الأكاديمية العربية الدولية
Arab International Academy

اسم المادة: تحليل الأدلة الرقمية

المحاضِر: م. خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

مقدمة

الأجهزة الرقمية موجودة في كل مكان في عالم اليوم، مما يساعد الناس على التواصل محليًا وعالميًا بسهولة .يعتقد معظم الناس على الفور أن أجهزة الكمبيوتر والهواتف المحمولة والإنترنت هي المصادر الوحيدة للأدلة الرقمية، ولكن يمكن استخدام أي قطعة تقنية تعالج المعلومات بطريقة إجرامية .على سبيل المثال، يمكن أن تنقل الألعاب المحمولة رسائل مشفرة بين المجرمين وحتى الأجهزة المنزلية الجديدة، مثل الثلاجة المزودة بتلفزيون مدمج، يمكن استخدامها لتخزين الصور غير القانونية وعرضها ومشاركتها .الشيء المهم الذي يجب معرفته هو أن المستجيبين بحاجة إلى أن يكونوا قادرين على التعرف على الأدلة الرقمية المحتملة والاستيلاء عليها بشكل صحيح.

ما هي الأدلة الرقمية:

تعريف:

يُعرَّف الدليل الرقمي على أنه معلومات وبيانات ذات قيمة للتحقيق يتم تخزينها أو استلامها أو إرسالها بواسطة جهاز إلكتروني. يمكن الحصول على هذه الأدلة عند مصادرة الأجهزة الإلكترونية وتأمينها للفحص .الدليل الرقمي:

- كامنة (مخفية): مثل بصمات الأصابع أو أدلة الحمض النووي DNAاذاً لا يتم كشفه بسهولة.
- يتجاوز الحدود القضائية بسرعة وسهولة
- يمكن تغييرها أو إتلافها أو تدميرها وإلحاق الضرر بها بسهولة بجهد ضئيل
- يمكن أن تكون حساسة للوقت : أي انه اذا لم يتم استثمارها والاستفادة منها خلال فترة محددة يمكن فقدانها

مبادئ الأدلة الرقمية

يقال إن المعلومات التي يتم تخزينها إلكترونيًا "**رقمية**" لأنها مقسمة إلى أرقام؛ الوحدات الثنائية من الآحاد (1) والأصفار (0) ، يتم حفظها واسترجاعها باستخدام مجموعة من التعليمات تسمى البرنامج أو الكود .يمكن إنشاء أي نوع من المعلومات - الصور والكلمات وجداول البيانات - وحفظها باستخدام هذه الأنواع من التعليمات .يعد العثور على الأدلة المحفوظة بهذه الطريقة واستغلالها مجالًا متناميًا للأدلة الجنائية ويتغير باستمرار مع تطور التكنولوجيا.

الإنترنت :كان إطلاق الإنترنت أو شبكة الويب العالمية في منتصف التسعينيات إيذانا ببدء "عصر الوصول ."لأول مرة ، يمكن للأفراد من خارج العالم الأكاديمي استخدامه للتواصل مع الآخرين (وأجهزة الكمبيوتر الخاصة بهم) بطريقة جديدة تمامًا .أتاح الإنترنت الوصول إلى عالم من المعلومات والموارد ، ولكنه وفر أيضًا طريقًا سريعًا لتهريب الصور والمعلومات والتجسس غير القانونيين.

مبادئ الأدلة الرقمية

كيف يعمل: أي جهاز كمبيوتر يتصل بموفر خدمة الإنترنت (ISP) جزءًا من شبكة مزود خدمة الإنترنت، سواء كان جهاز كمبيوتر واحدًا أو جزءًا من شبكة محلية (LAN) في مكان العمل .كل ISP يتصل بشبكة أخرى، وهكذا .وبهذه الطريقة، فإن الإنترنت عبارة عن شبكة من الشبكات حيث يمكن إرسال المعلومات واستلامها إلى أي نقطة على الويب من أي نقطة أخرى .هذه المجموعة العالمية من الشبكات ليس لها "مالك" أو شبكة تحكم عامة، لذا فهي تعمل كمجتمع به جميع الإيجابيات والسلبيات التي قد تجدها في أي مجتمع آخر.

بسبب الوصول العالمي إلى المعلومات وأجهزة الكمبيوتر الأخرى، يمكن للمجرمين استخدام هذا الوصول لاختراق الأنظمة المالية وأنظمة الاتصالات والشركات الكبرى والشبكات الحكومية لسرقة الأموال والهويات والمعلومات أو لتخريب الأنظمة .يتمثل أحد أكبر التحديات في جرائم الإنترنت في أن يفهم المحققون والمختبرات والموظفون الفنيون كيفية سير العملية ويظلوا منخرطين بشكل وثيق مع التطورات في البرمجيات وتقنيات التتبع.

الأدلة الرقمية

أجهزة الكمبيوتر :في أواخر السبعينيات، استخدم الموظفون في Flagler Dog Track في فلوريدا جهاز كمبيوتر لإنشاء وطباعة تذاكر فائزة احتيالية .دفع هذا بولاية فلوريدا إلى سن أول قانون لجرائم الكمبيوتر، قانون جرائم الكمبيوتر في فلوريدا ، الذي أعلن أن الاستخدام غير المصرح به لمنشآت الحوسبة جريمة .اتبعت القوانين الفيدرالية في عام 1984.

