دولة ليبيا

مكتب النائب العام

قسم ضبط شؤون المعلوماتية والاتصالات

الموضـــوع:

(مقترح استحداث وحدة الطب الشرعي الرقمي).

السيد// رئيس قسم ضبط شؤون المعلوماتية والاتصالات.

عن طريق السيد// أمين سر قسم ضبط شؤون المعلوماتية والاتصالات.

بعد التحية،،،

بالإشارة... للمقترح المقدم من قبلنا بشأن توفير أدوات الطب الشرعي الرقمي وبعد الاطلاع على تأشيرة السيـــد الأستـــاذ المستشـــار النـــائب العـــام باعتماد رأي السيد رئيس القسم وسرعة التنفيذ الذي نص على (*التواصل مع الشركات المصنعة لطلب عروض الطب الشرعي الرقمي والأدلـــة الرقمية والذكاء الاصطناعي*)،

وفي... إطار تطوير العمل بوحدة التفريغ الالكتروني بشكل خاص وبالقسم بشكل عام وذلك باستخدام وسائل تقنية المعلومات للطب الشرعي الرقمي وخوارزميات الذكاء الاصطناعي.

عليه... نحيل لسيادتكم مقترح استحداث وحدة الطب الشرعي الرقمي وفق المعايير القياسية المتعارف عليها دوليا مع تصور عام لاستخدامات الذكاء الاصطناعي في مجال التحقيقات الجنائية الرقمية.

مهندس مقـــدم //

حســـام الدين مصطفي ابوشحمة

وحدة التفريغ الرقمي

بقسم ضبط شؤون المعلوماتية والاتصالات

دولة ليبيا

مكتب النائب العام

قسم ضبط شؤون المعلوماتية والاتصالات

السيد\ مشرف قسم ضبط شؤون المعلوماتية والاتصالات

بعد التحية،،،

نظـــراً للتطور السريع في مجال صناعة الهواتف الذكية وسعي الشركات المصنعة لحماية بيانات المستخدمين من الاختراق وذلك باعتمادها علي تقنيات حديثة متل بصمات الأصابع والوجهة وغيرها من وسائل الأمان مما ترتب عنه صعوبة كبيرة في استخراج البيانات والوصول الى الدليل الرقمي بالطرق الفنية والتقليدية المتعارف عليها من قبل جهات إنفاذ القانون علي مستوي العالم الأمر الذي أدي الي تطور موازي لعلوم الطب الشرعي الرقمي في صناعة أجهزة استخراج وتحليل الدليل الرقمي بشكل مقبول أمام المحاكم الدولية والتي تعمل علي تخطي كلمات المرور بجميع أنواعها واسترجاع ما تم حذفه من قبل المستخدم من بيانات قد تحتوي في الأغلب علي معلومات تفيد التحقيقات الجاري بالإضافة الي إعداد التقارير الفنية بشكل مفصل وفق الضوابط والمعايير المتعارف عليها دوليا.

عليـــــــه

أحيـــل أليكم قائمة بأهم الأجهزة المعنية بالتحقيقات الجنائية الرقمية المتعارف عليها دولياً أملاً منكم العمل علي توفيرها كي يتسني لنا أنجاز مهام وحدة التفريغ الرقمي بالقسم علي الوجهة المطلوب.

مهندس مقـــدم //

حسام الدين مصطفي ابوشحمة

وحدة التفريغ الرقمي

بقسم ضبط شؤون المعلوماتية والاتصالات

بمكتب النائب العام

دولة ليبيا

مكتب النائب العام

قسم ضبط شؤون المعلوماتية والاتصالات

مقترح استحداث وحدة الطب الشرعي الرقمي بقسم ضبط شؤون المعلوماتية والاتصالات بمكتب النائب العـــام

إعـــداد

مهندس مقـدم // حسـام الدين مصطفي ابوشحمة

ماجستير الطب الشرعي الرقمي تخصص إدارة المختبرات الجنائية الرقمية

جامعة هادرزفيلد المملكة المتحدة

إعداد: (12)

(المقـــدمة)

في العصر الحالي باتت الجريمة التقليدية لا تخلو من دليل رقمي وغالبا ما يكون معززا للقرارات المتخذة من الجهات القضائية. وبمعنى أبسط وأوضح فإنه لا يخلو أي مسرح جريمة من دليل رقمي مهما كانت نوعية الجريمة وتداعياتها. والسبب في ذلك يعود إلى الاستخدام الهائل لتقنية المعلومات في كل أنماط الحياة، وفي جميع الأدوات والمكونات التي يستخدمها البشر.

فالتقنية الآن موجودة في المحفظة الخاصة بالأشخاص والهاتف الخلوي والشبكات المتنوعة للشركات المزودة لخدمات الاتصالات والانترنت، كذلك يمكن إيجادها في الملحقات الأخرى مثل الساعات الرقمية الذكية والطائرات بدون طيار وأنظمة الملاحة الالكترونية للمركبات الحديثة. وتزامنا مع هذا التواجد الضخم للتقنية نجد أن المحرك الرئيسي لها وهو الإنترنت وشبكات الاتصالات المختلفة والتي أصبحت منتشرة في كل مكان وبسرعات عالية، مما أدى إلى التواصل المستمر في نقل البيانات.

جميع هذه العوامل أبرزت دور الأدلة الرقمية وعلوم الطب الشرعي الرقمي بالإضافة لخوارزميات الذكاء الاصطناعي في مكافحة جميع أشكال الأنشطة الإجرامية، مما يقتضي تعاملا خاصا مع هذه النوعية من الأدلة، ويتطلب إجراءات قياسية متبعة لتنظيم آلية التعامل معها، وكيفية التحقق منها، وإبرازها بشكل صحيح (فني وقانوني) للجهات القضائية.

أهـــداف المقـــترح ...

المختبر الجنائي الرقمي.

استحداث مختبر جنائي رقمي يعتمد على تقنيات الطب الشرعي الرقمي المتعارف عليها دولياً في التعامل مع الجرائم الالكترونية بشكل فني وقانوني مقبول أمام المحاكم المحلية والدولية.

الإجراءات القياسية في المختبرات الخاصة بالتحقيقات الجنائية الرقمية.

التقيد بالإجراءات القياسية والمعايير الدولية في التعامل مع الدليل الرقمي من بداية التحريز من مسرح الجريمة ونقل الي المختبر والتخزين واستخراج الدليل الرقمي وإعداد تقارير الخبرة بشكل فني وفق الضوابط المعمول بها عالمياً.

الرفع من كفاءة الكادر الفني في البحث والاستدلال الرقمي.

تدريب الكادر الفني علي فهم وسائل الطب الشرعي الرقمي في مكافحة جرائم تقنية المعلومات والأساليب الإجرامية التي تستخدم في ارتكابها، والأسس الفنية والقانونية في التحقيقات الجنائية الرقمية، وكذلك الأسس والمناهج الفنية لمختلف جوانب التحقيق الرقمي باستخدام تقنيات الذكاء الاصطناعي في الوصول الي الدليل الرقمي بالطرق الفنية والقانونية المتعارف عليها دولياً.

دمج تقنيات الذكاء الاصطناعي بوسائل الطب الشرعي الرقمي.

توفر خوارزميات وتقنيات الذكاء الاصطناعي مجموعة من الفوائد الهامة مثل تقليل الوقت وتجنب الخطاء البشري عند البحث والاستدلال الرقمي، مما يعزز القرار الأمني ويرفع كفاءة وفعالية التحقيقات الرقمية ويساعد المؤسسات المعنية بإنفاذ القانون على التخفيف بشكل استباقي من المخاطر الأمنية القائمة على الاستخدام الغير مشروع لوسائل تقنية المعلومات.

الإجراءات القياسية في المختبرات الخاصة بالتحقيقات الجنائية الرقمية

الإجراءات القياسية والمعايير الفنية المتعارف عليها دوليا هي الخطوات والقيود والدليل لتسلسل العمل داخل أي مؤسسة مهما كانت طبيعة عملها. وفي المعامل الجنائية بشكل عام تخضع هذه الضوابط الفنية الي الكثير من التدقيق والمعايرة. وتزداد الدقة في تطبيق أعلي مستوي في المعامل الجنائية الرقمية وذلك لحساسية التعامل مع الدليل الرقمي ويعود ذلك لطبيعة الأدلة الرقمية، حيث إنها عبارة عن بيانات رقمية ذات خصائص مختلفة كلياً عن الأدلة التقليدية مما قد يؤدي الخطاء في تطبيق المعاير والضوابط الفنية الي تلف الدليل الرقمي فتصبح تقارير الخبرة هي والعدم سواء.

