الأخرى عبر الحدود.

يشار أحيانا إلى جرائم الإنترنت التي تعبر الحدود الدولية وتتضمن أعمال دولة واحدة على الأقل باسم الحرب الإلكترونية (cyberwarfare) (Kerr 2005).

قدر تقرير برعاية McAfee ، نشر في عام 2014 ، أن الأضرار السنوية التي لحقت بالاقتصاد العالمي بلغت 445 مليار دولار . (Europol 2020)

وقع فقدان ما يقرب من 1.5 مليار دولار في عام 2012 بسبب الاحتيال عبر الإنترنت في بطاقات الائتمان والخصم في الولايات المتحدة. في عام 2018 ، خلصت

دراسة قام بها مركز الدراسات الاستراتيجية والدولية (CSIS) ، بالشراكة مع McAfee ، إلى أن ما يقرب من 600 مليار دولار ، أي ما يقرب من واحد في المئة من الناتج المحلي الإجمالي العالمي ، تفقد بسبب الجرائم الإلكترونية كل عام. (Europol 2020)

3.3 ظهور وتطور الانترنت Internet Evolution

اسهم تطور الانترنت في ابتداع شكل جديد من اشكال التعامل التجاري والاجتماعي فاصبحت منصة الانترنت ذاخرة بالمصالح والتعاملات التجارية وغيرها مما ادي لظهور انواع جديدة من التعديات على الحقوق والافعال التي يمكن ان تعد في حكم الجرائم لذا خصصنا هذه الجزئية من البحث التي نتعرض فيها بقليل من التفصيل لظهور وتطور الانترنت وكيفية عمله وعمل الضوابط المتعلقة به فقد كان له الاثر الاعظم على الجريمة بشكل عام والجرائم المتعلقة بالكمبيوتر والجرائم الالكترونية بشكل خاص .

بعد إطلاق القمر الصناعي الروسي سبوتنيك (Sputnik)، بدأ كثير من الأمريكيين التفكير بجدية أكبر في العلوم والتكنولوجيا .

أضافت المدارس الامريكية دورات في الكيمياء والفيزياء وحساب التفاضل والتكامل.

أخذت الشركات الامريكية المنح الحكومية واستثمرتها في مجال البحث العلمي والتطوير وشكلت الحكومة الاتحادية نفسها وكالات جديدة (NASA) وإدارة وكالة مشاريع البحوث المتقدمة للدفاع (ARPA) لتطوير تكنولوجيا عصر الفضاء مثل الصواريخ والأسلحة وأجهزة الكمبيوتر (GROUP 2020).

4.3 ولادة وظهور التجارة الالكترونية:

نتج الجهد الذي تمخض عنه ولادة الانترنت بشكله المتطور من ان العلماء والخبراء العسكريين الاميريكيين اصيبوا بالقلق، خصوصا حول ما قد يحدث في حال وقوع هجوم سوفياتي على نظام الهاتف الاميركي، اذ يمكن لصاروخ واحد فقط، أن يدمر شبكة كاملة من الخطوط والأسلاك التي جعلت كفاءة الاتصالات لمسافات طويلة ممكنة.

في عام 1962 تم خلق شبكة في مجرة واحدة، من الكمبيوترات تستطيع التواصل مع بعضها (Galactic Network) (J Khakurel 2016) .

في العام 1969 برز اسلوب جديد لارسال المعلومات من كمبيوتر الى اخر (Packet Switching) بتقسيم المعلومات الى قطاعات (Blocks) قبل ارسالها الى الكمبيوتر الاخر، فاصبحت المعلومات تاخذ طريقها بدون التأثر بالقطاعات الاخرى، وبدون التعرض لخطر الاعتراض.

نظام الشبكة الحكومية التي تعرف الان باربانت (ARPAnet) اوصلت اول معلومة لها في العام 1969 (node-to-node) ، بين كمبيوتر في الكا (Ulca) والاخر في ستانفورد (Stanford). كلا الجهازين بحجم غرفة..

بنهاية العام 1969ارتفع عدد الكمبيوترات الى اربعة كمبيوترات. خلال الاعوام 1970و1971 تمت اضافة جامعة لندن (London's University College)، وسبقتها جامعة هاواي (University of Hawai) ، وبتزايد عضوية نظام (packet-switching) اذدادت صعوبة تكامل عضويتها في شبكة عالمية واحدة.

في العام 1970 بدأ توصيل الكمبيوترات ببعضها في شبكات صغيرة (TCP) للسيطرة على الانتقال (Transmission Control Protocol) عن طريق هذا الاختراع اي برتكول السيطرة على الانتقال، ثم اضافة برتكول اخر هو برتكول الانترنت، اكتمل اختراع مايسمى اليوم (TCP/IP) وهو ما قدم الكبيوترات لبعضها البعض، في الفضاء الافتراضي. في شبكة عالمية استعملت في تبادل الملفات حول العالم خلال الثمانينات J).

Khakurel 2016)

في العام 1991 تغير وضع الانترنت مرة اخرى الى Web وليس ناقلا للملفات فقط، بل في امكان كل المشاركين البحث فيه والحصول على ما هو متوفر فيه من معلومات وهو الانترنت الذي نعرفه اليوم.

وفي العام 1992 ظهر متصفح موسياك (Mosiac)، و الذي اصبح اسمه فيما بعد نت اسكيب (Netscape)، وقد مكن هذا المتصفح مستخدميه من تصفح شبكة الانترنت، ومكنهم من رؤية الكلمات والصور في ذات الصفحة لاول مرة، وتم استخدام ادوات التصفح (scrollbars) و (clickable links)وفي ذات العام قرر المشرع الامريكي التصريح بالانترنت كوسيلة من وسائل التجارة، فاستجابت الشركات بشتى اشكالها لقرار المشرع بتفعيل صفحاتها على الانترنت كبداية لازدهار التجارة الالكترونية، التى تلتها شبكات التواصل الاجتماعي ((1997) Wilding).

5.3 مـــلـــكيـــة الانـــتـــرنـــت:

الانترنت ليس مملوكا لجهة معينة وانما هو شبكة عالمية مربوطة بالعديد من طرق التوصيل مثل كيبل الألياف البصرية (Fiber Optic) والساتلايت (Satellites) و غيرها من وسائل التوصيل بينما تتوفر خدمة الانترنت بواسطة جهات مختصة (ISP) مثل (Comcast) في امريكا وسوداني (Sudani) في السودان وغيرهما .

ليس للانترنت مركز فهو غير مركزي وكل نظام معروف في الانترنت بالعنوان الذي يحمله (IP) الذي تمنحه مؤسسة الانترنت لتخصيص الاسماء والارقام ايكان (ICANN).

تعمل مؤسسة ايكان (ICANN) علي مساعدة عدة جهات من الجهات العاملة على تنظيم الانترنت فهي تعمل على مساعدة سلطة (IANA) للقيام بعملها نحو الخدمات الفنية المفتاحية والاساسية المتعلقة بدليل العناوين، نطاق نظام الاسماء (DNS) ،تشمل مهام (IANA):

اولا: المستوى الاعلى للمعامل الفني للبروتوكول شاملا ادارة منطقة معامل التوجيه (ARPA).

ثانيا : ادارة مسؤليات معينة مرتبطة بنظام اسماء النطاق (DNS) المتعلق بادارة منطقة الجزرمثل مستوي النطاق الاعلى ورمز الدولة (ccTDL) و (gTDL)

ثالثا : مصادر ترقيم مواقع الانترنت. رابعا تشمل مهام (IANA) ايضا خدمات اخرى.(ICANN 2020)

معلوم ان الانترنت لا نهائي، الا انه محدود بعدد الانظمة المرتبطة به، و يتكون من خادم وعميل (Server & Client).

يقوم الخادم بنقل الملفات المكونة من لغات خلفية (Backend) مثل (PHP) ولغات العرض (Frontend) مثل (JavaScript) ولغات العلامة مثل (HTML) لعرض الملفات عبر الانترنت، من الخادم للعميل عن طريق برتكولي (HTTP) (HTTPS) حيث يقوم المتصفح Web) (Browserيتحويل الملفات الى واجهة مقرؤة والمقصود هنا هو الشبكة العنكبوتية web وليس الانترنت الذي يخدم برتكولات كثيرة اخرى مثل(SSH, FTP, XMPP, IRC) (ICANN 2020)

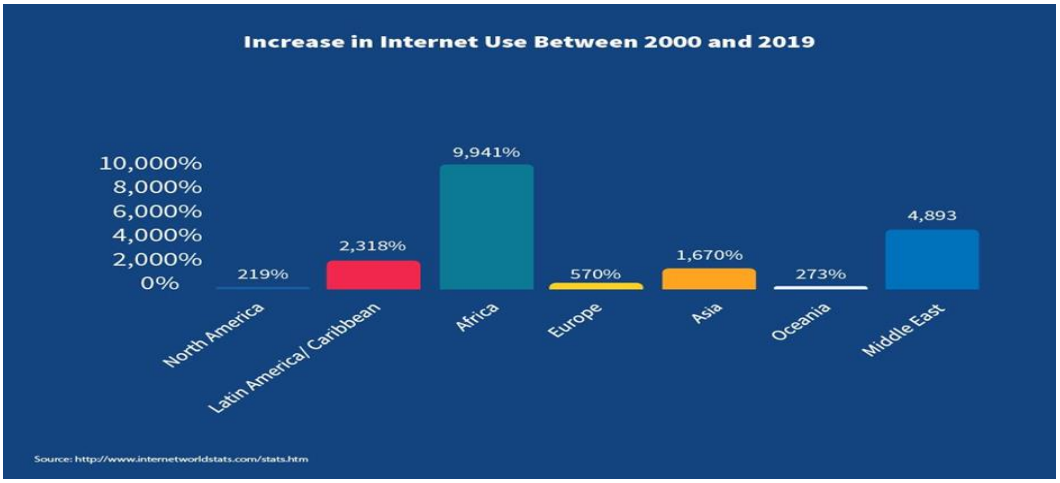
6.3 مستخدمي الانترنت حول العالم :

يتزايد اعتماد الناس في جميع أرجاء العالم يوما بعد آخر على شبكة الانترنت العالمية في كل أعمالهم وتواصلهم الاجتماعي وتفاصيل حياتهم اليومية؛ حيث كشفت إحصاءات عالمية حديثة زيادة قاعدة مستخدمي الانترنت حول العالم لتسجل مع نهاية النصف الأول من العام 2019 قرابة 4.54 مليار مستخدم، أكثر من نصفهم يتواجدون في قارة آسيا.

وأظهرت الأرقام العالمية التي نشرها مؤخرا موقع "انترنت وورلد ستاتيستك" -المتابع لتطورات مؤشرات خدمات الانترنت حول العالم- أن عدد مستخدمي الإنترنت حول العالم، ومع تسجيله هذا المستوى، فإن نسبة استخدام الشبكة العنكبوتية ترتفع الى 58.8 % من عدد سكان العالم المقدر مع نهاية النصف الأول من

العام الحالي بحوالي 7.7 مليار نسمة (http 2020). انظر الشكل (3-1)

الهواتف الذكية، وانتشار شبكات الإنترنت عريضة النطاق من الجيلين الثالث والرابع وشبكات الفايبر، فيما تستعد أسواق العالم في الوقت الراهن وتتحضر لاستقبال وإطلاق شبكات الجيل الخامس بسرعات عالية جدا تتلاءم وتطبيقات الثورة الصناعية من الذكاء الاصطناعي ومفاهيم المدن الذكية والمنازل الذكية وتطبيقات الانترنت والهواتف الذكية في القطاعات الاقتصادية كافة. (ICANN 2020)



1

شكل 1.3 معدل زيادة مستخدمي النت عالميا (http 2020)

خلال فترة الأعوام العشرة الماضية، زاد استخدام وانتشار الإنترنت بشكل لافت، لا سيما وأن هذه الفترة شهدت طفرة استخدام الهواتف الذكية التي أسهمت في دخول أعداد كبيرة من الناس في سجلات الخدمة، فالإحصاءات العالمية تشير إلى أن عدد مستخدمي الشبكة بلغ في نهاية 2007 -وهو العام الذي يعد بداية انتشار الهواتف الذكية- حوالي 1.3 مليار مستخدم فقط. ويرى مراقبون أن شبكة الإنترنت، التي نشأت قبل حوالي 51 عاما عندما جرى إرسال أول رسالة

إلكترونية ناجحة بين جهازي حاسوب، تعد من أهم منجزات القرن العشرين (المبيضين 2019) وشهدت خلال فترة التسعينيات منه طفرة واستخداما متزايدا لا حدود له في مضمار نقل البيانات والأخبار والمعلومات، ويمكن تعريفها ببساطة بأنها عبارة عن مجموعة من شبكات الحواسيب المتصلة معا عن طريق أسلاك نحاسية وكابلات ألياف بصرية وتوصيلات لاسلكية، لتصبح وسيلة يستخدمها الأفراد، والمؤسسات، للتواصل، وتبادل المعلومات.

إلى ذلك، أظهرت البيانات العالمية أن قارة آسيا جاءت في المرتبة الأولى عالميا بأكبر عدد من مستخدمي الانترنت نهاية النصف الأول من العام 2019 بحوالي 2.3 مليار مستخدم لتشكل نسبة تصل الى 50.7 % من إجمالي مستخدمي الانترنت حول العالم. وذكرت البيانات أن عدد المستخدمين في قارة أوروبا سجل قرابة 728 مليون مستخدم في نهاية النصف الأول من العام 2019 بنسبة تصل الى 16 % من قاعدة المستخدمين العالمية.

وأشارت الى أن عدد المستخدمين في القارة السمراء "أفريقيا" حوالي 523 مليون مستخدم مستحوذة على حصة بلغت 11.5 % (المبيضين 2019) من إجمالي مستخدمي الانترنت حول العالم.

وقالت الأرقام إن قارة أميركا اللاتينية استحوذت على حصة تصل الى 10 % من إجمالي مستخدمي الشبكة العنكبوتية حول العالم نهاية النصف الأول بعدد مستخدمين بلغ حوالي 453 مليون مستخدم.

وأشارت البيانات إلى أن عدد مستخدمي الإنترنت في أميركا اللاتينية حوالي 438 مليون مستخدم، فيما بلغ عدد المستخدمين في أميركا الشمالية حوالي 345

مليون مستخدم. وبحسب البيانات العالمية، بلغ عدد مستخدمي الإنترنت في قارة أميركا الشمالية حوالي 328 مليون مستخدم بنسبة تصل الى 7 % من إجمالي مستخدمي الانترنت في العالم. (المبيضين 2019)

. وبلغ عدد مستخدمي الانترنت في منطقة الشرق الأوسط نهاية النصف الأول 176 مليون مستخدم، مستحوذة على حصة تصل الى 4 % من إجمالي مستخدمي الانترنت في العالم. محليا، وكما هو الحال في معظم أسواق الاتصالات حول العالم، تشهد استخدامات الإنترنت في كل دول العالم خصوصا العالم الثالث توسعا وانتشارا كبيرين، مع انتشار شبكات الجيلين الثالث والرابع؛ إذ تظهر أرقام رسمية أن نسبة الأسر المقتنية لخدمة الانترنت في السودان تتجاوز 79% مشاركة في التطبيقات المعروفة Facebook، Twitter، LinkedIn و WhatsApp والراجح ان ارقاما قريبة مما اوردنا تتواجد في بقية الدول. (UN 2020ع)

7.3 جـــــرائـــــم الإنـــــترنـــــت:

جرائم الانترنت من الجرائم التي برزت مع تطور وانتشار استخدام الانترنت، واصبحت تشكل هاجسا ومهددا حقيقيا. (Svedman 2020) هناك العديد من المشكلات والصعوبات العملية والفنية والإجرائية التي تظهر عند ارتكاب أحد جرائم الإنترنت، ومن هذه المشكلات:

أ. صعوبة إثبات وقوع الجريمة.

ب. صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي.

ت. صعوبة إلحاق العقوبة بالجاني المقيم في الخارج.

ث. تنازع القوانين الجنائية وبروز مشاكل اقليمية القوانين.

ج. صعوبة التوصل إلى الجاني.

ح. القصور في القوانين الجنائية القائمة.

خ. افتراض العلم بقانون جميع دول العالم.

د. اختلاف التشريعات حول الفعل المجرم فقد يختلف التكييف القانوني للفعل من بلد لاخر.

ذ. الافتقار للتعاون الدولي المؤثر.

8.3 أهم صور الاعتداء الجنائي في الإنترنت:

تتمثل أهم صور الاعتداء الجنائي في الجرائم الالكترونية في التالي :

أ. جرائم النصب والاحتيال عبر الإنترنت.

ب. جرائم سياسية عن طريق التجسس على الدول عبر الإنترنت، ومحاولة اختراق أنظمتها العسكرية .

ت. جرائم التدمير والعبث بأنظمة الحاسب، وذلك عن طريق الدخول على الشبكة وتدمير برامج الحاسب، أو نشر مواقع تخريبية وفيروسات.

ث. جرائم سرقة حقوق الملكية الفكرية عن طريق نسخ البرامج الأصلية وتسويقها أو استخدامها دون إذن مسبق، مما يعرض الشركات المنتجة لهذه البرامج للكثير من الخسائر المالية.

ج. الجرائم المتعلقة بإعادة إنتاج المعلومات المسجلة عبر الإنترنت بصورة غير مشروعة، أو تقليدها.

ح. سرقة المعلومات بحسبها مجرد معلومات معنوية.

خ. جرائم السب والقذف عبر الانترنت.

د. جرائم الاعتداء علي الحياة الخاصة للأفراد.
ذ. جرائم الاباحية والدعارة والجرائم ضد الاطفال.
ر. التهديد ونشر المعلومات الكاذبة.
ز. انتحال الشخصية.
س. اهانة المعتقدات الشخصية والدينية.

9.3 قرصنة الفضاء الإلكتروني

قسم بعض الباحثين في مجال المعلومات قرصنة الفضاء الإلكتروني إلى نوعين رئيسيين:

الأول: وهم ما يطلق عليهم الهاكرز (Hackers)، وجلهم يستهدف بالأساس إلحاق الأذى بالمحتويات التي تضمنتها الذاكرات والدوائر الإلكترونية في شبكات الحواسيب، سواء الخاصة بالمؤسسات والشركات أو الأفراد، لمجرد إثبات أنهم قادرون على هذا، لذلك فهم ينظرون إلى أنفسهم على أنهم أبطال أذكياء، بينما لا يعتبرهم الآخرون كذلك.

الثاني: وهم لصوص ومافيا السرقات الإلكترونية عبر الإنترنت، وهدفهم الرئيس هو سرقة أموال أو بيانات أو أسرار، تتضمنها شبكات الحاسب بعينها، وذلك باستخدام تقنيات خاصة بالاختراقات المعلوماتية. (Computer Breaches)

وتتسم هذه النوعية من الجرائم الإلكترونية بسهولة ارتكابها، ما لم تكن ثمة احتياطات وتقنيات مضادة قوية تقف سدا منيعا أمامها، وهي أيضا تمتاز بسهولة إخفاء معالمها.

10.3 التعاون الدولي و الجريمة الالكترونية :

تكنلوجيا السايبر (Cyberspace Technology) اصبحت هي المسيطر على غالبية الانشطة الانسانية.الا انه وبرغم ذلك يمكن القول بان هذه التكنلوجيا مازالت تتلمس طريقها الى كل المجالات. فهذه التكنلوجيا حتى الان لم تكمل رحلتها الى كل ما يمكنها الوصول اليه، اذ ما زال الدرب امامها طويلا خلافا لبقية العلوم التي تكاد تكون قد وصلت مرحلة النضج، سيما فيما يتعلق بتناول المسائل الاخلاقي والقانونية والامنية وقضايا الخصوصية وقضايا الملكية الفكرية (Intellectual Property) فضلا عن مشكلة سرعة التطور الذي يحدث وباستمرار مدهش في المجال التكنلوجي، ثم ان المفاهيم المتعلقة باخلاقيات المهنة بالنسبة لقضايا السايبر لم تقترب من التوحد حتى في المجال الواحد وبدون النظر والبحث عن توحد المبادئ العامة يمكن ملاحظة نسبية (Proportional) المعايير واختلافها من مؤسسة الى اخرى حتى ان البعض يرى ان ظروف كل مؤسسة هي التي تحدد المعايير التي تنظر بها كل مؤسسة للقضايا المتعلقة بالقضايا موضوع البحث ودون سائر انواع العلوم نجد ان تكنلوجيا السايبر ما زالت تتمدد افقيا ورأسيا و في كل الاتجاهات بشكل يجعل التأريخ او رصد تطورها امرا في غاية الصعوبة والتعقيد فضلا عن التأسيس باستخدام ما يصلح لعملية الضبط الاخلاقي والقانوني في عموم مستجدات المسائل المستقبلية الخاصة بالجانب الفني في قضايا الاثبات والتحقيق وجمع البينات (Evidence Collection) .

بسبب الانتشار المخيف للجرائم الإليكترونية كظاهرة عالمية، والتهديد المستمر لكل النشاط الانساني،

وللمصالح المرتبطة بالتقنيات الجديدة، اصبح من الضروري البحث عن كيفية إيجاد حلول فعالة، واتخاذ تدابير وقائية، وردعية لوقف التهديد المتصاعد للجريمة الإليكترونية، التي باتت تهدد اقتصاديات وأمن واستقرار الدول.

بعد تطور الجريمة الإليكترونية من إطارها الكلاسيكي المعروف، إلى التقنية العلمية الحديثة، هددت الجريمة الإليكترونية التجارة إلاكترونية، التي اصبحت رائجة وسادت كل التعاملات بين الافراد والشركات والدول، وهو ما اصطلح على تسميته بالاقتصاد الرقمي.

اثارت الشكاوى الرسمية التي اعتمدها المركز العالمي لشكاوى الانترنت منذ بدايتها كثيرا من الرعب، فقد بلغت تكلفتها سنة 2000 خسارة مادية قدرت بـــ12 بليون دولار جراء النتائج التدميرية التي تسببت فيها فيروسات إتلاف برامج المعلوماتية. وقد قدرت مجمل الشكاوى الرسمية التي قدمها الضحايا للمركز بـــ 275284 شكوى في ذلك العام وحده، (Hayes 2013)

في كثير من الدول خصصت وسائل مختلفة للتبليغ عن جرائم الانترنت ولهذا ومن أجل حماية فعالة لبرامج المعلوماتية وقاعدة البيانات كان لابد من اعتماد السبل القانونية الوقائية من خلال الدخول لقواعد البيانات عن طريق كلمات المرور و تجنب استخدام كلمات السر المكونة من كلمات يمكن حزرها مع الحرص على تغييرها دوريا كل مرة إن تطلب الأمر ذلك.

تشمل الجوانب الوقائية، تكثيف برامج الرقابة على نوادي ومقاهي الانترنيت، والعمل على ترصد وحجب المواقع الإباحية كما هو الحال في كثير من الدول

وضمنها السودان، مع اعتماد برامج خاصة مضادة للفيروسات التدميرية واستعمالها بشكل مستمر. (Morgan 2016)

جمعت الشبكة العالمية الملايين من اجهزة الكمبيوتر المتمركزة في العديد من دول العالم مما اتاح لها تبادل والحصول على المعلومات.

هذا الانتشار والاتصال وفر مناخا جيدا لعملية ارسال النقود والمعاملات البنكية والتجارية، فالى جانب الفائدة العظيمة في هذا الجانب نجد انه قد وفر مناخا افضل لنوع جديد من الجريمة العالمية، وبالتالي فان مطبقي القانون في يومنا هذا اصبحوا مواجهين بمكافحة والتحقيق في جرائم تكنلوجيا الكمبيوتر العابرة للحدود. (Shinder 2010)

تشكل الجريمة الإليكترونية تهديدا كبيرا كعمل غير مشروع فالانترنت اعطي المجرمين

القدرة على اخفاء الشخصية وانعدام الحواجز الحدودية جعل الانترنت سلاحا فعالا في ايدي المجرمين بشكل حول التحقيق ومنع الجريمة الى صداع دائم للقائمين على تطبيق القانون، لان مجرمي الكمبيوتر دائما ما يرتكبون الجريمة في الفضاء الافتراضي، من دول اخرى مما يحتم التعاون مع مطبقي القانون في الدول الاخرى، وهو امر من غير الممكن ان يحدث في كل الاحوال (Sommer 2004) .

تمهيدا لمناقشة موضوع التنسيق والتعاون الدولي الخاص بمكافحة الجريمة الإليكترونية سنقوم بتقسيم الجهود الدولية الى:

I. جهود احترافية. (Professional)

II. جهود اقليمية. (Regional)

III. جهود عالمية متعددة الجنسيات.(Multinational Global Actions)

بالنسبة للقوانين التي تعالج الجريمة التقليدية والنص عليها وفرض العقوبة على ارتكابها نجدها دائما قوانين محلية (Local) ، اقليمية (Regional) ، او وطنية (National) وهو امر كثيرا ما يعرقل مسيرة مكافحة الجريمة الإليكترونية ، لما تتسم يه الجريمة الإليكترونية من طبيعة عابرة للحدود. وقد حتمت هذه الطبيعة النظر والبحث في مسألة خلق الية قانونية عالمية للمساعدة في مكافحتها.

11.3 التشريع المحلي والتنسيق العالمي:

ستتناول هذه الجزئية من البحث اربعة من محاور مكافحة الجريمة الإليكترونية :

أ.جهود المتخصصين القائمين على فرض القانون .

ب. الجهود الاقليمية

ت. الجهود متعددة الجنسيات.

ث. الجهود المبذولة على مستوى العالم.

كما انه يمكن تقسيم الجهود العالمية وفقا للموضوع الى تقسيمات اضافية تشمل:

رفع درجة الاستعداد الامني على المستويين المحلي والعالمي. (Hayes 2013)

أ.زيادة تقارب التشريعات.

ب.رفع درجة التعاون بين المؤسسات القائمة على فرض القانون عالميا.

ت. ادارة خطوات مكافحة الجريمة الإليكترونية.

ثم بعد ذلك نتلمس مستوى استجابة الدول للاطار العام لمواجهة الجريمة الإليكترونية وفقا لتحليل فاعلية الجهود المبذولة نحو التنسيق العالمي.

التداخل بين فضاء الانترنت والفضاء العالمي اصبح عامل جذب مؤثر على مستخدمى الانترنت، وبرغم حقيقة ان نظم المعلومات قد قلصت المسافات بين القارات والجزر والمجتمعات في فضاء افتراضي، الا ان الدول ما زالت تتمسك بسيادتها التقليدية، مما دفع بعض المنظمات للسعي نحو تشجيع التناغم الدولي لمكافحة هذه المشكلة، من منطلقات مختلفة وباساليب متعددة، ولكن وعلى الرغم من ان الدراسات والجهود قد قامت على معلومات اولية واحدة تدور حول جهود خلق الانسجام العلمي لمكافحة الجريمة الإليكترونية ، الا ان استخراج معرفة مختلفة من طرق التفكير المختلفة اصبح هو المحصلة التي ما زال العمل عليها جاريا، وسنتناول ذلك على النحو الذي سبق تفصيله:

12.3 الجهود الاحترافية لمنظمة الشرطة الجنائية العالمية: (Interpol)

تعد كثير من المنظمات منظمات متخصصة، و احترافية لان اهدافها وانشطتها تتركز في مجالات بعينها، ومن بين هذه المنظمات البوليس الدولي (Interpol)، الاتحاد العالمي للاتصالات International Telecommunication Union (ITU) وغيرهما من المنظمات المعنية، وبهذا المفهوم فقد عنيت منظمة البوليس الدولي بالجريمة بشكل متخصص في مجال

مكافحة الجريمة بكل اشكالها ويتمثل ذلك في التعاون بين الدول الاعضاء في هذه المنظمة (Interpol 2007).

تضم منظمة البوليس الدولي 184 عضوا وقد بدأت هذه المنظمة الوقوف في وجه الجريمة الإليكترونية مبكرا وذلك بالتنسيق بين مؤسسات فرض القانون، او الدول الاعضاء فيها، وخلق الانسجام بين التشريعات العالمية وهي مجهودات لرفع قدرات اجهزة مكافحة الجريمة الإليكترونية ، على مستوي العالم، وهي مجهودات امتدت لتشمل مؤسسات فرض القانون جنبا الى جنب مع مجهودات تنسيق التشريعات الوطنية. (Interpol 2007)

في الوقت الحالي نجد ان هناك اربعة مجموعات عمل في اطار البوليس الدولي تشمل مجموعات عمل أفريقية، وامريكية، وجنوب اسيا والباسفيك، الى جانب مجموعة العمل الاوروبية التي تعمل في مجال جريمة تقنية المعلومات (Info. Tech. Crime).

الى جانب هذه المجموعات توجد لجنة قيادة (Steering Committee for Information Technology Crime) لمسألة جريمة تقنية المعلومات وتنسيق مبادرات (initiatives) مجموعات العمل الاقليمية .

المثال الواضح لفاعلية هذه اللجنة مصادقة مجموعة العمل الافريقية على قواعد المجلس الاوروبي للجريمة الإليكترونية (Council of Europe Cybercrime Convention) (COE 2001).

وفي مجال فرض القانون فان البوليس الدولي قد قدم موجهات تقنية في مجال التحقيق في الجريمة الإليكترونية وجمع الادلة الجنائية (Interpol Information Technology Crime Investigation Manual) والتي جاءت نتيجة لجهود مجموعة العمل

الاوروبية (European Working Party) بخصوص جريمة تقنية المعلومات(Information Technology Crime) ، وهذه الموجهات قد تسببت في بروز القواعد الخاصة بالجريمة الإليكترونية ، (Convention on Cybercrime)التي نعرفها اليوم .

13.3 الجهود الاقليمية:Regional effort

هناك الكثير من المنظمات الاقليمية العالمية التي قامت بجهود لتوفير امن تكنلوجيا السايبر، والتنسيق الدولي لتوحيد المقاييس الكفيلة بتوفير سبل مكافحة الجريمة الإليكترونية ، وسنعرض فيما يلي لاربعة منظمات توحدت لديها معايير المكافحة:

i. **منظمة التعاون الاقتصادي لاسيا والباسفيك APEC**

في اقليم اسيا والباسفيك تعمل APEC لتنسيق جهود اعضائها ال21 لتقديم امن تكنلوجيا السايبر لمعالجة المخاطر التي تنتج عن الجريمة الإليكترونية ، كما انها بذلت جهودا لبناء قدرات المتعاملين مع الجريمة الإليكترونية ، سواء بتدريب القانونيين او القائمين على مسألة التجقيق في الجريمة الإليكترونية

بعد هجوم الحادي عشر من سبتمبر في الولايات المتحدة اصدر قادة منظمة ال APECبيانا ادانوا فيه الارهاب وصرحوا ان مسألة مكافحة الارهاب هي مسألة ملحة وعاجلة ونادوا بتفعيل التعاون في عدة محاور .

نادى قادة الAPEC بتفعيل انشطتها لحماية البنيات الاستراتيجية .

كما اصدر وزراء الاتصالات والمعلومات في الدول الاعضاء بيانا دعوا فيه الى برنامج عمل بخصوص امن المعلومات، والبنيات الاساسية للاتصالات، مدعوما من الدول الاعضاء ضد الاستخدام السئ للمعلومات (APEC 2005).

اصدر اجتماع الوزراء توصيات تعد هي الاساس لجهد المنظمة في سبيل منع الجريمة الإليكترونية مكوناتها هي تطوير القانون، وتبادل المعلومات، والموجهات التقنية والامنية، رفع مستوى الادراك العام، التوعية والتدريب، كما اوصت لجنة للخبراء بتفعيل قوانين شاملة لامن تكنلوجيا السايبر، والجريمة الإليكترونية ، تتوافق مع القوانين العالمية واعلان الامم المتحدة رقم 63/55 والقواعد التي تحكم الجريمة الإليكترونية لسنة 2003 (UN 2003) .

استجابة لهذا النداء تم البحث في القوانين التي تحكم الجريمة الإليكترونية ، كما تم استقبال استجابات من الاعضاء اقترحت فيها الولايات المتحدة قيام مشروع لمجموعة امن الانترنت، من الاتصالات ومجموعة عمل المعلومات. واول مراحل هذا المشروع هو عقد اجتماع يضم خبراء الجريمة الإليكترونية من جميع اجزاء الاقليم وقد تم عقد الاجتماع بالفعل في 21-25 يوليو 2003 في بانكوك، تايلاند وحضره 120 مندوبا من 17 دولة وكان الهدف من الاجتماع هو المساعدة في خلق اطر قانونية لذيادة قدرات اجهزة فرض القانون وتقوية التعاون بين القطاعين الخاص والعام لمواجهة الجريمة الإليكترونية .

في العام 2005 عقد الاجتماع الوزاري السادس لل (APEC) الذي اخرج اعلان ليما الذي يشجع كل الدول لدراسة قواعد الجريمة الإليكترونية 2001 وتعمل على

تطوير قوانين تنظم الامن السبراني والجريمة الإليكترونية التي تتوافق مع الاليات القانونية العالمية ويشمل ذلك قرار الامم المتحدة 63/55 -2003 (APEC 2005).

ادى الاختلاف الكبير بين دول المجموعة الى عدم التمكن من خلق الية قانونية موحدة تفي بالغرض. بينما اعلنت بعض الدول توافق قوانينها مع القواعد العالمية وشرعت بعض الدول في تبني نصوص مماثلة وظلت بعض الدول تستخدم قوانين مختلفة تماما واخرى لا تملك قانونا.

دعت الولايات المتحدة الى مشروع لتطوير قدرات القضاة وممثلي النيابات لمواجهة الجريمة الإليكترونية في 2006 . واقترحت ايضا ان يشارك في هذا المشروع الخبراء في الحكومات والقطاع الخاص وان يترجم القرار الى اللغات المحلية بواسطة الخبراء انفسهم وان يتم تدريب المدربين TOT (Hawthorne 2014).

ii. المجلس الاوروبي: (COE)

ظل المجلس الاوروبي يعمل على تخفيف القلق العالمي، الذي سببته عملية معالجة المعلومات الشخصية اتوماتيكيا، منذ مطلع الثمانينيات1980.

في العام 1981 تبنى المجلس الاوروبي قواعد حماية الافراد، فيما يتعلق بمعالجة البيانات الشخصية اتوماتيكيا، حفاظا على حقوق الافراد الاساسية، وعلى وجه الخصوص حماية الخصوصية لان المعالجة الالكترونية تسبب عبور المعلومات الشخصية للحدود تلقائيا دون الاعتداد بهذه الحقوق. (COE 1981)

اصدرت لجنة الخبراء المعينة في 1985 توصياتها في1989 و1995 الخاصة بقوانين الحقوق والاجراءات في خصوص الجريمة الإليكترونية .

في العام 1997 بدأ المجلس الاوروبي اعداد القواعد الخاصة بالجريمة الإليكترونية والتي قدمت للتوقيع في 2001 واصبحت سارية في 2004 (COE 2001) .

في العام 2003 بدأ اعداد البرتكول الاضافي لقواعد الجريمة الإليكترونية ، والخاص بتجريم الافعال ذات الصفة العنصرية، والكره ضد الاجانب (Acts of a Racist and Xenophobic Nature Committed Through Computer System) الذي يتم عبر انظمة الكمبيوتر، كما تناولت القواعد القوانين الخاصة، والقوانين الاجرائية، واقليمية القوانين.

وتعد هذه القواعد علامة بارزة في تأريخ مكافحة الجريمة الإليكترونية. وكان التوقع ان يكون له اثر عميق في التحولات القانونية والتعاون الفني بين الدول الاعضاء(46 دولة).

في مؤتمر2004 دعى المجلس الاوروبي لتبني قواعد الجريمة الالكترونية ورفع الاهتمام السياسي وتشجيع التعاون بين القطاعين العام والخاص .