الأجهزة المحمولة :على الرغم من أن أجهزة الإرسال الصوتي المحمولة التي تستخدم الإرسال اللاسلكي مستخدمة منذ الأربعينيات) جهاز (Walkie-Talkie ، فإن الإصدار الأول مما نسميه الآن بالهاتف الخلوي لم يتم تطويره حتى الثمانينيات .ارتفع استخدام الهواتف المحمولة في جميع أنحاء العالم في التسعينيات ووصل إلى 4.6 مليار اشتراك في الهواتف المحمولة بنهاية عام 2009. وقد توسعت تكنولوجيا الهواتف المحمولة واللاسلكية لتشمل العديد من أنواع الأجهزة المحمولة مثل أجهزة الكمبيوتر اللوحية وألعاب الفيديو المحمولة باليد.

لماذا و متى يتم فحص الأدلة الرقمية؟

قد تلعب الأدلة الرقمية دورًا في أي تحقيق جنائي خطير مثل القتل والاغتصاب والمطاردة وسرقة السيارات والسطو وإساءة معاملة الأطفال أو استغلالهم والتزوير والابتزاز والقمار، والقرصنة، وجرائم الملكية، والإرهاب .

معلومات ما قبل الجريمة وما بعدها هي الأكثر صلة بالموضوع، على سبيل المثال، إذا كان المجرم يستخدم برنامجًا عبر الإنترنت مثل Google Maps ™ أو التجوّل الافتراضي قبل ارتكاب جريمة؛ أو نشر العناصر المسروقة للبيع على مواقع التسوق الالكتروني والشراء عبر الانترنت أو التواصل عبر الرسائل النصية مع المتواطئين للتخطيط لجريمة ما أو تهديد شخص ما .يمكن ارتكاب بعض الجرائم بالكامل من خلال الوسائل الرقمية، مثل قرصنة الكمبيوتر أو الاحتيال الاقتصادي أو سرقة الهوية.

لماذا و متى يتم فحص الأدلة الرقمية؟

كيف يتم ذلك؟

دليل يمكن جمعه رقمياً:

تعد مستندات الكمبيوتر ورسائل البريد الإلكتروني والرسائل النصية والرسائل الفورية والمعاملات والصور وتاريخ الإنترنت أمثلة على المعلومات التي يمكن جمعها من الأجهزة الإلكترونية واستخدامها بشكل فعال كدليل .على سبيل المثال، تستخدم الأجهزة المحمولة أنظمة النسخ الاحتياطي المستندة إلى الإنترنت، والمعروفة أيضًا باسم "السحابة" cloud، والتي توفر لمحققين ادلة الجنائية إمكانية الوصول إلى الرسائل النصية والصور المأخوذة من هاتف معين .تحتفظ هذه الأنظمة بمتوسط 1000-1500 أو أكثر من الرسائل النصية الأخيرة المرسلة والمستلمة من هذا الهاتف.

لماذا و متى يتم فحص الأدلة الرقمية؟

من يقوم بالتحليل؟

بحسب **المعهد الوطني للعدالة**، "يجب فحص الأدلة الرقمية فقط من قبل أولئك المدربين خصيصًا لهذا الغرض ".مع وجود مجموعة متنوعة من الأجهزة الإلكترونية المستخدمة اليوم والسرعة التي تتغير بها ، يمكن أن تكون مواكبة هذه الأجهزة صعبة للغاية بالنسبة لتطبيق القانون المحلي .

لا يوجد لدى العديد من الوكالات خبير في الأدلة الرقمية، وإذا كان الأمر كذلك ، فقد يكون الضابط متخصصًا في الهواتف المحمولة ولكن ليس في وسائل التواصل الاجتماعي أو الاحتيال المصرفي .قد يكون المحقق قادرًا على تسجيل الدخول إلى مواقع التسوق الالكتروني او مواقع الشراء عبر الانترنت والبحث عن الممتلكات المسروقة ولكنه قد يكون غير قادر على التقاط سجلات الرسائل النصية للهاتف الخلوي ويمكن أن يدمر الأدلة بمجرد المحاولة .

يهتم الكثيرون بالمنطقة ويتعلمون ما في وسعهم، ولكن لا يوجد مسار واحد لخبرة الأدلة الرقمية - فالمؤهلات والشهادات ليست موحدة في جميع أنحاء البلاد.

لماذا و متى يتم فحص الأدلة الرقمية؟

من يقوم بالتحليل؟

تمتلك معظم الولايات مختبرًا أو قسمًا واحدًا على الأقل للأدلة الجنائية الرقمية ومجموعة متنوعة من فرق العمل بما في ذلك جرائم الإنترنت ضد الأطفال Internet crimes against children (ICAC)، وفرقة العمل المشتركة لمكافحة الإرهاب Joint Anti-Terrorism Task Force (JTTF)، وجرائم المخدرات والممتلكات .تتكون هذه القوات من ضباط ذوي تدريب متخصص، بما في ذلك البحث عن الأدلة الرقمية وضبطها واستغلالها من حيث صلتها بمجال خبرتهم .