وتعد هذه الإجراءات من أهم المكونات التي تضمن العمل بشكل صحيح خارج وداخل المختبر الرقمي، ولا سيما أن المخارج دائماً ما تكون مرتبطة بجهة قضائية قد تعتد بالدليل المعطى أو تقوم بإقصائه إذا ما كان هناك خلل واضح في أحد الإجراءات المتبعة في التحقيق الجنائي الرقمي. وفي عصر تكنولوجيا المعلومات فإن الأدلة الرقمية تعتمد وبشكل مباشر على الإجراءات القياسية لتحقيق المصداقية.

وفي هذا المقترح سوف يتم التركيز علي المعايير والضوابط الفنية والقانونية التي يتم الاعتماد عليها دولياً من قبل المنظمات الدولية المعنية بوضع مثل هذا النوع من الإجراءات القياسية ومن أهمها:

1. (مكتب الأمم المتحدة المعني بالمخدرات والجريمة) (UNODC). الجوانب العملية للتحقيقات في الجرائم الالكترونية والطب الشرعي الرقمي
2. مجلس رؤساء الشرطة الوطنية في المملكة المتحدة (NPCC) .الضوابط الفنية للدليل الرقمي والطب الشرعي الرقمي
3. منظمة الإنتربول- مجمع الإنتربول العالمي للابتكار (INTERPOL General Secretariat).المبادئ التوجيهية العالمية للطب الشرعي الرقمي مختبرات الرقمية

4. (مكتب الأمم المتحدة المعني بالمخدرات والجريمة)(UNODC).المعايير وأفضل الممارسات الفضلى للاستدلال الجنائي الرقمي
5. منظمة الإنتربول- مجمع الإنتربول العالمي للابتكار (INTERPOL General Secretariat).إرشادات للمستجيبين الأوائل للطب الشرعي الرقمي (أفضل الممارسات للبحث ومصادرة الأدلة الإلكترونية والرقمية).
6. المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية الدولية (IES).

- المبادئ التوجيهية لتحديد الأدلة الرقمية وجمعها والحصول عليها والحفاظ عليها (ISO/IEC 27037:2012) تم التأكيد (2018) دون تغيير.
- يقدم معيار ISO/IEC 27041 إرشادات حول جوانب الضمان في الطب الشرعي الرقمي ، على سبيل المثال ضمان استخدام الأساليب والأدوات المناسبة بشكل صحيح.
- يغطي المعيار ISO/IEC 27042 ما يحدث بعد جمع الأدلة الرقمية، أي تحليلها وتفسيرها.
- تغطي المواصفة القياسية ISO/IEC 27043 أنشطة التحقيق في الحوادث الأوسع، والتي يتم من خلالها عادةً إجراء الطب الشرعي.
- تتعلق المواصفة القياسية ISO/IEC 27050 (المكونة من 4 أجزاء) بالاكتشاف الإلكتروني وهو ما تغطيه المعايير الأخرى إلى حد كبير.
- المعيار البريطاني BS 10008:2008 -الوزن الإثباتي والمقبولية القانونية للمعلومات الإلكترونية. تخصيص- قد تكون أيضًا ذات أهمية. تم التعميم كمعيار عالمي.

اختصاصات مختبر الطب الشرعي الرقمي حسب ما جاء في المبادئ التوجيهية العالمية للطب الشرعي الرقمي مختبرات الرقمية الصادر عن المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية الدولية (IES) لسنة 2022م والتي تم اعتمادها وتعميمها دولياً عن طريق مجمع الإنتربول العالمي للابتكار (INTERPOL General Secretariat) - منظمة الإنتربول

جرائم وسائط التخزين الالكترونية المختلفة (Storage media)

- الكمبيوتر المكتبي والمحمول (Personal Computers – Laptops)
- الهواتف الذكية التي تعمل بأنظمة التشغيل المختلفة (IOS-ANDROID-WINDOWS)
- بطاقة الاتصالات الخلوية (SIM)
- بطاقات الذاكرة المختلفة (Memory Cards)
- الكاميرات الرقمية المختلفة (IP,concealed , Digital, Cameras & CCTV)
- أجهزة أنظمة الملاحة للمركبات الحديثة والسفن (GPS navigation systems)
- أنظمة التصوير الذكي (Dash Cameras)
- الساعات الذكية والتلفزيون ذكي (Smartwatches- Smart TV)
- محركات الأقراص المحمولة والثابتة والضوئية (Flash Drives-Discs CD & DVD HDD & SSD)
- الطائرات بدون طيار (Drones)

جرائم الشبكات وخوادم تخزين البيانات (Networks & Servers)

- الشبكات وخوادم أنظمة الاتصالات الخلوية والشركات المزودة لخدمات الاتصالات والانترنت (GSM)
- الشبكات وخوادم المنظومات السيادية والمصرفية والاستضافة للمواقع.
- الشبكات وخوادم الانترنت العام (المتاح للعام والذي لا يشكل إلا (10٪) من الشبكة الحقيقية للأنترنت.
- شبكات وخوادم الانترنت المظلم والعميق (Deep web & Dark Web) ويحتوي علي أكثر من 90٪ من إجمالي الشبكة الحقيقية للأنترنت.
- أجهزة الأصول الافتراضية والعملات الرقمية المشفرة (Virtual assets devices)
- أجهزة إنترنت الأشياء والذكاء الاصطناعي (IoT devices & AI)
- الشبكات وخوادم البيانات السحابية والتي يتم تخزين البيانات في خوادم متصلة بشبكة الانترنت.

الجرائم المرتبطة بوسائل الميديا المختلفة (Media)

- وسائل التواصل الاجتماعي علي شبكة الانترنت (Social Media)
- وسائل الاستدلال الرقمي من المصادر المفتوحة (OSINT)
- بصمة الصـوت الرقمية (Voice Inspector)
- مقارنة الصور وتحليلها (analysis Image comparison)
- مقاطع الفيديو المفبركة (Fabricated videos)
- الذكاء الاصطناعي المضلل (Shaded AI)
- أنظمة الذكاء الاصطناعي (AI Systems)

وهنا يجب علينا سرد الإجراءات القياسية للتعامل مع الأدلة الجنائية الرقمية ويجب أن نوضح الضوابط الفنية والقانونية العامة في التعامل مع المراحل الخمسة الأساسية في التعامل مع الأدلة الرقمية بشكل خاص والمبرزة الإلكترونية بشكل عام.

الضوابط الفنية لتحريز المبرزات من مسرح الجريمة ونقلها الي المختبر الجنائي الرقمي

الضوابط الفنية لاستلام المبرزات داخل المختبر الرقمي وتخزينها بشكل فني صحيح

الضوابط الفنية لستخراج البيانات من المبرزات باستخدام أجهزة الطب الشرعي الرقمي

الضوابط الفنية لتحليل البيانات وفك تشفيرها واسترجاع المحذوف منها واستخراج الدليل الرقمي

الضوابط الفنية لإعداد تقارير الخبرة بشكل فني وبصبغة قانونية مقبولة بالمحكمة

أولا التحريز والنقل. :(Seizure)

من خصائص الأدلة الرقمية أنها من الممكن أن تتلاشى نتيجة أي خطاء فني أو بشري اثنا مراحل التحريز، وفي بعض الحالات لا يمكن نقل المبرزة من مسرح الجريمة حيث لا يمكن فصل التيار الكهربائي عليها نتيجة اتصالها بشبكات ومنظومات وخوادم لا يمكن تعطيلها لنقل المبرزات الي المختبر الرقمي واستخراج البيانات مما يستوجب نقل أجهزة الطب الشرعي الي مسرح الجريمة لأخذ نسخة طبق الأصل من البيانات (IMEG) ونقلها الي المختبر باستخدام حقائب مخصصه تسمى (Faraday bags).

ثانيا الاستلام والتخزين. :(Receiving and storage)

اعتمادا على الضوابط والمعايير الفنية المتعارف عليها في مرحلة الاستلام المبرزات في المختبر الرقمي يتوجب استخدام نظام رقمي متكامل يوثق فيه الكترونياً جميع المراحل منذ لحظة دخول المبرزة الي المختبر الرقمي الي حين استخراج الدليل الرقمي في تقرير الخبرة واحالته للجهات القضائية والهدف من أرشفة القضايا وما تحتويه من بيانات هو أمكانية ربطها بمنظومات الذكاء الاصطناعي التابعة للطب الشرعي الرقمي والتي يمكنها تحليل الدليل الرقمي لقواعد البيانات المخزنة واستنباط العلاقات المتشعبة بين القضايا المخزنة مسبقاً والقضايا قيد التحقيق.