في مؤتمره 2005 بخصوص الجريمة الإليكترونية اوضح المجلس اهتماما بالتنامي السريع للمهدادات الاجتماعية والاقتصادية للجريمة الإليكترونية ، ويشمل ذلك النشاط الارهابي في الانترنت، مبينا ان الجريمة الإليكترونية في معظمها جريمة عالمية، داعيا الى قوانين فاعلة وادوات مكافحة مؤثرة وتعاون عالمي، ومشجعا ايضا للتعاون العام و الخاص، والدخول في منظومة قواعد الجريمة الإليكترونية .

في العام 2006 اصدر المجلس الاوروبي مشروعا ضد الجريمة الإليكترونية بغرض الحصول على المساعدة اللازمة للتوفيق بين القوانين الوطنية ونصوص قواعد الجريمة الإليكترونية ، تدريب القضاة، ووكلاء النيابة، والقائمين على عملية فرض القانون، ومسؤلي العدالة الجنائية، وتفعيل نقاط اتصال مستديمة على مدار اليوم للتعاون الدولي. (Hayes 2013)

iii. **الاتحاد الاوروبي**

اتخذ الاتحاد الاوروبي مجموعة من الخطوات نحو تنسيق عملية مكافحة الجريمة الإليكترونية، عن طريق تفعيل التعاون الفني بين القائمين على فرض القانون، وتنسيق التعاون في مجال السياسات القانونية. كما اهتم ايضا بمسألة الحقوق والحريات في مجال مكافحة الجريمة الإليكترونية (EUR-LEX 1997).

في العام 1995 اصدر البرلمان الاوروبي والمجلس الاوروبي موجهات في اكتوبر 1995 خاصة بحماية الافراد، فيما يخص معالجة المعلومات الشخصية وحركتها. واختصت المادة 8 من الموجهات بسرية المعالجة وامن المعلومات الشخصية، وقد عمدت الموجهات لحفظ حقوق الاشخاص الطبيعيين الذين تتم معالجة بياناتهم اتوماتيكيا (المادة3-1)، وتبنى التوجه ان تكون هذه العملية منضبطة فنبا وان يراعى فيها الموجهات والمقاييس التي تحمي البيانات والمعلومات الخاصة بالافراد، وفوق ذلك نجدها قد فرضت عقوبات على مخالفتها وتعويض عن اي خسائر على من يخالف نصوصها (المادة17-1)

في العام 1997 اصدر البرلمان الاوروبي والمجلس الاوروبي الموجهات 66/97 لسنة 1997 الخاصة بمعالجة البيانات الشخصية في قطاع الاتصالات، وهو توسيع

لمسألة الحماية الشخصية لتحقيق درجة من الحماية للافراد ومصالحهم (المادة 23)، وفرض التعويض عن الضرار (المادة24). استهدفت الموجهات خلق متطلبات يقع عبء توفيرها مباشرة على موفري الخدمة (ISP) ، وليس على الدول الاعضاء، اذ يقع عبء توفير الامن للافراد من خلال تأمين الخدمات (المادة4-1)، . ونصت الوجهات على ان تتبنى الدولة لوائح تضمن سرية الاتصالات، وتمنع التصنت والتسجيل، والتخزين، وكل انواع الاعتراض والمراقبة بدون ترخيص، من قبل الاشخاس القانونيين الرسميين الطبيعيين، كما منعت الموجهات الاتصالات غير المشروعة (المادة12) ،ويشمل ذلك الاتصالات الاتوماتيكية او الفاكس وليس الرسائل الالكترونية (EUR-LEX 1997).

في نوفمبر 2001 انعقدت جلسة عامة الاتحاد الاوروبي وكان النقاش الرئيسي قد دار حول استبقاء المعلومات (retention of traffic data) (http 2008)

iv. منظمة الدول الامريكية :(OAS)

منظمة الدول الامريكية OAS بعضويتها التي تبلغ 35 دولة هي الاخرى منشغلة بقضية الجريمة الإليكترونية.

خلال اجتماع وزراء العدل او النواب العامين للدول الاعضاء الامريكية (REMJA) ، امن المؤتمرون على الدور المحوري الذي يلعبه تنسيق الاطر القانونية في عملية مكافحة الجريمة الإليكترونية ، وعملية حماية الانترنت. هذا الاهتمام ادي لصدور توصية لخلق مجموعة الخبراء الحكوميين في الجريمة الإليكترونية في مارس1999 .

عقدت لجنة الخبراء اربعة اجتماعات ناقشت فيها وسائل التعاون الدولي و تحليل قوانين الجريمة الإليكترونية الوطنية.

حث اجتماع وزراء الدول الامريكية لاتخاذ خطوات عملية نحو جعل التعاون الدولي ممكنا، كما اوصى الاجتماع الدول الاعضاء لتقييم مسألة الاستفادة من مبادئ اتفاقية الجريمة الإليكترونية Convention on) (Cybercrimeالاوروبية ودراسة مسألة الانضمام لها .

في العام 2004 اجاز اجتماع الجمعية العمومية لمنظمة الدول الامريكية قرارا بتبني استراجية شاملة لمكافحة الجريمة الإليكترونية ، ومهددات الامن السيبراني.

كما اقترحت الوصول الى استراجية فاعلة حيال العلاقة التشاركية بين الدولة وقطاع الاعمال العامل في نطاق الشبكة الرابطة لنظم المعلومات المكون منها للانترنت .

14.3 جهود المنظمات متعددة الجنسيات: (MNE)

بخلاف المنظمات المتخصصة التي تنحصر مجهوداتها في مجال معين، لاتنحصر عضوية المنظمات متعددة الجنسيات في اقليم او دول بعينها، اذ ان هذا النوع من المنظمات تتنوع اهتماماته وجهوده، لتشمل اهتمامات متنوعة ومتعددة وغالبا ما تتكون عضويتها من دول تقع في اقاليم نطاقها اوسع.

فيما يلى سنعرض لثلاثة منظمات متعددة الجنسيات لنستعرض جهودها في مجال مكافحة الجريمة الالكترونية:

(i) رابطة الامم: Commonwealth of Nations

اتخذت رابطة الامم خطوة مبكرة فيما يتعلق بتنسيق قوانين الدول الاعضاء فيها المتعلقة بالجريمة الإليكترونية (commonwealth 2013) . في اكتوبر2002 اعد سكرتير رابطة الامم نموزج قانون الكمبيوتر والجرائم المتعلقة بالكمبيوتر. اثر هذا القانون على كل القونين الوطنية الخاصة بالدول ال 53 الاعضاء في الرابطة. اصبح الاتفاق الخاص بالجريمة الإليكترونية من الخيارات التشريعية الواردة في نموزج القانون الذي قدمه سكرتير الرابطة ويغطي جرائم الدخول غير المشروع والتعرض للمعلومات، والانظمة، واعتراض انتقال المعلومات، والتحرش بالاطفال (commonwealth 2013).

مقارنة باتفاقية الجريمة الإليكترونية فان نموزج القانون قد مدد المسؤلية الجنائية لتشمل المساس بالمعلومات، والانظمة، واستعمال الاجهزة غير المشروعة.

عالج النموزج او غطي مسألة اقليمية القوانين بالنص على التجريم حتى ان وقع الفعل المجرم خارج اقليم الدولة طالم ان الفعل يشكل جريمة بموجب قانون الدولة.

(ii) مجموعة الثمانية : (G8)

منذ التسعينات خلقت مجموعة الثمانية مجموعات عمل استصدرت بيانات رسمية من رؤساء الدول واصدرت خطط عمل من وزراء العدل بدول المجموعة.

في العام1995 اعلنت مجموعة السبعة ان النجاح في مكافحة الجريمة يستدعي ان تعتبر كل الدول غسيل الاموال من الجرائم الخطيرة والالتزام بمحاربة

الجريمة المنظمة العابرة للحدود بفاعلية . في اجتماع ليون G7/P8 Lyon Summit اصدرت المجموعة توصياتها لذيادة جهود محاربة الجريمة الإليكترونية عبر تجريمها ، والتحقيق فيها ، والتعاون بين دولها ، مع مراعاة حقوق الانسان. في اجتماع دنفر بولاية كلورادو بالولايات المتحدة الامريكية اقترح المجتمعون زيادة وتقوية الجهود لتنفيذ توصيات مؤتمر ليون عن طريق معاقبة المجرمين ذوي القدرات الفنية العالية ورفع قدرات الدولة الفنية والقانونية للاستجابة للجريمة العابرة للحدود . (http 2020)

(iii) منظمة التعاون الاقتصادي والتنمية : (OECD)

تضم منظمة التعاون الاقتصادي في عضويتها 30 دولة.

واجهت منظمة (OECD) التعاون الاقتصادي الجريمة الإليكترونية لعشرات السنين.

في العام 1983 قامت منظمة التعاون الاقتصادي والتنمية بتعيين لجنة خبراء لمناقشة ظاهرة الجريمة الإليكترونية .

ادت الموجهات التي اصدرتها منظمة التعاون الاقتصادي والتنمية لبروز تسعة مبادئ تمثلت في الجاهزية ، والمسؤلية والاستجابة والاخلاق والديمقراطية وتقدير المخاطر وتصميم التأمين والاخذ به وادارته واعادة تقييمه (OECD 1983) .

(iv) المجهودات العالمية المبذولة من الامم المتحدة : (UN)

توجد العديد من المنظمات العالمية الا ان الامم المتحدة باعضائها ال191 تعد المنظمة الاكثر تأثيرا والاكثر فاعلية.

مقارنة ببقية المنظمات الاقليمية و المتخصصة و العالمية الاخرى فان الامم المتحدة لا تحصر نشاطها في مجالات محدودة او دول محدودة، خصوصا في مجال تحقيق الامن السيبراني ومنع الجريمة الإليكترونية فاننا نجد ان تحركات الامم المتحدة ذات اثر فاعل، خصوصا في مجال خلق وتنسيق المواقف والتعاون الدوليين.

في العام 1985 اصدرت الامم المتحدة قرارها الذي نادت فيه الدول والمنظمات الدولية للالتزام بتوصيات المنظمة الخاصة بالقيمة العالية لسجلات الكمبيوتر، في محاولة لتشجيع العمل بهذه المعالجة للمعلومات بشكل اوسع.

في العام 1990 تبنت الامم المتحدة الموجهات الخاصة بالمعلومات الشخصية الإليكترونية. وقد اوصت باتخاذ الاجراءات المناسبة لحماية الملفات من الاخطار الطبيعية والاصطناعية. خلاصة القول ان المجهودات التي بذلتها الامم المتحدة كان ممكنا جدا ان يكون نجاحها باهرا في مواجهة الجريمة الإليكترونية، لولا استضامها بالنظم القانونية الكثيرة والمتباينة لاعضائها.

15.3 نقاط اهتمام التنسيق الدولي:

الاستعراض السابق للجهود الدولية يمكن ان يقود الى ان نقاط تركيز هذه المنظمات انحصرت في ثلاثة نقاط تتمثل في:

أ. رفع درجة الاهتمام الامني عالميا وللدول منفردة.

ب. تنسيق التشريعات والتعاون الشرطي.
ت. تنسيق اجراءات مكافحة الجريمة الإليكترونية المباشرة. (المواجهة الفعلية)

أ.رفع درجة الاهتمام الامني عالميا

المثال والعمل الاهم في هذا الخصوص هو قرار الامم المتحدة 55 والقرار 63 لعام 2000 والقرار 121/56 2001 حول سوء استخدام تقنية المعلومات، نادت قرارات الامم المتحدة بالاخذ بمبادئ مجموعة الثمانية.

اصدرت الامم المتحدة الكثير من القرارات التي نادت بالتصدي للجريمة الإليكترونية الحاضر والمستقبل. وكذلك فعلت الكثير من المنظمات التي تصدت لظاهرة الجريمة الإليكترونية مثل منظمة APECوسعيها بعد 911 لحماية البنيات الاساسية.

غير الامم المتحدة الكثير من المنظمات الاممية والاقليمية ذات التخصصات المتعددة والعضوية الاقليمية او العالمية سعت لحماية البنيات الاساسية. (UN 2000)

ب) رفع درجة الاهتمام الامني للدولة:

كل المنظمات العالمية بذلت جهدا لترقية الاهتمام الامني على المستوى المحلي للدولة .

منظمة APEC قادت اعضاءها والاقليم لترقية امن السايبر ومواجهة مخاطر الجريمة الإليكترونية. كما انها قادت مشروعا لتشجيع الدول المتقدمة لترقية وتدريب افراد من الدول الاخرى (APEC 2005) .

ج) تنسيق التشريعات:

التنسيق القانوني (Legislations Harmony) ظل هو الهم الاكبر لمعظم المنظمات العالمية. بدأت محاولات التنسيق في اوروبا في بداية الثمانيات وابرز الانجازات ظلت على الدوام هي اتفاقية الجريمة الإليكترونية وفي العام 1981 اجري الانتربول مسحا لقوانين الدول الاعضاء للوقوف على العيوب وبذل الجهد للتنسيق بينها. (UN 1990)

مجموعة العمل الافريقية في الانتربول تعمل الان على مشروع الجريمة الإليكترونية لاقناع الدول الافريقية للتوقيع والمصادقة على اتفاقية الجريمة الإليكترونية. ايضا نجد ان جهدا مماثلا قامت به منظمة التعاون الاقتصادي لاسيا والباسفيك لتشجيع اعضائها للاخذ باتفاقية الجريمة الامريكية والمواثيق ذات الصلة الصادرة من الامم المتحدة (APEC 2005) .

اصدر الاتحاد الاوروبي في العام 2002 قرارا بالزام الدول الاعضاء بتجريم الدخول غير المشروع (illegal access) او التدخل في انظمة المعلومات .

على وجه العموم دعت جل المنظمات الدولية والاقليمة الدول الاعضاء فيها للتوقيع على اتفاقية الجريمة الإليكترونية او على الاقل الاخذ بمبادئها وقد ذادت على ذلك مجموعة الثمانية بالدعوة بتبني قانون عقابي عالمي ومشاركة القطاعين العام والخاص في تحقيق هذا الهدف وصولا للمكافحة الفاعلة للجريمة الإليكترونية.

التنسيق والتعاون لتطبيق القانون :

لعب الانتربول دورا مشهودا في هذا الجانب اذ سعى مع مجموعة العمل الاوروبية للجريمة الإليكترونية لجمع

موجهات عمل فنية لتنظيم العمل الخاص بفرض القانون و العمل الشرطي الخاص ضد الجريمة الإليكترونية واهتم الاتحاد الاوروبي بنقل المعلومات الشخصية 2001 واهتمت المجموعة الامريكية للخبراء بخلق التعاون بين اعضائها لمكافحة الجريمة الإليكترونية، كما اهتمت مجموعة الثمانية بسد الفراغات وايجاد طرق التعاون الفني وقد حثت هذه المنظمات اعضاءها لتجريم الانتهاكات الالكترونية ورفع فاعلية المقاضاة والتحقيق وقد حث مؤتمر دنفر بولاية كلورادو سابق الاشارة اليه على الاهتمام بالقانون والنواحي الفنية والتكنلوجية ورفع امكانيات الدول الفنية مثلها مثل القانونية للتدخل عند الحاجة. كما دعى مؤتمر برمنجهام للتوقيع على اتفاقية تتعلق بالحصول على الادلة والمحافظة عليها وخلق تعاون دولي بخصوصها الى جانب حماية الخصوصية والتبادل الدولي للادلة لزيادة فاعلية مكافحة الجريمة وخصوصا الإليكترونية (Interpol 2007).

16.3 المكافحة المباشرة للجريمة الإليكترونية:

اهتمت المكافحة المباشرة للجريمة الإليكترونية بجانبين :

أ. المنع

و

ب. التحقيق.

حظي الجانبان المتعلقان بالمنع والتحقيق في الجريمة الإليكترونية باهتمام بالغ حتي قبل الاهتمام العالمي بتنسيق الجهود الدولية الرامية للمنع والمقاضاة عند ارتكاب الجريمة الإليكترونية (Hayes 20013).

اخذت بعض المنظمات خطوات منفردة بتركيز محدد مثلما طور الانتربول تعاونا مشتركا مع شركات بطاقات الائتمان لمحاربة الغش المتعلق بعمليات الدفع.

اصدرت منظمة التعاون الاقتصادي والتنمية (OECD) موجهات حماية المستهلك المتعلقة بالتجارة الالكترونية (Guidelines for Consumer Protection in the Context of Electronic Commerce 1999) مثلما هو الحال في التجارة التقليدية.

نادت موجهات امن نظم المعلومات والشبكات (Guidelines for the Security of Information Systems and Networks 2002) الدول الاعضاء بان تولي اولوية قصوى للتخطيط الامني وان تبني ثقافة امنية فاعلة كوسيلة من وسائل حماية النظم المعلوماتية والشبكات.

17.3 من الحوار الى توقيع الاتفاقيات:

من اهم انجازات التعاون الدولي هي الاتفاقية الخاصة بالجريمة الإليكترونية والبرتكول الخاص بها، وقد كانت هذه الاتفاقية مقدمة قد هدفت لمكافحة الجريمة الإليكترونية التي استهدفت ووقفت ضد السرية ، والمصداقية ، والتواجد وتبنت سؤ استخدام نظم المعلومات، الى جانب ان البرتكول يساعد ويدعم تجريم الافعال العنصرية (racist) والافعال ذات الطبيعة المعادية للاجانب (xenophobic) التي ترتكب من خلال استخدام انظمة المعلومات. وهذا البروتكول يعد علامة تحول للاطار الموضوعي و القانوني على المستوى الاقليمي والعالمي للوقوف ضد الجريمة الإليكترونية .

قدمت الاتفاقية عنصرين هامين للجريمة الإليكترونية الاول هو العنصر الموضوعي وهو النية والثاني هو العنصر المادي اي اتيان الفعل دون سند قانوني.

سمحت الاتفاقية ايضا للتشريعات المحلية اضافة عناصر اخرى وتقديم التحفظات الخاصة بكل تشريع فهي قد وفرت حرية القرار للدول الاعضاء فيما يتعلق بسياستها الجنائية، الا ان ذلك لا يعني ان الاتفاقية قد عالجت كل المعضلات بل على العكس من ذلك فان البعض يرى ان هذه الحرية وتنوع القوانين قد اضعف القدرة على قياس الضرر من الافعال المجرمة كما انه قد وضع المعوقات امام الجهود العالمية وقلل فاعلية التقاشات المطولة والمكلفة للدول للوصول لاتفاق برغم ان النصوص ذاتها قد تم نقاشها.

تم ايضا انتقاد الاتفاقية من نشطاء الحقوق المدنية بانها تتجاهل حق الخصوصية وتعطي حق الرقابة على الافراد للسلطات بصورة موسعة اذ ان للاتفاقية القدرة على الوصول لمسافات بعيدة اكثر من اللازم - البحث والمصادرة للحقوق بدون وضع حدود او ضوابط لحماية الحقوق الشخصية بينما القاعدة الاساسية المتعلقة بحماية الحقوق هي عدم اطلاق سلطة الدولة في التعدي على خصوصيات الافراد ومراقبتهم وتجاوز الحدود لتجريمهم.مع غزو الإنترنت لدول العالم أصبح من الصعوبة بمكان ضبط وكشف الجرائم الإليكترونية نظرا لكونها عابرة للحدود وتتم بسرعة فائقة دون رقيب أو حسيب مع صعوبة وجود رقابة فاعلة مما يؤدي الي ارتكاب كافة صور وانواع الجرائم المتعارف عليها عبر الانترنت ويشمل ذلك حتي القتل والسطو على برامج الحاسوب كم ان التعدي قد يكون بغرض سرقة البيانات من قاعدة المعلومات Databases خصوصا السرية منها

واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة والسطو على الأموال. (Shinder 2010)

صفوة القول ان صور الجريمة الإليكترونية قد تعددت بشكل مذهل وكثرت صورها فمنها كمثال فيروسات الكمبيوتر (computer viruses) ثم ما اصطلح على تسميته بالإرهاب الإلكتروني (Electronic Terrorism) الذي هدد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الجنسية الإباحية، خاصة الموجهة منها للأطفال والمقدرة بأكثر من 1000 موقع يقدم مواد جنسية إباحية خاصة بالأطفال ما دون سن البلوغ (children pornography) . هذه الجرائم يتم فيها استخدام دعارة الأطفال والنساء (prostitution)، سواء بالغين أو قصر عن طريق تصويرهم (imaging) مباشرة أو بالمحاكاة (simulation) والتمثيل الرقمي للصورة باستعمال وسائل الترغيب والترهيب كالإغراء والتحذير أو التهديد. (Halder D 2011)

18.3 الملخص والمناقشة:

دون سائر انواع العلوم فان تكنلوجيا السايبر ما زالت تتمدد بشكل ملحوظ في كل الاتجاهات بشكل يجعل التأريخ او رصد تطورها امرا في غاية الصعوبة والتعقيد فضلا عن التأسيس باستخدام ما يصلح لعملية الضبط الاخلاقي والقانوني في عموم مستجدات المسائل المستقبلية الخاصة بالجانب الفني في قضايا الاثبات (Evidence) والتحقيق وجمع البينات.

مع غزو الإنترنت لدول العالم أصبح من الصعوبة بمكان ضبط وكشف الجرائم الالكترونية نظرا لكونها عابرة للحدود وتتم بسرعة فائقة دون رقيب أو حسيب مع

صعوبة وجود رقابة فاعلة مما يؤدي الي ارتكاب كافة صور وانواع الجرائم المتعارف عليها عبر الانترنت ويشمل ذلك حتي القتل والسطو على برامج الحاسوب كما ان التعدي قد يكون بغرض سرقة البيانات وقاعدة البيانات المعلوماتية (Databases) خصوصا السرية منها واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة والسطو على الأموال. صفوة القول ان صور الجريمة الالكترونية قد تعددت بشكل مذهل فمنها ما اصطلح على تسميته بالإرهاب الإلكترو الذي هدد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الجنسية الإباحية، خاصة الموجهة منها للأطفال تقدم مواد جنسية إباحية خاصة بالأطفال ما دون سن البلوغ . (child pornography) هذه الجرائم يتم فيها استخدام دعارة (prostitution) الأطفال والنساء، سواء بالغين أو قصر عن طريق تصويرهم (imaging)مباشرة أو بالمحاكاة (simulation) والتمثيل الرقمي للصورة باستعمال وسائل الترغيب والترهيب كالإغراء والتحذير أو التهديد.

يتزايد اعتماد الناس في جميع أرجاء العالم يوما بعد آخر على شبكة الانترنت العالمية في كل أعمالهم وتواصلهم الاجتماعي وتفاصيل حياتهم اليومية؛ حيث كشفت إحصاءات عالمية حديثة زيادة قاعدة مستخدمي الانترنت حول العالم لتسجل مع نهاية النصف الأول من العام الحالي قرابة 4.54 مليار مستخدم، أكثر من نصفهم يتواجدون في قارة آسيا.

وتواصل شبكة الإنترنت العالمية توسعها وانتشارها في مختلف أرجاء العالم مدعومة بزيادة استخدام الهواتف الذكية، وانتشار شبكات الإنترنت عريضة النطاق من

الجيلين الثالث والرابع وشبكات الفايبر، فيما تستعد أسواق العالم في الوقت الراهن وتتحضر لاستقبال وإطلاق شبكات الجيل الخامس بسرعات عالية جدا تتلاءم وتطبيقات الثورة الصناعية.

قسم بعض الباحثين في مجال المعلومات قرصنة الفضاء الإلكتروني إلى نوعين رئيسيين:

الأول: وهم ما يطلق عليهم الهاكرز Hacker والثاني: وهم لصوص ومافيا السرقات الإلكترونية عبر الإنترنت.

تعددت صور الجريمة الإليكترونية بشكل مذهل تبعا للتطور التكنولجي الذي صاحب ظهور الانترنت فمنها كمثال فيروسات الكمبيوتر (computer viruses) ثم ما قام عالميا الاصطلاح على تسميته بالإرهاب الإلكتروني الذي هدد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الجنسية الإباحية، خاصة الموجهة منها للأطفال.

نادت موجهات امن نظم المعلومات والشبكات (Guidelines for the Security of Information Systems and Networks 2002) الدول الاعضاء بان تولي اولوية قصوى للتخطيط الامني وان تبني ثقافة امنية فاعلة كوسيلة من وسائل حماية النظم المعلوماتية والشبكات.

اصدرت الامم المتحدة الكثير من القرارات التي نادت بالتصدي للجريمة الإليكترونية الحاضر والمستقبل.

قرار الامم المتحدة55 والقرار 63 لعام 2000 والقرار 121/56 2001 حول سوء استخدام تقنية المعلومات،

نادى بمثل ما نادت به قرارات الامم المتحدة بالاخذ بمبادئ مجموعة الثمانية.

ركز الجهد العالمي الذي رفع راية الكفاح ضد الجريمة الالكترونية على ثلاثة نقاط:

i. رفع درجة الاهتمام الامني عالميا وللدول منفردة.
ii. تنسيق التشريعات والتعاون الشرطي.
iii. تنسيق اجراءات مكافحة الجريمة الالكترونية المباشرة. (المواجهة الفعلية)

IV. الباب الرابع
التحقيق في الجرائم الالكترونية

1.4 المـــــقدمـــــــة :

قبل الدخول في عملية وصف التحقيق ، نحتاج إلى تحديد المفاهيم الأساسية المتعلقة به.

هناك القليل من التعريفات المتفق عليها في مجال البحوث الجنائية الرقمية ، لذلك سنعرض في هذا الجزء من البحث بوضوح للتعاريف التي نستخدمها خلال التعرض لوصف التحقيق، وقد يشمل ذلك الكثيرمما هو معروف وابتدائي حتى نوحد المفاهيم المقصودة في هذا البحث.

بالنسبة لاجهزة الكمبيوتر الحديثة ، من الشائع أن يتم تمثيل البيانات داخليا في تشفير ثنائي، (bits) بالرغم من ان هذا التمثيل ليس شرطا في كل الاحوال. (Carrier. 2003)

2.4 طبيعة الكائن الرقمي

الكائن الرقمي عبارة عن مجموعة منفصلة من البيانات الرقمية ، مثل ملف أو قطاع قرص ثابت أو حزمة شبكة أو صفحة ذاكرة أو عملية.

البيانات الرقمية لها تمثيل مادي بالإضافة إلى تمثيلها العددي. (Mark Reith 2002)

على سبيل المثال، الثنائيات (BITs) في القرص الصلب هي الدوافع المغناطيسية على الصحون التي يمكن قراءتها مع واحد من أجهزة الاستشعار (السجل). تحتوي أسلاك الشبكة على إشارات كهربائية تمثل حزم الشبكة وكابلات لوحة المفاتيح، التي تتضمن إشارات كهربائية تمثل المفاتيح التي تم ضغطها.

يحول الكمبيوتر الإشارات الكهربائية إلى تمثيل رقمي، مثل ان التصوير الفوتوغرافي الرقمي والفيديو هما تمثيل رقمي للضوء المرتبط بالأشياء المادية.

يمكن للبيانات الرقمية ان يتم تخزينها على العديد من وسائل التخزين، و كل وسيلة تخزين لها خصائص مختلفة تحدد المدة التي تكون فيها البيانات موجودة في وسيلة التخزين .

على سبيل المثال ، البيانات تبقى على كابل لوحة المفاتيح لجزء من الثانية، لكنها قد تكون موجودة على القرص الصلب لسنوات. (Anderson2015)

3.4 خصائص الكائنات الرقمية

الكائنات الرقمية لها خصائص ، أو ميزات فريدة ، بناء على منشئها ووظيفتها.

على سبيل المثال، فإن الخصائص المميزة للقطاع الخاص بالقرص الصلب تكون مختلفة عندما يتم استخدامها لتخزين محتويات مستند نص ASCII مقابل صورة ذات خصائص القطاع المستخدم لتخزين صورة JPEG مما يعني انه من الممكن استخدام الخصائص لتحديد البيانات، وان حالة الكائن هي قيمة خصائصه.

إذا تم تغيير حرف في مستند نصي ASCII ، فسيكون الكائن المقابل للملف في حالة جديدة، وبالمثل ، تتغير حالة عملية تشغيل الكمبيوتر في كل مرة تتم فيها كتابة البيانات إلى ذاكرة الكومبيوتر.

4.4 الحدث الرقمي

الحدث الرقمي هو واقعة قد تغير حالة واحدة أو أكثر من الأجسام الرقمية، كما ان حالة الكائن تتغير نتيجة لهذا الحدث، أو بتأثير هذا الحدث. (Spafford 2004)

بعض أنواع الكائنات لديها القدرة على إحداث الأحداث وتسمى الأسباب، مع ملاحظه أنه نظرا لتخزين الكائنات الرقمية في شكل مادي ، يمكن تغيير حالتها من خلال الأحداث المادية والرقمية على حد سواء .

الكائن هو دليل على حدث إذا عبر الحدث عن حالة الكائن، هذا يعني أنه يمكن فحص الكائن للحصول على معلومات حول الحدث الذي حدث. ومع ذلك ، يمكن أن تتسبب الأحداث المستقبلية في عدم وجود معلومات عن الأحداث السابقة لكائن ما .

كل كائن هو دليل على حدث واحد على الأقل، لأنه لا بد من وجود حدث إنشاء الكائن. وضعت بعض البيئات والسياسات قوانين هادفة لان تمنع حدوث بعض الأحداث.

الحادث هو حدث أو سلسلة من الأحداث التي تنتهك سياسة وأكثر تحديدا، فان الجريمة هي حدث أو سلسلة أو الأحداث التي تنتهك القانون. (Saferstein 2000)

التحقيق هو عملية تطوير واختبار الفرضيات للإجابة على الأسئلة حول الأحداث التي وقعت. وتشمل الأسئلة على سبيل المثال ما الذي تسبب في الحادث ليحدث؟، "متى وقع الحادث؟، و أين وقع الحادث؟.

لتطوير واختبار الفرضيات حول الأحداث التي وقعت من قبل، او أثناء او بعد و قوع الحادث، لابد من تحديد ما حدث فعلا.

المؤشر الوحيد لاحتمال وقوع حدث ما هو امكانية حيازة او شبهة وجود دليل على وقوعه.

إذا كان الكائن الذي تم تغييره بسبب الحدث لا يزال موجودا، فهذه معلومة تؤكد انه يمكننا النظر في ذات الكائن للحصول على معلومات حول الحدث و حول غيره من الأشياء التي كانت أسبابا للحدث او تشكل احد آثر هذا الحدث.

لذلك، يمكننا أن نشير لوجود أدلة سابقة أكثر تحديدا تؤكد أن الهدف من ذلك هو اقامة الدليل على وجود الحادث في حالته التي كانت وما استخدم للتسبب في الحدث المتعلق بالحادث أو بتمام تغيير حالته التي كان عليها قبل هذا الحدث الذي له علاقة بالحادث. (Rynearson 2002)

كل شيء يمثل دليل على بعض الأحداث. المفتاح هو تحديد ثم التقاط الأدلة المتعلقة بالحادث المعني (Rynearson 2002)، اعتمادا على هذا الفهم ، فنحن نستخدم بعض التعاريف التي لا تركز على العلاقة بين السبب والنتيجة. ألدليل المادي على وقوع حادث هو وجود شيئ مادي ملموس او محسوس يحتوي على معلومات موثوقة يمكن أن تدعم أو تدحض او تنطوي على فرضية حول الحادث و الأدلة الرقمية.

وقوع حادث هو البيانات الرقمية التي تحتوي على معلومات موثوق منها تدعم أو تدحض فرضية حول الحادث (Carrier. 2003).

من المعلوم أن الشيئ لديه معلومات عن الحادث لأنه كان سببا أو له تأثير في أي حدث ذو صلة بالحادث.

نظرا لأن البيانات الرقمية لها شكل مادي ، فإن الأدلة المادية يمكن أن تحتوي على أدلة رقمية . باستخدام هذا التعريف ، يعد القرص الثابت دليلا ماديا والقطاعات والملفات التي تحتوي على معلومات حول الحادث دليل رقمي. مع ملاحظة أن الأدلة الأخرى لم تقدم تمييزا واضحا . يصف دليل التحقيق في مسرح الجريمة الإليكترونية (Investigation-TWG 2001) .الاعتراف بقرص صلب أو جهاز تخزين آخر وجمعهما كمجموعة من الأدلة الرقمية.

في الإطار العملي ، فإن جمع القرص الصلب هو جمع الأدلة المادية ومجموعة الأشياء الرقمية من القرص الصلب هي مجموعة الأدلة الرقمية.

5.4 الفرق بين الأدلة المادية والرقمية

الفرق بين الأدلة المادية والرقمية يكون في شكلها وليس له علاقة بنوع الحادث.

الاختلاف بين الدليل المادي والرقمي يكون في الشكل فقط فانه يمكن أن يكون لدينا أدلة رقمية لحادث مادي أو جريمة.

اوضح مثال لما سبق ذكره ، فان كاميرا الفيديو الرقمية تنشئ تمثيلا رقميا لحدث مادي وبالتالي فان الملف الناتج يصلح ان يكون دليلا رقميا على الحدث.

يمكن أيضا الحصول على أدلة مادية للتحقيق الجنائي الرقمي. (Hayes 2013)

يعرف قاموس التراث الأمريكي جمع الادلة الجنائية بأنها صفة تتعلق باستخدام العلم أو التكنولوجيا

في التحقيق وإثبات الحقائق أو الأدلة في محكمة قانونية (Hrtage 1969). لذلك ، لكي يتم النظر في الادلة التي تم الحصول عليها ، يجب أن يستخدم في عملية الحصول عليها العلم والتكنولوجيا كما يجب أن تكون النتائج قابلة للاستخدام في محكمة قانونية.

مع الأدلة الرقمية، هناك حاجة إلى التكنولوجيا دائما لمعالجة البيانات الرقمية و الفيصل هو امكانية الاستفادة مما تم الحصول عليه من ادلة وبينات امام محكمة القانون واستخدامها امام القضاء لاثبات اي واقعة.

تحقيقات وجمع الادلة هي العملية التي تستخدم العلم والتكنولوجيا لتطوير واختبار النظريات التي يمكن إدخالها في محكمة قانونية، وتصلح ايضا للرد على الأسئلة التي تدور حول الأحداث التي وقعت.

للحصول على الدليل الرقمي فان التحقيق هو عملية تسخير العلم والتكنولوجيا لفحص الادلة الرقمية ، التي يمكن إدخالها في محكمة قانونية، للإجابة على الأسئلة حول الأحداث التي وقعت، وتوفير المتطلبات لدخول الأدلة الرقمية في محكمة قانونية.

كمثال على ذلك المبادئ التوجيهية التي تم استخدامها بواسطة بعض المحاكم الأمريكية لتحديد موثوقية الأدلة العلمية والتقنية. (Bace 2003).

تعتبر المبادئ التوجيهية انها قاعدة قامت على ما هو مسلم به عموما من قبل المجتمع، وقد تم اختبار الإجراء، فان كان الإجراء يمثل خطأ ما فان علاجه يعتمد على أنواع التحليل الرقمي الذي يتم استخدامه.

من الصعب التقليل من أهمية جمع الادلة الجنائية الرقمية مع وجود أنواع كثيرة من الأدلة متاح في شكل ملفات رقمية مخزنة على القرص الصلب لجهاز الكمبيوتر ، فتزداد اهمية هذه الادلة بصورة تراكمية يمكن ان تقود في نهاية العمل لانجاح عملية التحقيق. (Nelson 2008)

أصبح السعاة الفوريون (Messengers) وسيلة اتصال مهمة للملايين من الناس ، بغض النظر عن العمر او الجنس اومهارات الكمبيوتر.

لهذا السبب يمكن الآن العثور على المزيد والمزيد من الأدلة في تاريخ الدردشة وعلى سبيل المثال لا الحصر (Messenger)و (ICQ) و (Yahoo) تعد (Messenger) و (AOL) و Trillian() و ()Skype و Miranda IM() من بين الأكثر استخداما والاكثر استعمالا.

في الصين ، تحظى (QQ Messenger) بشعبية كبيرة مع ما يقرب من مليار حساب مسجل (Nelson 2008).