يجب أن تعمل الوكالات والمحققون معًا لضمان استخدام أعلى مستوى من الأمان ومعالجة الأدلة .مثلاً في الولايات المتحدة، يمكن لمكتب التحقيقات الفيدرالي تقديم المساعدة في بعض المجالات المتخصصة.

كيف يتم تجميع الأجهزة الرقمية؟

في المشهد :كما يعلم أي شخص أسقط هاتفًا خلويًا في بحيرة أو تعرض جهاز الكمبيوتر الخاص به لأضرار في حركة أو عاصفة رعدية، فإن المعلومات المخزنة رقميًا حساسة للغاية ويمكن فقدها بسهولة .

هناك أفضل الممارسات العامة، التي طورتها منظمات مثل SWGDE و NIJ ، للاستيلاء على الأجهزة وأجهزة الكمبيوتر بشكل صحيح .بمجرد أن يتم تأمين المشهد وتأكيد السلطة القانونية لضبط الأدلة، يمكن جمع الأجهزة .يجب جمع أي كلمات مرور أو رموز أو أرقام PIN من الأفراد المعنيين، إن أمكن، ويجب جمع أجهزة الشحن والكابلات والأجهزة الطرفية والأدلة المرتبطة بها .يتم فحص محركات الأقراص والهواتف المحمولة والأقراص الصلبة وما شابه ذلك باستخدام أدوات وتقنيات مختلفة، وغالبًا ما يتم ذلك في مختبر متخصص.

كيف يتم تجميع الأجهزة الرقمية؟

ضبط الأجهزة المحمولة:

يجب إيقاف تشغيل الأجهزة على الفور وإزالة البطاريات إن أمكن .

يؤدي إيقاف تشغيل الهاتف إلى الاحتفاظ بمعلومات موقع برج الهاتف الخلوي وسجلات المكالمات، ويمنع استخدام الهاتف، مما قد يؤدي إلى تغيير البيانات الموجودة على الهاتف .بالإضافة إلى ذلك، إذا ظل الجهاز قيد التشغيل، فيمكن استخدام أوامر التدمير عن بُعد دون علم المحقق .تحتوي بعض الهواتف على مؤقت تلقائي لتشغيل الهاتف للحصول على التحديثات، مما قد يعرض البيانات للخطر، لذا فإن إزالة البطارية هي الأمثل.

كيف يتم تجميع الأجهزة الرقمية؟

الاستيلاء على أجهزة الكمبيوتر والأجهزة المستقلة :

لمنع تغيير الأدلة الرقمية أثناء الجمع، يجب أولاً على المستجيبين توثيق أي نشاط على الكمبيوتر أو المكونات أو الأجهزة عن طريق التقاط صورة وتسجيل أي معلومات على الشاشة .يمكن للمستجيبين تحريك الماوس (بدون الضغط على الأزرار أو تحريك العجلة) لتحديد ما إذا كان هناك شيء ما على الشاشة .إذا كان الكمبيوتر قيد التشغيل، يوصى بشدة بالاتصال بخبير في ادلة الجنائية للكمبيوتر حيث قد يتم فقد الاتصالات بالنشاط الإجرامي عن طريق إيقاف تشغيل الكمبيوتر .إذا كان الكمبيوتر قيد التشغيل، ولكنه يشغل برنامجًا مدمرًا (تنسيق المعلومات أو حذفها أو إزالتها أو مسحها)، فيجب فصل الطاقة عن الكمبيوتر على الفور للحفاظ على ما تبقى على الجهاز.

كيف و أين يتم اجراء التحليل؟

استغلال البيانات في المختبر :بمجرد إرسال الدليل الرقمي إلى المختبر، سيتخذ المحلل المؤهل الخطوات التالية لاسترداد البيانات وتحليلها:

1- **منع التلوث:** من السهل فهم التلوث المتبادل في مختبر الحمض النووي أو في مسرح الجريمة ، لكن الأدلة الرقمية لها مشكلات مماثلة يجب منعها من قبل ضابط الجمع .قبل تحليل الأدلة الرقمية، يتم إنشاء صورة أو نسخة عمل من جهاز التخزين الأصلي .عند جمع البيانات من جهاز مشتبه به ، يجب تخزين النسخة على شكل آخر من الوسائط للحفاظ على الأصل الأصلي .يجب أن يستخدم المحللون وسائط تخزين "نظيفة" لمنع التلوث أو إدخال البيانات من مصدر آخر.

على سبيل المثال: إذا قام المحلل بوضع نسخة من الجهاز المشتبه فيه على قرص مضغوط يحتوي بالفعل على معلومات، فقد يتم تحليل هذه المعلومات كما لو كانت على الجهاز المشتبه فيه.