ثالثاً استخراج البيانات. :(Acquisition)

عملية استخراج البيانات الرقمية ليست مجرد اجراء نسخ للملفات او المحتويات الى اجهزة اخرى ولكن يتم انشاء دليل جديد او قرص صلب جديد مطابق للأصل يتم التعامل معه وكأنه هو الدليل الاصلي حيث ان النسخة الجديدة متطابقة تماما مع الاصل ويتم التأكد من محتوياتها بحساب القيمة الهامشية (Hash Value) للأصل والنسخة للتأكد من عدم وجود بت (Bit) واحد اضافي.

رابعاً تحليل البيانات. :(Analysis)

وفي هذه المرحلة يتم فحص الملفات المستخلصة من الأجهزة، وإيجاد الأدلة التي لها ارتباط بالقضية والأدلة المساعدة في اتخاذ القرار من قبل السلطات القضائية. ويتم الفحص من خلال برامج متطورة ومعتمدة في المحاكم الدولية كبرامج موثوقة لفحص الأدلة الجنائية الرقمية مثل برنامج (Encase و FTK و XRY و Cellebrite) لفحص مكونات الأجهزة المحمولة.

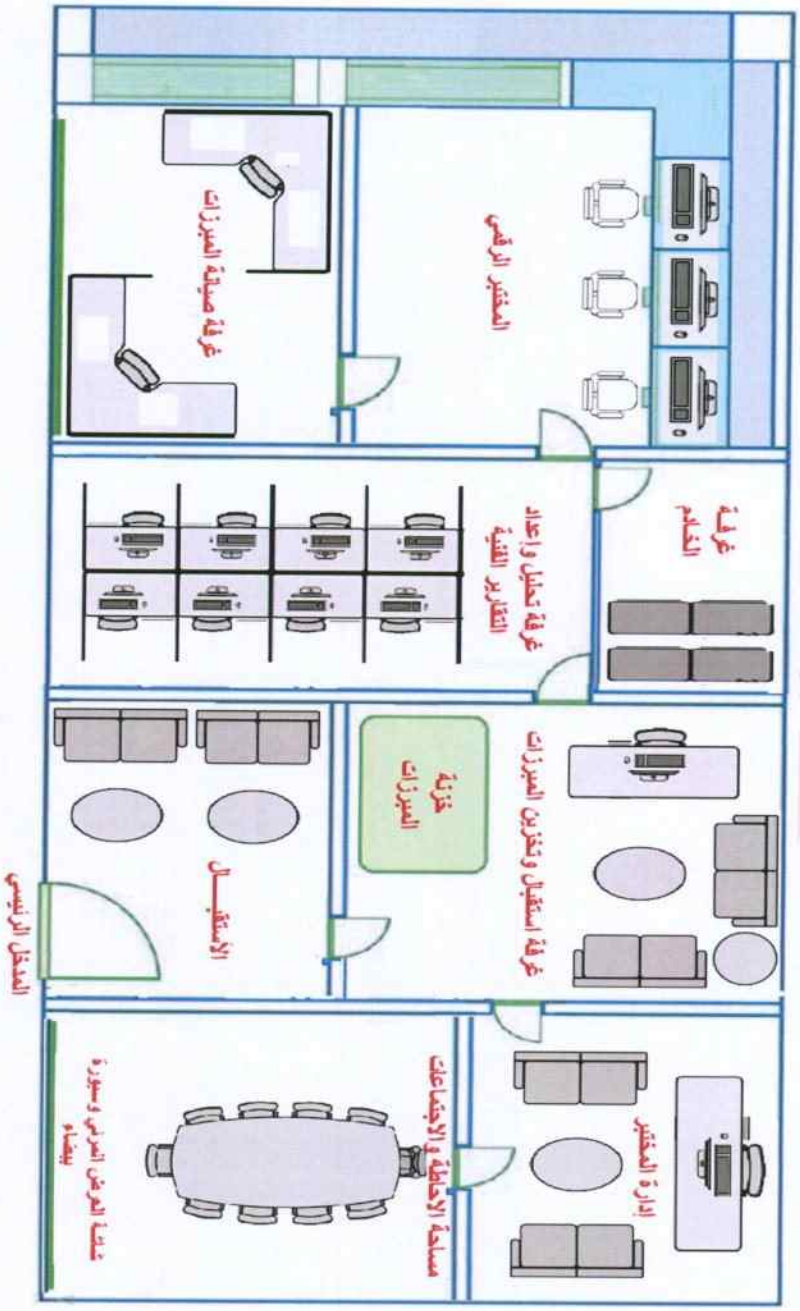
خامساً إعداد تقارير الخبرة. :(Reporting)

وهي المرحلة النهائية التي يتم من خلالها إعداد تقرير تفصيلي سهل القراءة والفهم بشكل فني وصبغة قانونية يحتوي على الأدلة الجنائية الرقمية التي تم إيجادها مدعمة بشرح توضيحي لأهميتها في القضية وعلاقتها بتحديد ملابسات الجريمة.

أهم المحاور الأساسية للتدريب في مجال التحقيق الجنائي الرقمي والطب الشرعي الرقمي المقرونة بالذكاء الاصطناعي وفق الضوابط والمعايير القياسية المتعارف عليها دولياً...