شبكات التواصل الاجتماعي

يتم ترحيل المزيد والمزيد من الاتصالات من غرف الدردشة العامة والمراسلين الخاصين في الشبكات الاجتماعية عبر الإنترنت لذا يمكن أن تكون الاتصالات المستخرجة من الشبكات الاجتماعية قيمة للغاية للمحققين في الجريمة الإليكترونية.

متصفحات الانترنت

تصفح الويب نشاط شائع ، كما ان تحليل محفوظات استعراض الويب والإشارات المرجعية وصفحات الويب المخزنة مؤقتا والصور وقيم النماذج المخزنة وكلمات

المرور توفر مفاتيح لأدلة مهمة غير متوفرة في غيرها من المواقع.

قد تحتوي ذاكرة التخزين المؤقت لمتصفح الويب على صور ذات محتوى غير مشروع ، بالإضافة إلى (JavaScript)برامج ضارة قد تكون مسؤولة عن بعض الأنشطة المشبوهة.

يمكن اكتشاف وتحليل عمليات بحث قوقل (Google) ، مما يساعد غالبا في حل الجرائم الاكثر تعقيدا (Rogers 2006).

توجد العشرات من متصفحات الويب (Microsoft Internet Explorerو Mozilla Firefox Chrome)

البريد الإلكتروني

على الرغم من زيادة الدردشات الفورية والشبكات الاجتماعية ، لا يزال البريد الإلكتروني هو الناقل الرئيسي للمعلومات ، وهذا ينطبق بشكل خاص على بيئات الشركات، من عملاء البريد الإلكتروني .

ومن امثلة البريد الالكتروني Microsoft Outlook و Outlook Express و Windows Mail و Live Mail و Thunder bird و The Bat.

كما ان العديد من تطبيقات البريد الإلكتروني الأخرى على اختلافها متوفرة في الاسواق(Jones 2007).

نظير إلى نظير وبرامج تبادل الملفات

قد يحتوي عملاء P2P وتبادل الملفات مثل برنامج تبادل Torrent الرائج على أهمية أساسية من الأدلة بما في ذلك الصور أو مقاطع الفيديو غير القانونية ، وحقوق الملكية الفكرية المسروقة.

يمكن أن تكون المعلومات حول الملفات التي يتم تنزيلها ومشاركتها وتحميلها إضافة مهمة إلى قاعدة أدلة تم جمعها.

ألعاب متعددة اللاعبين عبر الإنترنت

تحدث المحادثات بين جلسات اللعب وأثناءها في العديد من الألعاب الشائعة متعددة اللاعبين

فيتم توسيع قاعدة الأدلة من خلال تحليل سجلات الدردشة المستخرجة من هذه الألعاب اذ يمكن الحصول على ما يفيد اثناءها.

محتوى الوسائط المتعددة

يجب تحليل الصور الثابتة وملفات الفيديو اذ يمكن أن يساعد التحليل المحققين من خلال الكشف عن أشياء مثل المواد الإباحية ، الوجوه البشرية ، أو صور ممسوحة ضوئيا لمستندات نصية محفوظة كملفات صور (Rogers 2006)

أنواع الأدلة الرقمية

تشمل أنواع الأدلة الرقمية ما يلي والمزيد:

- دفاتر العناوين وقوائم الاتصال.
- الملفات الصوتية والتسجيلات الصوتية.
- تاريخ المتصفح
- النسخ الاحتياطية للبرامج تشمل النسخ الاحتياطية للاجهزة المحمولة.
- التقاويم
- أرشيف مضغوط ZIP ، RAR وما إلى ذلك بما في ذلك المحفوظات المشفرة التي قد تحتوي على معلومات الحساب وتواريخ الوصول الأخيرة وما إلى ذلك

- رسائل البريد الالكتروني والمرفقات وقواعد بيانات البريد الالكتروني.
- ملفات تعريف الارتباط
- قواعد البيانات
- المستندات
- الأحداث
- الملفات المخفية والنظام
- ملفات الدخول
- عناصر المنظم
- ملفات الصفحات وملفات الإسبات وملفات التخزين المؤقت للطابعة
- صور رقمية
- مقاطع فيديو
- الأجهزة الافتراضية
- ملفات النظام
- الملفات المؤقتة

استرداد السجلات وملفات المحفوظات

تحتوي السجلات وملفات المحفوظات على قدر كبير من الأدلة الأساسية. غالبا ما تكون اتصالات الدردشة مصحوبة بطوابع زمنية وألقاب للأطراف الأخرى ، مما يسمح بتحديد و بدقة من كان المستجيب . يعد تحديد الموقع الدقيق لهذه الملفات واسمها أمرا ضروريا وربما هو الخطوة الأولى المطلوبة لإجراء مزيد من التحليل (Rynearson 2002) عادة ما تحتفظ الإصدارات الأخيرة من (Windows) بالبيانات التي ينشئها المستخدم ويولدها التطبيق مجلدات (AppData) وملفات البرنامج والمستندات والإعدادات. بالإضافة إلى ذلك، تحتفظ هذه الأنظمة بتخزين افتراضي للتطبيقات التي

تم إطلاقها باستخدام الأذونات الإدارية \ AppData) .
Local \ VirtualStore)

هذه المواقع عادة ما يتم تجاهلها من قبل المحققين.

حتى الوثائق والإعدادات المعروفة يمكن أن تحمل أسماء مختلفة اعتمادا على اللغة الافتراضية لإصدار معين من (Windows) . (Rogers 2006)

يمكن أن يعقد التحليل بشكل أكبر من خلال نقل أو إعادة تسمية الملفات الشائعة.

بعد العثور على الملفات المهمة من خلال تحليل سجل (Windows)وتكوين تطبيقات

الملفات أو إجراء بحث يدوي / آلي ، فلاستخراج البيانات منها يجب معرفة التنسيق الدقيق لكل ملف من ملفات المصدر.

تستخدم العديد من التطبيقات الحديثة تنسيقات موثقة جيدا سهلة التحليل. على سبيل المثال ، يتم استخدام قواعد بيانات (SQLite) بواسطة (Skype و ICQ) ، تنسيق (XML) الشائع

يستخدم برنامج (Mirc chat) باستخدام برنامج MSN)
(messengerملفات نصية بسيطة، وما إلى ذلك .
(Rogers 2006)

يمكن التحقق من قواعد بيانات (SQLite) باستخدام برنامج عارض قاعدة بيانات (SQLite) المجاني ، بينما ملفات (XML) يمكن فتحها بسهولة باستخدام (Internet Explorer)ومع ذلك ، هناك العديد من التنسيقات الموجودة التي هي أقل ملاءمة لجمع الادلة الرقمية.

عقبات شائعة

لدى مستخدمي الكمبيوتر طريقة سهلة لجعل التحقيقات أبطأ وأكثر صعوبة.

وهي الأساليب التي يستخدمها المجرمون لإبطاء الاكتشاف:

تغيير الموقع الافتراضي لملفات المحفوظات ؛

نقل أو إعادة تسمية ملف أو مجلد المحفوظات ؛إخفاء و / أو حماية ملفات المحفوظات باستخدام سمات وأذونات نظام الملفات ؛

حذف ملفات المحفوظات ؛

تهيئة القرص الصلب بالكامل في محاولة لتدمير الأدلة

تشفير المجلد بأكمله ؛

عدم الاحتفاظ بالسجل عن طريق تعطيل كل التسجيل (إذا كان مدعوما بالتطبيق). (Anderson2015)

غالبية مستخدمي الكمبيوتر ليسوا متخصصين في أمن تكنولوجيا المعلومات ، لذا فإن معظم هذه العقبات ليست أكثر من إزعاج بسيط يمكن التغلب عليه بسهولة من خلال إنفاق القليل من الجهد.

للتغلب علي العقبات ، كحجب المعلومات فإن الطريقة الأكثر وضوحا لإخفاء المعلومات الموجودة على القرص هي إعطاء الملف اسم غامض أوحفظه في مكان غير عادي.

هذه الخدعة واضحة للغاية وتوفر القليل من الحماية بحيث لا توجد سياسة أمنية معقولة يمكن ان تسمح لها بالمرور ؛ ولكن يتم استخدامها من قبل المجرمين لان المحققون مقيدين بالوقت اذ لديهم دقائق معدودة إلى

ساعات قليلة كحد أقصى ، لاستخراج كل ما يمكنهم من الأدلة الممكنة ليقوموا بتحليلها .

يلتزم المحققون بقواعد صارمة لانه من خلال كسر أي من القواعد بفعل المحققين فان هذا المسلك قد يبطل جميع الأدلة المستخرجة .

استرداد الملفات المحجوبة : عند تغيير موقع الملف لا ينبغي للمرء أن يتوقع العثور على جميع معلومات المستخدم الموجودة في الموقع الافتراضي ، أو أن تكون موجودة فيه مهما كان الموقع الافتراضي لنوع معين من الملفات (مثل بيانات التطبيق أو مجلد مماثل) .

مطلوب البحث في القرص الثابت بأكمله من أجل تحديد موقع جميع ملفات السجل والمحفوظات غير المشفرة .

قد ينتج عن هذا عدد معين من الإيجابيات الزائفة على سبيل المثال ، ليس كل ملف (XML) هو ملف محفوظات (MSN)، لذا غالبا ما تكون عمليات التحقق الإضافية مطلوبة على سبيل المثال ، التحقق من وجود (MessageLog.xsl) بجوارملف (XML) (Anderson2015)

الأدلة المدمرة

محاولات تدمير الأدلة الرقمية شائعة جدا . يمكن أن تكون هذه المحاولات أكثر أو أقل نجاحا تبعا للإجراءات المتخذة والوقت المتاح لتدمير الأدلة ، فضلا عن نوع جهاز تخزين القرص الصلب المغناطيسي ، بطاقة الذاكرة المحمولة أو محرك (SSD) .

الملفات المحذوفة

غالبا ما ينتهي الدليل المهم في سلة المحذوفات (recycle bin) هذا ينطبق بشكل خاص على أجهزة الكمبيوتر التي تعمل بنظام (Windows) يمكن استرداد الملفات المحذوفة بنجاح عن طريق تحليل محتوى سلة التخزين المؤقتة ، حيث يتم وضعها قبل مسحها .

إذا لم تظهر الملفات المحذوفة في سلة المحذوفات ، فلا تزال هناك فرص جيدة لاستعادتها . (Akin2011).

باستخدام واحدة من العديد من أدوات استعادة البيانات التجارية مبدأ استعادة الملفات المحذوفة

استنادا إلى حقيقة أن (Windows) لا يمسح محتويات الملف عند حذفه .

بدلا من ذلك ، يتم وضع علامة على سجل نظام الملفات الذي يخزن الموقع الدقيق لذلك الملف على القرص "تم الحذف". يتم الإعلان عن مساحة القرص التي كان يشغلها الملف سابقا على أنها متاحة و من الأمثلة الجيدة على أدوات استعادة البيانات المنتجات التي طورتها ، (DiskInternals Partition Recovery) من خلال تحليل نظام الملفات و / أو مسح القرص الصلب بأكمله بحثا عن خصائص التوقيعات.

من أنواع الملفات المعروفة ، يمكن للمرء أن يسترد بنجاح ليس فقط الملفات التي تم حذفها من قبل المستخدم ، ولكن أيضا أدلة اخرى مثل النسخ المؤقتة لمستندات (Office). (Akin2011)

يمكن استكمال المعلومات المخزنة في الملفات المحذوفة بالبيانات التي تم جمعها من مصادر أخرى. على سبيل المثال ، تخزن (Skype) سجلات الدردشة

الخاصة بها في قاعدة بيانات المحفوظات ، وتحتفظ بالبيانات الداخلية التي قد تكون كذلك تحتوي على أجزاء وقطع من محادثات المستخدم في مجلد (chatsync) . هناك أدوات متاحة يمكنها تحليل مثل هذه الملفات مثل Belkasoft Evidence). Center2012)

محركات الأقراص الصلبة المهيأة

يمكن استرداد المعلومات من محركات الأقراص الثابتة التي قام المستخدم بتنسيقها باستخدام نحت البيانات أو باستخدام أداة استعادة البيانات التجارية.

تحليل ذاكرة الوصول العشوائي المباشر

يمكن استخراج أدلة رقمية إضافية من خلال تحليل محتوى ذاكرة الوصول العشوائي للكمبيوتر ، جهاز الكمبيوتر ذاكرة تشغيل متقلبة. بشكل عام ، يجب تشغيل الكمبيوتر الشخصي من أجل الأداء

تحليل ذاكرة الوصول العشوائي المباشر. هذا هو سبب توجيه المحققين لترك المشتبه بهم أجهزة الكمبيوتر قيد التشغيل إذا كانت قيد أوتركها في حالة الإيقاف.

هناك العديد من أدوات جمع الادلة المتاحة التي يمكن أن توفر لقطة لذاكرة الكمبيوتر والتي سنعرض لها لاحقا .

السيناريو الأسوأ

ماذا لو فعل المستخدم كل شيء بشكل صحيح لحماية معلوماته؟ ماذا إذا قام بتخزين كل شيء على وحدة تخزين مشفرة تم تكوينها لإزالتها عند قفل جهاز الكمبيوتر ؛ القفل تلقائيا بعد فترة من عدم النشاط ؛ منع سائقي (FireWire) لمنع هجمات (FireWire) ؛

تعيين كلمة مرور (BIOS) وقفل تسلسل التمهيد ؛ تعطيل السجلات وملفات المحفوظات حيثما أمكن ، أو مسحها بشكل آمن إذا لم يكن كذلك ؛ تعطيل ملفات الترحيل ... إذا قام المتعدي بكل ذلك لن يتمكن المحققون من استخراج الكثير من هذا الكمبيوتر إن وجد .

رغم ذلك لا يزال بإمكان المحققين البحث في أجهزة كمبيوتر الضحايا وتحليل سجلات مزود الإنترنت وجمع الأدلة من الهواتف المحمولة والأجهزة اللوحية المشتبه بها . (Hayes 2013)

كما ان معظم المجرمين من الناس العاديين ومستخدمي الكمبيوتر العاديين. غالبا ، إنهم يؤمنون بالأمن من خلال الغموض. إنهم يميلون إلى التضحية بالأمن من أجل الراحة .

إنهم ليسوا عادة متخصصين في أمن تكنولوجيا المعلومات المدربين ، لذلك من المرجح أن يفوتهم واحد أو أكثر من الأشياء ، مما يفتح الطريق أمام المحققين لاقتحام وجمع الأدلة المطلوبة باستخدام الأساليب المدربين على استخدامها .

6.4 أنواع التحليل

تعتمد أنواع التحليل المختلفة على التفسير ، أو التجريد ، والطبقات ، والتي تعد عموما جزءا من تصميم البيانات (Carrier. 2003) .

على سبيل المثال ، البيانات الموجودة على القرص الصلب، الذي تم تصميمه مع عدة طبقات.

أقل طبقة قد تحتوي على 3 أقسام أو حاويات أخرى تستخدم لإدارة وحدة التخزين.

يوجد داخل كل قسم بيانات تم تنظيمها في نظام ملفات أو قاعدة بيانات. و البيانات في ملف النظام هي تفسير لإنشاء الملفات التي تحتوي على بيانات في شكل تطبيق محددة. كل طبقة من هذه الطبقات لديها تقنيات ومتطلبات التحليل الخاصة بها .

تتضمن أمثلة أنواع التحليل الرقمي الشائعة:

تحليل الوسائط: تحليل البيانات من جهاز تخزين. لا يعتبر هذا التحليل أي أقسام أو هياكل بيانات محددة خاصة بنظام التشغيل.

إذا كان جهاز التخزين يستخدم وحدة ذات حجم ثابت ، مثل القطاع ، فيمكن استخدامه في هذا التحليل. (Kaspersky Lab 2015)

تحليل إدارة الوسائط: تحليل نظام الإدارة المستخدم لتنظيم الوسائط. يتضمن هذا عادة أقساما وقد يشمل إدارة وحدة التخزين أو أنظمة (RAID) التي تقوم بدمج البيانات من أجهزة تخزين متعددة في جهاز تخزين افتراضي واحد.

تحليل نظام الملفات: تحليل بيانات نظام الملفات داخل قسم أو قرص. يتضمن هذا عادة معالجة البيانات لاستخراج محتويات الملف أو لاستعادة محتويات الملف المحذوف.

تحليل التطبيق: تحليل البيانات داخل الملف. يتم إنشاء الملفات من قبل المستخدمين والتطبيقات ويكون تنسيق المحتويات مخصصا للتطبيق .

تحليل الشبكة: تحليل البيانات على شبكة الاتصالات. حزم الشبكة يمكن أن درست باستخدام نموذج (OSI) لتفسير البيانات الخام إلى تيار على مستوى

التطبيق. تحليل التطبيق هو فئة كبيرة من تقنيات التحليل لأن هناك العديد من أنواع التطبيقات.

بعض من أنواع التطبيقات الأكثر شيوعا :

تحليل نظام التشغيل: نظام التشغيل هو تطبيق ، على الرغم من أنه تطبيق خاص لأنه أول نظام يتم تشغيله عند بدء تشغيل جهاز كمبيوتر. يفحص هذا التحليل ملفات التكوين وبيانات المخرجات لنظام التشغيل لتحديد الأحداث التي قد حدثت. (Kaspersky Lab 2015)

التحليل القابل للتنفيذ: الملفات القابلة للتنفيذ هي كائنات رقمية يمكن أن تتسبب في حدوث أحداث ويتم فحصها بشكل متكرر أثناء تحقيقات الاختراق لأن المحقق يحتاج إلى تحديد الأحداث التي يمكن أن يسببها الملف التنفيذي.

تحليل الصورة: الصور الرقمية هي الهدف من العديد من التحقيقات الرقمية. يبحث هذا النوع من التحليل عن معلومات حول مكان التقاط الصورة ومن أو ماذا يوجد في الصورة. يتضمن تحليل الصورة أيضا فحص الصور بحثا عن أدلة إخفاء المعلومات. (Acharya 2013)

تحليل الفيديو: يتم استخدام الفيديو الرقمي في كاميرات الأمن وكاميرات الفيديو الشخصية وكاميرات الويب. يمكن أن تتضمن التحقيقات في الحيوانات المفترسة عبر الإنترنت أحيانا فيديو رقمي من كاميرات الويب. يفحص هذا النوع من التحليل مقطع الفيديو للتعرف على الكائنات الموجودة في الفيديو والمكان الذي تم تصويره فيه

قد يلزم إعادة النظر في مفهوم وجود صورة للقرص مع زيادة حجم القرص وتصبح عملية نسخ كل قرص غير ممكنة. في حين أنه من المفيد أن تكون قادرة على

إعطاء نسخة شبيهة من القرص او صورة، فبالنظر الى مشهد الجريمة المادية نجد ان المحققون المكلفون بإنفاذ القانون يجتهدون في مكان الحادث بحثا عن أدلة ويقدمون الدليل ضد الدفاع ، بينما الدفاع غير قادرعلى إجراء تحقيقه الخاص. (Jang 2018)`

مثال لضرورة اعادة النظر فانه ترفع بصمات الأصابع من الجدران في مكان الجريمة ، لكن الجدار لا يمسك به كدليل. (Kaye 1995)

قد تظهر التحديات الجديدة المتمثلة في جمع الادلة الرقمية في الوقت الفعلي ومتطلبات الجهوزية للخوادم يكون من الممكن تقديم الأدلة إلى المحكمة حتى في حالة عدم عمل صورة كاملة.

كما إن عدم وجود صورة كاملة قد يؤدي لإجراء استنتاجات خاطئة و أدلة متناقضة غير مقبولة بواسطة المحكمة. لا يتعلق الأمر بالحفاظ على الأدلة لأننا لم نتعرف بعد على أي دليل.

يعد الحفاظ على مسرح الجريمة الرقمية أمرا مهما ، وعادة ما يتم الاحتفاظ ببيانات الوثائق المرتبطة بمرحلة ما قبل الحفظ. (Akin 2011)

جعلت MD5 أو SHA-1 أي تغييرات للصور وغيرها من البيانات التي يتم نسخها من على النظام من الاجزاء التي يمكن ان يتم الكشف عنها.

تتم دعوة وتشجيع الهيئات الحكومية التقليدية المكلفة بإنفاذ القانون إلى التحقيق في الجرائم التقليدية او المعروفة في العالم ، و أيضا تتم الدعوة والتشجيع فيما يخص التحقيق في الجرائم التي تقع على الإنترنت.

تقوم العديد من الوكالات الحكومية المعروفة في معظم دول العالم بنشر وتحديث قائمة المطلوبين من مجرمي الإنترنت ، بنفس الطريقة التي تقوم بها تجاه المجرمين التقليديين المدرجين في القائمة الخاصة بمجرمي الانترنت.

7.4 ما هو التحقيق في جرائم الإنترنت

يشمل هذا الجزء من البحث استكشاف الأدوات والتقنيات التي تستخدمها وكالات التحقيق في الجرائم الإلكترونية العامة والخاصة للتعامل مع أنواع مختلفة من الجرائم الإليكترونية.

قبل الانتقال إلى اطر التحقيق ، لا بد من ان نعود إلى الأساسيات:

اولا: نؤكد ان الجريمة الرقمية أو الجريمة الإليكترونية هي جريمة تنطوي على استخدام جهاز كمبيوتر أو هاتف أو أي جهاز رقمي آخر متصل بشبكة.

ثانيا: يمكن استخدام هذه الأجهزة الإلكترونية في شيئين: تنفيذ الجريمة الإليكترونية (أي شن هجوم سيبراني) ، أو التصرف كضحية ، من خلال تلقي الهجوم من مصادر ضارة أخرى.

ثالثا: فإن التحقيق في الجرائم الإليكترونية هو عملية التحقيق في البيانات الرقمية الشرعية الجنائية المهمة وتحليلها واستعادتها من الشبكات المعنية بالهجوم - وقد يكون ذلك هو الإنترنت و / أو الشبكة المحلية - من أجل تحديد مخططي ومرتكبي الجريمة الرقمية ومقتضيات النوايا الحقيقية.

رابعا: يجب أن يكون محققو الجرائم الإليكترونية خبراء في علوم الكمبيوتر ، وايضا يكونوا قادرين

على فهم ليس فقط البرامج وأنظمة الملفات وأنظمة التشغيل ، ولكن أيضا كيف تعمل الشبكات والأجهزة. (Akin2011)

خامسا: يجب أن يكون المحققون على دراية كافية لتحديد كيفية حدوث التفاعلات بين هذه المكونات ، وللحصول على صورة كاملة لما حدث ، ولماذا حدث ذلك ، ومن ارتكب الجريمة الإلكترونية نفسها ، وكيف يمكن للضحايا حماية أنفسهم في المستقبل ضد هذه الأنواع من التهديدات الإليكترونية.

8.4 من الذي يجري التحقيقات في جرائم الإنترنت؟

أ. وكالات العدالة الجنائية

وكالات العدالة الجنائية هي الجهات التي تقف وراء حملات منع الجريمة الإليكترونية والتحقيق مع المجرمين الرقميين ورصدهم ومحاكمتهم.

غالبا ما تتعامل وكالة العدالة الجنائية (مثال الشرطة والنيابة حسب السلطة المتعلقة بالتحقيق الممنوحة) مع جميع القضايا المتعلقة بجرائم الإنترنت.

على سبيل المثال ، في الولايات المتحدة ووفقا للحالة ، يمكن التحقيق في الجريمة الإليكترونية من قبل مكتب التحقيقات الفيدرالي (FBI) أو الخدمة السرية الأمريكية أو مركز شكاوى الجريمة عبر الإنترنت أو دائرة التفتيش البريدي في الولايات المتحدة أو لجنة التجارة الفيدرالية. (Kaspersky 2015).

في بلدان أخرى مثل إسبانيا ، تتولى الشرطة الوطنية والحرس المدني العملية بأكملها وحتى المحكمة، بغض النظر عن نوع الجرائم الإلكترونية التي يجري التحقيق فيها .

في السودان تتولى شرطة المعلوماتية، ونيابة المعلوماتية ومحكمة المعلوماتية العملية باكملها .

ب. وكالات الأمن القومي

يتغير هذا أيضا من بلد إلى آخر ، ولكن بشكل عام ، يحقق هذا النوع من الوكالات عادة في الجرائم الإلكترونية المرتبطة مباشرة بالوكالة .

على سبيل المثال ، يجب أن تكون وكالة الاستخبارات مسؤولة عن التحقيق في الجرائم الإلكترونية التي لها صلة ما بمنظمتهم ، مثل شبكاتها أو موظفيها أو بياناتها ؛ أو تم تنفيذها من قبل الجهات الفاعلة .

في الولايات المتحدة ، هناك مثال جيد آخر هو الجيش ، الذي يدير تحقيقاته الخاصة بجرائم الإنترنت باستخدام موظفين داخليين مدربين بدلا عن الاعتماد على الوكالات الفيدرالية..

ج. وكالات الأمن الخاصة

أجهزة الأمن الخاصة مهمة أيضا في مكافحة الجريمة الإليكترونية ، خاصة أثناء عملية التحقيق. بينما تدير الحكومات والوكالات الوطنية شبكاتها وخوادمها وتطبيقاتها الخاصة ، فإنها لا تشكل سوى جزء صغير من البنية التحتية الهائلة والرمز الذي تديره الشركات الخاصة والمشروعات والمؤسسات والأفراد حول العالم .

مع وضع ذلك في الاعتبار ، ليس من المستغرب أن يلعب خبراء الأمن السيبراني الخاص وشركات الأبحاث والفرق

المهنية دورا مهما عندما يتعلق الأمر بمنع ومراقبة وتخفيف والتحقيق في أي نوع من جرائم الأمن السيبراني ضد الشبكات أو الأنظمة أو البيانات التي تعمل على بيانات خاصة تابعة لجهات خارجية كالمراكز والشبكات والخوادم أو أجهزة الكمبيوتر المنزلية البسيطة.

لا تعرف المجموعة الواسعة من جرائم الإنترنت التي تحقق فيها الوكالات الخاصة حدودا، ولا تشمل على سبيل المثال لا الحصر ، الاختراق والتكسير وتوزيع الفيروسات والبرامج الضارة وهجمات DDoS والاحتيال عبر الإنترنت وسرقة الهوية والهندسة الاجتماعية. (Jang 2018)

9.4 تقنيات التحقيق في الجرائم الإلكترونية

بينما قد تختلف التقنيات اعتمادا على نوع الجريمة الالكترونية قيد التحقيق ، او من الذي يقوم بالتحقيق ، فإن معظم الجرائم الإليكترونية تخضع لبعض التقنيات الشائعة المستخدمة أثناء عملية التحقيق.

i **التحقق من الخلفية :**

إن إنشاء وتعريف خلفية الجريمة مع الحقائق المعروفة يساعد المحققين على تحديد نقطة للبداية لتحديد ما يواجهونه ، ومقدار المعلومات التي لديهم عند التعامل مع تقرير الجرائم الالكترونية الأولية.

ii **جمع المعلومات :**

من أهم الأشياء التي يجب على أي محقق في الجريمة الإليكترونية القيام بها هو الحصول على أكبر قدر ممكن من المعلومات حول الحادث.

هل كان هجوما آليا أم جريمة مستهدفة إنسانية؟ هل كانت هناك أي فرصة مفتوحة لهذا الهجوم؟ ما هو نطاقها وتأثيرها؟ هل يمكن تنفيذ هذا الهجوم من قبل أي شخص أو أشخاص معينين لديهم مهارات محددة؟ من هم المشتبه بهم المحتملين؟ ما الجرائم الرقمية التي ارتكبت؟ هل يمكن توفير الدليل أن وجدت الجريمة الرقمية؟ هل توجد إمكانية للوصول إلى مصادر الأدلة المطلوبة؟

هذه الأسئلة وغيرها هي اعتبارات قيمة أثناء عملية جمع المعلومات. (Jang 2018)

تستخدم الكثير من الوكالات الوطنية والاتحادية المقابلات وتقارير المراقبة للحصول على دليل على الجرائم الإليكترونية. لا تشمل المراقبة الكاميرات الأمنية ومقاطع الفيديو والصور فحسب ، بل تشمل أيضا المراقبة الإلكترونية للأجهزة التي تعرض بالتفصيل ما يتم استخدامه ومتى وكيف يتم استخدامه وكل السلوكيات الرقمية المعنية.

تتمثل إحدى الطرق الأكثر شيوعا لجمع البيانات من مجرمي الإنترنت في تكوين مصيدة مخترقي الشبكات التي تعمل كضحية أثناء جمع الأدلة التي يمكن استخدامها لاحقا ضد الهجمات.

iii **تتبع وتحديد المخططين :**

يتم تنفيذ هذه الخطوة التالية في بعض الأحيان أثناء عملية جمع المعلومات ، اعتمادا على كمية المعلومات الموجودة بالفعل.

من أجل تحديد هوية المجرمين وراء الهجوم السيبراني ، تعمل وكالات الأمن الخاصة والعامة

على السواء مع مزودي خدمات الإنترنت وشبكات التواصل للحصول على معلومات قيمة عن سجلات اتصالاتهم ، فضلا عن الخدمة التاريخية والمواقع الإلكترونية والبروتوكولات المستخدمة أثناء اتصالهم .
غالبا ما تكون هذه هي أبطأ مرحلة ، حيث تتطلب إذنا قانونيا من المدعين العامين وأمر من المحكمة للوصول إلى البيانات المطلوبة 2011) . (Akin

10.4 الادلة الشرعية الرقمية :

بمجرد قيام الباحثين او المحققين بجمع بيانات كافية حول الجريمة الإليكترونية ، فقد حان الوقت لفحص الأنظمة الرقمية التي تأثرت ، أو تلك التي من المفترض أن تكون متورطة في أصل الهجوم. تتضمن هذه العملية تحليل البيانات الأولية لاتصال الشبكة والأقراص الصلبة وأنظمة الملفات وأجهزة التخزين المؤقت وذاكرة (RAM) وغيرها .

بمجرد بدء العمل للحصول على الدليل الشرعي، يقوم المحقق المعني بمتابعة جميع المسارات المعنية التي تبحث عن بصمات الأصابع في ملفات النظام ، وسجلات الشبكة والخدمات ، ورسائل البريد الإلكتروني ، وسجل تصفح الويب ، إلخ.

11.4 أهم أدوات جمع الادلة الشرعية للتحقيق في جرائم الإنترنت

تتضمن أدوات التحقيق في جرائم الإنترنت الكثير من الأدوات المساعدة ، اعتمادا على التقنيات التي تستخدمها والمرحلة التي تمر بها. ومع ذلك ، لا بد من التأكد من أن معظم هذه الأدوات مخصصة للتحليل

الجنائي للبيانات بمجرد الحصول على الأدلة في متناول اليد .

هناك الآلاف من الأدوات لكل نوع من أنواع الجرائم الإلكترونية ، لذلك ، لم يقصد البحث بالاشارة الى هذه الادوات أن تكون قائمة شاملة ، بل هي مجرد إلقاء نظرة سريعة على بعض أفضل الموارد المتاحة لأداء نشاط الادلة الشرعية . (Akin2011)

1-محطة عمل SIFT

سفت (SIFT) هي عبارة عن مجموعة من أدوات جمع الادلية الشرعية تم إنشاؤها لمساعدة فرق الاستجابة للحوادث والباحثين في جمع الادلية الشرعية و فحص بيانات جمع

شكل4-2 محطة عمل سفت(SIFT 2017)

الادلة الشرعية الرقمية على العديد من الأنظمة .

يدعم أنواعا مختلفة من أنظمة الملفات مثل FAT 12/16/32بالإضافة إلى NTFS و (HFS +) و (/ EXT2 3/4) و (UFS1 / 2v) و (vmdk) و (swap) و (RAM و data) و .(RAW)

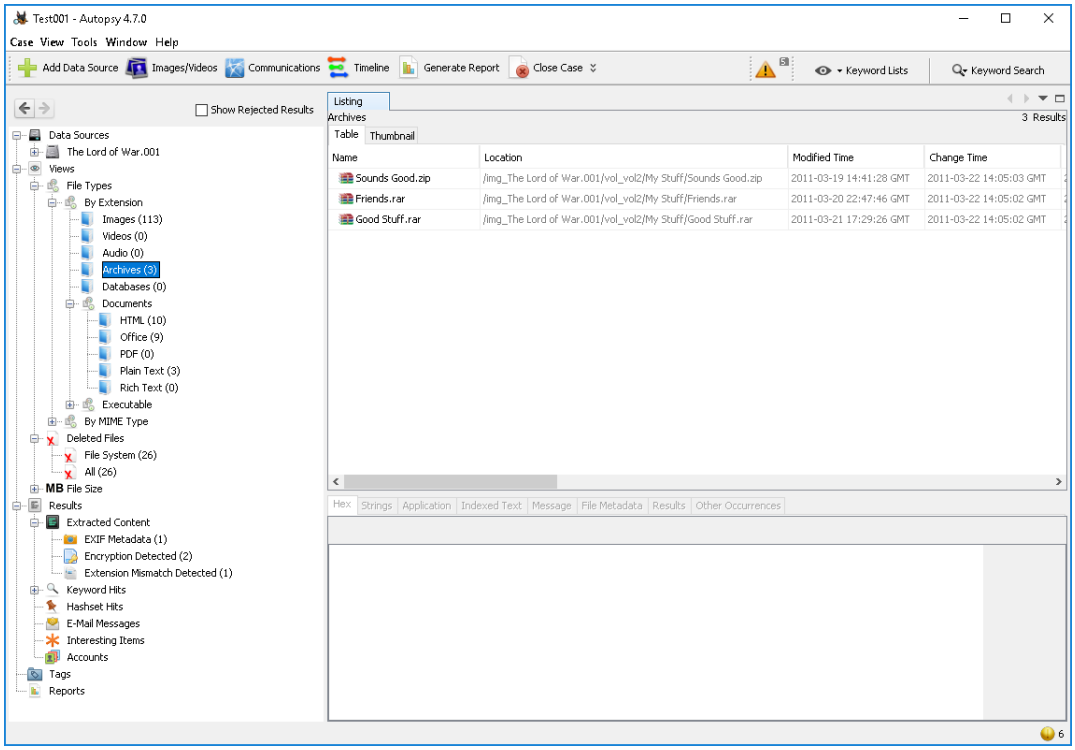
عندما يتعلق الأمر بدعم الصور ، فهو يعمل تماما مع ملفات صور خام واحدة ، و (AFF) تنسيق الادلة الشرعية المتقدم ، و (EWF) وتنسيق الشهود الخبراء ، و (EnCase)، و (AFM) (AFF) مع البيانات الوصفية الخارجية، وغيرها الكثير. (SIFT 2017)

لتشمل الميزات المهمة الأخرى نظام Ubuntu LTS) (64 16.04بت ، وأحدث ادوات جمع الادلة الشرعية ، والتوافق المتبادل بين نظامي (Linux) و (Microsoft Windows)، وخيار التثبيت كنظام مستقل ، ووثائق واسعة للرد على جميع الاحتياجات الجنائية. (Jang 2018)

وتعد هذه المحطة هي الأفضل للجميع ، لانها مفتوحة المصدر وخالية تماما.

2-طقم الأسنان The Sleuth Kit

يعد طقم الأسنان (The Sleuth Kit) ، الذي كتبه براين كاريير والمعروف باسم (TSK) ، مجموعة مفتوحة المصدر من ادوات جمع الادلة الشرعية المستندة إلى نظامي (Unix) و (Windows) والتي تساعد الباحثين على تحليل صور القرص واستعادة الملفات من تلك الأجهزة.