كيف و أين يتم اجراء التحليل؟

2.**عزل الأجهزة اللاسلكية :**يجب فحص الهواتف المحمولة والأجهزة اللاسلكية الأخرى مبدئيًا في غرفة عزل ، إذا كانت متوفرة .هذا يمنع الاتصال بأي شبكات ويحافظ على الأدلة بأكبر قدر ممكن .يمكن فتح حقيبة Faraday داخل الغرفة ويمكن استغلال الجهاز، بما في ذلك معلومات الهاتف وبطاقات SIM وما إلى ذلك. يمكن توصيل الجهاز ببرنامج التحليل من داخل الغرفة .إذا لم يكن لدى الوكالة غرفة عزل، فعادة ما يضع المحققون الجهاز في حقيبة فاراداي ويحولون الهاتف إلى وضع الطائرة لمنع الاستقبال.

حقيبة فارداي أو قفص فاراداي هو عبارة عن هيكل فلزي مصنوع من مادة موصلة، تستخدم لعزل ما بداخله عن المؤثرات الكهرومغناطيسية والمؤثرات الكهربية الخارجية. وقد سمي قفص فاراداي تيمناً بمكتشفه الكيميائي والفيزيائي الإنجليزي مايكل فاراداي والذي قام باختراعه عام 1836 .

كيف و أين يتم اجراء التحليل؟

3. **تثبيت برنامج حظر الكتابة :**لمنع أي تغيير في البيانات الموجودة على الجهاز أو الوسائط ، سيقوم المحلل بتثبيت كتلة على نسخة العمل بحيث يمكن عرض البيانات ولكن لا يمكن تغيير أو إضافة أي شيء.

4. **تحديد طرق الاستخراج :**بمجرد إنشاء نسخة العمل ، سيحدد المحلل طراز الجهاز وطرازه ويختار برنامج الاستخراج المصمم "لتحليل البيانات" بشكل كامل أو عرض محتوياته.

5. **إرسال الجهاز أو الوسائط الأصلية لفحص الأدلة التقليدية :**عند إزالة البيانات ، يتم إرسال الجهاز مرة أخرى كدليل .قد يكون هناك حمض نووي، أو أثر أو بصمة أو أي دليل آخر يمكن الحصول عليه منه ويمكن للمحلل الرقمي الآن العمل بدونه .تعرف على المزيد حول **الحمض النووي** أو **تتبع الأدلة** أو **بصمات** الأصابع.

كيف و أين يتم اجراء التحليل؟

6. **متابعة التحقيق :** في هذه المرحلة ، سيستخدم المحلل البرنامج المحدد لعرض البيانات .سيتمكن المحلل من رؤية جميع الملفات الموجودة على محرك الأقراص، ويمكنه معرفة ما إذا كانت المناطق مخفية وقد يكون قادرًا على استعادة تنظيم الملفات مما يسمح بعرض المناطق المخفية .تكون الملفات المحذوفة مرئية أيضًا، طالما لم يتم الكتابة فوقها بواسطة بيانات جديدة .يمكن أن تكون الملفات المحذوفة جزئيًا ذات قيمة أيضًا.

الملفات الموجودة على جهاز كمبيوتر أو أي جهاز آخر ليست هي الدليل الوحيد الذي يمكن جمعه .قد يضطر المحلل إلى العمل خارج الأجهزة للعثور على دليل موجود على الإنترنت بما في ذلك غرف الدردشة والرسائل الفورية ومواقع الويب والشبكات الأخرى للمشاركين أو المعلومات .باستخدام نظام عناوين الإنترنت ومعلومات رأس البريد الإلكتروني والطوابع الزمنية على الرسائل وغيرها من البيانات المشفرة، يمكن للمحلل تجميع سلاسل من التفاعلات التي توفر صورة للنشاط.

أسئلة و أجوبة

ما نوع النتائج التي يمكن توقعها من تحليل الأدلة الرقمية؟

إذا تم جمع الأدلة وتحليلها بشكل صحيح، يمكن للفاحصين تأمين المعلومات التي يمكن أن تدعم دعاوى النشاط الإجرامي من خلال الحوار أو تبادل الرسائل والصور والوثائق .سيقدم الفاحص بشكل عام جميع الوثائق الداعمة، مع إبراز المعلومات ذات الصلة ، ولكن أيضًا تقريرًا يوضح بالتفصيل ما تم القيام به لاستخراج البيانات .كما هو الحال مع الأدلة من الأنواع الأخرى، تعتبر سلسلة العهدة وأساليب الجمع والاستخراج المناسبة أمرًا بالغ الأهمية لمصداقية الأدلة ويجب توثيقها بدقة.

أسئلة و أجوبة

ما هي القيود المتعلقة بالأدلة التي يمكن الحصول عليها من الأجهزة الرقمية؟

ترجع القيود الاستقصائية في المقام الأول إلى التشفير والأنظمة الاحتكارية التي تتطلب فك التشفير قبل حتى الوصول إلى البيانات .على عكس ما يتم تصويره في برامج الجريمة التلفزيونية الشهيرة، يمكن أن يستغرق فك تشفير كلمة مرور مشفرة وقتًا طويلاً جدًا، حتى مع البرامج المتطورة.

ناك قيود قانونية وتقنية في هذا المجال من التحقيق .تختلف القوانين التي تحكم المعالجة والمقاضاة من دولة إلى أخرى .

يمكن للجريمة الرقمية أن تتخطى الولايات القضائية بسهولة، مما يجعل التوحيد مسألة حاسمة بشكل متزايد لإنفاذ القانون.