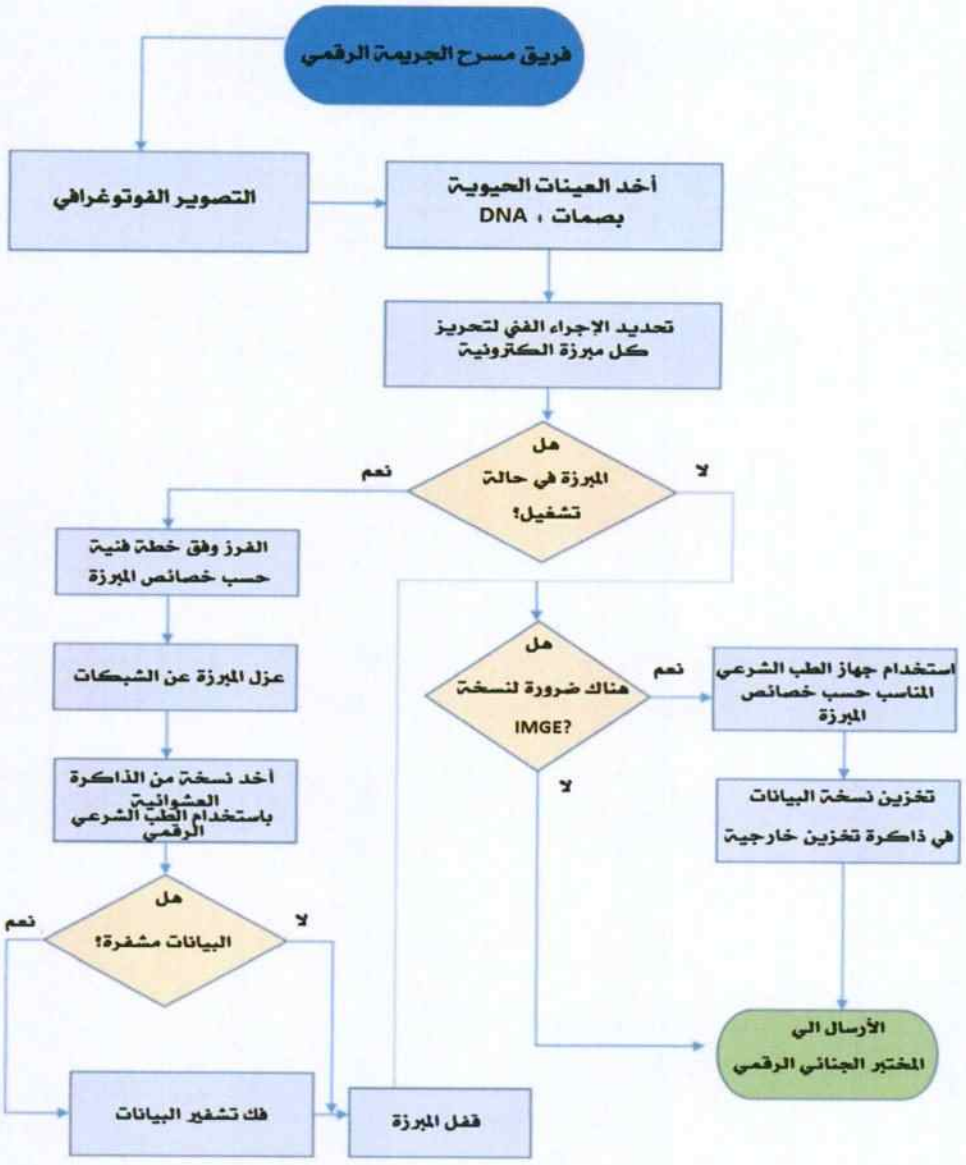
- التدريب علي استيعاب الجرائم السيبرانية بشكل عام والإلمام بكافة المعلومات التي تهيئ الكادر الفني علي التعامل مع مختلف أنواع الجرائم الالكترونية.
- تمكين المتدرب من العمل مع الفريق الأمني للاستجابة الأولى في التحقيق الجنائي الرقمي، لأن العمل الجنائي الرقمي يعتمد على طاقة الفريق من كافة التخصصات والمرجعيات.
- الإلمام بعملية تجميع وتحليل الدليل الرقمي باستخدام خوارزميات الذكاء الاصطناعي للطب الشرعي الرقمي، للتمكن من تقديم نتاج البحث بأفضل صورة.
- القدرة على فهم وكتابة التقرير الجنائي الرقمي، للتمكن من تقديم النتائج بشكل مكتوب ومرتب امام المحكمة وأجهزة القضاء المحلية والدولية.
- معرفة المسائل التقنية المرتبطة بالمرافعة في المحكمة، حيث ان البحث والتحقيق مرتبطتان ارتباطا وشيكا مع القضاء والقانون في الجوانب الفنية.
- التمييز بين الجرائم السيبرانية والأمن السيبراني كعامل أساسي.
- تعلم طرق استقبال البلاغات حول الجرائم المعلوماتية وكيفية التعامل مع مسرح الجريمة الرقمي.
- شرح مفاهيم المختبر الجنائي الرقمي وتدريس أدوات الطب الشرعي الرقمي.
- تدريس مهام الفاحص والخبير الجنائي الرقمي ومهام كل منهما.
- تهيئة الطاقات التي تستطيع تشكيل وترتيب مهام الفريق الامني للاستجابة الاولية للبلاغ.
- تدريس كل ما يتعلق بالدليل الرقمي.
- ضوابط اجراء المعاينة والتحليل بعد وقوع الجريمة والتمكن من اتمامها.
- تجميع واستخراج الأدلة وترتيبها لعرض القضية والأدلة.
- تدريس ماهية عمل معمل وأدوات التحقيق الجنائي الرقمي والطب الشرعي الرقمي.
- التمكن التام من فحص ومعالجة الدليل في مختبر الطب الشرعي الرقمي.
- مهنية كتابة وصنع التقرير الفني الجنائي بشكل فني مقبول قانوناً.
- تطبيق التدريب عملي لكل النقاط التي ذكرت أعلاه.

التصور العام لمختبر الطب الشرعي الرقمي



مخطط الإجراءات القياسية للتعامل مع المبرزات الالكترونية خارج

مختبر الطب الشرعي الرقمي



إعداد: (12)

أهم أجهـــزة الطـــب الشـــــرعي الرقمـــي للتعامل

مع

وسائط التخزين المختلفة

A G النائب العام

إعداد: (12)

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
جهاز محقق الطـــب الشرعـــي الأكسجين **Oxygen Forensic Detective Full Kit**	

المواصفات الفنية

يدعم استخراج وتحليل واعداد التقارير الفنية معتمداً علي برامج الذكاء الاصطناعي للوصول الي **الحسابات وكلمات المرور و تحليل سجل المكالمات و البيانات السحابية و استخراج البيانات المحذوفة و تصنيف الصور** بالإضافة الي تحليل وسائل التواصل الاجتماعي المختلفة وغيرها من المميزات.

أجهزة الكمبيوتر + الهواتف الذكية + الطائرات بدون طيار + كاميرات المراقبة

التدريب

- وضع جدول زمني للتدريب من المستوي التأهيلي للمبتدئين الي المستوي الاحترافي بشكل تدريجي يتم فيه مراعات الجوانب الفنية في التعامل مع تقنيات الذكاء الاصطناعي التي يوفرها جهاز الطب الشرعي.
- الحصول علي شهادة معتمدة دولياً للمتدربين من الشركة المصنعة حيث أن لا يجوز للمتدرب الترشح الي دراسة المستوي المتخصص أو الاحترافي إلا بالحصول علي الشهادات المعتمدة من الشركة المصنعة.
- توفير وسيلة اتصال مباشر للمتدربين علي مدار الساعة للحصول علي الأجوبة والحلول لجميع المشاكل التي قد تواجههم عند الاستعمال.
- التركيز علي التدريب العملي لقضايا حقيقية لمجموعة متنوعة من المبرزات المختلفة وكيفية التعامل مع القضايا من الجوانب الفنية والقانونية بشكل مفصل منذ استلام المبرزة الالكترونية الي حين الانتهاء من إعداد تقرير الخبرة.
- توفير ورش العمل الفنية والندوات المجانية عبر الإنترنت، والفصول الدراسية الشخصية التي يقدمها مقدمو التدريب الموثوقون والمعتمدين لذي الشركة المصنعة.
- يجب تفعيل الأجهزة والبرامج داخل إطار المختبر الطب الشرعي بليبيا والاتفاق علي ألية واضحة لتجديد الرخصة السنوية وتحديث برامج التشغيل للأجهزة بشكل دوري.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
جهاز الطـــب الشرعـــي المحمول **MSAB** **XRY** **Forensic** **Full Kit**	

المواصفات الفنية

يختص بنسخ صورة من الذاكرة الداخلية لجميع المبرزات التي تعمل بأنظمة التشغيل
(IOS) + (Android)
بالإضافة علي القدرة علي التعامل مع المبرزات بمسرح الجريمة.

الهواتف الذكية + الطائرات بدون طيار + الأجهزة اللوحية + الساعات الذكية

التدريب

- وضع جدول زمني للتدريب من المستوي التأهيلي للمبتدئين الي المستوي الاحترافي بشكل تدريجي يتم فيه مراعات الجوانب الفنية في التعامل مع تقنيات استخراج وتحليل البيانات من الهواتف الخلوية الذكية المختلفة والتي يوفرها جهاز الطب الشرعي (XRY Forensic).
- الحصول علي شهادة معتمدة دولياً للمتدربين من الشركة المصنعة حيث أن لا يجوز للمتدرب الترشح الي دراسة المستوي المتخصص أو الاحترافي إلا بالحصول علي الشهادات المعتمدة من الشركة المصنعة.
- توفير وسيلة اتصال مباشر للمتدربين علي مدار الساعة للحصول علي الأجوبة والحلول لجميع المشاكل التي قد تواجههم عند الاستعمال.
- التركيز علي التدريب العملي لقضايا حقيقية لمجموعة متنوعة من المبرزات المختلفة وكيفية التعامل مع القضايا من الجوانب الفنية والقانونية بشكل مفصل منذ استلام المبرزة الالكترونية الي حين الانتهاء من إعداد تقرير الخبرة.
- توفير ورش العمل الفنية والندوات المجانية عبر الإنترنت، والفصول الدراسية الشخصية التي يقدمها مقدمو التدريب الموثوقون والمعتمدين لذي الشركة المصنعة.
- يجب تفعيل الأجهزة والبرامج داخل إطار المختبر الطب الشرعي بليبيا والاتفاق علي آلية واضحة لتجديد الرخصة السنوية وتحديث برامج التشغيل للأجهزة بشكل دوري.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
مجموعة أدوات يوفد سيلبرايت **Cellebrite UFED Forensic Full Kit**	

المواصفات الفنية

يدعم UFED أكثر من 31.000 جهاز من Apple و Android ، من بين أجهزة أخرى .يمكن للتطبيق جمع البيانات من الهواتف المحمولة والطائرات بدون طيار وبطاقات SIM وبطاقات SD وأجهزة GPS والمزيد .كما يوفر الوصول إلى أكثر من 40 تطبيقًا لوسائل التواصل الإجتماعي