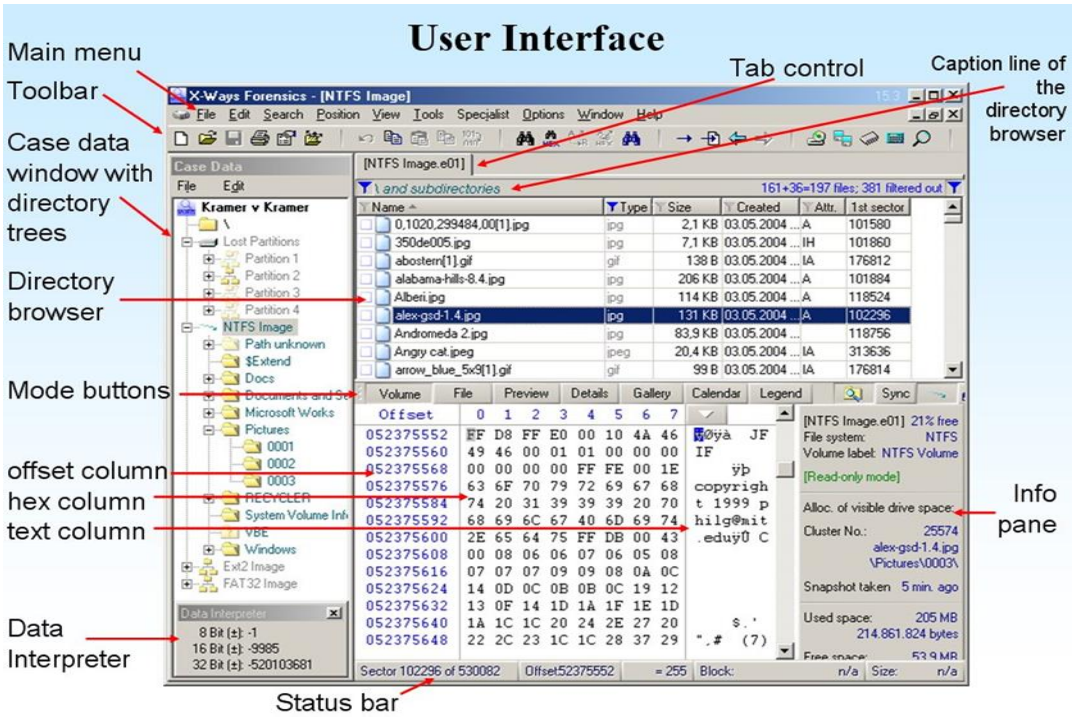


شكل 4-3 طقم الأسنان (kit 2017)

تشمل ميزاته

دعم التحليل الكامل لأنظمة الملفات مثل / FAT) (ExFATو (NTFS) و (Ext2/ 3/4) و (UFS 1/2) و (HFS)و (ISO 9660) و (YAFFS2)، مما يؤدي إلى تحليل أي نوع من الصور أو الأقراص تقريبا لنظام التشغيل (Windows) وأنظمة التشغيل (Unix) وايضا المستندة إلى (Linux).

يعد (Sleuth Kit)، المتوفر من سطر الأوامر أو المستخدم كمكتبة ، الحليف المثالي لأي شخص مهتم باستعادة البيانات من أنظمة الملفات وصور القرص الخام. (kit 2017)



شكل4-4 طرق جمع الادلة الشرعية X: (ways 2017)

3 - طرق جمع الادلة الشرعية X:

يعد هذا البرنامج واحدا من أكثر مجموعات الأدلة الجنائية اكتمالا لأنظمة التشغيل المستندة إلى (Windows)، لانه مدعوم على نطاق واسع لأي إصدار من (Windows) تقريبا ،

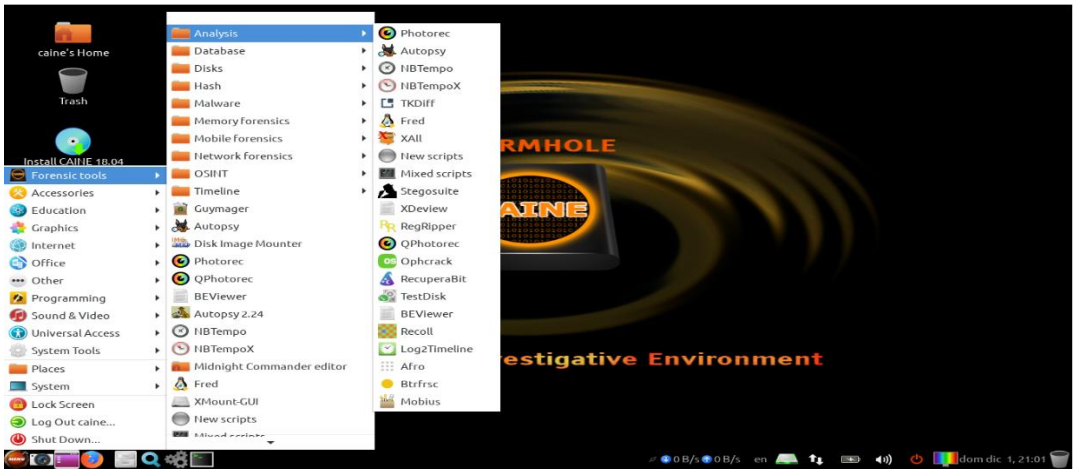
مما يجعله أحد الأفضل في هذا السوق المعين ويتيح العمل بسهولة مع إصدارات مثل (Windows XP / 2003 / 2012/10 / 8.1 / 2008/7/8 / Vista //) كلا 32 بت / 64 بت. واحدة من أروع معالمه هو حقيقة أنه محمول تماما ، مما يجعل من الممكن تشغيله وسهولة الحصول عليه من جهاز كمبيوتر إلى آخر. (ways 2017)

تشمل ميزاته الرئيسية: القدرة على أداء استنساخ القرص والتصوير ، وقراءة الأجزاء من ملفات الصور الخام ، (HDDS) ، صفائف (RAID) ، (LVM2) وأكثر من ذلك بكثير.

كما يوفر الكشف المتقدم عن الأقسام المحذوفة في (FAT12) و (FAT16) و (FAT32) و (ExFAT) و (TFAT)و (NTFS) و) و (Ext2) و (Ext3 و (Ext4) وغيرها ، وكذلك نحت الملفات المتقدم وإنشاء كتالوج الملفات والدليل. (Alghafli & Martin 2011)

4-كـــــيـــــن CAINE

وهذا ليس تطبيقا بسيطا للتحقيق في جرائم الإنترنت أو مجموعة ، إنه توزيع كامل لنظام (Linux) يستخدم لتحليل الادلة الشرعية الرقمية.



شكل4-5 كين (caine 2017) (caine 2017)

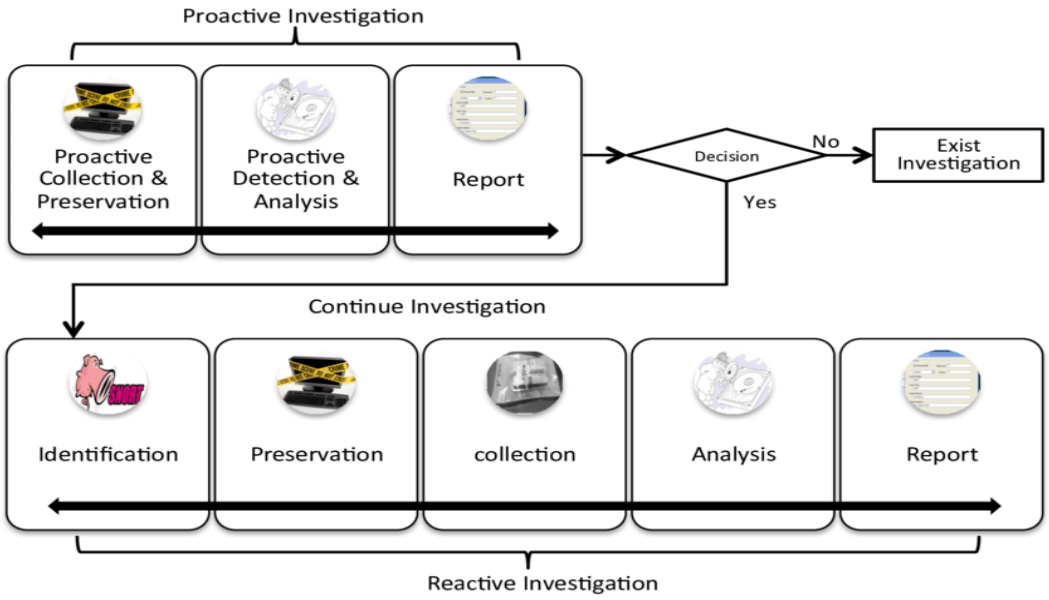
إنه يعمل من القرص المضغوط المباشر ، ويمكن أن يساعد في استخراج البيانات التي تم إنشاؤها على أنظمة تشغيل متعددة مثل (Linux) و (Unix) و (Windows).

نظام الملفات أو الذاكرة أو استخراج بيانات الشبكة ، يمكن لـــ (CAINE) أن يفعل كل ذلك من خلال الجمع بين أفضل برامج الادلة الشرعية التي تعمل على كل من واجهات سطر الأوامر والقائمة على واجهة المستخدم الرسومية.

ويشمل تطبيقات شهيرة للتحقيق في الجرائم الرقمية مثل (The Sleuth Kit) و (Autopsy) و (Wireshark) و (PhotoRec)و (Tinfoleak) وغيرها الكثير. (caine 2017)

5-إطار جمع الادلة الشرعية الرقمية

يعرف (Digital Forensics Framework) ، المعروف باسم (DFF) ، بأنه برنامج مفتوح المصدر للادلة الشرعي للكمبيوتر يسمح لمحترفي الطب الشرعي الرقمي باكتشاف وحفظ نشاط النظام على كل من أنظمة تشغيل (Windows)و (Linux).



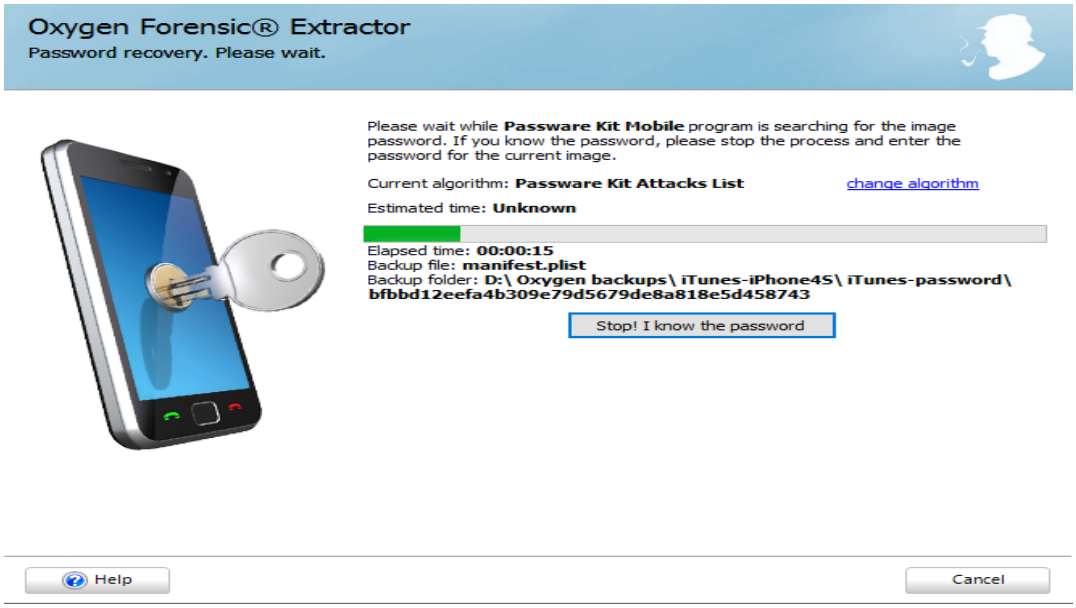
شكل4-6 إطار جمع الادلة الشرعية الرقمية (framework 2017)

يسمح للباحثين بالوصول إلى الأجهزة المحلية والبعيدة مثل محركات الأقراص القابلة للإزالة ، ومحركات الأقراص المحلية ، وأنظمة ملفات الخادم عن بعد ، وكذلك إعادة بناء الأقراص الافتراضية لبرنامج (VMware) عندما يتعلق الأمر بأنظمة الملفات ، يمكنه استخراج البيانات من (FAT12 / 16/32) و (EXT)

(NTFS) و 2/3/4) على كل من الملفات و الدلائل النشطة و المحذوفة. كما أنه يساعد على فحص و استعادة البيانات من بطاقات الذاكرة بما في ذلك اتصالات الشبكة و الملفات و العمليات المحلية framework) . 2017)

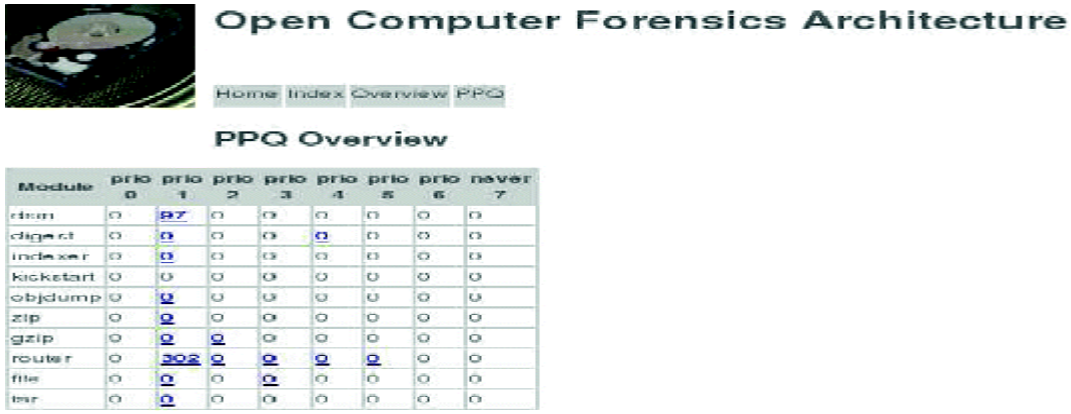
6-مخبر الأكسجين الشرعي Oxygen Forensic Detective

هذه الأداة هي واحدة من أفضل تطبيقات الادلة الشرعية متعددة المنصات المستخدمة من قبل الباحثين في مجال الأمن و المهنيين في الادلة الشرعية لتصفح جميع البيانات الهامة في مكان واحد باستخدام هذه الاداة يمكن استخراج البيانات من العديد من الأجهزة المحمولة و الطائرات بدون طيار ونظام تشغيل الكمبيوتر ، بما في ذلك:



شكل 4-7 مخبر الأكسجين الشرعي (Detective 2017)

7- فتح هندسة الدليل الشرعي للكمبيوتر Open Computer Forensics Architecture



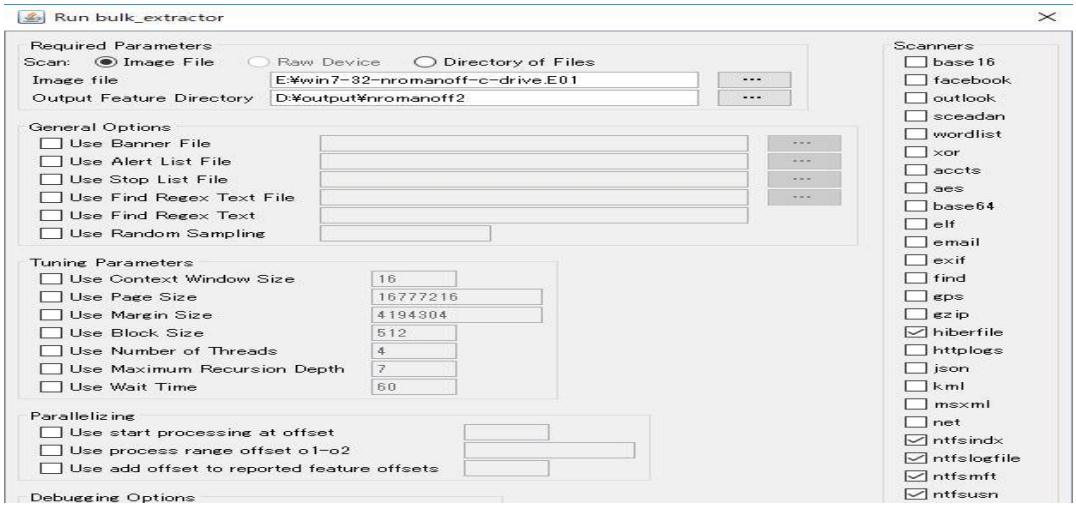
شكل 4-8 فتح هندسة الدليل الشرعي للكمبيوتر (Architecture 2017)

الحصول على كلمات المرور من النسخ الاحتياطية لنظام التشغيل المشفر ، وتجاوز قفل الشاشة على نظام (Android)، والحصول على بيانات المكالمات المهمة. يعتبر هذا الجهاز ، المعروف باسم (OCFA) ، إطار عمل لتحليل الدليل الشرعي للكمبيوتر وقد كتبته وكالة الشرطة الوطنية الهولندية.

8-النازع بالجملة Bulk Extractor

لقد طور الهولنديون هذا البرنامج سعيا لتحقيق الهدف الرئيسي المتمثل في تسريع التحقيقات في الجرائم الرقمية ، والسماح للباحثين بالوصول إلى البيانات من واجهة موحدة وصديقة لل (UX). لقد تم دمجها في جزء من العديد من أدوات التحقيق في جرائم الإنترنت الشائعة مثل (The Sleuth Kit) و (Scalpel) و (PhotoRec) أو غيرها ، أو جزء منها. (Extractor 2017)

على الرغم من توقف المشروع الرسمي منذ وقت ليس بالقصير ، إلا أن هذه الأداة لا تزال تستخدم كأحد أفضل حلول الادلة الشرعية بواسطة وكالات من جميع أنحاء العالم.



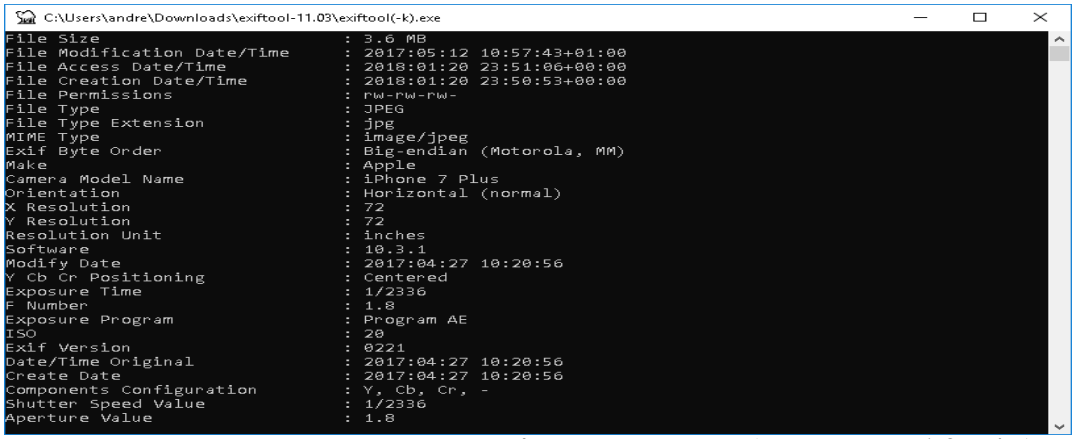
شكل4-9 النازع بالجملة (Extractor 2017)

هناك العديد من المشاريع الأخرى ذات الصلة التي لا تزال تعمل مع قاعدة كود (OCFA)، ويمكن الاطلاع على تلك على الموقع الرسمي في (SourceForge)

يعتبر التطبيق أحد أكثر التطبيقات المستخدمة لاستخراج المعلومات الهامة من بيانات الأدلة الرقمية شيوعا.

إنه يعمل عن طريق استخراج ميزات مثل عناوين (URL) وعناوين البريد الإلكتروني وأرقام بطاقات الائتمان وغير ذلك الكثير من الصور والدلائل الموجودة على قرص (ISO) أو الملفات ببساطة - بما في ذلك الصور ومقاطع الفيديو والملفات المستندة إلى المكتب والملفات المضغوطة فهو أداة لا تستخدم فقط لاستخراج البيانات ، ولكن أيضا للتحليل والتجميع. واحدة من أفضل سماتها هي دعمها الواسع لأي نظام تشغيل تقريبا ، بما في ذلك (Linux) و (Unix) و (Mac) و (Windows) ، كل ذلك دون مشكلة.

.



شكل4-10 اداة الخروج Exitool

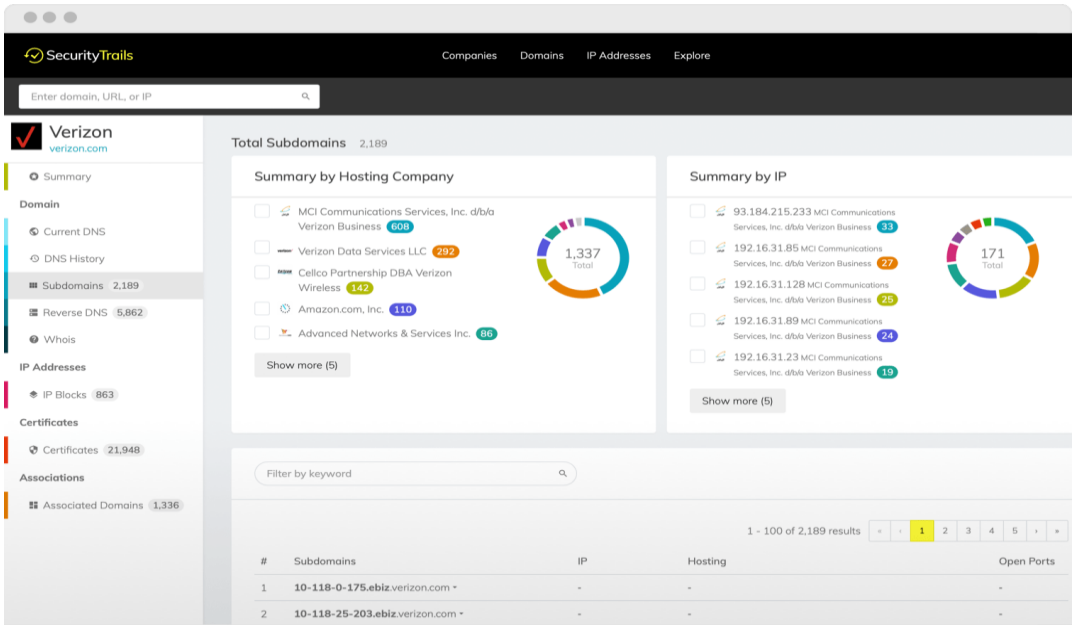
9- اداة الخروج ExifTool :

هذه الأداة الشرعية التي تم كتابتها في بيرل والتي طورها (Phil Harvey) هي أداة مساعدة قائمة على سطر الأوامر يمكنها قراءة البيانات الوصفية وكتابتها ومعالجتها من العديد من ملفات الوسائط مثل الصور ومقاطع الفيديو.

يدعم (ExifTool) استخراج (EXIF) من الصور والفيديو (بيانات التعريف العامة والمحددة) مثل إحداثيات (GPS)، والصور المصغرة ، ونوع الملف ، والأذونات ، وحجم الملف ، ونوع الكاميرا ، إلخ.كما يسمح لك بحفظ النتائج بتنسيق نصي أو (HTML) عادي.

10- متجول السطح SurfaceBrowser

يعتبر (SurfaceBrowser) واحدا من الحلفاء المثاليين للمحقق لاكتشاف البنية التحتية الكاملة عبر الإنترنت لأي شركة ، وللحصول على بيانات استخبارية قيمة من سجلات (DNS) ، وأسماء النطاقات وسجلات (WHOIS)



شكل 4-11 متجول السطح

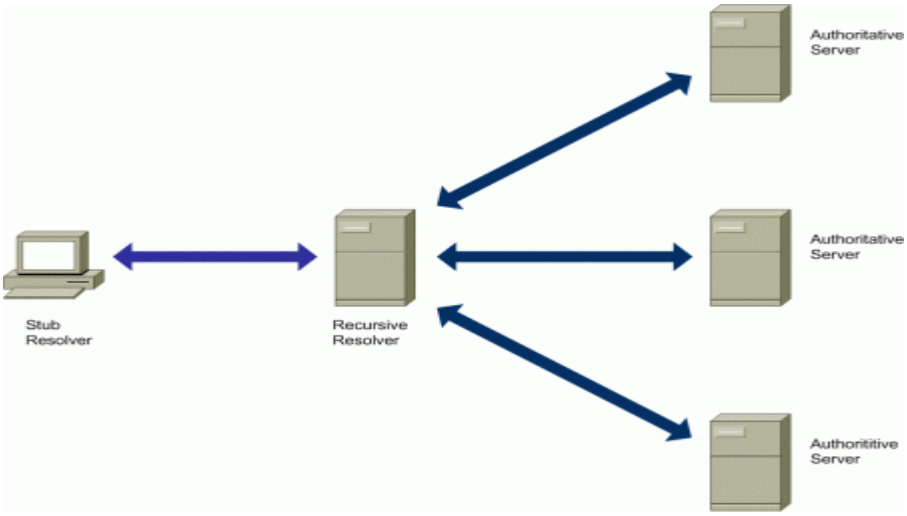
التاريخية ، والنطاقات الفرعية المكشوفة، وبيانات شهادات (SSL) ، وغير ذلك الكثير

يعد تحليل بيانات لأي شركة أو اسم مجال على الإنترنت بنفس أهمية تحليل محركات الأقراص المحلية ، فقد يؤدي التحليل إلى العثور على بيانات مهمة يمكن ربطها بجريمة او جرائم وقعت على الإنترنت.

11- الحصول على بيانات DNS الحالية

تعد سجلات (DNS) مصدرا غير محدود للذكاء عندما يتعلق الأمر بالأمن السيبراني . إنهم يملكون مفتاح جميع أصول الإنترنت المكشوفة للويب والبريد الإلكتروني والخدمات الأخرى.

يسمح (SurfaceBrowser) بعرض سجلات (A) و (AAAA) و (MX) و (NS) و (SOA) و (TXT) على الفور:



شكل 4-12 الحصول على بيانات DNS الحالية

بيانات DNS :

تحليل سجلات DNS التاريخية

يميل الكثير من المجرمين إلى تغيير سجلات (DNS) عندما يرتكبون أنشطتهم الضارة عبر الإنترنت ، تاركين مسارات أين وكيف فعلوا الأشياء على مستوى (DNS) بغض النظر عن نوع سجل (DNS) الذي استخدمه المعتدي على النظام ، يمكن استكشاف أي سجل (A) أو (AAAA) أو (MX) أو (NS SOA) أو (TXT) ؛و الحصول على تغطيته .

شكل 4-13 تحليل سجلات DNS التاريخي

عندما لا يتم توجيه الهجوم إلى الخوادم أو التطبيقات ولكن إلى أسماء النطاقات ، فإنه غالبا ما يتضمن بيانات (WHOIS) .

بالنسبة لهذا النوع من المواقف ، يصبح الجدول الزمني لسجل (SurfaceBrowser) (WHOIS) هو أفضل معين ، اذ انه يتيح رؤية أي تغييرات على مستوى المسجل لجميع معلومات (WHOIS) الخاصة.

الجدول الزمني لتاريخ WHOIS

يتيح سجل (WHOIS) هذا الانتقال للخلف وللأمام فورا ، للحصول على معلومات دقيقة حول مسجل النطاق ومسجل (WHOIS) والمشرف والاتصال التقني في غضون ثوان معدودة.

تفاصيل WHOIS

الاستيلاء على بيانات كتلة IP كاملة

أثناء التحقيق في جريمة رقمية تنطوي على الشركات والشبكات وخاصة عناوين (IP) ، يعد الحصول على خريطة (IP) الكاملة للبنية التحتية المعنية أمرا بالغ الأهمية.

بيانات كتلة IP

يسمح (SurfaceBrowser) باستكشاف عناوين (IP) مفردة وكتل (IP) كاملة ، كما يمكن تصفية نطاقات (IP) حسب المسجل الإقليمي أو حجم الشبكة الفرعية.

كتل (IP) القائمة الكاملة

بمجرد الحصول على قائمة كاملة من كتل (IP) ، يمكن الحصول على عدد (IP) الكامل لكل واحد ، وكلاء

مستخدم فريد ، (RIR)، أسماء المضيفين المعنية ، المجالات المستضافة، وكذلك المنافذ المفتوحة.

استكشاف المجالات المرتبطة

عند التحقيق في البرامج الضارة أو الفيروسات أو مجالات التصيد الاحتيالي أو عمليات الاحتيال عبر الإنترنت ،نجد انه من المدهش أحيانا يمكن ان نجد أن الحادث الذي يجري التحقيق فيه ليس حالة منعزلة ، بل انه يرتبط فعليا بالآخرين ويتصرف كشبكة ضارة تتضمن العديد من المجالات، ويمكن اكتشاف هذا باستخدام ميزة المجالات المرتبطة.

استكشاف المجالات المرتبطة

تتيح المجالات المرتبطة إمكانية استكشاف أسماء النطاقات المرتبطة بالشركة او المؤسسة أو المجال الرئيسي الذي تبحث عنه ، كما يمكن بسهولة تصفية النتائج حسب المسجل والمنظمة والتأسيس وانتهاء الصلاحية.

طرق وادوات وخطوات استخدام تكنلوجيا حماية الانظمة واسترجاع المعلومات:

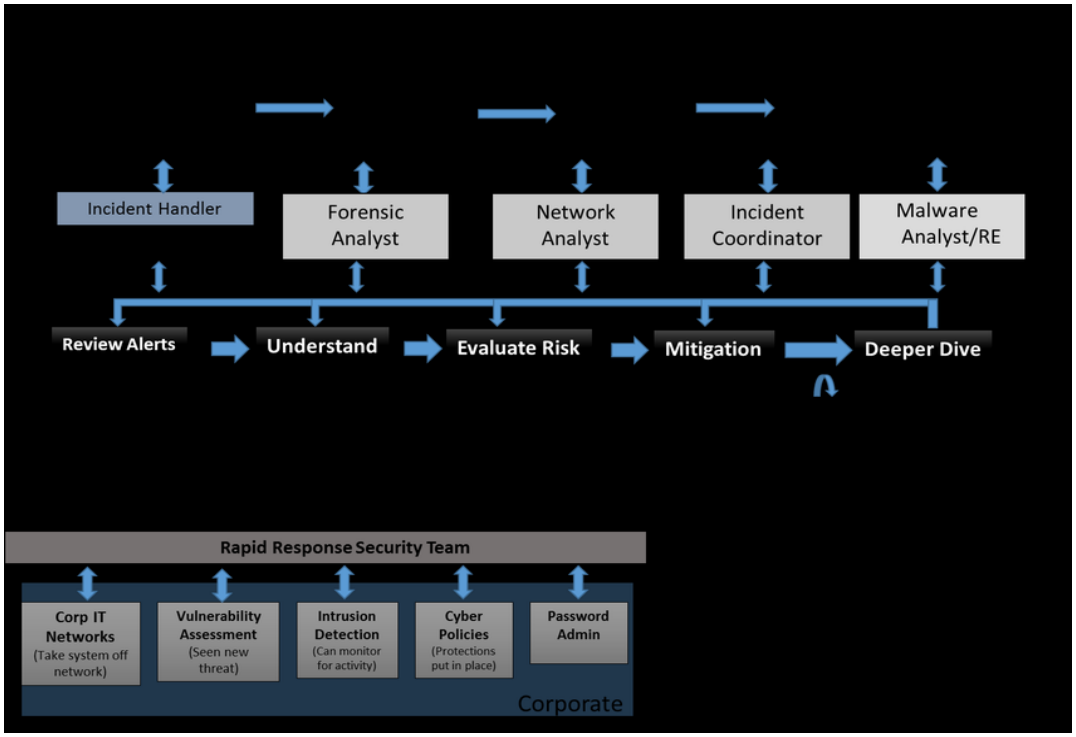
تنوعت محاولات حماية الانظمة والمعلومات و تنامت مشكلة الجريمة الإليكترونية و تواتر الجهد الفني والتقني لتوفير اسلوب وادوات تساعد على استرجاع البيانات المفقودة، او اثبات المسؤلية عن الفعل المجرم، وكشف كيفية ارتكاب التعدي على الانظمة وزيادة فاعلية حمايتها الى غير ذلك من ادوات كشف الجريمة الإليكترونية و التحقيق الجنائي .

سنعرض فيما يلي لاهم ادوات كشف الجريمة الإليكترونية و التحقيق الجنائي وأكثرها استخداما

والتي تم الاجماع على اهمية دورها في مسألتي الحماية والتحقيق في الجريمة الإليكترونية بشكل نرى ان المام المحقق في الجريمة الالكترونية بها يجب ان يعد اساسيا :

12-4 الحصول على بقايا المعلومات الممغنطة Magnetic Residue:

المعلومات التي تم استبدالها في قرص الكمبيوتر الصلب يبدو امر استرجاعها للوهلة الاولى غير ممكنا باتباع الفنيات الخاصة بالاسترجاع الذي سبقت الاشارة اليها في العرض المتعلق بنظامي وندوز و يونيكس، الا ان حقيقة ان القرص الصلب يتكون من كومة او مجموعة من الاقراص المغطاة بمادة مغنطيسية تحفظ سلسلة من الواحد والصفر، التي تكون البيانات المكتوبة في مسارات القرص المغنطيسي (Concentric)مجموعة مسارات دائرية ترتكز على مركز واحد وانه عندما يتم استبدال المعلومة المكتوبة على المدار لا يمكن ان يكون التسجيل الجديد بالدقة التي تمكن من تغطية المعلومة القديمة فانه يمكن عن طريق جهاز متخصص (Magnetic Force Microscopy) (MFM) استرجاع اجزاء المعلومة التي لم يغطيها الاستبدال وبكفاءة عالية جدا - هذا النوع من استعادة المعلومات نادرا ما يستخدم بسبب التكاليف الباهظة للجهاز الذي ينجز العملية.

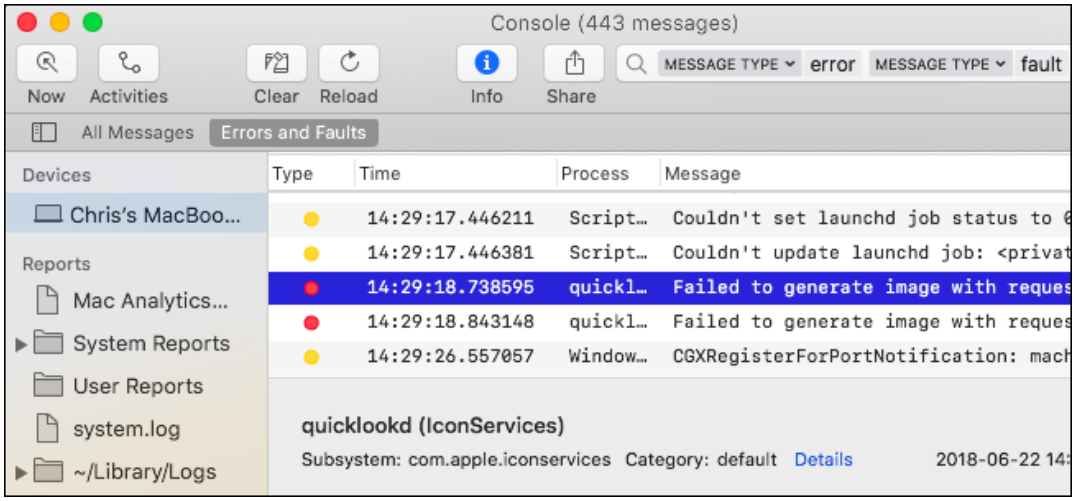


شكل 14-4 Workflow for Cyber Security

13-4 التعامل مع الاعتداء: Intrusion Handling

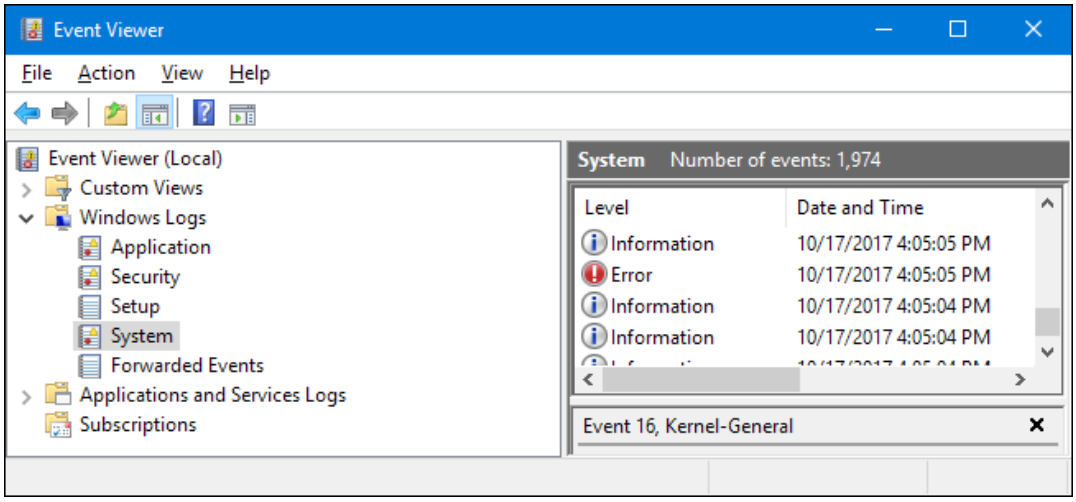
كثير من مديري الانظمة تكون ردة فعلهم خاطئة عند حدوث الاعتداء وذلك باعادة تشغيل النظام (Restart) بينما الافضل هو التأكد من الحصول على صورة (image) من حالة النظام التي يجب ان يتم تسجيلها بدقة قبل ان تتعرض ولو بالصدفة للتعديل (modification) وخلق نسخة دقيقة (exact copy) من محتويات الملف (file contents) لان الهجوم قد يتكرر. لذا فان الحصول على الدليل (evidence) يجب ان يكون هو الهاجس مع نسخة من نظام الملفات (File System) وهذه النسخة يتم الحصول عليها باستخدام برامج تصوير القرص (disk imaging software). ينصح دائما عند الحصول على النسخة المطلوبة يحفاظ القرص الاصلي بصورة امنة سجلات الأنظمة (Systems Logs) وان

يستخدم عند الضرورة القصوى وبالحد الادني، بعدها يبدأ التحقيق.