أسئلة و أجوبة

يمكن أن تكون ملكية البيانات مشكلة أيضًا .في حكم صدر مؤخرًا في كولورادو، أُجبر صاحب كلمة المرور على الكشف عن كلمة المرور ، ولكن عند القيام بذلك لم يكن عليه الاعتراف بمعرفة أو ملكية البيانات المحمية بكلمة المرور . هذا يشبه قدرة المالك على فتح شقة مستأجرة دون أي مسؤولية عما قد يكون داخل الشقة .في هذه الحالة، سيظل الأمر متروكًا للمحقق لربط الاثنين معًا.

يمكن أيضًا أن تدخل قوانين التنصت على المكالمات الهاتفية حيز التنفيذ خاصة فيما يتعلق بمصادرة الهواتف المحمولة .اعتراض مكالمة بدون أمر من المحكمة ينتهك توقع الخصوصية .حتى بعد الاستيلاء على الهاتف، لا يمكن استخدام أي مكالمات أو رسائل يتلقاها هذا الهاتف لأن حاملي الهاتف ليسوا المستلمين المقصود.

أسئلة و أجوبة

المبادئ التوجيهية للمصادقة على الأدلة وسلامتها:

1. لا ينبغي لأي إجراء تتخذه وكالات إنفاذ القانون أو وكلائها تغيير البيانات الموجودة على جهاز كمبيوتر أو وسائط تخزين والتي يمكن الاعتماد عليها لاحقًا في المحكمة.
2. في ظروف استثنائية، عندما يجد الشخص أنه من الضروري الوصول إلى البيانات الأصلية المحفوظة على جهاز كمبيوتر أو على وسائط التخزين، يجب أن يكون هذا الشخص مؤهلاً للقيام بذلك وأن يكون قادرًا على تقديم أدلة تشرح أهمية وتأثيرات أفعاله.
3. يجب إنشاء مسار تدقيق أو سجل آخر لجميع العمليات المطبقة على الأدلة الإلكترونية القائمة على الكمبيوتر والمحافظة عليه .يجب أن يكون الطرف الثالث المستقل قادرًا على فحص هذه العمليات وتحقيق نفس النتيجة.
4. يتحمل الشخص المسؤول عن التحقيق (ضابط الحالة) المسؤولية الكاملة عن ضمان الالتزام بالقانون وهذه المبادئ.

يتم قبول هذه الإرشادات على نطاق واسع في محاكم إنجلترا واسكتلندا، لكنها لا تشكل مطلبًا قانونيًا واستخدامها طوعي.

أسئلة و أجوبة

كيف يتم تنفيذ مراقبة الجودة والتأكيد؟

تتشابه مراقبة الجودة والتأكيد مع تخصصات الادلة الجنائية الأخرى من حيث إن المختبر يجب أن يكون لديه إرشادات ويتبعها بالإضافة إلى المستجيبين والمحللين .

تجمع مجموعة العمل العلمية حول الأدلة الرقمية SWGDE :The Scientific Working Group on Digital Evidence بين المنظمات المشاركة بنشاط في مجال الأدلة الرقمية والوسائط المتعددة في الولايات المتحدة ودول أخرى لتعزيز التواصل والتعاون وكذلك لضمان الجودة والاتساق داخل مجتمع الادلة الجنائية

تم الاستشهاد بالممارسات من قبل(المعهد الأوروبي لعلوم الادلة الجنائية - مجموعة عمل تكنولوجيا المعلومات الجنائية) :

ENFSI: European Institute of Forensic Sciences

FITWG: Forensic Information Technology Working Group

أسئلة و أجوبة

ما هي المعلومات التي يتضمنها التقرير وكيف يتم تفسير النتائج؟

مثل أشكال الأدلة الأخرى، يجب أن تظل الأدلة الرقمية أصيلة وغير متغيرة .في قاعة المحكمة، من المرجح أن يتم مشاركة الرسائل النصية على الهاتف الفعلي أو الجهاز الرقمي، ولكن قد تتم طباعة أدلة أخرى ، مثل سلسلة من رسائل البريد الإلكتروني أو رؤوس البريد الإلكتروني.
يمكن أن يُظهر هذا سجل تتبع لتبادل المعلومات، و "قيمة التجزئة" **Hash Value** ، والتي يشار إليها أيضًا باسم المجموع الاختباري أو رمز التجزئة أو التجزئة **Hash or Hash Value** ، هي علامة الأصالة ويجب أن تكون حاضرة و للمشاركين في قاعة المحكمة.

قيمة التجزئة **Hash Value** هي نتيجة عملية حسابية (خوارزمية تجزئة) يتم إجراؤها على سلسلة نصية أو ملف إلكتروني أو محتويات القرص الصلب بالكامل .