الكمبيوتر + الهواتف الذكية + الطائرات بدون طيار + الأجهزة اللوحية

التدريب

- **وضع جدول زمني للتدريب من المستوي التأهيلي للمبتدئين الي المستوي الاحترافي بشكل تدريجي يتم فيه مراعات الجوانب الفنية في التعامل مع تقنيات استخراج وتحليل البيانات من الهواتف الخلوية الذكية المختلفة والتي يوفرها جهاز الطب الشرعي (Cellebrite UFED Forensic).**
- **الحصول علي شهادة معتمدة دولياً للمتدربين من الشركة المصنعة حيث أن لا يجوز للمتدرب الترشح الي دراسة المستوي المتخصص أو الاحترافي إلا بالحصول علي الشهادات المعتمدة من الشركة المصنعة.**
- **توفير وسيلة اتصال مباشر للمتدربين علي مدار الساعة للحصول علي الأجوبة والحلول لجميع المشاكل التي قد تواجههم عند الاستعمال.**
- **التركيز علي التدريب العملي لقضايا حقيقية لمجموعة متنوعة من المبرزات المختلفة وكيفية التعامل مع القضايا من الجوانب الفنية والقانونية بشكل مفصل منذ استلام المبرزة الالكترونية الي حين الانتهاء من إعداد تقرير الخبرة.**
- **توفير ورش العمل الفنية والندوات المجانية عبر الإنترنت، والفصول الدراسية الشخصية التي يقدمها مقدمو التدريب الموثوقون والمعتمدين لذي الشركة المصنعة.**
- **يجب تفعيل الأجهزة والبرامج داخل إطار المختبر الطب الشرعي بليبيا والاتفاق علي ألية واضحة لتجديد الرخصة السنوية وتحديث برامج التشغيل للأجهزة بشكل دوري.**

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
جهاز تخطي حماية الهواتف الذكية Magnet GRAYKEY Forensic	

المواصفات الفنية

- دعم الوصول الأكثر شمولاً لأجهزة (iOS وAndroid) الحديثة، مع تحديثات منتظمة لأحدث الإصدارات.
- القدرة على الوصول إلى الأدلة واستخراجها من الأجهزة المحمولة بغض النظر عن حالة الجهاز.
- الوصول إلى مخازن بيانات الاعتماد مثل Keychain وKeystore لفك تشفير المحتوى.

التدريب

- يجب أن يشمل التدريب جميع النماذج مختلفة من الهواتف الذكية التي تعمل بأنظمة التشغيل مختلفة مع التركيز علي وسائل فك التشفير.
- يجب ان يتم التركيز علي كيفية التعامل مع الهواتف التالفة والمحطمة والتي لا يمكن استخراج البيانات منها بالطرق التقليدية المتعارف عليها.
- الحصول علي شهادة معتمدة دولياً للمتدربين من الشركة المصنعة حيث أن لا يجوز للمتدرب الترشح الي دراسة المستوي المتخصص أو الاحترافي إلا بالحصول علي الشهادات المعتمدة من الشركة المصنعة.
- توفير وسيلة اتصال مباشر للمتدربين علي مدار الساعة للحصول علي الأجوبة والحلول لجميع المشاكل التي قد تواجههم عند الاستعمال.
- التركيز علي التدريب العملي لقضايا حقيقية لمجموعة متنوعة من المبرزات المختلفة وكيفية التعامل مع القضايا من الجوانب الفنية والقانونية بشكل مفصل منذ استلام المبرزة الالكترونية الي حين الانتهاء من إعداد تقرير الخبرة.
- توفير ورش العمل الفنية والندوات المجانية عبر الإنترنت، والفصول الدراسية الشخصية التي يقدمها مقدمو التدريب الموثوقون والمعتمدين لذي الشركة المصنعة.
- يجب تفعيل الأجهزة والبرامج داخل إطار المختبر الطب الشرعي بليبيا والاتفاق علي ألية واضحة لتجديد الرخصة السنوية وتحديث برامج التشغيل للأجهزة بشكل دوري.

استخدام وسائل الطب الشرعي الرقمي والذكاء الاصطناعي

في

تحليل البيانات واستخراج الدليل الرقمي

من

الشبكات وقواعد البيانات

إعداد: (12)

خوارزميات الذكاء الاصطناعي وتقنيات الطب الشرعي الرقمي.

AI algorithms and techniques digital forensic

تلعب خوارزميات الذكاء الاصطناعي في علوم الطب الشرعي الرقمي دورًا حاسمًا في عالم اليوم والذي يحركه تبادل البيانات والمعلومات المشفرة والمخفية والمحذوفة عبر مختلف وسائل تقنية المعلومات من أجهزة والشبكات وقواعد بيانات، مما يمكّن جهات إنفاذ القانون من كشف الجرائم المعقدة وجمع الأدلة الرقمية بشكل قانوني مقبول أمام جميع الهيئات القضائية حول العالم. ومع تزايد حجم وتعقيد البيانات الرقمية، أصبح دمج الذكاء الاصطناعي (AI) في تكنولوجيا الطب الشرعي الرقمي أمرًا ضروريًا. توفر خوارزميات وتقنيات الذكاء الاصطناعي مجموعة من الفوائد الهامة مثل توفير الوقت وتجنب الخطاء البشري، مما يعزز كفاءة وفعالية التحقيقات الرقمية ويساعد المؤسسات المعنية بإنفاذ القانون على التخفيف بشكل استباقي من المخاطر الأمنية القائمة على البيانات.

وبدءًا من التحليل الآلي للسجل البيانات واكتشاف البرامج الضارة والاختراق والتلاعب وحتى تحليل حركة مرور الشبكة وفرز الأدلة الجنائية، يمكن للذكاء الاصطناعي أن يلعب دورًا هاماً في العديد من أنشطة الأدلة الجنائية الرقمية ويكون له تأثير جوهرياً على مجريات التحقيق الرقمي بشكل عام.

فيما يلي ست طرق يمكن للذكاء الاصطناعي من خلالها إحداث ثورة في الطب الشرعي الرقمي في الوقت الحالي.

1. تحليل السجل الآلي لقواعد البيانات باستخدام تقنيات الذكاء الاصطناعي للطب الشرعي الرقمي.

غالبًا ما تتعامل جهات إنفاذ القانون مع عدد كبير جداً من ملفات السجل التي تحتوي علي كم هائل من البيانات التي تم إنشاؤها بواسطة أنظمة وتطبيقات وأجهزة وشبكات مختلفة، ولكن تحليل هذه السجلات يدويًا يمكن أن يستغرق وقتًا طويلاً جداً وعرضة للأخطاء البشرية. وهنا يأتي دور استخدام تقنيات الذكاء الاصطناعي للطب الشرعي الرقمي لتحليل السجل الآلي.

حيث تتفوق خوارزميات الذكاء الاصطناعي في معالجة كميات هائلة من ملفات السجل وتحليلها بحثًا عن الأنماط والشاذة والعلاقات المتشعبة لجميع الأنشطة الإجرامية. ومن خلال تحليل السجل المدعوم بالذكاء الاصطناعي، يمكن للمحققين تحديد الأنشطة المشبوهة والحوادث الأمنية المحتملة والمناطق التي تتطلب مزيدًا من التحقيق الميداني بشكل أسرع. كما يعزز الذكاء الاصطناعي سرعة ودقة تحليل السجل، مما يمكّن المحققين من تركيز جهودهم على مجالات الاهتمام ذات الصلة وتجنب إنفاق الوقت والموارد في المراجعة باستخدام العنصر البشري.

2.الكشف عن البرامج الضارة

التطور السريع للبرامج الضارة يستدعي أساليب الكشف المتقدمة. تعمل أنظمة الكشف عن البرامج الضارة المدعومة بالذكاء الاصطناعي على الاستفادة من التعلم الآلي لمراجعة التعليمات البرمجية ومسحها ضوئيًا ودراسة أنماط سلوك المستخدم، والكشف عن البرامج الضارة بشكل أكثر فعالية ومساعدة المحققين على إزالة البرامج الضارة من الأنظمة المخترقة للحماية من المزيد من الهجمات.

على سبيل المثال، تستخدم شركات الأمن خوارزميات الذكاء الاصطناعي للتعلم المستمر من عينات البرامج الضارة المعروفة وخصائصها. ومن خلال تدريب هذه الخوارزميات على مجموعات بيانات كبيرة، يمكنها اكتشاف وتصنيف سلالات البرامج الضارة الجديدة وغير المعروفة سابقًا استنادًا إلى أوجه التشابه مع التهديدات التي تم تحديدها مسبقًا والإبلاغ عن أي هجوم محتمل قبل حدوثه.