شكل4-15 (استخدام ماك log file MC)

اكثر الادلة فاعلية وتمكينا للمحقق من ربط الوقائع هي سجلات الانظمة (Systems Logs)، وكلا النظمين وندوز او يونكس يستطيعان تسجيل الاحداث الهامة بتفاصيلها عند حدوثها مما يستدعي ان تكون في حالة تشغيل قبل حدوث التعدي لتكون صورة التعدي اكثر وضوحا. ومن اكثر سجلات الانظمة فائدة هو سجل الدخول (Login Log) وسجل التوصيل (Connection Log) وهذا السجل يعطي صورة واضحة لتأريخ وزمن الدخول والعنوان (IP Address) الى جانب اي بداية للتحرك غير الطبيعي او محاولة الدخول من عنوان غير معروف لموقع غير عادي. في حالة نجاح المعتدي في الخول فان السجل يكون قادرا على الاحتفاظ بسجل اوامر تأريخي (shell command history) يفسر بصورة واضحة هدف المتعدي من دخول النظام والملفات التي تمكن من اقتحامها او تغييرها .



شكل 4-16 (event viewer- Windows)

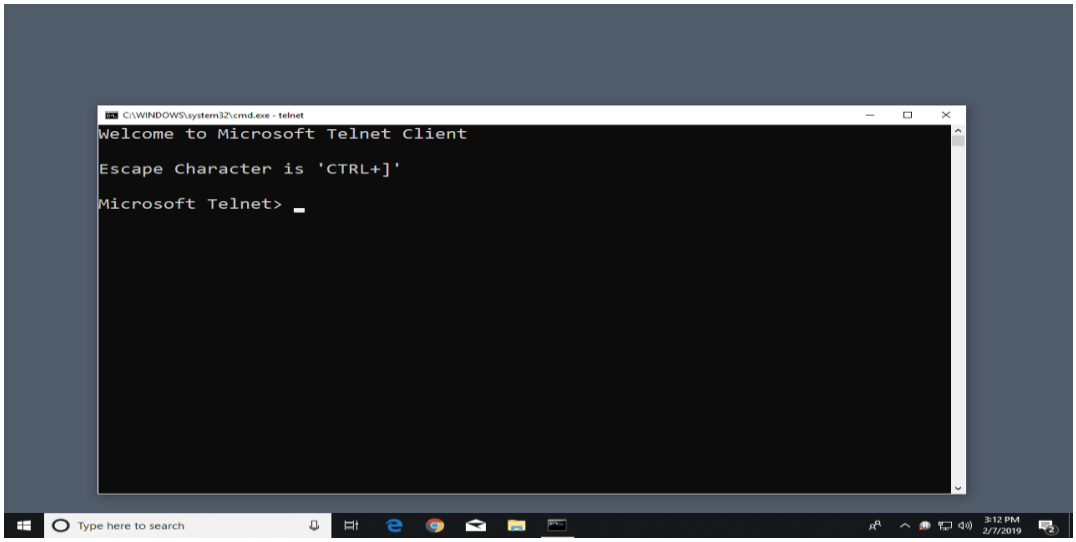
وقد تكون هناك صعوبات متعلقة باجراءات ما هو في طور التنفيذ الذي قد يستمر دون ملاحظة، الا ان توقف الاجراء يتيح استخراج جدول الرموز (symbol table)والمحتويات الاساسية (core stack) واجراء التحليل عليها .

4-14 صيانة النظام :

يترك المتعدين الكثير من الادلة وكثيرا ما يتركون بعض البرامج و المعلومات في

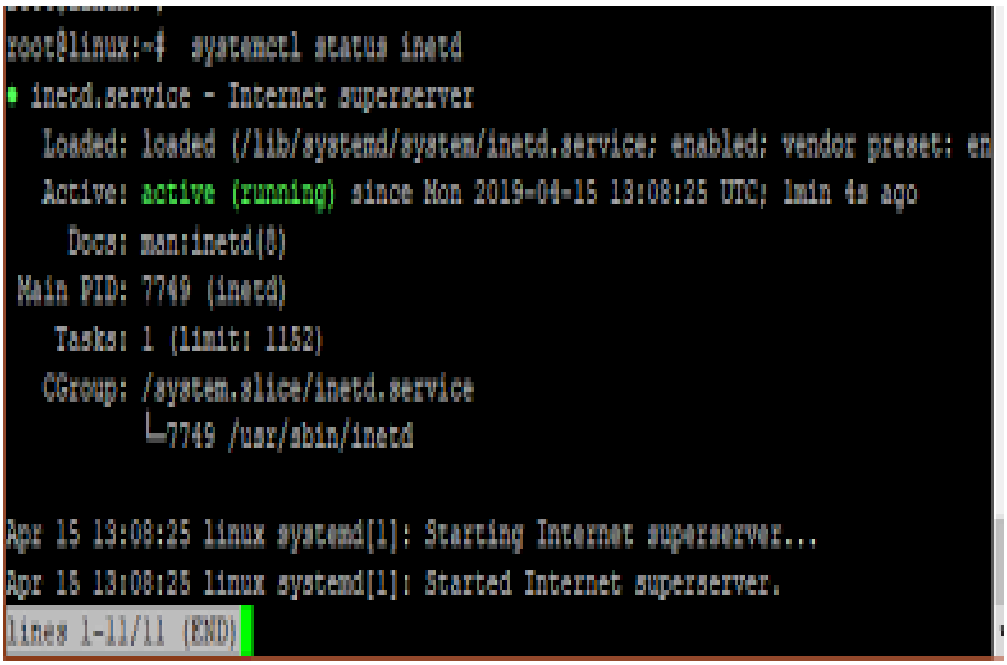
النظام المعتدى عليه وذلك غالبا لاستخدامها في الاعتداء على انظمة اخرى، وتسمى بقايا

ملفات وقد تحوي اي شئ شامل الفيروسات لمذيد من التحطيم وغالبا ما يستبدلون البرامج القابلة للتنفيذ، (telnet, find - example) ببرامج معدلة من اخراجهم لها خصائص مدمرة لذا لابد من مراجعة الانظمة بشكل منظم واجراء اختباريات مثل (Massage) (MD5)او (SHA-1) في ملفات النظام .



شكل 4-17 استخدام تلنت في وندوز (TELNET2020)

في حالة حدوث اي طارئ يمكن اجراء المقارنة للتأكد من عدم حدوث اي عبث .



شكل 4-18 (Telnet Command) استخدام تلنت

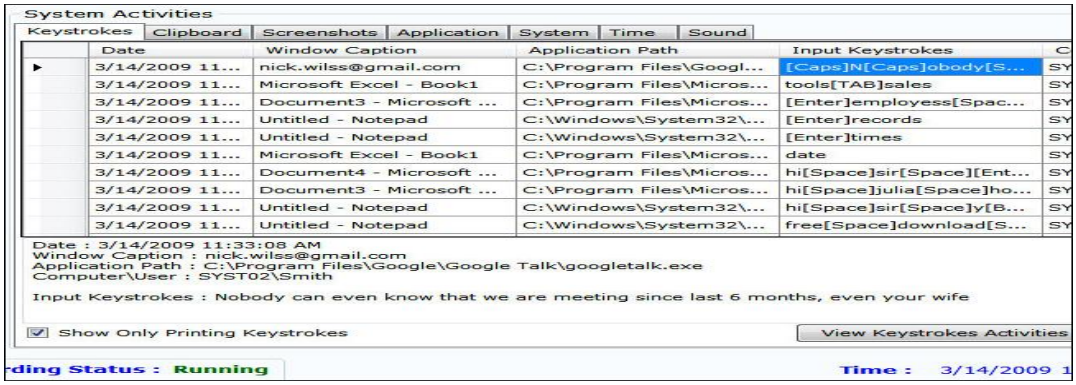
قد يلجأ المعتدي لاخفاء الملفات في مناطق غير متوقعة ومنحها اسماء غير مألوفة يصعب الوصول اليها الا ان هذه الملفات المخفية يمكن الوصول اليها باستخدام الادوات المناسبة المتوفرة كأدوات او تقنية .

15-4 متابعة المتعدي :

بعد فحص السجل والقيام بالتفسير المناسب لنشاط المتعدي يكون الوقت قد حان لتتبع المجرم وهو امر ليس بالهين. سجل النظام هو الطريق الوحيد لمعرفة المسؤل عن الهجوم، اذ جرت العادة ان يقوم المعتدون بتعديل او مسح السجل الذي يساعد على تتبعهم لذا يفضل دائما اعداد النظام ليقبل كتابة السجل في offline file system لمنع المعتدي من الدخول ويفضل تبني طريقة التشفير والاختبارية في ترتيبات النظام وتنفيذه وهذا امر يضمن امكانية استرجاع البيانات وربما القبض على المتعدي. وتشمل هذه الاجراءات سجلات جهاز توجيه الشبكة لان مجرد الوصول للعنوان يجعل الوصول الى النظام في حكم المؤكد، الا ان ذلك قد لايعني نهاية المطاف اذا لا شئ يمنع تكرار المحاولة بعد الفشل لان التكرار حتي بلوغ الهدف ليس محظورا ما لم تتسبب سلسلة المحاولات في الدخول في نطاق قانوني اخر ليبقى الافضل دئما هو التعلم من الاخطاء. (Lee 2001)

16-4 ادوات التلصص:Keystroke Loggers

أدوات التلصص Keystroke Loggers هي ادوات تعمل في الخفاء وهي قادرة على الاختفاء تماما خصوصا ما تحدثه من تعديل في اعدادات النظام، وقد تطورت هذه الادوات لحد بعيد فقد اصبحت قادرة على تصوير كل ما يظهر او يعرض على الشاشة



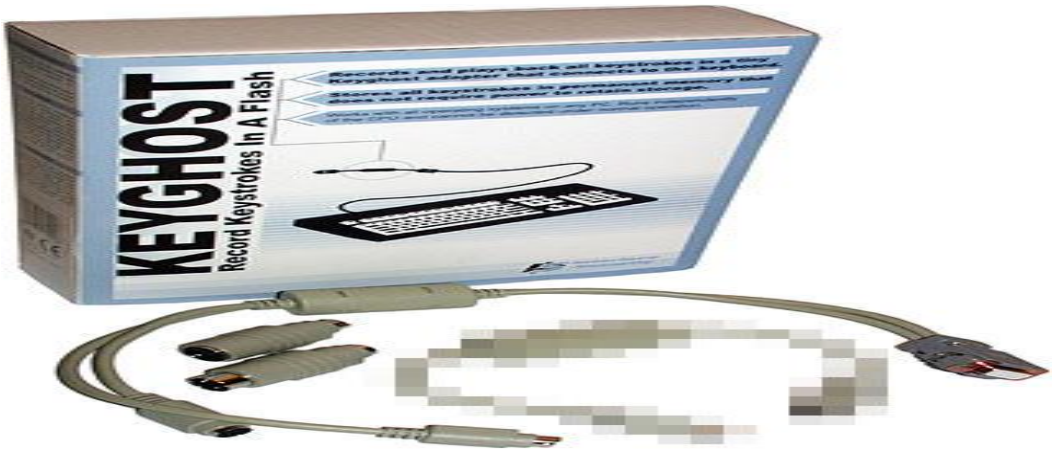
شكل4-19 ادوات التلصص Keystroke Loggers

من احداث باوقات محسوبة وهذه الاداة تتكون عادة من جزئين (DLL) (Dynamic-link Library) الذي يختص بالتسجيل و (exe) (Executable) الذي يتولى تحميل (DLL)وايصال صنارة (hook) لوحة المفاتيح. والصنارة يقصد بها التقنية التي تستخدم وظيفة (Function)لاعتراض احداث (Events) قبل وصولها الى برنامج (Application) ومن ثم يسيطر على لوحة المفاتيح قبل الوصول الى البرنامج المعني تأتي الصنارة (hook) في صورتين الاولى على نطاق النظام (system wide) والاخرى محددة الموضوع-thread) specific) اما ال(DLL) فهي ملفات تحمل وظائف ومعلومات اخرى متصلة ببرنامج في وقت التشغيل-run) time.) فعندما يتصل ال(DLL) بالعمليات (the process) ويأخذ مكانه في مساحة عنوان العملية (process address space) يكون من الممكن استدعاءهم من العملية .ال (DLL) تستخدم لل(keyboard hooks)لان اي برنامج في هذه الحالة يستطيع استدعاء تسجيل الدخول منها وبالتالي تسجيل كل ما يحدث من كل البرامج. (Lee 2001)

17-4 الوصول للمتلصص:

يمكن توصيل برامج التلصص (Keystroke logging programs) بصورة مباشرة او عن بعد باستخدام برامج الفيروسات او متعدي لديه مدخل اساسي (root access) للنظام. برامج التلصص عادة ما تحتاج ذاكرة قليلة لا تؤثر على اداء النظام لذا فهي تبقى بدون ان تتم ملاحظتها او الوصول اليها. هناك منتجات فاعلة ضد التطفل قادرة على الوصول للمتطفلين هذه البرامج تعمل باستثارة بحث الذاكرة وملاحظة البرامج التي تتصرف بشكل غير طبيعي منها برنامج يدعى (Key Patrol) وهي تستخدم خوارزميات للكشف عن السلوك (behavior-detecting) و خوارزميات النمط المتطابق (pattern-matching algorithm).
يعمل هذا النوع من الادوات على كشف برنامج التلصص بمجرد اتصاله بلوحة المفاتيح بكشف استدعاء اجراء لوظيفة التلصص (keystroke procedure call) كما يمكن لهذه الادوات تفتيش الذاكرة ومقارنة البرامج ببرامج التلصص العديدة مثل ما يحدث في ال (anti-virus software logging function)

هناك خيار اخر لمراقبة برامج التلصص هو الخيار المادي والذي يتم بايصال جهاز بلوحة المفاتيح واشهر هذه الاجهزة هو (KeyGhost) وهو جهاز صغير يلحق بنهاية وصلة لوحة المفاتيح ويثبت في الجزء الخلفي للكمبيوتر. هذا الجهاز يعمل مع كل انظمة التشغيل، ولا يمكن كشفه ببرامج التطفل، ولا يحتاج اية خبرة لتركيبه ولايشترط لتركيبه ان يكون الكمبيوتر في وضعية معينة،



شكل 4-20 KeyGhost

https://www.google.com=isch&sxsrf

وهو مستقل عن نظام التشغيل فهو لا يحتاج برنامج لتحميله، فقط هو يقرأ ما يحدث في لوحة المفاتيح كما هي، يسجل المعلومات في ذاكرة مثبتة فيه بينما كل شئ في النظام يسير كما هو دون تغيير، فهو قادر على التسجيل حتى قبل ان يتم تحميل نظام التشغيل ويمكنه تخزين كلمات المرور الخاصة ب (BIOS) كما انه لا يحتاج اي طاقة خارجية ولا يبطئ عمل النظام باستخدام الطاقة الخاصة به. اما المعلومات التي يسجلها فهي تحفظ في (128- bit encryption) لمنع استخراج المعلومات الا باتباع سلسلة معقدة من نقر المفاتيح مثل كلمة المرور بعدها يمكن رؤية المعلومات على (text editor) وتحميل المعلومات واعادة اعداد الجهاز.

عيوب هذا النظام انه يحتفظ بمساحة تخزينية بين 2,000,000-128,000 وبمجرد امتلاء الذاكرة وقبل تفريغها يبدأ في الاستبدال و التسجيل فوق المادة الموجودة اصلا. وعيب اخر هو انه يمكن ملاحظة وجود الجهاز المثبت في الجهاز . .(Svedman 2020)

18-4 تحليل الادلة الجنائية في نظام وندوز Windows systems:

بالرغم من اي عيوب يمكن تعدادها وهي في غير صالح نظام الوندوز الا ان ذلك لا يغير في كونه الاكثر استخداما كنظام تشغيل للكمبيوتر، لذا فان اي محقق لابد من ان يكون ملما بكيفية عمل هذا النظام وخصوصياته (Attributes) حتى يكون قادرا على اجراء تحقيق بنتائج مرجوة. وتبدأ اساسيات هذه المعرفة من معرفة تخصيص اماكن الملفات (File Allocation) الى عملية مسح الملفات (File Deletion) وهو امر تقتضيه عملية استرجاع الملفات الممسوحة.

الوندوز (NT) والوندوز (2000) والاصدارات الاعلى تستخدم نظام الفايلات (NTFS) وهو نظام يحتفظ بسمات الملفات في ملف يسمى (MFT) (Master File Table) والسمات الاكثر اهمية في هذا الملف بالنسبة للمحقق هي (MAC TIMES) وهو الملف الذي يحتفظ بالتأريخ والزمن الذي تم فيه التعديل والدخول او خلق الملف، والبيانات ومكان المعلومات في القرص مع الملفات كما ان سمات اخرى كالفهارس يجب ان تحظى هي الاخرى باهتمام المحقق في ملف . (MFT)

في ملفات (NTFS) تكتب البيانات على القرص في شكل قطع ملتصقة تسمى عناقيد (Clusters) باحجام تتحكم فيها المساحة المقتطعة من القرص Disc) (Partitionواصدارة الوندوز (Windows Version) ويستخدم في ذلك ملفات ($BITMAP) لمتابعة العناقيد في القرص وهذا الملف يستخدم للافادة عن تخصيص موقع للعناقيد بالقرص.

عندما يخصص الموقع يتم خلق سجل بال (MFT) ورقم فهرست، وعندما يتم حزف الملف من مكان المتابعة

($BITMAP) ويرقم ال (BIT) صفرا ويعلم ال (MFT) للمسح يرفع الفهرست الى اعلى للمسح ولكن في حالة ان الدخول قد جاء الاخير فان معلومات الدخول تظل مرئية ويكون ممكنا استرجاع سمات الملف File) (Attributesالتي قد تتضمن زمن الدخول ومعلومات اخرى مفيدة في التحقيق. يقوم ال (NTFS) باستبدال السجلات الممسوحة لخلق سجل جديد لذا فان الاستبدال لا يتم فتكون سمات الملف موجودة في ذات الحين وربما استرجاع المعلومات ايضا، وفي احيان اخرى يكون ممكنا استرجاع المعلومات حتى بعد الاستبدال في (MFT)وفهرست الملف الاساسي فان كانت المعلومات كبيرة بمايكفي فانها تستقر باحد العناقيد بدلا عن (MFT)نفسه. والعناقيد الحاوية للملفات الممسوحة تستقر بالتالي بالمساحات غير المخصصة وهذه بدورها يحتاج الوصول اليها استخدام ادوات التحقيق وهذا يدفع للقول باهمية البحث في المساحات غير المخصصة فربما لم يحدث فيها استبدال بعد خلافا للفهارس الخاصة بالملفات المزالة. .(Svedman 2020)

يمكن للمحقق ايضا مقارنة الملفات المعاد تسميتها بالملفات الممسوحة وبانطباقها يكون قد حصل على دليل بعلم المتهم بوجودها اذا كان هو من قام بتحويلها. كما ان (MAC) تفيد علم المتهم عندما تؤكد ازمان الخلق والتعديل واخر دخول.

يمكن للمحقق تفتيش ال (Recycle Bin) ملف (INFO) للحصول على معلومات تخص الملف المعين وهي معلومات مفيدة كالمكان السابق للملف والاسم الاصلي وتأريخ المسح وهي معلومات قد تفيد ربط المتهم باي فعل.

مناطق اخري عديدة لابد من اعتبارها عند البحث كالمنطقة بين العناقيد (Clusters) التي قد تحوي

بقايا ملفات ممسوحة وتسمي بملفات الركود (File Slack) وتذيد مع كبر العناقيد. ومساحات المبادلة لابد ايضا من اعتبارها في البحث فهي قد تحوي بقايا هامة لملفات ممسوحة قريبا لتستقر في مكان خاص في مساحة المبادلة (Swap Space) وعندما لا يكون هناك مجال لاستقرارها في ال (RAM) فيحولها نظام التشغيل (OS)الى مساحة المبادلة. كما يمكن للمحقق البحث في ملفات الانترنت المحفوظة مؤقتا (Index.DAT) التي تحتوي عناوين (URL) وتأريخ اخر تعديل او دخول ومثلما يمكن مسح هذه الملفات فانه يمكن استرجاعها في المواقع الاخري التي تم ذكرها. الى جانب البحث في سجل البرنامج للحصول على الدليل فان المحقق يمكنه استخدام مصدر اخر لاسترجاع الملفات والحصول على الدليل وهو (NTFS $LOGFLE) الذي يمكن المحقق من الحصول على كل العمليات التي تمت في (NTFS) كما ان هذا الملف يستخدم لما بعد انهيار النظام. من هذا الاستعراض الخاص بنظام الوندوز يمكن القول ان النظام يتيح مصادر عديدة ومفيدة للحصول على معلومات متنوعة تمكنه من اثبات الجرم وهي مصادر تفوق ما تم ذكره من امثلة. (Svedman 2020)

19-4 تحليل الادلة الجنائية في نظام يونكس Unix Systems :

استشراف التحقيق في نظام يونكس يماثل كثيرا مباشرته في نظام الوندوز اذ يلزم المحقق الالمام بكيف يخصص النظام المساحات ، وكيف يقوم بمسح الملفات للوصول للملفات المخبأة او الممسوحة في حين انه يجب القول ان خصائص اليونكس تمنح المحقق فرصا افضل او اكثر تعددا منها في نظام الوندوز. فالاختلاف بين النظامين تمحور في مفاهيم التعامل مع

الملفات اذ بعد ان تعرضنا لتعاملات الوندوز فيجدر ذكر ان اليونكس يستخدم مفهوم العقد او نقاط التلاقي (Index Nodes)لتمثيل الملف وكل (node) تحوي مؤشرات للمعلومات الفعلية في القرص (hard disc) مما يشكل معلومة مفيدة للمحقق فهي تحوي هوية المالك واذن الدخول (كل الصلاحيات) وارقام الدلائل المرجعية (directory numbers)، وال (MAC) واحجام الملفات مع ملاحظة ان اسماء الملفات يتم تخزينها كمدخل في الدالة مع موقع نقطة التلاقي او العقدة كما تجدر الاشارة الى ان اليونكس يخصص المساحات للملفات في كتل او قطع (BLOCKS) موازية لل (NTFS) في الوندوز. وبالمثل يمكن البحث في (File Slack) عن بقايا الملفات والسمات بين القطاعات او الكتل (Blocks) لذات الاحتمال الذي يتم البحث بسببه في الوندوز بين ال. (NTFS)

مسح الملفات في اليونكس يتضمن الاشارة الى اسم الملف في الدالة كغير مستخدم (Unused) ويؤدي ذلك لفقدان الصلة بين اسم الملف (file name) وملف البيانات الفعلية (actual file data) وسمات الملف (attributes) والتأشير على الملف بغير مستخدم مع فقدان بعض السمات وليس جميعها ويشمل التأشير بغير مستخدم (Data Blocks) (Svedman 2020)

وفقا لادوات التحقيق (Coroner Toolkit) (TCT) في ملفات المعلومات وسماتها فان الملفات الممسوحة في نظام يونكس تبقى لفترة طويلة في الانظمة المستخدمة بكثافة لان نظام الملفات في يونكس مرتبط ببعضه ولايخلي المساحات بصورة عشوائية الامر الذي يبقي الملفات الممسوحة لزمن اطول بافتراض ان

الملفات الجديدة لا تتطلب ذات المساحات الخاصة بالملفات الممسوحة وهذه الخاصية تتيح الفرصة لاستعادة الملفات افضل مما هو عليه الحال في نظام الوندوز وبالتالي فان فرص المحقق في الحصول على ما يحتاجه تظل افضل باستخدام (Coroners Toolkits) واخرى تساعد في استعادة الملفات مثل (Unrum) اضافة لاستعادة السمات باستخدام (Ils Tool) المتوفرة في ال (TCT) وهي اجزاء هامة للمحقق خصوصا عند مراجعة ال (MAC time) لاي ملف، وتأتي الاهمية من ان المحقق يحتاج الى تحديدها لمعرفة التغيير الذي يحدث في الملفات المتصلة بها، علما بان المعلومات في نظام اليونكس تحفظ في شكل ملفات وبالتالي فان اي تغيير قد يثبت علم المتهم بالتغييرالذي حدث . تحتوي ال (TCT) على اداة تسمى (Mactime) تعرض ملفات ال (MAC times)، التي يستطيع ذوي الخبرة من المجرمين تغييرها، لاخفاء ال(Inodes) وهنا يجب تجنب الاعتماد كلية على. (Iovation 2020) (MAC times)

اليونكس يمنح المحقق الفرصة لتكرار الاوامر المستخدمة في الجلسات السابقة (Sessions). لذا تحفظ الاوامر في ملفات تأريخية محمية (shell history file). وهذه بدورها تخضع للتحليل لتتبع خطوات المجرم، برغم قدرته على محو هذه الملفات التي لا تكون ذات فائدة للمحقق الا لوقت محدود. عموما يمكن ان نخلص الى ان عملية استخلاص الادلة في اليونكس تشبه كثيرا العملية في الويندوز غير انه يمكن استخدام ادوات اليونكس لاستخلاص المعلومات للبحث في منظومات بعينها بفاعلية اكثر. (Iovation 2020).

20-4 الملخص و المناقشة : Conclusion and Discussion

التحقيق في الجرائم الإلكترونية ليس بالعلم السهل نظرا لمتطلبات المعرفة وتعقيدات الادوات المختلفة والنظر ايضا لدقة الاختيار.

يتطلب التحقيق المعرفة الصحيحة مع توفر التقنيات والأدوات المختلفة للقفز إلى مسرح الجريمة الرقمية بشكل فعال ومنتج.

بمجرد أن يكون ما يحتاجه التحقيق في متناول يد المحقق ، يمكن للمحقق تحليل البيانات بشكل صحيح والتحقيق في السبب الجذري ، وكذلك تعقب من يقف وراء أي نوع من الانواع المختلفة للجرائم الإلكترونية.

مع تزايد عدد مستخدمي الأجهزة المحمولة والذين يستخدمون الأجهزة المترابطة، تكون أجهزة الكمبيوتر غالبا في مركز الحوادث والتحقيقات. (Iovation 2020)

تتضمن أدوات التحقيق في جرائم الإنترنت الكثير من الأدوات المساعدة ، اعتمادا على التقنيات التي تستخدمها والمرحلة التي تمر بها.

ومع ذلك ، لا بد من التأكد من أن معظم هذه الأدوات مخصصة للتحليل الجنائي للبيانات بمجرد الحصول على الأدلة في متناول اليد.

هناك الآلاف من الأدوات لكل نوع من أنواع الجرائم الإلكترونية . وقد شمل البحث عرضا لبعضها مما قد يتيح إلقاء نظرة سريعة على بعض أفضل الموارد المتاحة لأداء نشاط الادلة الشرعية.

يتم جمع الأدلة للمناقشة في محكمة قانونية بفضل مهارات خبراءالادلة الجنائية الرقمية الذين يمكنهم استخراج البيانات المهمة من الأجهزة الإلكترونية التابعة للأطراف المتأثرة.

يعتمد مسؤولوا القانون في وقت ما على شهادة محللي الطب الشرعي بالكمبيوتر المتخصصين في الاكتشاف الإلكتروني.

يتم استدعاء هؤلاء الخبراء للعمل مباشرة مع ضباط الشرطة والمحققين للمساعدة في تحديد وحفظ وتحليل وتقديم الأدلة الرقمية للمساعدة في حل قضايا الجريمة.

في نظام وندوس (windows) يمكن البحث في سجل البرنامج للحصول على الدليل فان المحقق يمكنه ايضا استخدام مصدر اخر لاسترجاع الملفات والحصول على الدليل وهو (NTFS $LOGFLE) الذي يمكن المحقق من الحصول على كل العمليات التي تمت في (NTFS) بنظام الوندوز.

يمكن القول ان النظام يتيح مصادر عديدة ومفيدة للحصول على معلومات متنوعة تمكنه من اثبات الجرم وهي مصادر تفوق ما تم ذكره من امثلة.

نظام الملفات في يونكس مرتبط ببعضه ولايخلي المساحات بصورة عشوائية الامر الذي يبقي الملفات الممسوحة لزمن اطول بافتراض ان الملفات الجديدة لا تتطلب ذات المساحات الخاصة بالملفات الممسوحة وهذه الخاصية تتيح الفرصة لاستعادة الملفات افضل مما هو عليه الحال في نظام الوندوز وبالتالي فان فرص المحقق في الحصول على ما يحتاجه تظل افضل باستخدام

(Coroners Toolkits) واخرى تساعد في استعادة الملفات.

(TCT) او مجموعة أدوات الطبيب الشرعي (Coroner's Toolkits) عبارة عن مجموعة من البرامج التي قام بها (Dan Farmer) و (Wietse Venema) من أجل تحليل ما بعد الوفاة لنظام (UNIX). تم تقديم البرنامج لأول مرة في فصل تحليل الطب الشرعي في الكمبيوتر في أغسطس 1999. (Venema 1999)

V. االباب الخامس

مشاكل الاختراق و التداخل القانوني و الالكتروني

1.5 المقدمة

هناك الكثير من الطرق التي يستخدمها مرتكبي الجريمة الإليكترونية نذكر منها لطريقتين هما أشهر طرق الاختراق استخداما من القراصنة واللصوص:

i **طريقة بث الفيروسات**، وهي الطريقة المفضلة لدى القراصنة بوجه عام.

اشتهرت بعض الفيروسات وشكلت حضورا في هذه الطريقة بشكل خاص و منها: فيروس (الحب) وفيروس (حصان طروادة)، وفيروس (المصيدة)، وفيروس (سيركام)، وفيروس (كليز)، وبعض فيروسات اخرى.

ii **طريقة سرقة الشرائح**: وهي من أكثر الطرق تداولا بين لصوص الإنترنت(APEC 2005) .

هذه الجزئية من البحث ستعرض لاهم معضلات التحقيق في الجريمة الإليكترونية ويمكن تلخيصها في ثلاثة نقاط:

أولا : لا تخلف الجرائم الإليكترونية آثارا ظاهرة خارجية فهي تنصب على البيانات والمعلومات

المختزنة في نظم المعلومات والبرامج مما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم الإليكترونية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام

سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحي من السجلات ومما يزيد من هذه

الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانيا : يتم ارتكاب الجريمة الإليكترونية عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثا : تبدو أكثر المشاكل جسامة لا في مجال صعوبة اكتشاف وإثبات الجرائم الإليكترونية بل وفي دراسة هذه الظاهرة في مجملها الا وهي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد انظمة الحاسب الخاص بهم وهو ما يعرف بالرقم الأسود حيث لا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل. (Halder D 2011)

2.5 جمع الأدلة الجنائية الرقمية:

كما قد اشار البحث مسبقا فان جمع الأدلة الشرعية الرقمية يعنى بجمع وفحص الأدلة الإلكترونية و تقييم الأضرار التي لحقت بالكمبيوتر نتيجة للهجمات الإلكترونية، و يشمل أيضا العمل به السعي لاستعادة المعلومات المفقود التي تمكن من تقديم مرتكب الجريمة الإليكترونية للمحاكمة. و مع تزايد أهمية أمن الكمبيوتر وخطورة الجريمة الإليكترونية .اصبح من الضروري لمحترفي الكمبيوتر التمتع بالفهم القانوني و فهم التكنولوجيا التي تستخدم في جمع الادلة الرقمي وكل ما هو دائر حول المعلومات الأساسية المتعلقة بالتقنيات المستخدمة في هذا الاطار. ويشمل ذلك استرداد البيانات والاستجابة الأساسية لاي متسلل على النظام، وكل ما يتعلق بتكنولوجيا برمجيات الدخول الرئيسية و الأجهزة ،

والجوانب القانونية والأخلاقي لتكنلوجيا جمع الادلة الشرعية الرقمية (HalderD 2011).