أسئلة و أجوبة

```
Received: from SERVERNAME-Exch1.place.com ([172.16.102.10]) by SERVERNAME-exch1
 ([172.16.102.10]) with mapi; Mon, 27 Feb 2012 09:53:10 -0500
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Bad Guy  Bad.Guy@place.com
To: Worse Guy worse.guy@place.com
Date: Mon, 27 Feb 2012 09:53:09 -0500
Subject: Here's the plan
Thread-Topic: Here's the plan
Thread-Index: Acz1X4VRzKScTInUTWSTqYrRhGJhqg==
Message-ID: <2E95727AD62F534E9A60644CAB99079D011790B7E201@servername-exch1>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <2E95727AD62F534E9A60644CAB99079D011790B7E201@server-exch1>
MIME-Version: 1.0
```

أسئلة و أجوبة

ما هي المعلومات التي يتضمنها التقرير وكيف يتم تفسير النتائج؟

تُستخدم قيم التجزئة لتحديد الملفات المكررة وتصفيتها (مثل البريد الإلكتروني والمرفقات والملفات غير الثابتة) من مصدر معين والتحقق من التقاط صورة شرعية أو نسخة طبق الأصل بنجاح .على سبيل المثال، يجب أن تنشئ وظيفة التجزئة التي يتم إجراؤها على محرك الأقراص الثابتة للمشتبه به تقرير قيمة التجزئة الذي يتطابق تمامًا مع التقرير الذي تم إنشاؤه باستخدام نفس الخوارزمية على صورة محرك الأقراص الثابتة، والتي يتم إنشاؤها عادةً بواسطة المختبر لاستخدامها في التحقيق.

قيم التجزئة المحسوبة للسلسلة النصية "علم الادلة الجنائية ."يحتوي كل سطر على قيمة مصطلح البحث المحسوبة باستخدام الخوارزمية الفريدة في العمود الأيسر .اضغط على الصورة لعرض أكبر.

تعد قيم التجزئة طريقة موثوقة وسريعة وآمنة لمقارنة محتويات الملفات والوسائط الفردية .سواء كان ملفًا نصيًا واحدًا يحتوي على رقم هاتف أو خمسة تيرابايت من البيانات على الخادم، فإن حساب قيم التجزئة هو عملية لا تقدر بثمن للتحقق من الأدلة في الاكتشاف الإلكتروني وادلة الجنائية للكمبيوتر

أسئلة و أجوبة

هل هناك أي مفاهيم خاطئة حول الأدلة الرقمية؟

يمكن دائمًا استرداد أي شيء على القرص الصلب أو الوسائط الإلكترونية الأخرى .هذا غير صحيح لأن الملفات المكتوبة بشكل زائد عن الحد أو التالفة، أو التلف المادي للوسائط يمكن أن يجعله غير قابل للقراءة .قد تتمكن المعامل عالية التخصص مع الغرف النظيفة من فحص مكونات القرص الصلب وإعادة تكوين البيانات، ولكن هذه العملية شاقة للغاية ومكلفة للغاية.

يعد فك تشفير كلمة المرور أمرًا سريعًا وسهلاً، باستخدام البرنامج المناسب .مع التعقيد المتزايد لكلمات المرور بما في ذلك الأحرف الكبيرة والأرقام والرموز وطول كلمة المرور، هناك مليارات من كلمات المرور المحتملة .يمكن أن يستغرق فك التشفير وقتًا طويلاً يصل إلى عام في بعض الحالات، وذلك باستخدام موارد النظام وتعطيل التحقيقات .يعد جمع كلمات المرور من المتورطين في إحدى القضايا أكثر فاعلية ويجب القيام به كلما أمكن ذلك.

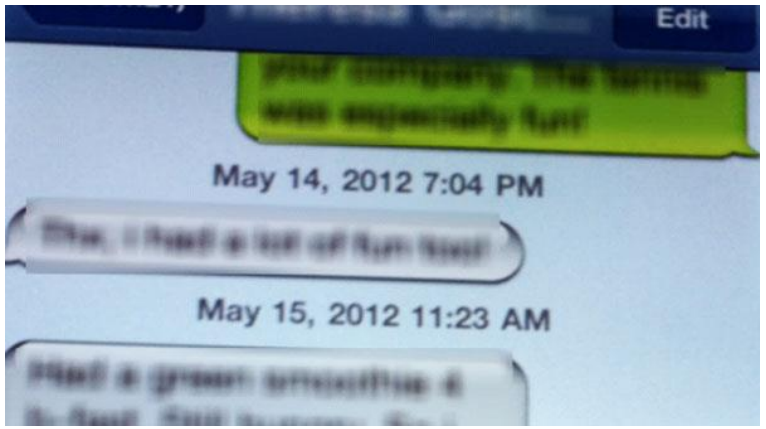
أسئلة و أجوبة

هل هناك أي مفاهيم خاطئة حول الأدلة الرقمية؟

يمكن تحسين أي صورة رقمية إلى جودة عالية الوضوح: يمكن أن تكون الصور مفيدة جدًا في التحقيقات، ولكن يتم إنشاء صورة منخفضة الدقة عن طريق التقاط عدد أقل من وحدات البيانات (وحدات البيكسل) من الصور عالية الدقة .لا يمكن تحسين وحدات البيكسل غير الموجودة في المقام الأول.