3.تحليل الصور والفيديو

يعد تحليل الصور ومقاطع الفيديو الرقمية عنصرًا حاسمًا في الطب الشرعي الرقمي. على سبيل المثال، يمكن لخوارزميات الذكاء الاصطناعي التدقيق في كميات كبيرة من محتوى الوسائط المتعددة - التعرف بسرعة على الوجوه أو الأشياء أو النص داخل الصور ومقاطع الفيديو، وبالتالي تسريع عملية البحث عن الأدلة المهمة واستخلاصها بشكل كبير - ودعم مجموعة واسعة من سيناريوهات التحقيق.

لنأخذ على سبيل المثال حالة يحتاج فيها المحققون إلى تحديد هوية المشتبه به الذي تم التقاطه في لقطات المراقبة من منطقة مزدحمة. غالبًا ما تكون مراجعة لقطات الفيديو أمرًا مملاً ويمكن أن تستغرق ساعات. يمكن لتقنية التعرف على الوجه المدعومة بالذكاء الاصطناعي إجراء مسح سريع لكميات هائلة من بيانات الفيديو، وتحديد الأفراد محل الاهتمام وتقليل الجهد اليدوي المطلوب بشكل كبير. تعمل هذه التكنولوجيا على تسريع عملية تحديد الهوية، مما يمكّن المحققين من تركيز جهودهم على الخيوط الأكثر صلة وتسريع تقدم التحقيق.

4.معالجة اللغات الطبيعية

تتيح تقنيات الذكاء الاصطناعي مثل معالجة اللغات الطبيعية (NLP) تحليل المعلومات ذات الصلة من كميات كبيرة من البيانات النصية. على سبيل المثال، غالبًا ما تحتوي البيانات النصية، بما في ذلك رسائل البريد الإلكتروني وسجلات الدردشة لوسائل التواصل الاجتماعي والمستندات الرقمية، على أدلة قيمة في التحقيقات الرقمية. يمكن أن يكون استخدام الذكاء الاصطناعي الاستخراجي أكثر كفاءة ودقة للكشف عن العلاقات واكتشاف الأنماط وتحديد الأفراد الرئيسيين أثناء التحقيقات التي تركز على النص.

فعند فحص مجموعة ضخمة من سجلات الدردشة لتحديد المتعاونين المحتملين في جريمة إلكترونية وتحليل العلاقات المتشعبة بين مجموعة كبيرة من المستخدمين. يمكن لخوارزميات البرمجة اللغوية العصبية المدعومة بالذكاء الاصطناعي معالجة البيانات النصية وتحليلها بسرعة، وتحديد العبارات المتكررة والأنماط المشبوهة والاتصالات بين الأفراد. وهذا يمكّن المحققين من تحديد الأشخاص الرئيسيين موضع الاهتمام والكشف عن الشبكات المخفية، وتسريع عملية التحقيق وتمكين التدخلات في الوقت المناسب.

.5تحليل حركة مرور الشبكة

تعد مراقبة وتحليل أنماط حركة مرور الشبكة أمرًا ضروريًا لاكتشاف الهجمات الإلكترونية والرد عليها. بدلاً من إجراء تدقيق يدوي وتحليل أنماط حركة مرور الشبكة على فترات زمنية محددة مسبقًا، يمكن لفرق الطب الشرعي تدريب خوارزميات الذكاء الاصطناعي لتحليل حزم الشبكة تلقائيًا، وتحديد الانحرافات عن أنماط حركة المرور العادية، وإصدار التنبيهات عندما تستحق حالة شاذة مزيدًا من التحقيق. يمكن أن يساعد الذكاء الاصطناعي أيضًا في ربط أحداث الشبكة بأنماط الهجوم المعروفة، مما يوفر رؤى قيمة لفرق الاستجابة للحوادث للحد من الآثار السلبية للهجمات الالكترونية وتقليل الأضرار والتي تصل الي مكافحة الجريمة الرقمية قبل وقوعها.

.6الفرز الشرعي

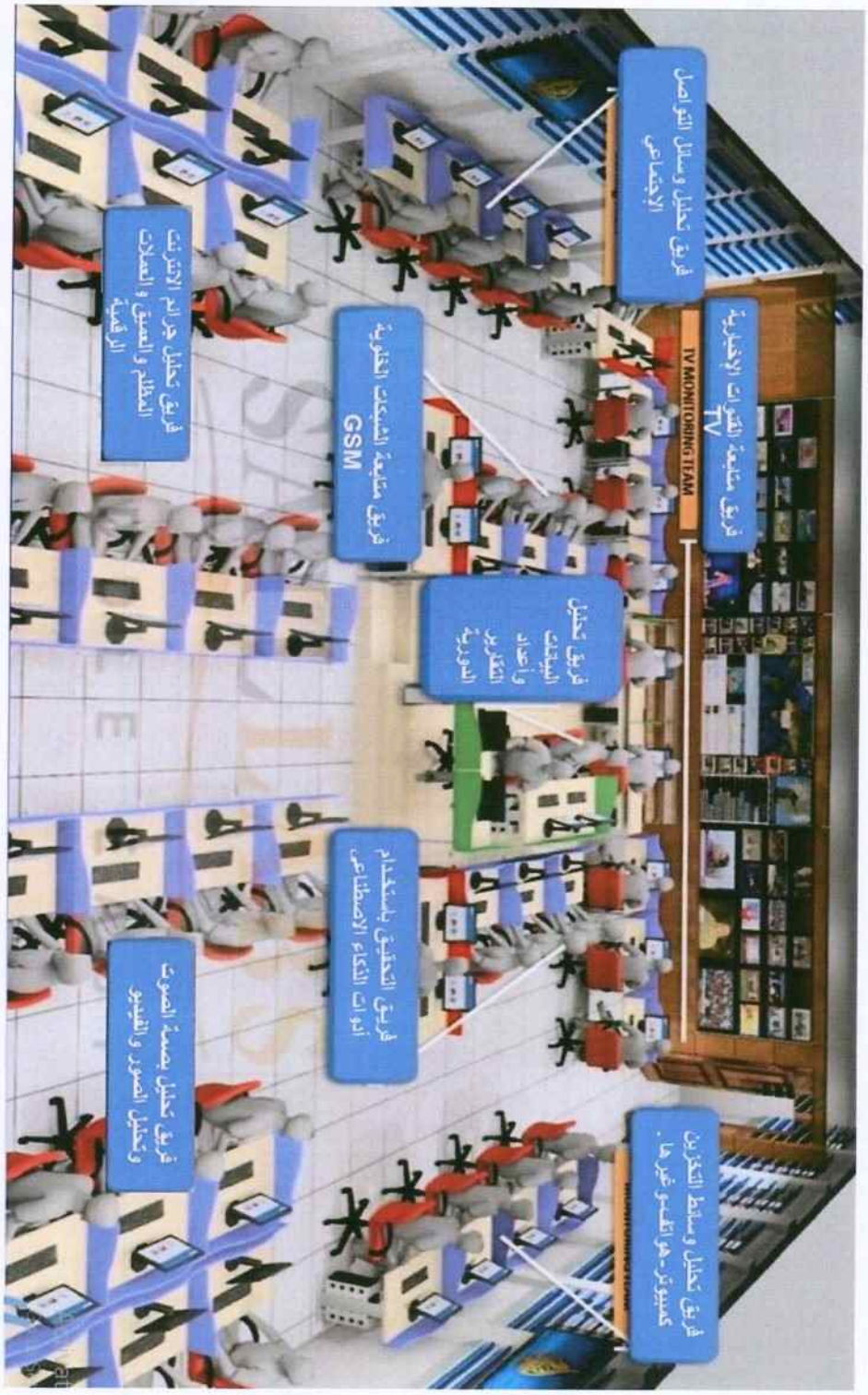
تتضمن التحقيقات الرقمية كميات هائلة من البيانات، مما يتطلب من المحققين فحص الأدلة ذات الصلة بسرعة وتحديد أولوياتها. غالبًا ما يتضمن الذكاء الاصطناعي في فرز الطب الشرعي استخدام خوارزميات التعلم الآلي لتصنيف وتصنيف أعداد كبيرة من الملفات الرقمية بناءً على مدى صلتها بالتحقيق. تقوم هذه الأدوات بتحليل البيانات الوصفية للملف والمحتوى والسمات الأخرى لتحديد أولويات الملفات لإجراء فحص دقيق، و"التعلم" المستمر لتحديد المواد ذات الصلة بدقة متزايدة مع إضافة بيانات جديدة إلى التحقيق. تستطيع فرق الطب الشرعي تحديد الأدلة الأكثر أهمية والتركيز عليها بسرعة في وقت مبكر، مما يؤدي إلى تحقيقات أسرع وأكثر فعالية مع تحسين تخصيص الموارد.