سبقت الاشارة ضمن هذا البحث الى ان تطور استخدام البينة الرقمية كان دائما بسبب ان المحاكم اصبحت تقبل تقديم البينة الرقمية للفصل في القضايا المعروضة امامها مما استدعى توفر قوانين قادرة على معالجة قضايا السايبر الحالية والمتوقعة كما انه قد حتم ابتداءا التعاون البناء بين اهل الفكر القانوني ومحترفي الكمبيوتر و تقانة المعلومات(Kelly & Wearne 1998)

عموما فان بعض القائمين على تكنلوجيا السايبر وبسبب مصاعب التشغيل وارتفاع تكاليفه تنازلوا عن درجات الامان الاعلى بعدم تفعيل اجهزة الدفاع و الامن بصورة فاعلة، فضلا عن تعطيل اليات الامن مما ادي لتذايد الاهتمام بالحماية القانونية (David Icove 1995) و فنياتها خصوصا في مجال جمع الادلة الشرعية الرقمية ومراحل التحقيق بوجه عام، لذا تحتم النظر لهذه الفنيات (Technicalities) من زاوية اكثر شمولا، تتضمن كل ما يدخل او يتعلق بمحاور تكنلوجيا السايبر و جمع الأدلة الشرعية الرقمية. (Rob van den Hoven van Genderen 2008)

3.5 موجهات التحقيق في الجريمة الالكترونية:

عند استشراف عملية التحقيق بواسطة منفذي القانون لابد من تشجيع المحققين لتبني المصادر المتعددة لقواعد (Regulations) وموجهات

جدول 5-1 دليل اجراءات التحقيق في الجريمة الالكترونية

العنوان	النطاق	المحتويات
دليل عام	جميع أفراد الشرطة	**تعريف الجرائم الإلكترونية ، الفئة ، التحقيق الأولي معالجة البحث والاستيلاء، المقابلة والاستجواب، قوائم المراجعة.**
تتبع الإنترنت (مصنف)	المحققون عبر الإنترنت (إلزامي)	**بروتوكولات الإنترنت والعنونة البريد الإلكتروني ، خدمة تتبع ، خط المشترك، تتبع في الوقت الحقيقي والأدوات**
تحليل الأدلة الرقمية (مصنف)	المحققون عبر الإنترنت (إلزامي)	**الأساس والعملية ، تحليل نظم تحليل الشبكات، أدوات (ILook Encase (Final, ForensicsX-ways،**
التحقيق في الجرائم الإليكترونية (مصنف)	المحققون عبرالإنترنت بقية افراد الشرطة	**القرصنة والتحقيق ، توزيع المحتويات غير القانونية، التحقيق في التجارة الإلكترونية ، تقديم الشكاوى**
المبادئ التوجيهية القياسية للتعامل مع الأدلة	العامة (يفضل)	**جمع الأدلة، نقل وطلب فحص ، تحليل الأدلة كتابة التقارير.**
كتيب الطب الشرعي الرقمي الفني (مصنف)	المحققون عبرالانترنت (الزامي) المدققون الشرعيون (إلزامي)	**الإجراء القياسي : جمع الأدلة ، استعادة القرص، القرصنة وتحليل الويب، البريد الإلكتروني والرسائل الفورية، قاعدة البيانات، الوسائط المتعددة ، الكشف عن إخفاء المعلومات ، تحليل شبكة الاتصالات ، تحليل الجهازالمحمول ، قوائم المراجعة**

(Guidelines) التحقيق الواجب مراعاتها والمتمثلة بشكل اجمالي في المصادر التالية:

i. القانون الوطني او المحلي: بمعنى مراعاة الاجراءات الجنائية واجبة الاتباع بنص القانون، او القواعد القانونية الخاصة بطريقة جمع ادلة الجريمة الالكترونية بما يوفر البينة محل التحقيق لان البينة المقبولة لابد ان يتم الحصول عليها وفقا للقانون والا اصبحت غير مقبولة. (UN 2013)

ii. معايير (Standards) وموجهات (Guidelines) القانون الدولي (International Law) واطره التقليدية الاتفاقيات والهيئات الدولية كالبوليس الدولي (Interpol) التي تعمل في اطار التعاون الدولي في مكافحة الجريمة الالكترونية خاصة او الجريمة عموما. (Howard 2004)

iii. المبادئ والتوجيهية والكتيبات (Guideline and Manuals) التي تمد المحققين بالمرجعية التي تستند للتجربة العملية (Practical Reference) التي تساعد على اتخاذ القرار المناسب في الوقت المناسب مع شتى ضروب مراحل التحقيق.

4.5 الاحتياطات القانونية: Legal Precautions

التحقيق في الجريمة الإليكترونية تعترضه مسألتان من مسائل الخصوصية لابد ان يضعها المحقق في اعتباره:

اولها : ضرورة تجنب الوقوع في خطأ التفتيش وحيازة الادلة دون سند قانوني.

ثانيها : ان الانترنت يعد منتدى عاما يوفر حرية الكلام وتوصيل صوت الاقلية الا ان هذه الحرية محدودة بكونها لا تهدد امن النظام ولا تدخل في توصيف اخر يصل لدرجة انه يعد جريمة. (Jang 2013)

5.5 الخطوات العامة لعملية جمع الادلة الجنائية:

تشمل عملية جمع الادلة الشرعية الالكترونية الاحتفاظ (Preservation)، تحديد الهوية (Identification)، الاستخراج (Extraction)، التوثيق(Documentation)،والتفسير (Interpretation) المعلومات المحرزة. (Heiser 2001)

هناك ثلاثة خطوات رئيسية في عملية جمع الادلة الشرعية للجريمة الإليكترونية نتعرض لها في ايجاز فيما يلي:

i. **الاستحواز** تنحصر الحيازة او الاستحواز (Acquiring) في عملية النسخ(Copying) التي يقوم بها المحقق او المشرف علي جمع الادلة ويدور الجهد فيها حول الحصول على نسخة أو خلق نسخة من الادلة المخزنة في القرص الصلب للجهاز موضوع التحقيق بطريقة ممنهجة (Bit-By-Bit Copy). وينفق المحقق جزء من عملية التحليل في استعادة الملفات المحذوفة ولذلك يلاحظ انه من صميم وظيفة المحقق معرفة مكان والعثور على بقايا هذه الملفات وتفسير النتائج، واحرازأي بيانات عن الملف وسمات الملف (Files characteristics) ان وجدت، وفي كل الاحوال فان البيانات المحرزة قد تسفر عن ادلة قيمة كما هو الحال في عملية جمع الادلة التقليدية. (Miller 2012)

مما يؤكد على اهمية دقة الاحراز فان التحقيق في أنظمة ويندوز (Windows) ويونكس (Unix) كمثال يحتم معرفة ان السمات المتشابهة في النظامين لا تنفي تفردهما (Unique) عن بعضهما البعض في سمات اخرى يجب مراعاتها للحصول على افضل النتائج ، و يمكن للمحلل او جامع الادلة الرقمية الشرعية مراعاة الفروق عند التحقيق في واحد من النظم أو الأخر لأن كل نظام تشغيل يختلف عن الاخر وهو فريد في نوعه في بعض المناحي المؤدية الى اختلاف الطرق . (Howard 2004)

لا يمكن استعادة البيانات المحذوفة من خلال استخدام أدوات جمع الادلة الرقمية الشرعية المشتركة، وقد يقتضي الحال استخدام ادوات أكثر حساسية لاستخراج البيانات، ولكن هذا نادرا ما يحدث بسبب التكلفة العالية لهذه الادوات.

استعادة البيانات ليست سوى جانب واحد من التحقيق وجمع الادلة الشرعية الرقمية اذ نجد ان تتبع أنشطة القرصنة داخل النظام قد تربعت على مكانة اكسبتها اهمية لا يمكن اغفالها أيضا خاصة بالنسبة للنظم المتصلة بشبكة الإنترنت، اذ تصبح هجمات القراصنة شبه يقينية .

على الرغم من أنه من المستحيل حماية النظم تماما ضد جميع الهجمات،الا ان تتبع القراصنة في أقرب وقت ربما يقود عبر ما تركوه وراءهم من القرائن والأدلة التي يمكن استخدامها لتجميع ما تم القيام به الى ضبطهم ، او استخدام هذه الادلة والقرائن لتتبع القراصنة حتى المنزل كما يمكن استخدام طرق جمع الادلة الشرعية الرقمية لمعرفة كيف تمكن القراصنة

من دخول النظام، والوصول الى نقاط ضعف النظام وما اصابه من تلف أوكيفية تعديله. (Heiser 2001)

خلاصة القول ان هذه الخطوة تمكن الإداريين من ان يصبحوا قادرين على التعلم من الأخطاء التي ارتكبت في الماضي وتساعد كذلك على منع الاخطار من الحدوث في المستقبل.

ii. **التوثيق او المصادقة (Authenticating)**

iii. هي التأكد من أن النسخة التي تستخدم في التحقيق هي نسخة طبق الأصل (Exact Replica) من محتويات القرص الصلب الأصلي (hard drive) وذلك بالقيام باجراء مقارنة اختبارية بين النسخة والأصل. . وبعبارة أخرى، تظهر المصادقة اذا ما وقعت أية تغييرات على الأدلة أثناء سير التحقيق وبالتالي تقدم الدليل على تقديم أدلة مقبولة في أية محكمة. ويحصل المحققون على مصادقة الأدلة التي تم الحصول عليها من القرص الصلب عن طريق الاختبار لمحتويات القرص الصلب عن طريق الاجراء الاختباري وهذا الاجراء الاختباري هو بمثابة البصمة الإلكترونية في أنه يكاد يكون من المستحيل ان يكون لاثنين من محركات الأقراص الصلبة مع وجود بيانات مختلفة لديها نفس النتائج الاختبارية. حيث تبين أن اختبارية القرص الصلب المضبوطة ان وجدت لا تمكن المحققين من تبين النسخة غير المعدلة من اصل النسخة الاصلية لمحرك القرص الثابت الأصلي. (Adams 2013)

الخوارزميات الأكثر استخداما لتوليد ذلك هي اختبارية (MD5) و (SHA-1) وهي بعض الأدوات لتوليد اختبارية استخدام مزيج من الخوارزميات من أجل ضمان أعلى جودة من المصادقة. (Hawthorne 2014)

iv. **التحليل Analysis** وهي خطوة تحليل المعلومات المحرزة والتي تقود بدورها الى تجريم من ارتكب الفعل الاجرامي. (Fatah 1999) وهي أكثر مراحل التحقيق استنزافا للوقت.

مهمة المحقق (Investigator) هي معرفة اين يجد مخلفات الملفات المفقودة ويحلل (Analyze) نتائج المضبوطات. (TWG 2001)

لما كانت عملية التحليل هي الاهم في مراحل التحقيق يجب ان نراعي تفرد نظامي التشغيل الوندوز (Windows) ونظام التشغيل يونيكس (Unix) لذا سنعرض لعملية تحليل المعلومات في النظامين بشئ من التفريد. على وجه العموم فان المحقق يعتمد الى حد بعيد على ادوات التحقيق الجنائي (Forensic tools) ابتداءا من هكس ادتر (Hex Editor) الى ال -Full) (Blown forensic Toolkits كادوات التحقيق الجنائي مثل (Encase).

من اهم محاور التحقيق التأكد من ، من تولى اي جزء من التحقيق والجانب الاهم هو من الذي في حيازته الدلائل المحرزة (Chain of Custody) الى جانب الاحتفاظ بسجل منتظم يضم كل شئ حدث للدليل من الذي تولاه، اين وكيف تولاه واين تم الحفظ حتى يمكن التأكد من اعتمادية الدليل لان دفاع المتهم المجرم قادر على اضعاف الاثبات اذا لم يكن الاحتفاظ بسجل التحقيق منظما و منضبطا. (Howard 2004)

توفر المخترعات العلمية الالكترونية وما فيها من تقنيات متطورة لارتكاب الكثير من الجرائم بواسطة المجرم الالكتروني وتمكنه من الاستفادة من الامكانيات الهائلة لهذه التقنيات، كما يمكنه الوصول لاعداد

بشرية كبيرة في نفس الوقت، لان شبكة الانترنت كما هو معلوم لا تحدها حدود ولا زمان. (Halder D 2011)

اثارت الجريمة الالكترونية حال بروزها الى الوجود بعض المشاكل المتعلقة بالقانون الجنائي الموضوعي، وذلك فيما يتعلق بتطبيق النصوص التقليدية على جرائم الكمبيوتر، و في الحسبان مبدأ الشرعية ، والتفسير الضيق للنصوص الجنائية، كما ان الجريمة الالكترونية قد اثارت ايضا الكثير من المشاكل في نطاق القانون الجنائي الاجرائي، اذ ان نصوص قانون الاجراءات الجنائية قد وضعت لتحكم الاجراءات المتعلقة بالجرائم التقليدية، التي لا توجد صعوبة في اثباتها أو التحقيق فيها، وجمع الادلة المتعلقة بها، وخضوعها لمبدأ اقتناع القاضي للوصول الى الحقيقة الموضوعية بشأن الجريمة والمجرم.

المشكلات الاجرائية في مجال الجرائم الالكترونية تظهر في ناحيتين:

الناحية الاولى ان البيانات الالكترونية هي كيانات غير ملموسة بالتالي يصعب كشفها. (Yang TY 2016)

والناحية الثانية ان جمع الادلة بشأنها في بعض الاحيان ترتفع درجة الصعوبة فيه الى مستوي يصعب تصوره، كما ان صعوبة الاجراءات تعقدها سرعة، وحساسية، ودقة تنفيذ الجريمة وسهولة محو اثارها، كما ان التفبيش وجمع الادلة تقابله صعوبات كثيرة فوق الحصر، كما قد تتعلق ببيانات مخزنة في انظمة او شبكات الكترونية موجودة بدول اخرى، و هذا بدوره قد أنتج مسائل اكثر تعقيدا، كاقليمية القانون والتعاون الدولي في مجالات التفتيش والتحقيق وجمع الادلة وتسليم المجرمين وربما تنفيذ الاحكام الاجنبية الصادرة في هذا الشأن. ومن المشكلات التي لا يستبعد

ظهورها هي التساؤل حول تدفق البيانات والمعلومات ومدى صلاحية متابعة تدفقها او تدفق ما تعلق منها بما هو خارج اقليم الدولة المرتكب فيها الفعل المجرم، وما هي امكانية وضع الضوابط الاجرائية لعمليات التفبيش، والضبط، والمصادرة، في مجال انظمة الاتصال الالكترونية. (Fatah 1999)

6.5 طرق الإثبات في المواد الجنائية و الفرص المتاحة لمنفذي القانون:

وسائل الإثبات في القانون عموما هي البينة، الإقرار، القرائن، الخبرة، معلومات القاضي، الكتابة، اليمين. (Miller 2012)

اصبح في امكان وكالات إنفاذ القانون (law enforcement) الآن استخدام القوة المتزايدة (increasing power) لنظم الكمبيوتر لجمع الادلة الشرعية باستخدام برامج معقدة (complex forensic software) لتسريع التحقيقات (speed investigations) وأتمام (automate) إجراءات التفتيش (search procedures) .
ومثلما انه يبدو صعبا ومعقدا انجاز عمليات التحقيق اتوماتيكيا (automate investigation) فأن البحث القائم على استخدام الكلمة المفتاحية (key-word) للحصول على المحتوى غير القانوني يجعل الامر اكثرسهولة، في الوقت الذي نجد فيه ان تحديد الصور غير المشروعة (illegal pictures) يبدو أكثر صعوبة (لان النهج القائم على تجزئة القيمة (hash-value) لا يكون ناجحا الا اذا كانت الصورة قد تم حفظها وتقييمها من قبل، وتم تخزين قيمة التجزئة في قاعدة بيانات (database) والصورة التي تم تحليلها وحفظها لم يتم فيها اي تعديل (modification).

(Kerr 2005) والاجدر بالاعتبار هو، في الواقع ان برنامج جمع الادلة الشرعية دائما ما يكون قادرا على البحث تلقائيا عن صور الأطفال الإباحية (child pornography) خلال مقارنة الملفات على القرص الثابت (hard disk) للمشتبه به مع معلومات عن الصور المعروفة . على سبيل المثال، في أواخر عام 2007، تمكنت السلطات في الولايات المتحدة (Interpol 2007) من العثور على عدد من صور الاعتداء الجنسي (child abuse) على الأطفال، و من أجل اخفاء هوية الجاني (prevent identification) عدلت صورتظهر وجه الجاني رقميا ، قبل نشر الصور عبر الإنترنت، الا ان خبراء الادلة الشرعية (forensic experts) تمكنوا من الوصول للتعديلات وإعادة اظهارمن جديد (unpick the modification) وجه المشتبه به (suspects face). (Interpol 2007)

تختلف التوقعات باختلاف الجريمة في هذا النموزج، اذ انه على الرغم من أن هذا التحقيق الناجح يظهر بوضوح إمكانات علوم الحاسوب (computer forensic potentials)، الا ان هذه الحالة ليست دليلا على حدوث انفراجة (breakthrough) في التحقيق في جرائم الاباحية ضد الاطفال، لانه كان ممكنا جدا للجاني ان يغطي وجهه ببقعة بيضاء ليصبح كشفه مستحيلا. (Johansen 2020)

7.5 اطر التحقيق الاكثر شيوعا :

يتوفرحاليا عدة نماذج واطر للتحقيق في الجريمة الإليكترونية، وذلك من واقع الطرح المتوفر ضمن ادبيات (Literature) ونظريات التحقيق في الجريمة بشكل عام والجريمة الإليكترونية في الوقت نفسه.

يرد أدناه وصف موجز لأهم نمازج واطر التحقيق في الجريمة الإليكترونية.

تقتصر هذه النماذج إلى حد كبير على التحقيق في مسرح الجريمة والأدلة ، وبالتالي فهي أقل احتواءا وشمولا لعملية التحقيق في نطاقها .

i. نموذج لي Lee et al للتحقيق في مسرح الجريمة العلمية :

هذا النموذج يعتمد مناقشة التحقيق في مسرح الجريمة العلمية كعملية وليس كتحقيق متكامل.

النموذج يتعامل مع التحقيق في مسرح الجريمة ، وليس مع عملية التحقيق الكاملة، وعلى هذا الاساس فهو يحدد أربع خطوات لقيام العملية :

الخطوة الأولى: هي التعرف على الدليل في هذه الخطوة تعتبر العناصر أو الأنماط أدلة محتملة، وعليه فانه يجب لقيام هذه الخطوة أن يعرف المحقق ما يبحث عنه وأين يمكن العثور عليه.

يؤدي التعرف إلى نوعين من الانشطة الفرعية :

- التوثيق
- جمع المعلومات والحفاظ عليها .

الخطوة الثانية : هي تحديد أنواع الأدلة المختلفة وهذه الخطوة تقوم على تصنيف الأدلة ، مع نشاط فرعي واحد .

تتم مقارنة الخواص الفيزيائية والبيولوجية والكيميائية وغيرها من عناصر الأدلة بالخصائص القياسية المعروفة.

يشير التفرد إلى تحديد ما إذا كانت عناصر الأدلة المحتملة فريدة من نوعها بحيث يمكن ربطها بفرد أو حدث معين.

خلال الخطوطين السابقتين تأتي الخطوطين الثالثة والرابعة على النحو التالي.

الخطوة الثالثة: تقييم العناصر وتفسيرها .

الخطوة الرابعة: هي عملية إعادة الإعمار وتتمحور هذه العملية في جمع المخرجات من الأجزاء السابقة من العملية ، وأي معلومات أخرى ذات صلة قد يكون المحققون قد حصلوا عليها ، لتقديم سرد مفصل للأحداث والإجراءات في مسرح الجريمة .

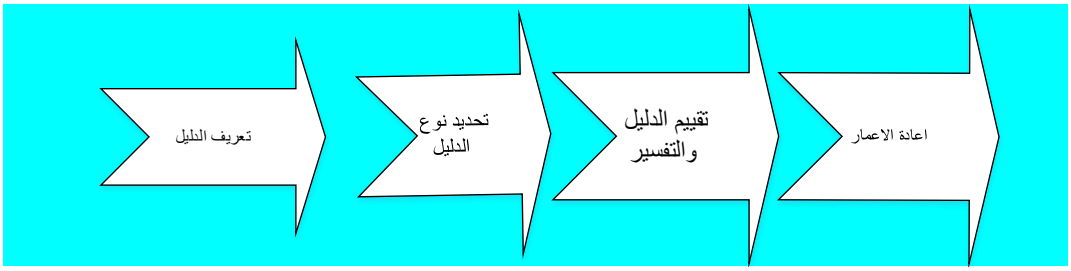
تقديم التقارير والعرض: استنادا إلى الخطوات المذكورة أعلاه ،.

ارجع لي وآخرون المنطق لعدة أنواع مختلفة من المشاهد ، أي سلسلة من الإجراءات ذات الصلة التي قد يستخدمها الباحث للتوجيه لضمان أعلى احتمال أن يتم التعرف على جميع الأدلة ذات الصلة وتحديدها وتفريدها ، مما يؤدي إلى إعادة بناء واعمار مفيدة ومثمرة في عملية التحقيق بشكل خاص.

لم يمدد لي ومن معه هذا النهج الذي يقوم عليه النموزج المفصل ليشمل التحقيق في الجريمة الإلكترونية في مسرح الجريمة .

يؤكد هذا النموذج على أن التحقيق في مسرح الجريمة يجب أن يكون منهجيا . (lee 2001)

يهدف هذا الاطار بشكل أساسي إلى إجراء التحقيقات باستخدام الأدلة المادية . ، ولكن سيتبين أدناه أن العديد من الجوانب تنعكس في الفحص الجنائي للمشاهد الإلكترونية . يتمثل القيد الرئيسي لهذا النموذج في أنه يشير فقط إلى الجزء القانوني من التحقيق ولا تتم معالجة قضايا مثل تبادل المعلومات



شكل 5-21 اطار لي للتحقيق في مسرح الجريمة

ii **نموزج كاسي:**

في العام 2000 قدم يوقهوين كاسي نموذجا لمعالجة الأدلة الرقمية وفحصها. يتضمن ذلك الخطوات الرئيسية التالية:

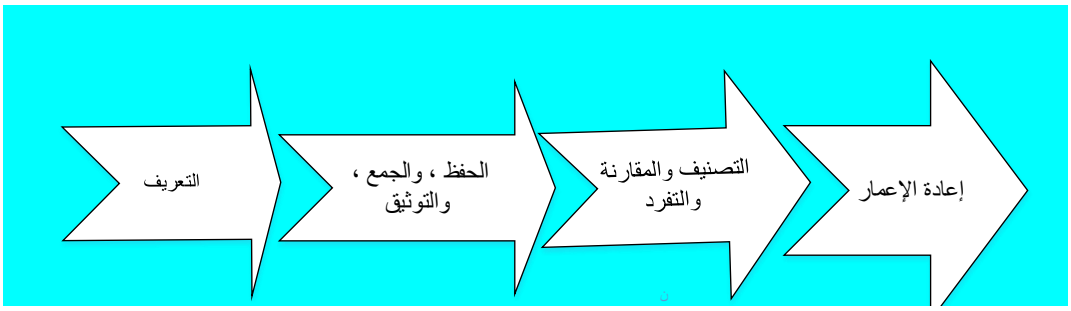
1. التعريف
2. الحفظ ، والجمع ، والتوثيق
3. التصنيف والمقارنة والتفرد
4. إعادة الإعمار

الخطوات الأخيرة هي الخطوتين اللتين يتم فيهما تحليل الأدلة.

يشير (Casey) إلى أن هذه دورة لمعالجة الأدلة ، لأن إعادة الإعمار يمكن أن تشير إلى أدلة إضافية تؤدي إلى بدء الدورة من جديد.

يتم تقديم النموذج لأول مرة من حيث أنظمة الكمبيوتر المستقلة ، ثم يتم تطبيقه على طبقات الشبكة المختلفة (من الوسائط الفعلية وحتى طبقة تطبيقات المستخدم ، بما في ذلك البنية التحتية للشبكة) لوصف التحقيقات على شبكات الكمبيوتر. (Casey 2000)

نموذج Casey عام جدا ويتم تطبيقه بنجاح على كل الأنظمة المستقلة والبيئات المتصلة بالشبكة.



شكل 22.5 اطار كيسي للتحقيق

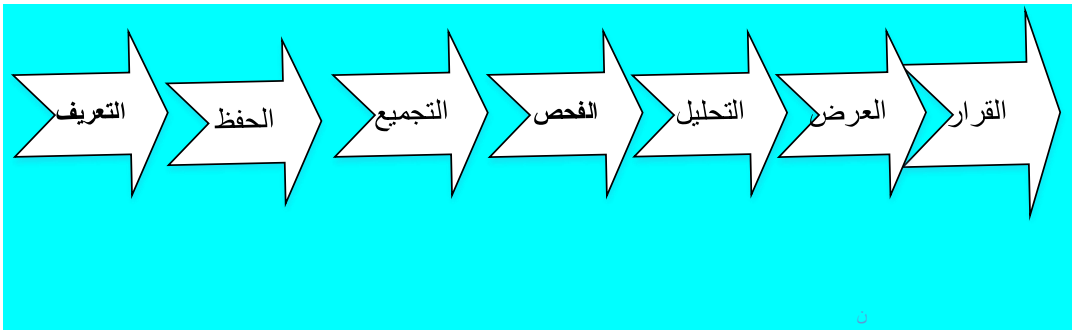
اطار ورشة عمل ابحاث جمع الادلة الرقمية : DFRWS

أنتجت أول ورشة عمل لأبحاث الطب الشرعي الرقمي (DFRWS) نموذجا يحدد خطوات تحليل الطب الشرعي الرقمي في عملية خطية. الخطوات هي كما يلي:

1. التعريف
2. الحفظ
3. التجميع
4. الفحص
5. التحليل
6. العرض
7. القرار

لا يقصد بالنموذج أن يكون نموذجا شاملا نهائيا ، بل كأساس للعمل في المستقبل والذي سيحدد النموذج الكامل ، وكذلك كإطار للبحث في المستقبل. (Palme 2001)

يتم تقديم نموذج بالمر او (DFRWS) على أنه خطي (Linear) ، ولكن تم ذكر إمكانية ردود الفعل من خطوة واحدة إلى الخطوات السابقة.



شكل5-23 اطار ورشة عمل ابحاث جمع الادلة

لا يناقش تقرير (DFRWS) خطوات النموذج بتفصيل كبير ولكن لكل خطوة يتم سرد عدد من القضايا ذات الصلة ، على سبيل المثال للحفاظ على القضايا ذات الصلة هي إدارة الحالات ، وتقنيات التصوير ، وسلسلة الحفظ.

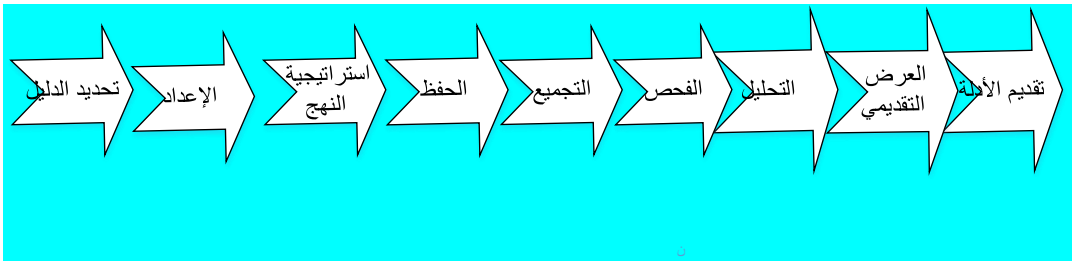
iii **اطار كار- ريث**

يصف (Reith) و (Carr) و (Gunsch Reith) و (Carr) و (Gunsch) (2002) نموذجا مستمدا إلى حد ما من نموذج (DFRWS).

الخطوات في نموذج كار- ريث هي:

1. **تحديد الدليل.**
2. **الاعداد.**
3. **استراتيجية النهج.**
4. **الحفظ.**
5. **التجميع.**
6. **الفحص.**
7. **التحليل.**
8. **العرض التقديمي.**
9. **تقديم الادلة.**

هذا النموذج واضح في أنه يهدف صراحة إلى أن يكون نموذج مجرد ينطبق على أي تكنولوجيا أو نوع من الجرائم الإليكترونية.



شكل 5-24 اطار كار- ريث للتحقيق

يهدف هذا النموذج إلى استخدام النموذج كأساس لتطوير أساليب أكثر تفصيلا لأنواع محددة من الاستقصاء ، مثل التعامل مع محركات الأقراص الثابتة أو الذاكرة غير المتطايرة المضمنة ، مع تحديد أي قواسم مشتركة ممكنة في الإجراءات أو الأدوات.
بالنظر إلى وجود عدد من النماذج بالفعل ، ما هو الدافع لتقديم نموذج آخر؟ الاجابة بكل بساطة هي ان الواقع يقول لا تغطي النماذج الحالية جميع جوانب التحقيق في الجرائم الإلكترونية ؛ وأنها تركز بشكل رئيسي على معالجة الأدلة الرقمية.
على الرغم من أن اطر التحقيق التي تم ذكرها وغيرها مما لم نتعرض لها نجدها جميعا ذات قيمة ، الا انها ليست عامة بما يكفي لوصف عملية التحقيق بشكل كامل بطريقة ستساعد في تطوير أدوات وتقنيات التحقيق الجديدة.

8.5 الخلاصة والمناقشة : Conclusion& Discussion

أشهر طرق الاختراق التي يستخدمها القراصنة واللصوص طريقة بث الفيروسات، وهي الطريقة المفضلة لدى القراصنة و طريقة سرقة الشرائح: وهي ايضا من أكثر الطرق تداولا بين لصوص الإنترنت

عرضت الدراسة لاهم معضلات التحقيق في الجريمة الجرائم الإليكترونية التي أمكن تلخيصها في ثلاثة نقاط:

أولا : لا تخلف جرائم الحاسب آثارا ظاهرة خارجية.

الجرائم المعلوماتية ينتفي فيها ولا توجد فيها آثار لاقتحام، وإنما هي أرقام ودلالات تتغير أو تمحي من السجلات ومما يزيد من هذه الصعوبة ان ارتكابها يتم في الخفاء، و يتم نقل المعلومات بواسطة النبضات الإلكترونية.

ثانيا : يتم ارتكاب الجريمة الإليكترونية عادة عن بعد حيث تتباعد المسافات بين الفاعل والنتيجة، بل تمتد إلى النطاق الإقليمي لدول أخرى.

ثالثا : تبدو أكثر المشاكل جسامة امتناع المجني عليهم عن التبليغ عن ما تعرضوا له.

بعض الجرائم المرتكبة ضد انظمة الحاسب الخاص او ما يعرف بالرقم الأسود، لا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل.

مع تزايد أهمية أمن الكمبيوتر وخطورة الجريمة الالكترون اصبح من الضروري لمحترفي الكمبيوتر التمتع بالفهم القانوني و فهم التكنولوجيا التي تستخدم في جمع الادلة الرقمية وكل ما هو دائر حول المعلومات الأساسية المتعلقة بالتقنيات المستخدمة في هذا الاطار.

الفهم القانوني و فهم التكنولوجيا يشمل استرداد البيانات والاستجابة الأساسية لاي متسلل (System Intruder) على النظام، وكل ما يتعلق بتكنولوجيا برمجيات الدخول الرئيسية (Technology of Key

Logging Software) ، و الأجهزة، والجوانب القانونية والأخلاقية (Cybercrime Ethics) لتكنلوجيا جمع الادلة الشرعية الرقمية (Digital Forensic) .

تطور استخدام البينة الرقمية Digital Evidence كان دائما بسبب ان المحاكم اصبحت تقبل تقديم البينة الرقمية للفصل في القضايا المعروضة امامها مما استدعى توفر قوانين قادرة على معالجة قضايا السايبر الحالية والمتوقعة كما انه قد حتم ابتداءا التعاون البناء بين اهل الفكر القانوني ومحترفي الكمبيوتر و تقانة المعلومات.

المشكلات الاجرائية في مجال الجرائم الالكترونية تظهر في ناحيتين:

الناحية الاولى: ان البيانات الالكترونية هي كيانات غير ملموسة بالتالي يصعب كشفها .

والناحية الثانية: ان جمع الادلة بشأنها في بعض الاحيان ترتفع درجة الصعوبة فيه الى مستوي يصعب تصوره، كما ان صعوبة الاجراءات تعقدها سرعة، وحساسية، ودقة تنفيذ الجريمة وسهولة محو اثارها .

وسائل الإثبات في القانون عموما هي البينة، الإقرار، القرائن، الخبرة، معلومات القاضي، الكتابة، اليمين.

اصبح في امكان وكالات إنفاذ القانون الآن استخدام القوة المتزايدة لنظم الكمبيوتروالوسائل المعقدة لجمع الادلة الشرعية باستخدام برامج معقدة لتسريع التحقيقات وأتمام إجراءات التفتيش.

يتوفرحاليا عدة نماذج واطر للتحقيق في الجريمة الإليكترونية وذلك من واقع الطرح المتوفر ضمن ادبيات ونظريات التحقيق في الجريمة بشكل عام والجريمة الإليكترونية في الوقت نفسه.

اورد البحث اربعة امثلة لاطر التحقيق اولها اطار لي وثانيها يوقهوين كاسي الذي قدم في العام 2000 نموذجا لمعالجة الأدلة الرقمية وفحصها ثم اطار ورشة عمل ابحاث جمع الادلة الرقمية واخيرا تعرض البحث لاطار كار- ريث للتحقيق وهذا النموذج يهدف بوضوح إلى أن يكون نموذجا مجردا ينطبق على أي تكنولوجيا أو نوع من الجرائم الإلكترونية.

VI. الباب السادس

الاطار الشامل (الاطار المقترح)

1.6 المقدمة :

النموذج الاكثر شمولا (General framework) للتحقيقات في جرائم الإنترنت يشكل اهمية ملوحظة في توحيد المصطلحات وتحديد المتطلبات ودعم تطوير التقنيات والأدوات الجديدة للمحققين .

في هذا الجزء من البحث، يتم تقديم نموذج من التحقيقات يجمع بين النماذج الحالية، ويعممها، ويوسع نطاقها (wide-ranging) عن طريق معالجة بعض الأنشطة غير المدرجة فيها صراحة .

على عكس النماذج التي تعرضنا لها في الباب السابق ، يمثل النموذج الذي نقترحه هنا بشكل صريح تدفقات المعلومات في التحقيق ويلتقط النطاق الكامل للتحقيق ، ويتجاوز بشكل ملحوظ نطاق معالجة الأدلة .

يتم عرض نتائج تقييم النموذج من خلال تقييم ممارسي التحقيق في الجرائم الجنائية وبعض من قاموا بممارسة دور محققي الجرائم الإليكترونية .

تتم مقارنة هذا النموذج الجديد ببعض النماذج الحالية الاكثر استخداما وشيوعا وتطبيقه على تحقيق افتراضي .

تتوافر للنموزج المقترح مواصفات النموزج الجيد للتحقيق في الجريمة الإليكترونية.

نحسب ان النموذج الجيد لتحقيقات جرائم الإنترنت يجب ان يعد أمرا مهما ، لأنه يوفر إطارا مرجعيا مجردا، بغض النظر عن أي تكنولوجيا أو بيئة تنظيمية محددة ، لمناقشة التقنيات والتكنولوجيا لدعم عمل المحققين .

يمكن أن يوفر النموذج المقترح أساسا للمصطلحات الشائعة لدعم مناقشة وتبادل الخبرات .

يمكن استخدام النموذج للمساعدة في تطوير وتطبيق المنهجيات على التقنيات الجديدة فور ظهورها وتصبح موضع تحقيقات.
وعلاوة على ذلك ، يمكن استخدام النموذج بطريقة استباقية لتحديد فرص تطوير ونشر التكنولوجيا لدعم عمل المحققين ، وتوفير إطار لالتقاط وتحليل متطلبات أدوات التحقيق ، وخاصة بالنسبة للأدوات التحليلية الآلية المتقدمة.
في الوقت الحالي ، هناك نقص في النماذج العامة الموجهة بالتحديد إلى تحقيقات جرائم الإنترنت . (cybercrime investigation frameworks) النماذج المتاحة تقوم فقط بالتركيز على جزء من عملية التحقيق (التعامل مع جمع وتحليل وتقديم الأدلة) ولكن يجب أن يشتمل النموذج العام بالكامل على جوانب شاملة من التحقيق (Kerr 2005) .
مثل هذا النموذج مفيد ليس فقط لتطبيق القانون، بل يمكن أن يفيد مديري تكنولوجيا المعلومات وممارسي الأمن والمدققين .
مديري تكنولوجيا المعلومات وممارسي الأمن والمدققين أصبحوا في وضع يسمح لهم بإجراء التحقيقات بسبب تزايد حالات الإجرام السيبراني ، وأيضا بسبب انتهاكات سياسات الشركة وإرشاداتها (مثل إساءة استخدام اتصالات الإنترنت في مكان العمل) .
يقدم هذا البحث نموذجا موسعا للتحقيقات في الجرائم الإلكترونية التي تحدد أنشطة عملية التحقيق والتدفقات الرئيسية للمعلومات في تلك العملية ، وهو جانب مهم في تطوير الأدوات الداعمة. (Casey 2009) .

مقارنة بعض اهم النماذج (frameworks) الحالية من الأدب (literature) والتي تم استعراضها في الباب السابق بالنموذج الجديد تمكن من الوصول الى اثبات أن النموذج المقترح هنا أوسع من النماذج التي تتعامل فقط مع معالجة الأدلة الرقمية ؛ اذ ان هذا النموذج يحاول ، الاستيلاء على أكبر قدر ممكن من عملية التحقيق في الجرائم الإليكترونية بأكملها بما في ذلك أنشطة معالجة الأدلة الرقمية .

تقتصر النماذج المتوفرة حاليا والتي تطرقنا لاكثرها شيوعا إلى حد كبير على التحقيق في مسرح الجريمة والأدلة ، وبالتالي فهي أقل شمولا في نطاقها من النموذج او الاطار المقترح في هذا الجزء من البحث .