يمكن للمحققين الاطلاع على الأدلة الرقمية في مسرح الجريمة أو في أي وقت مجرد النظر إلى قائمة الملفات لا يضر بالأدلة: من الأهمية بمكان ملاحظة أن فتح الملفات أو عرضها أو النقر عليها يمكن أن يضر بشدة بمعلومات ادلة الجنائية لأنه يمكن أن يغير تاريخ الوصول الأخير لملف أو قطعة من الأجهزة .يغير هذا الملف الشخصي

أسئلة و أجوبة



ويمكن اعتباره تلاعبًا بالأدلة أو حتى يجعله غير مقبول تمامًا .يجب فقط على المحققين الذين لديهم الأدوات والتدريب المناسبين عرض الأدلة واستعادتها.

تدريب المستجيب الأول يتخلف عن التطورات في مجال الإلكترونيات: دون تحديثات منتظمة لتدريبهم، قد لا يكون المستجيبون على دراية بالأجهزة الرقمية الجديدة التي قد تكون قيد الاستخدام وخاضعة للتجميع .على سبيل المثال، يجب أن يكون هناك وعي بأن محركات الأقراص المصغرة وبطاقات SD يمكن إزالتها بسهولة والتخلص منها من قبل المشتبه به في سياق مواجهة مع سلطات إنفاذ القانون.

مصطلحات شائعة

الحوسبة السحابية - **Cloud Computing** البرامج والتطبيقات والتخزين الرقمي الذي يتم الوصول إليه على الإنترنت من خلال متصفح الويب أو تطبيق سطح المكتب أو تطبيق الهاتف المحمول .يتم تخزين البرنامج وبيانات المستخدم على خوادم في مكان بعيد.

البيانات -معلومات في شكل تناظري أو رقمي يمكن نقلها أو معالجتها.

استخراج البيانات **Data Extraction** -عملية تحدد المعلومات التي قد لا تظهر على الفور وتستعيدها.

التشفير **Encryption** -إجراء يحول النص العادي إلى رموز لمنع أي شخص باستثناء المستلم المقصود من فهم الرسالة.

تنسيق الملف **File Format**- الهيكل الذي يتم من خلاله تنظيم البيانات في ملف.

مصطلحات شائعة

مسح الادلة الجنائية - **Forensic Wipe** إجراء يمكن التحقق منه لتعقيم منطقة محددة من الوسائط الرقمية عن طريق الكتابة فوق كل بايت بقيمة معروفة؛ هذه العملية تمنع التلوث المتبادل للبيانات.

الأجهزة المحمولة (المحمولة) -**Handheld (Mobile) Devices** الأجهزة المحمولة هي أجهزة تخزين البيانات المحمولة التي توفر الاتصالات والتصوير الرقمي وأنظمة الملاحة والترفيه وتخزين البيانات وإدارة المعلومات الشخصية.

ملف Log File السجل - سجل الإجراءات والأحداث والبيانات ذات الصلة.

الوسائط - **Media** الكائنات التي يمكن تخزين البيانات عليها .يشمل محركات الأقراص الثابتة ومحركات الأقراص الثابتة والأقراص المضغوطة / أقراص DVD والأقراص المرنة وبطاقات SIM من الأجهزة المحمولة وبطاقات الذاكرة للكاميرات وما إلى ذلك.

مصطلحات شائعة

قيمة التجزئة أو التجزئة Hash or Hash Value -القيم العددية التي تمثل سلسلة نصية (مصطلح البحث)، يتم إنشاؤها بواسطة وظائف التجزئة (الخوارزميات) .تُستخدم قيم التجزئة للاستعلام عن كميات كبيرة من البيانات مثل قواعد البيانات أو محركات الأقراص الثابتة لمصطلحات معينة .في ادلة الجنائية، تُستخدم قيم التجزئة أيضًا لإثبات سلامة الأدلة الرقمية و / أو مقارنات التضمين والاستبعاد مقابل مجموعات القيم المعروفة.

البيانات الوصفية Metadata -البيانات، المضمنة بشكل متكرر في الملف ، والتي تصف ملفًا أو دليلًا ، والتي يمكن أن تتضمن المواقع التي تم تخزين المحتوى فيها ، والتواريخ والأوقات ، والمعلومات الخاصة بالتطبيق ، والأذونات .أمثلة: تحتوي رؤوس البريد الإلكتروني وشفرة مصدر موقع الويب على بيانات وصفية.

مصطلحات شائعة

قسم Partition -قسم معرّف من قبل المستخدم من الوسائط الإلكترونية .يمكن استخدام الأقسام لفصل وإخفاء المعلومات الموجودة على القرص الصلب.

كود المصدر - Source Code التعليمات المكتوبة بلغة البرمجة المستخدمة لبناء برنامج كمبيوتر.

نسخة العمل Work Copy -نسخة أو نسخة مكررة من التسجيل أو البيانات التي يمكن استخدامها للمعالجة اللاحقة و / أو التحليل .تسمى أيضًا صورة.

حماية الكتابة / الحماية Write Block/Write Protect ضد الكتابة - طرق الأجهزة و / أو البرامج لمنع تعديل المحتوى على وحدة تخزين وسائط مثل القرص المضغوط أو محرك USB

تحسين جمع الأدلة الرقمية

يمكن أن تلعب الأدلة الرقمية دورًا مهمًا في حل الجرائم وإعداد القضايا أمام المحاكم .ولكن في كثير من الأحيان يمكن للتعقيد والحجم الهائل للأدلة الموجودة على أجهزة الكمبيوتر والهواتف المحمولة والأجهزة الأخرى أن تطغى على المحققين من وكالات إنفاذ القانون.