مستقبل الذكاء الاصطناعي والطب الشرعي الرقمي

أصبح دمج الذكاء الاصطناعي في تكنولوجيا الطب الشرعي الرقمي موضوعًا مهمًا للخبراء القائمين في هذا المجال خلال العقد الحالي. وستستمر التطبيقات المحتملة للذكاء الاصطناعي في الطب الشرعي في التوسع، مع التركيز بشكل خاص على قدرات الذكاء الاصطناعي المتقدمة في تحليل البيانات، والتعرف على الأنماط، واكتشاف الحالات الشاذة.

كما سيصبح من المهم بشكل متزايد تحديد الدقة في عصر الذكاء الاصطناعي، وقد يفكر الكثيرون في دمج المصادقة متعددة العوامل، مثل بصمة الإصبع أو مصادقة العين. ومع ذلك، يجب معالجة التحديات المتعلقة بخصوصية البيانات والتحيز والدقة بعناية لضمان أن استخدام الذكاء الاصطناعي في الطب الشرعي الرقمي يكون دائمًا أخلاقيًا ومسؤولًا.

التصور العام لتحليل البيانات باستخدام تقنيات الطب الشرعي الرقمي والذكاء الاصطناعي



جهاز الطب الشرعي الرقمي	الوصف التوضيحي
التحقيق الرقمي في الانترنت المظلم والعميق والعملات الافتراضية المشفرة Certified Cryptocurrency Forensic Investigator (CCFI)	

المواصفات الفنية

- على الرغم من صعوبة تعقب الأنشطة الإجرامية علي الويب المظلم، إلا أن تعقب حركة تداول العملات الرقمية المشفرة والتي تعتبر الوسيلة الوحيدة للدفع مقابل أي نشاط إجرامي علي الشبكة المظلمة مما يمكن جهات إنفاذ القانون حول العالم من الربط بين الشخصية الافتراضية للمجرم والشخصية الحقيقية.
- تعتمد أدوات الطب الشرعي الرقمي لتتبع وتحليل حركة التداول للعملات الافتراضية (blockchain - cryptocurrency) على حقيقة أن تدفق الأصول الرقمية والأموال يمكن أن يكون من السهل نسبياً تتبعها وتفسيره مساراتها إذا توفرت أدوات الطب الشرعي الرقمي اللازمة.
- تظهر سجلات المحاكم أن المحققين قادرون على تتبع سجلات معاملات العملة المشفرة إلى محفظة رقمية معينة، والتي تربط الهوية الرقمية بشخص مادي الذي يمتلك المحفظة.
- من خلال إنشاء هذا الربط بين الهويتين، يمكن لمسؤولين إنفاذ القانون الوصول إلى المحفظة الرقمية باستخدام المفاتيح الخاصة للمحافظ الرقمية وكلمات المرور للمفاتيح العامة والخاصة للمستخدمين.

التـــدريب

- دراسة عملية لألية التعدين للعملات الرقمية المشفرة.
  1. كيفية اختيار العملة الرقمية المناسبة لعملية التعدين.
  2. كيفية اختيار أجهزة التعدين المناسبة لعملية التعدين.
  3. إنشاء محافظ تخزين وتداول العملات الرقمية.
  4. الإجراءات الفنية لإعداد أجهزة التعدين وتهيئتها.
  5. الوسائل الفنية للانضمام إلى مجمع تعدين واختيار منصات التداول.
- دراسة معمقة لأنواع المحافظ الالكترونية المستخدمة في تخزين وتداول العملات الافتراضية التي تم تعدينها.
- دراسة طرق تعدين العملات الرقمية عبر الهواتف الذكية تطبيق وكيفية عمل تجزئة الكتل في Blockchain

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
التحقيق الرقمي في المصادر المفتوحة **OSINT** **Investigation**	

المواصفات الفنية

- أنواع مصادر المعلومات المفتوحة عبر الانترنت، ولماذا نحتاجها وكيفية الاستفادة منها في مجال التحقيقات الجنائية الرقمية.
- الأسس التقنية والفنية اللازمة قبل البدء في عملية جمع المعلومات من مصادرها المفتوحة عبر الانترنت.
- إطار مصادر المعلومات المفتوحة عبر الانترنت.
- استخدام أدوات جمع المعلومات من المصادر المفتوحة.
- استخدام أدوات جمع المعلومات من مواقع التواصل الاجتماعي.
- تحليل المعلومات من مصادر المعلومات المفتوحة عبر الانترنت.

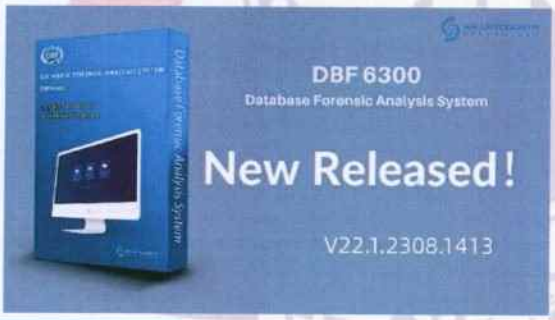
التدريب

- التعرف على المخاطر التي يمكن مواجهتها عند البحث في المصادر المفتوحة للمعلومات.
- إخفاء الهوية وتشفير المعلومات.
- إخفاء الاثار الرقمية للقائم بالبحث في مصادر المعلومات المفتوحة.
- البرمجيات التي يتم تحميلها على الجهاز المستخدم في عملية البحث.
- تطبيق عملي على الاعداد لاستخدام المصادر المفتوحة للمعلومات عبر الانترنت.
- ما المقصود بإطار استخبارات المصادر المفتوحة.
- كيف يمكن الاستفادة من أدوات إطار المصادر المفتوحة للمعلومات في جمع المعلومات.
- تطبيقات عملية على استخدام اطار جمع المعلومات المفتوحة عبر الانترنت.
- **أدوات جمع وتحليل المعلومات محتوى مواقع التواصل الاجتماعي.**
- خرائط الوقت الحقيقي.
- استخدام البيانات الوصفية في جمع المعلومات.
- التدريب علي برنامج (مالتيجو).
- التدريب علي برنامج (سبايدر فوت).

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
أنظمة الاعتراض التكتيكي للإشارات الخلوية **Global GSM Location Finder**	

المواصفات الفنية

- تختلف مواصفات أنظمة اعتراض الإشارات الخلوية باختلاف البيئة الجغرافية والبنية التحتية للشركات المزودة للخدمات الخلوية, ولذلك يجب اختيار وفق دراسة مفصلة لاحتياجات المناسبة من أنظمة الاعتراض الخلوي المتاحة عالمياً.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
نظام تحليل الطب الشرعي لقواعد البيانات **Database Forensic Analysis System**	

المواصفات الفنية

- تهدف هذه السلسلة إلى حل مشكلات ملفات قاعدة البيانات المحذوفة/التالفة/المجزأة, وأنظمة الملفات الزائفة, وتقييد إمكانية الوصول إلى نظام التطبيق .
- المحققون قادرون على استخدام سلسلة DBF لإجراء عمليات المعاينة والاسترداد والاستخراج وإعادة التنظيم والتحليل والتصدير لملفات قاعدة البيانات.
- تعد سلسلة DBF حلاً مثاليًا للوقت والتكلفة والذي يجب استخدامه على نطاق واسع في الوظائف ذات الصلة.

استخدام وسائل الطب الشرعي الرقمي والذكاء الاصطناعي

في

الجرائم المرتبطة بوسائل الميديا المختلفة

إعداد: (12)

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
أدوات الطب الشرعي الرقمي لتحليل الصوت Digital forensic tools for audio analysis	 SIS Audio visualization and editing

المواصفات الفنية

الطب الشرعي الصوتي هو الفحص الدقيق للملفات الصوتية للأغراض القانونية.
حيث يقوم خبراء الطب الشرعي الصوتي بفحص التسجيل في مختبر الطب الشرعي لتحديد صحته.
ويتضمن الفحص النقاط الأساسية الأتية:

- التحقق من صحة الصوت.
- تحسين وضوح الكلام.
- نسخ الحوار كتابياً.
- مقارنة الأصوات (بصمة الصوت).
- إعادة بناء الجداول الزمنية لتسلسل الأحداث.