لا تغطي النماذج الحالية جميع جوانب التحقيق في الجرائم الإلكترونية ؛ بل أنها تركز بشكل رئيسي على معالجة الأدلة الرقمية (Ciardhuáin 2004) .

على الرغم من أن النمازج والاطر الحالية ذات قيمة ، فهي ليست عامة بما يكفي لوصف عملية التحقيق بشكل كامل بطريقة ستساعد في تطوير أدوات وتقنيات التحقيق الجديدة .

يمكن أن يوفر النموذج الشامل المقترح إطارا مرجعيا مشتركا للمناقشة ولتطوير المصطلحات.

يمكن لهذا الاطار أن يدعم تطوير الأدوات والتقنيات والتدريب وإصدار الشهادات / واعتماد المحققين والأدوات.

يمكن أن يوفر أيضا هيكلا موحدا لدراسات الحالة / الدروس المستفادة التي سيتم تقاسمها بين الباحثين ، ولتطوير المعايير ، واختبار المطابقة ، وأفضل ممارسات التحقيق.

أكبر فجوة في النماذج الحالية هي أنها لا تحدد بوضوح تدفق المعلومات في التحقيقات.

جدول 6- 2 تسلسل وفاعلية انشطة الاطار المفترح

تسلسل النشاط	فاعلية النشاط
1. العلم والاذن.	نشاط العلم وطلب الاذن يسمح بالعلاقة مع الأحداث التي تتطلب إجراء تحقيق
2. التخطيط.	تتأثر الخطط باللوائح والتشريعات التي تحدد السياق العام للتحقيق
3. الإخطار.	إبلاغ موضوع التحقيق أو الأطراف المعنية الأخرى بأن التحقيق جار
4. البحث عن الأدلة وتحديدها.	تحديد موقع الأدلة وتحديد ماهية النشاط التالي
5. جمع الأدلة وحفظها.	تستحوذ فيه هيئة التحقيق على الأدلة في شكل يمكن حفظه مثل تصوير الأقراص الصلبة أو الاستيلاء على أجهزة كمبيوتر بأكملها.
6. تخزين الأدلة.	يأخذ التخزين في الاعتبار الحاجة إلى الحفاظ على سلامة الأدلة.
7. فحص الأدلة.	استخدام عدد كبير من التقنيات المحتملة للعثور على البيانات المهمة
8. الفرض.	إنشاء فرضية لما حدث وتعتمد شكلية هذه الفرضية على نوع التحقيق.
9. تقديم الفرضية.	يجب تقديم الفرضية إلى أشخاص غير المحققين. (النيابة/الادارة)
10. اثبات/ الدفاع عن الفرضية	على المحققين إثبات صحة فرضيتهم والدفاع عنها ضد النقد والتحدي التراجع للحصول على مزيد من الأدلة وفحصها ، وبناء فرضية أفضل.

على سبيل المثال ، مقدمو اطار كار-ريث Reith et al. (2002) أنفسهم لاحظوا عدم وجود أي ذكر صريح لسلسلة الاحتجاز في نموذجهم. وهذا عيب كبير عندما ينظر المرء في القوانين والممارسات واللغات المختلفة وما إلى ذلك والتي يجب معالجتها بشكل صحيح في التحقيقات. (Mark Reith 2002)

من المهم تحديد ووصف تدفقات المعلومات حتى يمكن حمايتها ودعمها تقنيا ، من خلال استخدام البنى التحتية الموثوق بها للمفتاح العام وختم الوقت لتحديد المحققين ومصادقة الأدلة .
هناك مشكلة أخرى في النماذج الحالية وهي أنها تميل إلى التركيز على الجزء الأوسط من عملية التحقيق ، أي جمع الأدلة وفحصها. ومع ذلك ، يجب أن تؤخذ المراحل السابقة والأخيرة في الاعتبار إذا ما أريد تحقيق نموذج شامل ، وخاصة إذا تم تحديد جميع المعلومات ذات الصلة من خلال التحقيق. (Palmer 2002).

2.6الأنشطة في التحقيق الشامل :

I. العلم والاذن.
II. التخطيط
III. الإخطار
IV. البحث عن الأدلة وتحديدها
V. جمع الأدلة وحفظها
VI. تخزين الأدلة
VII. فحص الأدلة
VIII. الفرض
IX. تقديم الفرضية
X. اثبات/ الدفاع عن الفرضية

3.6 مقارنة طريقة عمل الاطار المقترح مع الاطر الاكثر شيوعا :

بشكل عام ، يتم التحقيق وفقا للنموذج الشامل المقترح كأنشطة تتبع بعضها بشكل يحتم توفر شرط التتابع. ومع ذلك ، قد يتطلب أي نشاط إجراء تغييرات على نتائج نشاط سابق أو عمل إضافي في هذا النشاط ، وبالتالي فإن تسلسل الأنشطة التي يتضمنها النموذج يسمح بالتراجع واعادة الخطوة او تكرارها .

جدول 6-3 عمل الاطار الشامل والاطر الاكثر شيوعا

الاطار المقترح	الاطر الاكثر استخداما			
	جمع الادلة	كارنيث	كيسي	لي
1. العلم والاذن.		x		
2. التخطيط		x		
3. الإخطار				
4. البحث عن الأدلة وتحديدها	X	x	X	x
5. جمع الأدلة وحفظها	X	x	X	x
6. تخزين الأدلة				
7. فحص الأدلة	X	x	X	x
8. الفرض	X	x		x
9.تقديم الفرضية	X	x		x
10. اثبات/الدفاع	X			

استيفاء مرحلة النشاط المعين شرط اساسي للانتقال للمرحلة التي تليها مما يعني ان كل مرحلة تعتمد على المرحلة التي تسبقها لتبدأ. بمعنى ادق فان مرحلة العلم والاذن كاولى مراحل التحقيق

لا يمكن تجاوزها للانتقال لمرحلة التخطيط ما لم يتأكد حدوث ما يستلزم التحقيق اي ان مرحلة الاذن في الاساس تهدف للوصول الى تأكيد انه قد حدث ما يؤكد ضرورة قيام التحقيق، اذ

بمقارنة انشطة الاطار المقترح مع الاطر الاكثر شيوعا فمن المتوقع أن تكون هناك عدة تكرارات لبعض أجزاء التحقيق، و عادة ما يتم تكرار تسلسل أنشطة فرضية تقديم الفرضية - دليل - إثبات / الدفاع عدة مرات ، ربما مع فرضيات متزايدة التعقيد وتحديات أقوى في كل تكرار مع نمو فهم الأدلة أيضا

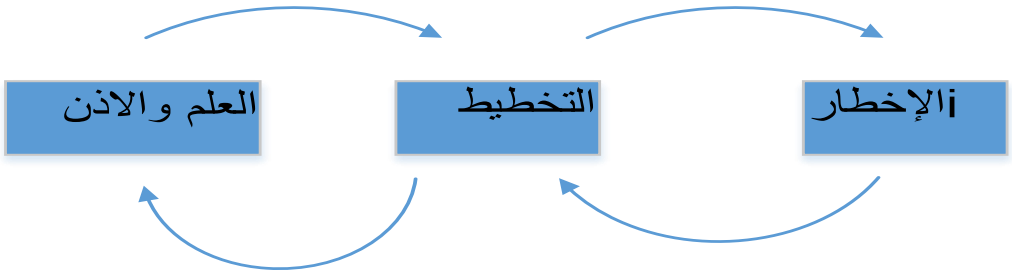
4.6 تدفقات المعلومات الرئيسية

أثناء التحقيق. تتدفق المعلومات حول التحقيق من نشاط إلى آخر طوال عملية التحقيق. على سبيل المثال ، تتكون سلسلة الاحتجاز من قائمة الأشخاص الذين تعاملوا مع بعض الأدلة ويجب أن ينتقلوا من مرحلة إلى أخرى مع إضافة أسماء في كل خطوة. هناك أيضا تدفقات من / إلى أجزاء أخرى من المنظمة ، وإلى / من كيانات خارجية. العلم والاذن بابتداء التحقيق هو الخطوة الأولى في التحقيق وهي خلق علم ووعي وطلب الاذن بأن التحقيق مطلوب. عادة ما يتم إنشاء هذا العلم او الوعي من خلال أحداث خارج المنظمة والتي ستقوم بالتحقيق ، على سبيل المثال يتم الإبلاغ عن جريمة إلى الشرطة أو يطلب من المراجع

إجراء مراجعة. قد ينتج أيضا عن أحداث داخلية ، ينبه نظام اكتشاف التسلل مسؤول النظام إلى تعرض أمان النظام للخطر.

بالنظر إلى وجود عدد من النماذج التي تؤطر للتحقيق في الجريمة الالكترونية ، ما هو الدافع لتقديم نموذج آخر؟ الاجابة بكل بساطة هي ان الواقع يقول لا تغطي النماذج الحالية جميع جوانب التحقيق في الجرائم الإلكترونية ؛ وأنها تركز بشكل رئيسي على معالجة الأدلة الرقمية .

على الرغم من أن اطر التحقيق التي تم ذكرها وغيرها مما لم نتعرض لها فهي جميعا ذات قيمة ، الا انها ليست عامة بما يكفي لوصف عملية التحقيق بشكل كامل بطريقة ستساعد في تطوير أدوات وتقنيات التحقيق الجديدة.



شكل25.6 بداية التحقيق

العلم والاذن: يتم توضيح نشاط العلم وطلب الاذن في هذا النموذج لأنه يسمح بالعلاقة مع الأحداث التي تتطلب إجراء تحقيق. لا تعرض معظم النماذج السابقة هذا النشاط بشكل صريح وبالتالي لا تتضمن علاقة مرئية بالأحداث المسببة. هذا هو ضعف النماذج الاخرى لأن الأحداث التي تسبب التحقيق قد تؤثر بشكل كبير على نوع التحقيق المطلوب. الواقع يقول لا تغطي النماذج

الحالية جميع جوانب التحقيق في الجرائم الإلكترونية ؛ لأنها تركز بشكل رئيسي على معالجة الأدلة الرقمية .

اطار كار- ريث والاطار الشامل:

من الأهمية بمكان مراعاة الاختلافات المصاحبة للتحقيق تبعا لصفة من يجري التحقيق لضمان اتباع النهج الصحيح في التحقيق في السياق المناسب، اذ يمكن للمدقق الدولي او المحقق في الجريمة العابرة للحدود توقع تعاون من عميل ، بينما قد لا يتلقى محقق الشرطة المحلية تعاونا من المشتبه فيهم في التحقيق. والاذن هو الجزء الثاني من المرحلة الاولي في الاطار الشامل فنجد ان التفويض بعد تحديد الحاجة إلى التحقيق ، يتمثل في ان النشاط التالي هو الحصول على تصريح للقيام بالتحقيق وهو اختلاف جوهري حيث لا نجد ان التفويض قد ذكر في اطار كار- ريث باعتباره شرط صحة للانتقال للنشاط التالي. كما قد يكون الحصول على التفويض او الاذن معقدا للغاية ويتطلب تفاعلا مع كيانات خارجية وداخلية للحصول على الترخيص اللازم، بينما قد يختلف مستوى الهيكل الرسمي المرتبط بالترخيص إلى حد كبير ، اعتمادا على نوع التحقيق.

من ناحية اخرى فانه بالنسبة للاطار الشامل المقترح ، فقد لا يحتاج مسؤول النظام سوى موافقة شفهية بسيطة من إدارة الشركة لإجراء تحقيق مفصل لأنظمة الكمبيوتر في الشركة ؛ بينما تحتاج، وكالات إنفاذ القانون عادة تفويضا قانونيا رسميا يحدد بالتفصيل الدقيق ما هو مسموح به في التحقيق (مثل أوامر المحكمة أو أوامر الاعتقال).

التخطيط: يتأثر نشاط التخطيط بشدة بالمعلومات الواردة من داخل وخارج منظمة التحقيق. وتشمل هذه المعلومات الواردة من الداخل او الخارج ، اللوائح

والتشريعات التي تحدد السياق العام للتحقيق والتي لا تخضع لسيطرة المحققين، بينما لا نجد اثرا لخطوة التخطيط لارتباطها ببداية التحقيق والاتجاه لجمع

جدول 6-4 مقارنة خطوات نموزج كار-ريث بخطوات النموزج الشامل

الخطوات في نموذج كار- ريث	الفرق	الخطوات في النموذج الشامل
نموذج كار- ريث واضح في آنه يهدف صراحة إلى أن يكون نموذج مجرد ينطبق على أي تكنولوجيا أو نوع من الجرائم الإليكترونية. وخطواته تتجه مباشرة نحو جمع الادلة		
1. تحديد الدليل	هذه الخطوة عند كار-ريث متجهة نحو الدليل مباشرة	1. العلم والاذن.
2. الاعداد.	الخطوة موجودة في كل باسلوب مختلف	2. التخطيط
3.استراتيجية النهج	الخطوات غير متوافقة	3. الإخطار
4. الحفظ	اورد الحفظ دون الاشارة لكيفية الحيازةغيرمتوافقة لاختلاف الخطوات . تختلف المعالجات باختلاف المداخل كار وريث لم يتعرضا للتخزين.	4. البحث عن الأدلة وتحديدها
5. التجميع		5. جمع الأدلة وحفظها
6. الفحص		6. تخزين الأدلة
7. التحليل		7. فحص الأدلة
لم يتعرض كار وريث لهذه الخطوة		8. الفرض
8.العرض التقديمي	مرحلة تسبق السلطة النهائية في الاطار الشامل ولكنها تقدم سلطة افتراضية تملك القدرة على الايقاف او الاستمرار.	9. تقديم الفرضية
9. تقديم الادلة	سلطة اعلى في الشامل وغير محددة عند كار وريث	10. اثبات/ الدفاع عن الفرضية

الادلة مباشرة بعد تسلم امر الشروع في عملية التحقيق بنية جمع الادلة دون سواها دون الاعتداد بالاخطار كخطوة مكملة لاحقة لعدم ورودها كنشاط في اطار كار-ريث يتطلب التقييم كنشاط قد يتطلبه القانون ومناقشة ما يتعلق به مثل الحصانات والحماية القانونية.
قد توجد هناك أيضا معلومات تم جمعها بواسطة المحققين من مصادر خارجية أخرى، او
من داخل المنظمة ، تشمل هذه المعلومات استراتيجيات وسياسات ومعلومات خاصة بالمنظمة حول التحقيقات السابقة وهي خاصية ينفرد بها الاطار الشامل بالرغم من انه قد يثير نشاط التخطيط الحاجة إلى التراجع والحصول على مزيد من التصريح ، على سبيل المثال عندما يكون نطاق التحقيق أكبر من المعلومات الأصلية.

الاخطار: يشير الإخطار في النموذج الشامل إلى إبلاغ موضوع التحقيق أو الأطراف المعنية الأخرى بأن التحقيق جار. قد لا يكون هذا النشاط مناسبا في بعض التحقيقات، على سبيل المثال عندما تكون هناك حاجة لاستخدام عنصر المفاجأة لمنع تدمير الأدلة. ومع ذلك ، في أنواع أخرى قد تكون مطلوبة ، أو قد تكون هناك منظمات أخرى يجب أن تكون على علم بالتحقيق. هذه الخطوة قد لا تنطبق على معظم اجراءات التحقيق المتعلقة بالاخطار وقد يكون السودان من المناطق القليلة التي قد يكون لعملية الاخطار فيها دور مؤثر خصوصا فيما يتعلق بالحصانات والحمايات القانونية لبعض الفئات. **البحث عن الأدلة وتحديدها:** يتناول هذا النشاط تحديد موقع الأدلة وتحديد ماهية النشاط التالي او ما من المهم القيام به.

في أبسط الحالات ، قد يتضمن ذلك العثور على جهاز الكمبيوتر الذي يستخدمه المشتبه فيه

والتأكيد على أنه هو موضع اهتمام المحققين. ومع ذلك ، في بيئات أكثر تعقيدا ، قد لا يكون هذا النشاط مباشرا ؛ على سبيل المثال ، قد يتطلب الأمر تتبع أجهزة الكمبيوتر من خلال عدة

شكل26.6 حيازة وحفظ وفحص الادلة

جهات من مزودي خدمات الإنترنت وربما في بلدان أخرى بناء على معرفة عنوان IP

جمع الادلة وحفظها : مجموعة جمع الادلة تمارس النشاط خلال الوقت الذي تستحوذ فيه هيئة التحقيق على الأدلة في شكل يمكن حفظه وتحليله ، مثل تصوير الأقراص الصلبة أو الاستيلاء على أجهزة كمبيوتر بأكملها . هذا النشاط هو محور معظم النقاش في الدراسات الخاصة بالادب literature بسبب أهميته لبقية التحقيق.

الأخطاء أو الممارسات السيئة في هذه المرحلة قد تجعل الدليل عديم الفائدة ، وتحديدا تحريك الادلة ليتم حفظها اذ دائما ما يلاحظ ان التحقيقات تخضع لمتطلبات قانونية صارمة. بعد جمع الادلة ، يجب نقل الادلة الى مكان مناسب وحفظها لفحصها لاحقا .

من المهم التأكد من أن الأدلة تظل صالحة للاستخدام في وقت لاحق أثناء النقل ، أي أن وسائل النقل المستخدمة لا تؤثر على سلامة الأدلة .

تخزين الأدلة : التخزين يجب أن يتم تخزين الأدلة التي تم جمعها في معظم الحالات لأن الفحص لا يمكن أن يتم على الفور . يجب أن يأخذ التخزين في الاعتبار الحاجة إلى الحفاظ على سلامة الأدلة .

فحص الأدلة : و يتضمن فحص الأدلة استخدام عدد كبير من التقنيات المحتملة للعثور على البيانات المهمة وتفسيرها . قد يتطلب الأمر إصلاح البيانات التالفة بطرق تحافظ على سلامتها . بناء على نتائج أنشطة البحث / التحديد وجمع البيانات ، قد يكون هناك كميات كبيرة جدا من البيانات التي يتعين فحصها ، لذا يلزم وجود تقنيات آلية لدعم الباحث.

شكل27.6 وضع وتقديم اثبات الفرضيات

إنشاء الفرضية : بناء على فحص الأدلة ، يجب على المحققين إنشاء فرضية لما حدث. تعتمد درجة شكلية هذه الفرضية على نوع التحقيق. على سبيل المثال ، يمكن ان يؤدي تحقيق الشرطة إلى إعداد فرضية تفصيلية تحتوي على مواد داعمة موثقة بعناية من الفحص، مناسبة للاستخدام في المحكمة. قد يكون إجراء التحقيق داخلي من قبل مسؤول أنظمة الشركة إلى تقديم تقرير أقل رسمية إلى الإدارة. من المتوقع التراجع عن هذا النشاط إلى نشاط الفحص ، حيث يطور المحققون فهما أكبر للأحداث التي أدت إلى التحقيق في المقام الأول.

تقديم الفرضية : العرض التقديمي يجب تقديم الفرضية إلى أشخاص غير المحققين.

بالنسبة لتحقيقات الشرطة في السودان، يتم وضع الفرضية أمام هيئة محكمة او جهة عدلية، بينما في حالة الشركة قد توضع ، فرضية التحقيق امام الإدارة لاتخاذ قرار بشأن الإجراء الواجب اتخاذه.

اثبات / الدفاع عن الفرضية: اما فيما يتعلق بالإثبات / الدفاع بشكل عام ، فقد لا تمر الفرضية دون تحديات ؛ اذ قد يتم وضع فرضية المخالفة والأدلة الداعمة أمام هيئة محكمة، على سبيل المثال.

يتعين على المحققين إثبات صحة فرضيتهم والدفاع عنها ضد النقد والتحدي. كما انه من المحتمل أن تؤدي التحديات الناجحة إلى التراجع إلى المراحل السابقة للحصول على مزيد من الأدلة وفحصها ، وبناء فرضية أفضل.

عادة ما تكون السياسات والإجراءات المعمول بها هي التي تحدد التفاصيل.

تؤثر المعلومات في التحقيقات المستقبلية وقد تؤثر أيضا على السياسات والإجراءات. وبالتالي ، يعد جمع هذه المعلومات وصيانتها جانبا رئيسيا لدعم عمل المحققين ومن المرجح أن يكون مجالا مثمرا لتطوير تطبيقات متقدمة تتضمن تقنيات مثل استخراج البيانات وأنظمة الخبراء.

وصف هاوك وآخرون مثال لنشاط النشر (2002) نظاما يسمى Coplink يوفر دعما في الوقت الفعلي لمحققي إنفاذ القانون في شكل أداة تحليل تستند إلى مجموعة كبيرة من المعلومات من التحقيقات السابقة.

اما هاريسون وآخرون (2002) فقد تعرض النموذج الأولي الخاص بهم ليس للوقت الفعلي ، ولكن لما يوفره من خاصية أرشيفية تشير لتجربة ومعرفة المحققين.

يظهر عدد من تدفقات المعلومات في النموذج المقترح. أولا ، هناك تدفق للمعلومات داخل منظمة التحقيق من نشاط إلى آخر.
قد يسود ذلك ضمن مجموعة واحدة من المحققين أو بين مجموعات مختلفة ، فعلى سبيل المثال عندما يتم تمرير الأدلة إلى مختبر الادلة الجنائية المتخصص لفحصها ، يعد تدفق المعلومات هنا هو الأهم في عملية التحقيق ، لكن قد لا يتم إضفاء الطابع الرسمي عليه لأنه داخل المنظمة ،

وعادة ما يكون ضمن فريق تحقيق واحد. ومع ذلك ، هناك فوائد يمكن الحصول عليها من خلال النظر في هذه المعلومات بشكل صريح.

من خلال القيام بالنظر في المعلومات ، يمكن تقديم الدعم في شكل إجراءات وأدوات آلية ، مثل
أدوات إدارة الحالات.قبل أن يبدأ التحقيق ، هناك حاجة إلى وصول المعلومات إلى المحققين، مما يخلق الوعي او العلم والتأكيد بأن هناك حاجة إلى التحقيق بالتالي طلب الاذن والتفويض لبداية التحقيق.

5.6 تصميم الاطار:

تم تصميم الاطار على أنه إما داخلي (على سبيل المثال نظام للكشف عن الاختراق ينبه مسؤول النظام إلى الهجوم) أو من مصادر خارجية (مثل شكوى يتم تقديمها للشرطة).
الحصول على إذن بالتحقيق يتضمن تدفقات إضافية من المعلومات من وإلى السلطات المختصة ، على سبيل المثال الحصول على ترخيص قانوني لإجراء عملية بحث

أو الحصول على موافقة من إدارة الشركة لتخصيص الموارد للتحقيق في أي هجوم.
يتضمن نشاط التخطيط عدة تدفقات للمعلومات إلى فريق التحقيق من خارج المنظمة ، فانه يحدد ولزم باتباع ما هناك من سياسات ولوائح وتشريعات تحكم كيفية سير التحقيق. وبالمثل، هناك سياسات داخلية لمنظمة التحقيق يجب أن يتبعها المحققون. كما يتم استخلاص معلومات أخرى من قبل المحققين لدعم عملهم ، على سبيل المثال البيانات الفنية عن البيئة التي سيعملون فيها.
إذا كان ذلك مناسبا لنوع التحقيق ، سينتج عن نشاط الإعلام تدفق المعلومات إلى موضوع التحقيق.
في الإجراءات القانونية المدنية ، تكون هناك طلبات للإفصاح عن المستندات.
تخضع هذه المعلومات لضوابط مثل سياسات سلطة التحقيق.
عندما يجب تبرير الفرضية المستندة إلى الأدلة والدفاع عنها في نشاط الإثبات / الدفاع ، فإن المعلومات تتدفق إلى فريق التحقيق من داخل منظمتهم وخاصة من الخارج (مثل الطعن في الأدلة المقدمة في المحكمة).
عندما ينتهي التحقيق (سواء كانت النتيجة ناجحة من وجهة نظر المحققين أم لا) ، سيكون هناك تدفق للمعلومات عند نشر النتائج. تخضع هذه التدفقات مرة أخرى للضوابط ؛ على سبيل المثال ، قد يتعين حجب الأسماء ، أو قد لا يتم الكشف عن تفاصيل تقنية معينة على الفور للسماح بتنفيذ حلول للمشاكل.
تؤثر المعلومات التي ينتجها المحققون على السياسات الداخلية للمنظمة ، وكذلك تصبح مدخلات للتحقيقات المستقبلية.

قد يتم تمريرها أيضا من خلال وظيفة توزيع المعلومات الخاصة بالمؤسسة لتكون متاحة للمحققين الآخرين خارج المنظمة ، على سبيل المثال في شكل دراسة حالة منشورة تستخدم بواسطة القائمين على التدريب ، أو كاستشارة أمنية لمسؤولي النظام.
في جميع الأوقات أثناء التحقيق ، قد تتدفق المعلومات داخل وخارج المنظمة استجابة لاحتياجات المحققين. تخضع تدفقات المعلومات العامة هذه لضوابط المعلومات التي تضعها منظمة التحقيق.
لا يمكن تحديد جميع التدفقات المحتملة بوضوح ، وبالتالي ، هناك حاجة إلى مزيد من البحث لتحسين هذا الجانب من النموذج لسياقات معينة.
قد يكون هناك عدد من الأنشطة في هذا النموذج والتي لم يتم توضيحها بوضوح في الأنشطة الأخرى.

6.6 مزايا وعيوب الاطار:

يتمتع هذا النموذج بالمزايا التي تم الحصول عليها من النماذج السابقة ، ولكنه يوسع نطاقها ويوفر بعض المزايا الإضافية.
يعد الإطار المرجعي ضروريا لتطوير التحقيق في الجرائم الإلكترونية لأنه يسمح بالتوحيد القياسي وتناسق المصطلحات وتحديد المجالات التي تحتاج إلى البحث والتطوير.
يمكن للنموزج أن يوفر أيضا أداة تدريبية وأساسا لشرح عمل المحققين لغير المتخصصين، سواء كانوامن القائمين على تحقيق العدالة أو إدارة شركة.
الميزة الأهم لهذا النموذج بالمقارنة مع النمازج الاخرى هي التحديد الواضح لتدفقات المعلومات في عملية التحقيق.

يتيح تحديد تدفقات المعلومات في عملية التحقيق تحديد الأدوات وتطويرها ، والتعامل مع إدارة الحالات ، وفحص الأدلة ، والنشر المتحكم فيه للمعلومات.
يمكن أن يساعد النموذج أيضا في الحصول على خبرة المحققين وخبرتهم بهدف تطوير أدوات متقدمة تتضمن تقنيات مثل استخراج البيانات وأنظمة الخبراء.
عمومية النموذج تشير الى بعض الصعوبات، لذا يجب تطبيقه في سياق المنظمة قبل أن يكون من الممكن توضيح تفاصيل العملية.
على سبيل المثال ، يظهر النموذج تدفق المعلومات بين الأنشطة التي تتضمن تسجيل سلسلة الحراسة ، ولكن الإجراءات الخاصة بذلك لا يمكن أن يتم تحديدها بالتفصيل إلا عندما يعرف السياق التنظيمي والقانوني للمحققين .

7.6 تقييم الاطار المقترح

أكملت مجموعة من المحققين استبيانا ثم تلى ذلك مناقشة الاطار للتحقق من الحصول على آراء مجتمع مستخدمي الاطار .
وقد تم ذلك من خلال تقديم العمل لعدد من محققي الشرطة ذوي الخبرة الذين تراوحت خبرتهم ما بين 5 سنوات و 12 سنة ومناقشتها معهم في شكل جماعي.
بالإضافة إلى ذلك، تمت مقابلة محققين متمرسين بشكل منفصل.
تم إعطاء جميع المشاركين في عملية التقييم مواد توضيحية بناء على أوصاف النموذج تمت الإشارة إلى الآراء التي تم التعبير عنها خلال المقابلات وأكمل المحققون استبيانا ، (ملحق) اسفر عن ما يلي من مخرجات:

حققت المقابلات استفادة كاملة من تجربة المشاركين حققتها طريقة تنفيذ المقابلات بسبب انه اصبح لدى المشاركين فهم أوضح للموضوع ، اذ تمكن المشاركون من طرح أسئلة حول العمل بدلا من مجرد الرد على مجموعة ثابتة من الأسئلة.

جدول 6-5 تقييم المشاركين لفاعلية الانشطة

النشاط	فاعلية النشاط				
	1	2	3	4	5
العلم والاذن					✓
التخطيط					✓
الإخطار					✓
البحث عن الأدلة وتحديدها					✓
جمع الأدلة وحفظها					✓
تخزين الأدلة			✓		
فحص الأدلة					✓
الفرض					✓
تقديم الفرضية					✓
اثبات/ الدفاع عن الفرضية					✓

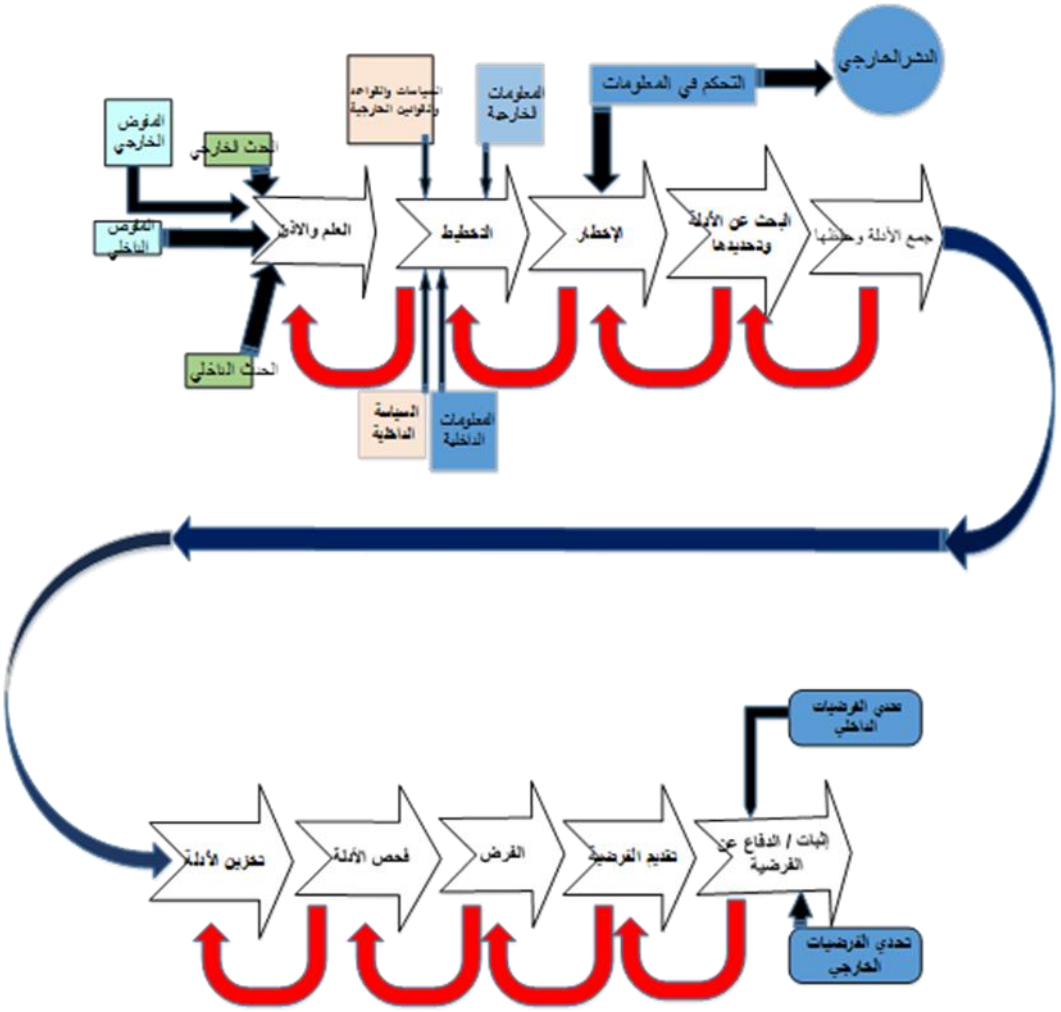
اصبح من الممكن للمشاركين إثارة ومناقشة النقاط التي قد لا يتم تحديدها بواسطة مسح بسيط.

8.6 استجابة المحققين للنموزج المقترح:

كانت استجابة المحققين لنموذج التحقيقات إيجابية للغاية. ذكرت المجموعة ردا على السؤال 1 (هل شعرت أن نموذج التحقيقات يمثل بشكل مناسب هيكل التحقيقات في مؤسستك؟) ، "النموزج على درجة عالية من الدقة ويتفوق على هيكل التحقيقات في المؤسسة ويصلح اطارا

للتحقيق في كل القضايا". كان من وجهة نظرهم أن النموذج كان أكثر قابلية للتطبيق بشكل عام من مجرد تحقيقات الجرائم الإليكترونية ؛ يمكن استخدامه لوصف أي تحقيق للشرطة. كما أظهر أنشطة لم يعتبروها أجزاء منفصلة من التحقيق، خاصة الفرضيات. ولوحظ أن التراجع او المراجعة المتأصلة في النموذج أمر مهم، لأن التحقيقات الحقيقية لا تسير بطريقة خطية بسيطة. شعرت المجموعة أنه لا أي عناصر يمكن حذف أي جزء من النموذج لعملهم (السؤال 3). ردا على السؤال 2 (هل تعتقد أن هناك عناصر لم يتضمنها النموزج ؟) ، اجابوا بأنه لا توجد عناصر مفقودة من النموذج الا انه قد ، اقترح أعضاء المجموعة تدفقات المعلومات الإضافية على النحو التالي:

أ. أثر السياسات الخارجية والتنظيم والتشريعات على سياسات المنظمة التي تقوم بالتحقيق، فرض على جهة التحقيق ربط السياسات واللوائح والتشريعات الخارجية والسياسات التنظيمية بضوابط المعلومات. المتعلقة بالعومل الامنية وسلامة البيانات وذلك لاسباب غالبا ما تتعلق



شكل28.6الاطار الشامل بكامل الانشطة

يتوفير السرية اللازمة للمعلومات وعدم تسربها إلى من هم خارج منظمة التحقيق ، او إلى أجزاء غير مناسبة من منظمة التحقيق نفسها .

منع هذا يتطلب ضوابط صارمة على تدفق المعلومات. محققو الشرطة حساسون بشكل خاص لهذا "التسرب" بسبب الحاجة إلى السرية التي تفرضها عليهم السياسات والتنظيمات والتشريعات الخارجية ، والاعتبارات العملية في إجراء التحقيق بنجاح كما يظهر في تطبيق النموذج على التحقيق (التطبيق بوقائع افتراضية للنموذج المقترح).

هذا التعديل المقترح لا يسبب أي تغيير جوهري في النموذج الأساسي. ومع ذلك ، فإنه يؤكد على أهمية

التقاط تدفقات المعلومات في التحقيق باستخدام نموذج من النوع المقترح في العمل الحالي ، ويوضح فائدة النموذج لفهم عملية التحقيق.
طلب من المشاركين في المجموعة النظر في اهمية وارتباط النموزج بعملهم (سؤال 4) مما يظهر تقييم المجموعة لأهمية أنشطة الاطار. على مقياس من واحد إلى خمسة ، مع كون خمسة هي أكثر أهمية ، تم اعتبار معظم الأنشطة "مهمة جدا". اذ ان ارتباط مجموعة من الانشطة كمجموعة خطوات اعطت قوة لانشطة الاطار ابعدت انشطة ثانوثة وفي ذات الوقت اكسبته العمومية والشمول.

اكد المشاركون يتجنب استبعاد فكرة الخطوة التي حملت ما هو فرعي فكرة جيدة وتجنب تضمين فكرة النقل التي عرضت كمقترح لتعديل الاطار بشكل ثانوي في رائي المشاركين يجعل النشاط ، في الوقت الحاضر ، تشتيت تركيز، مسؤولي الأنظمة الذين يجب عليهم صيانة ومراقبة نظام كشف التسلل من أجل أن يكونوا على دراية بالأحداث التي تتطلب التحقيق. اتفق المشاركون على أن من المرجح أن يصبح التعامل مع بعض الامور غير ذا قيمة مثيرة للقلق في المستقبل يزيد من نطاق التحقيقات.