ويمكن استخدام الملفات الصوتية التي تم فحصها وتوضيحها بواسطة خبير في الطب الشرعي الصوتي في المحكمة كدليل. يجوز لعالم الطب الشرعي الصوتي أن يعمل كشاهد خبير ويقدم تقارير وشهادات عن نتائج تحقيقاته. تتضمن المعلومات التي يقدمونها كل شيء بدءًا من منهجيتهم وحتى الآراء غير المتحيزة حول النتائج التي تم الحصول عليها.

التـــدريب

أهم تطبيقات الطب الشرعي الرقمي لتحليل الدليل الصوتي:

- De-Wind De-Hum
- De-Crackle
- De-Reverb

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
مجموعة أدوات التحليل الجنائي الرقمي الفيديو Video Investigation Forensic tools	

المواصفات الفنية

برنامج فيديو أكتيف Video Active

معالجة معيارية للفيديو في الوقت الفعلي ودمج نموذج إلى فيديو ثلاثي الأبعاد للقياسات وتحديد هوية المركبات والأشخاص

برنامج فيديو المحقق Video Investigator

يعد من البرنامج الأكثر شمولاً في العالم (23 براءة اختراع أمريكية) وبيئة برامج معالجة الفيديو/الصور الجنائية والتحليل ثلاثي الأبعاد مع ما يقرب من مائتي فلتر لأدوات الدمج للمعلومات الجغرافية لأي عدد عشوائي من مقاطع الفيديو للتحقيق وتتبع الأحداث الموزعة جغرافيًا وآثار المركبات.

برنامج القياس التلقائي Auto Measure

التصوير المساحي الشرعي بزاوية 360 درجة وجولات قياس لمسرح الجريمة الكبيرة مع القدرة على إنتاج قياسات دقيقة لمسرح الجريمة من كاميرات DSLR ، وقياس الأشياء (المركبات) والأبعاد البيومترية للمشتبه به في الفيديو (مثل الارتفاع وعرض الكتفين وما إلى ذلك).

تحقيق الفيديو المحمول Video Investigation Portable2.0 (VIP)

- يدعم إنشاء قيمة التجزئة MD5 و SHA-1للتحقق من الصورة. ومجهزة تلقائيا بإنشاء تقرير الطب الشرعي المعتمدة قانوناً.
- قادر على الوصول إلى بيانات فيديو المراقبة مباشرة من محركات الأقراص الثابتة CCTV DVR/NVR.
- تجاوز كلمة مرور تسجيل الدخول إلى نظام.DVR/NVR
- مجهزة باستخراج مقاطع الفيديو من مسجلات الفيديو الرقمية / مسجلات الفيديو الرقمية (DVR) التالفة أو التي يتعذر الوصول إليها.
- مجهزة لاستعادة ملفات الفيديو التي يتعذر الوصول إليها، بما في ذلك ملفات الفيديو المحذوفة والمفقودة والمجزأة.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
برنامج التحليل الرقمي إن كيس EnCase Forensic Suite	EnCase Forensic Suite

المواصفات الفنية

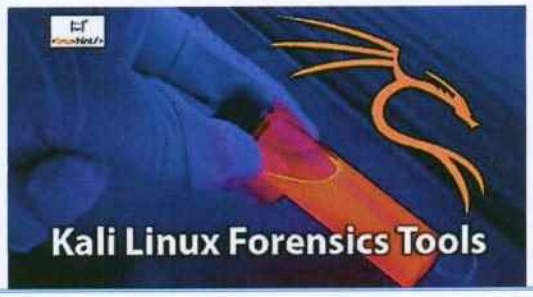
برنامج الطب الشرعي الرقمي القادر علي التعامل مع جميع النسخ (IMEG) المستخرجة من أجهزة الطب الشرعي الرقمي المتعارف عليها ويتميز

- الحصول علي الدليل الرقمي الموثوق من مجموعة واسعة من الأجهزة بما في ذلك أكثر من 25 نوعًا من الأجهزة المحمولة.
- أكمل تحقيقًا شاملاً على مستوى الذاكرة بالأخص الممسوحة أو التالفة.
- إعداد تقارير شاملة عن النتائج التي توصلت إليها مع الحفاظ على سلامة الأدلة الخاصة بك.
- حافظ على سلامة الدليل الرقمي بالشكل الذي تثق به المحاكم.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
برنامج التحقيق الرقمي للصور ومقاطع الفيديو Amped Software Forensic	AMPED SOFTWARE AUTHORIZED DISTRIBUTOR

المواصفات الفنية

- من أفضل برامج الطب الشرعي في التعامل مع الصور ومقاطع الفيديو في جميع التحقيقات، بدءًا من مسرح الجريمة، وحتى مختبر الطب الشرعي، ثم إلى قاعة المحكمة.
- يعتمد التطبيق على تطوير التقنيات الأكثر تقدمًا واكتمالًا مع بساطة وسهلة الاستخدام لجميع احتياجات معالجة الصور والفيديو المتعلقة بالطب الشرعي والسلامة العامة للبيانات.
- التركيز على شفافية المنهجيات المستخدمة، تعمل حلول Amped على تمكين الخبراء من خلال المبادئ الثلاثة الرئيسية للمنهج العلمي: الدقة والتكرار وإمكانية التكرار.

جهاز الطب الشرعي الرقمي	الوصف التوضيحي
أدوات الطب الشرعي لنظام الكالي ليونيكس Kali Linux Forensics Tools	

المواصفات الفنية

- يحتوي النظام علي مجموعة كبيرة من الأدوات المدفوعة التي تعمل علي حل مشاكل الطب الشرعي الرقمي في التعامل مع مواقع التواصل الاجتماعي.
- تطوير أدواتك الخاصة للتعامل مع قضايا الطب الشرعي الرقمي بشكل سهل في التعامل مع أنظمة تشغيل الهواتف الذكية التي تعمل بنظامي (IOS + Android).
- يأتي Kali Linux محملاً مسبقًا ببرامج الطب الشرعي مفتوحة المصدر الأكثر شيوعًا، وهي مجموعة أدوات سهلة الاستخدام عندما تحتاج إلى القيام بأعمال الطب الشرعي.

التدريب

تحتوي توزيعة Kali Linux على أكثر من 600 أداة في مجال الحماية والشبكات والاختراق والتحليل وتنقسم إلى فئات كثيره منها:

1. جمع المعلومات .
2. تحليل هجمات فك التشفير وكلمات المرور .
3. تحليل نقاط الضعف للشبكات.
4. الهندسة العكسية .
5. تحليل تطبيقات الويب .
6. هجمات لاسلكية .
7. أدوات الطب الشرعي الرقمي.
8. التحقيق الجنائي رقمي .
9. أدوات الهندسة الاجتماعية .

المراجـــــع: (References)

A. https://www.iso.org/standard/44381.html
B. https://www.unodc.org/e4j/ar/cybercrime/module-6/key-issues/intro.html
C. https://www.unodc.org/e4j/ar/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html
D. http://msn.iecs.fcu.edu.tw/report/data/ori_paper/2005-9-15/MD5%20collisions%20and%20the%20impact%20on%20computer%20forensics.pdf
E. https://www.eweek.com/security/researchers-from-google-cti-break-sha-1-hash-encryption-function/
F. https://www.unodc.org/e4j/ar/cybercrime/module-10/key-issues/intro.html
G. https://www.unodc.org/e4j/ar/cybercrime/module-2/key-issues/intro.html
H. file:///D:/%D9%83%D8%B1%D8%A7%D8%B3%D8%A9%20%D8%A7%D9%84%D9%85%D9%88%D8%A7%D8%B5%D9%81%D8%A7%D8%AA/1._forensic_examination_of_digital_technology_0.pdf
I. https://www.iso27001security.com/html/27050.html
J. https://www.iso27001security.com/html/27037.html
K. https://www.iso27001security.com/html/27043.html
L. https://www.iso27001security.com/html/27041.html
M. https://www.iso27001security.com/html/27042.html

أُهديت إلى

الأصيل حمزة الزياني