9.6 استنتاجات حول النموذج

بناء على التقييم أعلاه ، يمكن الاستنتاج أن النموذج يوفر أساسا جيدا لفهم عملية التحقيقات والتقاط معظم تدفقات المعلومات. هناك حاجة إلى التركيز على السيطرة على تدفق المعلومات في بيئة إنفاذ القانون. سمح النموذج باستخلاص بعض الاستنتاجات المهمة حول حالة تحقيقات جرائم الكمبيوتر في الوقت الحالي:

I. العلم بالحاجة إلى التحقيق ليس مسألة يرى المحققون في الشرطة أنها مشكلة؛ اذ لديهم امدادات ثابتة من العمل.

II. لا يزال حفظ الأدلة الرقمية وتخزينها في المستوى الأساسي.

III. من المفهوم أن اطلاع الغير بالمعلومة الجديدة مهم ولكنه لا يزال محدودا.

ستحتاج منصات الحوسبة الجنائية إلى معالجة نشاط تبادل المعلومة في النموذج من أجل جعله أكثر فعالية ، وربما التعلم من تجارب محترفي أمان الكمبيوتر في تبادل المعلومات.

هناك مجال لإحراز تقدم كبير في أنشطة يمكن اضافتها للنموزج فيما بين الحفظ والتخزين مع تطور التكنولوجيا.

التطبيق الافتراضي للنموذج:

في هذا القسم ، يتم تقديم دراسة حالة عن تحقيق افتراضي.

10.6 وصف التحقيق:

بدأ هذا التحقيق عندما تلقت الادارة في كلية البيان رسالة بريد إلكتروني تدعي أنها عثرت على ثغرة أمنية في خدمة التواصل بين الكلية وطلابها عبر الإنترنت لخدمة النتائج والجداول والمذكرات التي تقدمها الكلية لطلابها.

عرض البريد الإلكتروني تقديم تفاصيل الضعف في مقابل ان تقوم الكلية بدفع فدية اسماها المخترق حافز. شرع الفريق الفني المختص في مراجعة وضع الخدمة لديهم وعند التحقق من سجلاتهم ، خلص الفريق المختص إلى أنه قد تم الوصول غير المصرح به إلى

خادم الويب الخاص بالكلية. تلقى الفريق المزيد من رسائل البريد الإلكتروني التي تهدد بالكشف عن الضعف أمام الطلاب واولياء الامور والجمهور، ويفضح هذا الضعف فتفقد النظام مصداقيته امام الطلاب و الجميع، كما اوضح المخترق باعث الرسالة انه سيتوجه الى الصحافة مشككا في النتائج السابقة لاعداد كبيرة من الطلاب كل ذلك مع وجود رابط إلى موقع على شبكة الإنترنت الذي يعتزم المشتبه به استخدامه لنشر الثغرة الأمنية.

قامت الكلية بإبلاغ الأمر إلى شرطة الخرطوم (شرطة الخرطوم شمال) التي بدأت التحقيق. ولكن تكشف بعد الحصول على التفويض (الاذن) من نيابة الخرطوم شمال أن نظام الكمبيوتر الذي تعرض للخطر كان يقع في ولاية قضائية مختلفة (الخرطوم) مقر الكلية، وان مصدر رسائل البريد الإلكتروني كان في مدينة ود مدني. لذلك ، تم إجراء التحقيق من قبل قوة شرطة أخرى شرطة ود مدني.من خلال فحص رسائل البريد الإلكتروني وملفات السجل ، تمكنوا من التعرف على المشتبه فيهم وتم الحصول على أمر تفتيش لمباني أصحاب العمل المشتبه بهم. أثناء البحث تم الاستيلاء على جهاز كمبيوتر للفحص. باستخدام EnCase ، وجد المحققون نسخا من جميع رسائل البريد الإلكتروني وبعض المعلومات الأخرى ذات الصلة ، مما أدى إلى نجاح الملاحقة القضائية.

11.6 النتائج وتطبيق النموذج :

من الوصف ، يمكن ملاحظة وجود ثلاث منظمات تحقيق (قوتان للشرطة والكلية) في ولايتين قضائيتين. هذا يدل على أهمية التقاط تدفق المعلومات بين المنظمات في نموذج عام.

تألف، التحقيق ككل ، من ثلاثة تحقيقات متداخلة ، يتضمن كل منها أنشطة النموذج وتبادل المعلومات مع الآخرين. يظهر هذا في الشكل25 (صفحة 153).

- **العلم والاذن:** يمكن ملاحظة أن نشاط العلم والاذن قد حدث ثلاث مرات في هذا التحقيق:
  I. عندما تلقت ادارة الكلية البريد الإلكتروني.
  II. عندما أبلغت ادارة الكلية ذلك للشرطة.
  III. عندما تم تمرير التحقيق إلى قوة شرطة ثانية.

الاذن الذي يكمل خطوة العلم والاذن: وهو التفويض الأولي للتحقيق من قبل الكلية الذي كان ضمنيا ، لأنهم كانوا يحققون في الخوادم الخاصة بهم.
ثم كان هناك التفويض الضمني الثاني حيث بدأ التحقيق بواسطة شرطة الخرطوم شمال، تلى ذلك إدراك أن شرطة الخرطوم شمال في واقع الأمر غير مخولة لإجراء التحقيق، فتم نقل التحقيق إلى قوة شرطة اخرى (شرطة ود مدني) تمت الموافقة على قيامها بالتحقيق للاختصاص. مذكرة البحث هي مثال واضح على الحصول على إذن خارجي.

- **التخطيط:** حدث هذا النشاط في تحقيق الكلية عندما قرروا إجراء فحص للسجلات مع إمكانية الاتصال بالشرطة ، بناء على ما تم العثور عليه .

اشتمل تحقيق الشرطة على تخطيط النهج الواجب اتباعه لتحديد هوية المشتبه فيه وجمع الأدلة اللازمة .

- **الإخطار:** حدث هذا النشاط عندما تم إبلاغ شرطة الخرطوم شمال بالتحقيق. لاحظ أن هذا الإشعار هو الحدث الخارجي الذي يتسبب في نشاط العلم والاذن داخل قوة التحقيق الثانية. في هذا التحقيق ، لم يكن من المناسب إبلاغ موضوع التحقيق بأنه قد تم التحقيق .

في الواقع ، تم توخي الحذر لتجنب إخبار المشتبه به بالتحقيق من خلال عدم زيارة الموقع الذي أنشأه.

- **البحث / التحديد:** حدث هذا في البداية عندما حددت الكلية ملفات السجل الخاصة بها كوسيلة لتحديد ما حدث. في وقت لاحق ، نفذت كل من قوات الشرطة أنشطة مماثلة لتحديد مصدر رسائل البريد الإلكتروني ، ونتج عن تفتيش مادي من المعلومات التي تم الحصول عليها في عمليات البحث السابقة. قد يرى أيضا أن نشاط البحث / التعريف ونشاط الفحص اللاحق قد يتفاعلان ، لأن فحص السجلات أدى إلى مزيد من البحث.
- **الجمع والحفظ:** حدث هذا النشاط عندما أدى البحث عن أماكن عمل أصحاب العمل إلى الاستيلاء على جهاز كمبيوتر ، وفي الحفاظ

على رسائل البريد الإلكتروني وملفات السجل كدليل. ثم تم نقل الكمبيوتر المضبوط. ومع ذلك ، يمكن ملاحظة ذلك أيضا في نقل ملفات السجل من الخادم إلى الشرطة لفحصها ، وفي نقل رسائل البريد الإلكتروني من الكلية إلى الشرطة.

- **التخزين:** يمكن ملاحظة هذا النشاط في الاحتفاظ بالكمبيوتر المصادر من قبل الشرطة وفي تصوير قرص ذلك الكمبيوتر. يمكن أيضا رؤيته في تخزين السجل من الملفات ورسائل البريد الإلكتروني. (Venema 1999)
- **الفحص:** حدث هذا النشاط في فحص الكلية لملفات السجل الخاصة بها. كما حدث في فحص الشرطة لملفات السجل ورسائل البريد الإلكتروني والكمبيوتر المصادر.
- **الفرضية:** حدث هذا النشاط في تحقيق الكلية عندما استنتج من السجلات أن الوصول غير المصرح به قد حدث.

في تحقيقات الشرطة ، وضعت فرضية أولية لهوية المشتبه به ، مما أدى إلى مصادرة الكمبيوتر للحصول على مزيد من الأدلة.

تضمن هذا التراجع في النموذج ، وأسفر عن فرضية أكثر تفصيلا تم تقديمها بعد ذلك إلى المحكمة.

- **العرض التقديمي:**

حدث هذا النشاط عدة مرات:

I. داخل الكلية ، قبل اتخاذ قرار الاتصال بالشرطة ، وعندما تم فحص الأدلة من قبل الإدارة وربما تم طلب المشورة القانونية.
II. عندما قدمت الكلية دليلها على الحادثة إلى محققي الشرطة.
III. عندما نقلت قوة شرطة التحقيق إلى جهة اخرى (شرطة ود مدني).
IV. عند تقديم الأدلة للحصول على أمر تفتيش.
V. عند تقديم دليل الشرطة في المحكمة.

مع ملاحظة أن شكليات العرض تزداد كلما استمر التحقيق.

- **الإثبات / الدفاع:** حدث الإثبات / الدفاع أيضا عند تقديم القضية إلى المحكمة اذ يلزم تقديم الدليل ضد مرتكبي الفعل بما لا يدع مجالا للشك المعقول.

12.6 الخلاصة والمناقشة :

تم وصف نموذج مقترح للتحقيقات الجنائية في الجرائم الإليكترونية والحصول على الادلة الجنائية ومعالجتها .

تم ادراج تدفقات المعلومات في هذا النموذج ، وكذلك أنشطة التحقيق ، لجعلها أكثر شمولية من النماذج السابقة. إلاطار المقترح يوفر أساسا لتطوير التقنيات وخاصة الأدوات التي تدعم عمل المحققين. يجب اختبار قابلية التطبيق وإمكانية تطبيقه في السياقات والبيئات التنظيمية المختلفة. الشكر والتقديرلكل من اسهم في تقييم هذا النموذج من المحققين زوي الخبرة في التحقيق الجنائي.

VII. الخاتمة والتوصيات والعمل في المستقبل

خاتمة الدراسة :

الدافع للقيام بهذا البحث انه وخلال السنوات القليلة الماضية رأي العالم تطورا ملحوظا وزيادة في استخدام البينة الرقمية (Digital Evidence) ويرجع ذلك التطور بشكل مباشر الى أسباب متعددة ومتنوعة . واقوى هذه الاسباب هو تطور استخدام البينة الرقمية أمام المحاكم الجنائية والمدنية.
اصبحت المحاكم تقبل تقديم البينة الرقمية للفصل في القضايا المعروضة امامها وقد ادى ذلك بدوره الى تطور القوانين وتطور قدرتها على معالجة قضايا السايبر الحالية والمتوقعة. حتم التطور في ايتخدام البينة الرقمبة ايضا وابتداءا التعاون البناء بين اهل الفكر القانوني، ومحترفي الكمبيوتر، وتقانة المعلومات.

كل ما سبق لفت النظر لأهمية البينة الرقمية وتطور وسائل جمعها وتحليلها وتقديمها في المحاكم كما دفع للقيام بهذا البحث ليشمل تطبيق القانون في فضاء السايبر لبروز الحاجة لذلك لدى القطاعات المتعاملة مع تكنلوجيا السايبر (Cybertechnology) ، فضلا عن الجهد الدولي لمكافحة الجريمة الإليكترونية ذات الطبيعة العابرة للحدود والتي اجبرت العالم على التعاون لمكافحتها والوقوف في وجهها .

تحقيق اهداف الدراسة :

اولا الفرضيات:

شملت فرضيات الدراسة ستة فرضيات اتخذتها الدراسة موجها انبنت عليه مراحلها التي تأرجحت بين القانون والتكنلوجيا والعوامل الاجتماعية والاجتهادات الفردية والتعاون الدولي والممارسات البوليسية المتعلقة بالتحقيق:

اجمل البحث الفرضيات فيم يلي:

i الفرضية الولى: الجريمة الإليكترونية جريمة حديثة نسبيا وتتميز بانها عابرة لحدود الدول مما ادي لبروز عوامل مؤثرة على عملية كشفها والتحقيق فيها .
ii الفرضية الثانية: عدم وتوفر اطار تحقيق واحد متفق عليه يفتح مجال البحث عن اطارشامل للتحقيق في الجريمة الإليكترونية .
iii الفرضية الثالثة: الربط بين الفكر القانوني و التقني يخدم التحقيق في الجريمة الإليكترونية .
iv الفرضية الرابعة: دراسة الخصوصية في المجال القانوني وما طرأ عليها من تغيرات بسبب تكنلوجيا المعلومات واستعراض اثر التكنلوجيا على الخصوصية من حيث كمية المعلومات والسرعة في التداول وطريقة الحفظ ونوع التداول. كما ان الخصوصية في مجال السايبر (Cyberspace) اصبح امرها اكثر تعقيدا، لاسباب تتعلق بالتجدد المستمر لامكانية الاختراق وانواعه، اضافة لاسباب أخرى كثيرة، منها زيادة الاعتماد

في اكثر الامور خصوصية على التكنلوجيا اضافة الى دور الاخلاق.

iv الفرضية الخامسة: التطور التكنلوجي وتنامي مهددات النظم و امن المعلومات .

v الفرضية السادسة: مازال هناك جدل حول طبيعة الجريمة الاكترونية وطرق جمع البينات والتطور البرمجي والفني والجنائ ومتطلبات قبول البينة أمام المحاكم من الناحية الفنية والقانونية. كما توجد مجهودات مختلفة، لبعض الدول والمنظمات الدولية المهتمة بموضوع الجريمة الإليكترونية.

ثانيا اهداف الدراسة:

انحصرت اهداف البحث في اربعة محاور انجزت من خلال دراسة تكونت من قسمين وتسعة ابواب وتلخصت الاهداف في التالي:

1) تقديم اطار مقترح للتحقيق في جرائم الانترنت: وقد تم تقديم اطار شامل يمكن استخدامه والاستعانة به مع الكثير من تطبيقات الكمبيوتر والوسائل الفنية لاحراز البينة وتحليلها وتقديمها امام القضاء بصورة فاعلة .

2) هدف البحث لاستعراض و توفير المعلومة الاساسية عن وضع الجريمة الإليكترونية وطرق مكافحتها من الناحية الفنية المتعلقة بتكنلوجيا السايبر و القانون، والادوات المستخدمة في جمع البينات.

3) هدف البحث لاستعراض الدور المحتمل للفكر الانساني المتعلق بالقانون و الخصوصية والاخلاق والمعايير الاجتماعية والتعاون الدولي ضد الجريمة الإليكترونية.

4) اهتم البحث بايضاح الموقف العام لمسألة التحقيق والاثبات بصورة عامة تجاه الجريمة الإليكترونية من الجانب القانوني والتكنلوجي.

النتائج:

غطت الدراسة الجاتبين القانوني والتكنلوجي من خلال مناقشة واستعراض الاراء الفقهية في الجانب القانوني وفنيات التحقيق وحجية الدليل وقبوله امام المحاكم.

ايضا ناقش البحث الاستجابة التأريخة للجريمة الإليكترونية والدور الفني لاثبات الجريمة الإليكترونية.

لم تهمل الدراسة المبادئ المتعلقة بالخصوصية والاخلاق والمعايير الاجتماعية كمؤثرات محتملة عند مناقشة التكييف القانوني للجريمة الإليكترونية.

غطت الدراسة طبيعة الجريمة الإليكترونية العابرة للحدود وبروز التعاون الدولي لمكافحتها.

ناقش البحث ردات الفعل القانونية المتعلقة بتعريف الجريمة الإليكترونية وعناصرها واحراز الدليل وحفظه وتخزينه وتحليله ووضع فرضياته وتقديمها والدفاع عن هذه الفرضيات.

تم تطويراطار للتحقيق اتسم بالعمومية والشمول شهد على جدواه تقييم المشاركين من ذوي الخبرة من المحققين تمت مناقشة استجاباتهم في الفصل الخاص بتقديم الاطار واخضاعه للتقييم.

ثالثا معوقات الدراسة:

واجهت الدراسة بعض المعوقات التي جعلت العمل محاطا بالكثير من الصعوبات التي اطالت امد الدراسة وقعدت بالدراسة على ان لا تتعرض للكثير بالدراسة التي كان من الممكن ان تجعل العمل افضل فمنها ما تعلق بالظروف الخاصة ومنها ما نجم عن ظرف البلاد والاحداث التي سادت اثناء الدراسة الى جانب المعوقات العملية المتمثلة في:

i مشاكل جمع المعلومات.
ii شح المراجع المتوفرة بالمكتبات.
iii فقر المكتبة العربية وعدم توفر المعلومة عن العالم العربي والافريقي.
iv الجهات العدلية بالسودان لا تملك التجربة العلمية المتخصصة التي يمكن ان تفيد هذا البحث كثيرا. كما ان المجرم السبراني في السودان لا يهتم كثيرا باستخدام التكنلوجيا لارتكاب الجريمة وهذا يمكن ان يحسب للامن السبراني في السودان.

رابعا العمل في المستقبل والتوصيات:

النموذج المقترح يمكن استخدامه لتحديد الاحتياجات اللازمة لدعم التحقيقات، وعلى سبيل المثال الحوجة لأدوات تدعم تدفق المعلومات المحددة في النموذج. ينبغي دراسة تطبيق النموذج في أنواع مختلفة من التحقيق من أجل التحقق من صلاحيته وقابليته للتطبيق كإطار مرجعي عام. تشمل السياقات ذات الأهمية:

i. تحقيقات الشرطة (الجنائية) ؛
ii. المدققين؛

iii. التقاضي المدني ؛
iv. التحقيقات من قبل مسؤولي النظام ؛
v. الاستفسارات القضائية.

يجب تحديد خصائص أنواع التحقيق المختلفة ، مثل معايير الأدلة المعمول بها ، والتفاصيل المضافة لأنواع مختلفة من التحقيق. النموذج تم اقتراحه عبارة عن نموزج او اطار عام يمكن صقله وتوسيعه في سياقات معينة.

يلزم أيضا تحديد الجهات الفاعلة في التحقيقات وأدوارها بشكل أكثر وضوحا.

هناك حاجة إلى تطوير نموذج أكثر شمولا لكيفية معالجة هذا النوع من المعلومات لتحقيق أفضل ميزة مع الاستمرار في تلبية القيود المعقدة التي تفرضها اعتبارات مثل الخصوصية والاخلاق والمعايير الاجتماعية جنبا الى جنب حماية البيانات الحساسة وضمان قبول الدليل في مجلس القضاء وفقا للشروط القانونية لقبول البينة.

المراجع References

المراجع الانجليزية:

A. R. (2008). "Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective". 6th International Conference on E-Governance.

Acharya, M. P. (2013, November). The Adversarial v. Inquisitorial Models of Justice. KSL Journal, 1, 63-70. Retrieved on 11th November 2014 from http://ksl.edu.np/cpanel/pdf/adversial.pdf.

Adams, R. (2013). "'The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice" Murdoch University. M. University. Murdoch University, Murdoch University. Archived (PDF) from the original

Akin, T. (2011). Cybercrime: Response, investigation, and prosecution. Encyclopedia of Information Assurance (pp. 749-753). New York: Taylor and Francis.

Alghafli, K. A., Jones, A., & Martin, T. A. (2011).Guidelines for the digital forensic processing of smartphones. 9th Australian Digital Forensics Conference, SECAU Security Research Centre, Edith Cowan University, Perth, Western Australia.

Anderson, D. (2015, June 11). A Question of Trust - Report of the Investigatory Powers Review. Independent Reviewer of Terrorism Legislation. Retrieved on 11th June 2015 from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-reportof-the-investigatory-powers-review/ Anonymous (2015, June 20). Quantum computers - A little bit, better. The Economist. Retrieved on 21st June 2015 from http://www.economist.com/news/science-andtechnology/21654566-after-decades-languishing-laboratory-quantum-computers-areattracting. Apple (2015, April). iOS Security: iOS 8.3 or later.

iOS Security Guide White Paper. Retrieved on 3rd June 2015 from https://www.apple.com/business/docs/iOS_Security_Guide.pdf. Arms, W. Y. (2000). Digital Libraries. London: MIT Press.

APEC (2005). "{APEC, 2005 #112}." APEC. Retrieved 02/05/2017.2020 ،

APEC (2005). sixth ministrial meeting on telicommunication and information industry. APEC. WWW.asianlii.org, APEC

Architecture, O. C. F. (2017). "Open Computer Forensics Architecture." AVAILABLE AThttp://www,OpenComputerForensicsArchitecture.

Bace, F. S .R. (2003). A Guide to Forensic Testimony, AddisonWesley.

Bicchieri, C. (2006). The grammar of society: The nature and dynamics of social norms. , Cambridge University Press.

caine (2017). "caine forensics." AVAILABLE AT www.caine.net.RETRIEVED JUNE 2020

Carrier, B., Spafford, E .H and (2003). "Getting physical with the digital investigation process." International Journal of Digital Evidence.(.(2)2)،

Carrier, B. D. (2006). " "Basic Digital Forensic Investigation Concepts"." International Journal of Digital Evidence. 1.

Carrier., B. (2003). " Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers." International Journal of Digital Evidence Winter 2003.

Casey, E. (2009). Handbook of Digital Forensics and Investigation.

Chang, W. C., Wingyan; Chen, Hsinchun; Chou, Shihchieh. . (2003). An International Pere on Fighting Cybercrime. Lecture Notes in Computer Science.

Ciardhuáin, S. Ó. (2004). "An Extended Model of Cybercrime Investigations." International Journal of Digital Evidence Volume 3(Issue 1.(

COE (1981). "Treaty #108." COETreaty #108. Retrieved 07/06, 2020.

COE (2001). "Council of Europe Cybercrime Convention TREATY 185 " COE TREATY 185. Retrieved 02/03/2018, 2018.

COE (2001). "Treaty 189 ACTS OF RACISIT AND XENOPHOPIC NATURE COMMITED THROUGH COMPUTER SYSTEMS." COE. Retrieved 07/06, 2020.

commonwealth (2013). "commonwealth cybercrime initiatives." AVAILABLE AT https://www,cybersecurityintelegence.com. Retrieved june7, 2020.

Constitution, S الجريدة الرسمية. (2005). "دستور السودان." .

David Icove, K. S. W. V. (1995). Computer Crime,A Crimefighter's Handbook. Online Available at http://oreilly.com/catalog/crime/chapter/cri_02.html, O'Reilly & Associates.

David Icove, K. S. W. V. (2001). Computer Crime,A Crimefighter's Handbook. O. R. Associates. AVAILABLE ATttp://oreilly.com/catalog/crime/chapter/cri_02.html, RETRIEVED MAY 2020O'Reilly & Associates.

Detective, O. F. (2017). "Oxygen Forensic Detective".

DictHer, T. A. H. (2000). Houghton Mifflin Company.

EUR-LEX (1997). "Directive 97/66/EC." https://eur-lex.europa.eu. Retrieved 2/2, 2019.

Europol, W. (2020). Europol. wikipedia. http://en.wikipedia.org/wiki/Europol wikipedia

Extractor, B. (2017). "Bulk Extractor." http://www.BulkExtractor.RETRIEVED JUNE2020

Fatah, A., Higgins, Kathleen M. (1999). Forensic Laboratories: Handbook DIANE Publishing.

Fortinet, G. L. (2009). Fighting Cybercrime: Technical, Juridical and Ethical Challenges. VIRUS BULLETIN CONFERENCE.

framework, d. f. (2017). "digital forensic framework." AVAILABLE AT www.digitalforensicframework.RETRIEVED MAY2020

Gavison, R" .(1984) .Privacy and the Limits of the Law." The Yale Law Journal.

GROUP, C. L. (2020). "the-evolution-of-cybercrime-from-past-to-the-present/." Retrieved Jan.2020, 2020.

Halder D, J. K. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA, IGI Global.

Harrison, W., Heuston, G., Morrissey, M., Aucsmith, D. Mocas, S. & Russelle, S.)..: [] (2002) A Lessons Learned Repository for Computer Forensics. International Journal of Digital Evidence, Vol. 1 No. 3. Online ،

Hauck, R. V. (2002). " Using Coplink to analyze criminal-justice data." IEEE Computer Vol. 35 (No. 3): pp. 30-37.

Hawthorne, E. (2014). " Teaching digital forensics and cyber investigations online: Our experiences." European Scientific Journal

Hayes, E. (20013). "cyber crime." Networked Systems Survivability (NSS) Retrieved Jan 12, 2017.

Heiser, W. G. K. I. a. J. G. (2001). Computer Forensics: Incident Response Essentials. Boston, Addison Wesley.

Howard, T. (2004). "Don't Cache Out Your Case: Prosecuting Child Pornography." Berkeley Technology Law Journal Vol. 19, No. 4(Vol. 19, No. 4 (Fall 2004), pp. 1227-1273).

Hrtage, A. (1969). The american Hrtage Dictionary of the English Language. The american Hrtage Dictionary of the English Language. Boston Houghton Mifflin.

http (2020). "What is the G8?'." G8 Information Centre. 2020.

http (2020). "world internet users statisices." world internet users statisices. Retrieved June,7, 2020.

http (2008). "Convention on Cybercrime, ETS No. 1 ".85Retrieved 25 October,2008, 2008.

ICANN (2020). "Internet Corporation for Assigned Names and Number " ICANN. Retrieved 27 MAY, 2020.

Interpol (2007). Interpol in Appeal to find Paedophile Suspect. The New York Times. AVAILABLE AT www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin,.RETRIEVED MAY2016

Investigation-TWG, T. W. G. f. E. C. S. (2001). A Guide for First Responders. Electronic Crime Scene Investigation.

Iovation (2020). "what-is-cybercrime-definition-and-example." topics. 2020.

ITU (2009). Understanding Cybercrime A Guide for Developing Countries.

J Khakurel, H. M., J Porras (2016). " Information Technology& People." Journal of Network Security & Its.(2016)_

Jaishankar, D. H. K. (2011). cybercrime pakt.

Jang, J. (2018). "BEST PRACTICES IN CYBERCRIME INVESTIGATION IN THE REPUBLIC OF KOREA".

Jang, Y. (2013). "BEST PRACTICES IN CYBERCRIME INVESTIGATION

IN THE REPUBLIC OF KOREA." 140TH INTERNATIONAL TRAINING COURSE RESOURCE MATERIAL SERIES No.79AVAILABLE

AT(https://www.unafei.or.jp/publications/pdf/RS_No79/No79_09VE_Jang2.pdf).RETRIEVED MAY2020

Johansen, G. (2020). Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, Packt.

Jones, R. R. f. (2007). "Safer Live Forensic Acquisition." available at http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf retrieved june2017

Kanellis, P. (2006). Digital crime and forensic science in cyberspace.

Kaspersky Lab (2015, February 16). Carbanak APT: The Great Bank Robbery. Securelist.

Retrieved on 26th February 2015, from

https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

Katz v United States, 839 US 347 (1967).

Kaye, B. H. (1995). Science and the Detective – Selected Reading in Forensic Science. New

York: VCH Verlagsgesellschaft.

Kelly J. F., & Wearne, P. K. (1998). Tainting Evidence: Inside the Scandals at the FBI Crime

Lab. Sydney: The Free Press.

Kerr, O. (2005). "Searches and Seizures in a Digital World." 119 Harvard Law Review 119 Harvard Law Review(4 Apr 2005).

kit, s ".طقم الاسنان" .(2017) available at http://www.sleuthkit.org.retrieved

may2020

Lee, H. C., Palmbach, T. M., & Miller, M. T. .. . (2001). Henry Lee's Crime Scene Handbook, San Diego :Academic Press.

Library., A. G. (2017). "Identify & Refine your Topic." Basic Research Methods Retrieved jan,23, 2020.

Maravic &Bosnjak, S. (2014)). cybercrime and Digital Forensic- Technologies and Approaches.

Mark Reith, C. C., and Gregg Gunsch" .(2002) An Examination of Digital Forensics Models." International Journal of Digital Evidence(Fall 2002).

Miller, C. (2012). Evidence:Best Evidence Rule, CALI eLangdell®Press.

Mohay, G. M., Ed. (2003). Computer and intrusion forensics. Artechhouse ،Artechhouse..

Moore, R. (2005). Cyber crime: Investigating High-Technology Computer Crime, Anderson Publishing.

Morgan, S. (2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019." Retrieved Retrieved 22 September 2016.

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C.. . .).; (2008). Guide to Computer Forensics and Investigations. Course Technology, Cengage Learning, Boston, MA.

Ó Ciardhuáin, S. G., P. (eds.) . (2002). Guide to Best Practice in the area of Internet crime Investigation. Dublin, Ireland.:

OECD " منظمة التعاون الاقتصادي" .(1983) available at HTTP://WWW.OCED.ORG. Retrieved 03/05, 2020.

Palmer, G. (2002). " "Forensic analysis in the digital world"." International Journal of Digital Evidence(I Scientist;).

Patel, A. Ó. C ،.S. (2000). "The impact of forensic computing on telecommunications." IEEE Communications Vol. 38 (No. 11): pp. 64-67.

Posner, E. (2009). Law and social norms. books.google.com. USA. books.google.com.

Punja, S. (2008). "Mobile device analysis." Small Scale Digital Device Forensics Journal. vol. 4(no 1).

Reed, C. (2004). Internet Law: Texts and Materials. Cambridge, Cambridge University Press.

Reith, M., Carr, C. & Gunsch, G (2002). "An Examination of Digital Forensic Models." International Journal of Digital Evidence Vol. 1(No. 3).

Rob van den Hoven van Genderen, , (2008). Cybercrime investigation and the protection of personal data and privacy. Online Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-,.

Rogers, M. R. f. (2006). "Computer Forensics Field Triage Process Model." ProductsAndServices/index. 2018.

Rynearson, J. (2002). "Evidence and Crime Scene Reconstruction." National Crime Investigation and Training(6 edition).

Saferstein, R. (200 .(0Criminalistics: An Introduction to Forensic Science, Pearson.

Sammons, J. (2012). The basics of digital forensics: the primer for getting started in digital forensics.

Shinder, D. (2010). "what-makes-cybercrime-laws-so-difficult-to-enforce/." IT Security. Retrieved January 26, 2015.

Spinello, R. (2010). Morality and Law in Cyberspace, Jones & Bartlett Learning.

Svedman, K. (2020). "A Simplified Guide To Digital Evidence." Retrieved feb. 28th, 2020.

Tracy Cross, D. A. (2009). Morality, Ethics, and Gifted Minds. USA, Springer, Boston, MA.

TWG (2001). A Guide for First Responders. Electronic Crime Scene Investigation. T. W. G. f. E. C. S. Investigation.

UN (1990). Resol.121/45. 121/45. UN. UN, UN. 121/45.

UN (2000). Combating the Criminal Misuse of Information Technologies. GA Resolutions 55/63 () and 56/121.

UN (2003). Resol. 63/55. 63/55. UN. BANCOCK, UN. 63/55.

UN (2013). Comprehensive Study on Cybercrime. UNITED NATIONS OFFICE ON DRUGS AND CRIME Vienna UNITED NATIONS OFFICE ON DRUGS AND CRIME.

UNODC (2013). Comprehensive Study on Cybercrime February2013. U. N. O. O. D. A. CRIME. Vienna

Venema, D. F. W. (1999). Forensic Discovery book, ADDISON& wesley professional computing series.

Volonino, L. (2008). Computer forensics for dummies.

Warren G. Kruse, J. G. H. (2002). Computer forensics: incident response essentials, Addison-Wesley: p. 392.

ways, x. (2017). "x ways forensics." www.xways.forensic.org.

webster, m. (2020). " dictionary." 2020.

Wilding, E. ((1997)). Computer Evidence :a Forensic Investigations Handbook, London: Sweet & Maxwell.

Yang TY, D. A., Choo KK, Muda Z. (2016). "Windows Instant Messaging App Forensics: Facebook and Skype." journal.pone.0150300 doi:10.1371./

Zoltanszabodfw (2012) Digital Forensics is not just HOW but WHY. digital-forensics-is-not-just-how-but-why /

الركابي، ر. (2009). الأخلاق الليبرالية، موقع واي باك مشين. موقع واي باك مشين.

العنزي، ف. م. م. ا. A., FATMAH MUSLEF ؛ العصيمي، شاكر بن مقبل . مشرف (2019). التدابير الوقائية لمواجهة جرائم المرأة في المجتمع السعودي. رسالة ماجستير. ك. ا. ا. ق. أ. ا. ت. ا. و. الجنائي. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية.

المبيضين، إ. (2019) 4.54 مليار مستخدم للإنترنت حول العالم. alghad

حجاج، و. م. (2006). شرح قانون العقوبات القسم العام. كلية الحقوق جامعة أسيوط كلية الحقوق جامعة أسيوط

عثمان، ع. م. (2013). cyber norms and ethics. .sudan university for science and Tech

.sudan university for science and Tech .

عثمان، ع. م. (2013). اخلاق واعراف السايبر Sudan University for Science and Technology. S. U. f. s. &Technology. Sudan Un. for science &Technology .Sudan Un. for science &Technology. Lecture notes

مصري، ع. ع. ع. (2005). الجريمة الالكترونية، دار العلوم للنشر و التوزيع.

قـــائـــمـــة الـــنـــشـــر و الـمـقـا بـــلات

الاوراق المنشورة باللغة الانجليزية :

المجلات المحكمة :

i. Guidance to Africa and Sudan Cybercrime Forensic Investigation Framework.

مكان النشر:

جامعة دنقلا

المجلة العلمية

مجلة محكمة تصدر من ادارة المجلة نصف سنوية

(ملحق1)

Digital Evidence and Best Evidence Rule

مكان النشر:

جامعة السودان للعلوم و التكنلوجيا

المجلة العلمية (الهندسة و الكمبيوتر)

مجلة محكمة تصدر من ادارة المجلة (اون لاين)

(ملحق2)

الاوراق المنشورة باللغة العربية :

المؤتمرات:

جمع وتوثيق وتحليل الأدلة الجنائية الرقمية بطرق اكثر فاعلية

مكان النشر :

المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية

الرياض ، الرياض 10 - 12 نوفمبر، 2015

جامعة الامام محمد

(ملحق3)

المقابلات:

- **اسئلة المقابلات**
- هل شعرت أن نموذج التحقيقات يمثل بشكل مناسب هيكل التحقيقات في مؤسستك؟
- هل تعتقد أن هناك عناصرلم يتضمنها اطار التحقيق من عناصر التحقيق الهامة والضرورية لانجاح التحقيق ؟
- هل التراجع او المراجعة المتأصلة في النموذج أمر مهم، لأن التحقيقات الحقيقية لا تسير بطريقة خطية بسيطة؟
- ✓ استجاب المشاركون في التقييم لطلب اتقييم الاطار باختيار من1-5 في صالح الاطار بالاجماع.

اهم مخرجات الاجابات

النموزج على درجة عالية من الدقة ويتفوق على هيكل التحقيقات في المؤسسة ويصلح اطارا للتحقيق في كل القضايا.

استبعاد فكرة الخطوة التي حملت ما هو فرعي فكرة جيدة وتجنب تضمين فكرة النقل التي عرضت كمقترح لتعديل الاطار بشكل ثانوي في رائي المشاركين يؤدي لتشتيت تركيز، مسؤولي الأنظمة الذين يجب عليهم صيانة ومراقبة نظام كشف التسلل من أجل أن يكونوا على دراية بالأحداث التي تتطلب التحقيق.

هناك حاجة إلى التركيز على السيطرة على تدفق المعلومات في بيئة إنفاذ القانون.

الخاضعين لاسئلة المقابلات بلغ عددهم 35 محققا ومختصا في جمع الادلة الالكترونية تراوحت خبراتهم بين 5-12 سنة.