أثناء التحقيق في مواد الاعتداء الجنسي على الأطفال المشتبه بها ، على سبيل المثال ، عادةً ما يقضي محلل الأدلة الجنائية الحاسوبي ساعات في مراجعة مئات مقاطع الفيديو من الوسائط المضبوطة .ينظر المحلل إلى ما إذا كان الإنسان موجودًا في صورة معينة .بعد ذلك ، يحتاج المحلل إلى تحديد ما إذا كان الإنسان في الصورة بالغًا أم طفلًا .هذه العملية تستغرق وقتًا طويلاً ومرهقة وعرضة للخطأ.

هذا مجرد مثال واحد على التحديات التي تواجه وكالات إنفاذ القانون عندما يتعلق الأمر بالأدلة الرقمية .تجد الإدارات في جميع أنحاء البلاد نفسها غير قادرة على مواكبة التقنيات سريعة التطور وكمية الأدلة الرقمية التي تنتجها .العديد من الإدارات لديها ميزانيات محدودة وتفتقر إلى المعدات المناسبة وفرص التدريب للضباط .غالبًا ما تكون النتيجة تراكمًا كبيرًا في تحليل الأدلة الرقمية .

الأدلة الرقمية والأدلة الجنائية

تُستخدم أجهزة الكمبيوتر لارتكاب الجرائم، وبفضل العلم المزدهر للالا دلة الجنائية الرقمية، يستخدم تطبيق القانون الآن أجهزة الكمبيوتر لمكافحة الجريمة.

الدليل الرقمي هو معلومات مخزنة أو منقولة في شكل ثنائي يمكن الاعتماد عليها في المحكمة .يمكن العثور عليها على القرص الصلب لجهاز الكمبيوتر، والهاتف المحمول، من بين أماكن أخرى .يرتبط الدليل الرقمي عادةً بالجرائم الإلكترونية أو الجرائم الإلكترونية، مثل المواد الإباحية المتعلقة بالأطفال أو الاحتيال على بطاقات الائتمان .ومع ذلك، تُستخدم الأدلة الرقمية الآن لمقاضاة جميع أنواع الجرائم ، وليس فقط الجرائم الإلكترونية .على سبيل المثال، قد تحتوي ملفات البريد الإلكتروني أو الهاتف المحمول الخاصة بالمشتبه بهم على أدلة مهمة فيما يتعلق بنواياهم ومكان وجودهم في وقت ارتكاب الجريمة وعلاقتهم بالمشتبه بهم الآخرين .في عام 2005، على سبيل المثال ، قاد قرص مرن المحققين إلى القاتل المتسلسل BTK الذي أفلت من القبض على الشرطة منذ عام 1974 وأودى بحياة 10 ضحايا على الأقل.

مناهج جديدة لاكتساب الأدلة الرقمية وتحليلها

في محاولة لمكافحة الجريمة الإلكترونية وجمع الأدلة الرقمية ذات الصلة لجميع الجرائم، تقوم وكالات إنفاذ القانون بدمج جمع وتحليل الأدلة الرقمية في بنيتها التحتية.

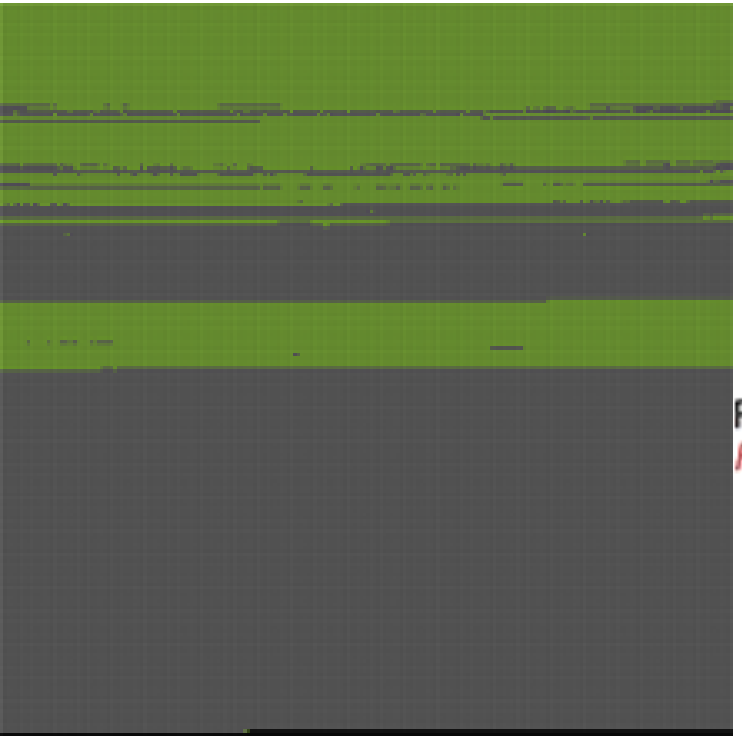
يتضمن الادلة الجنائية الرقمية بشكل أساسي عملية متتابعة من ثلاث خطوات:

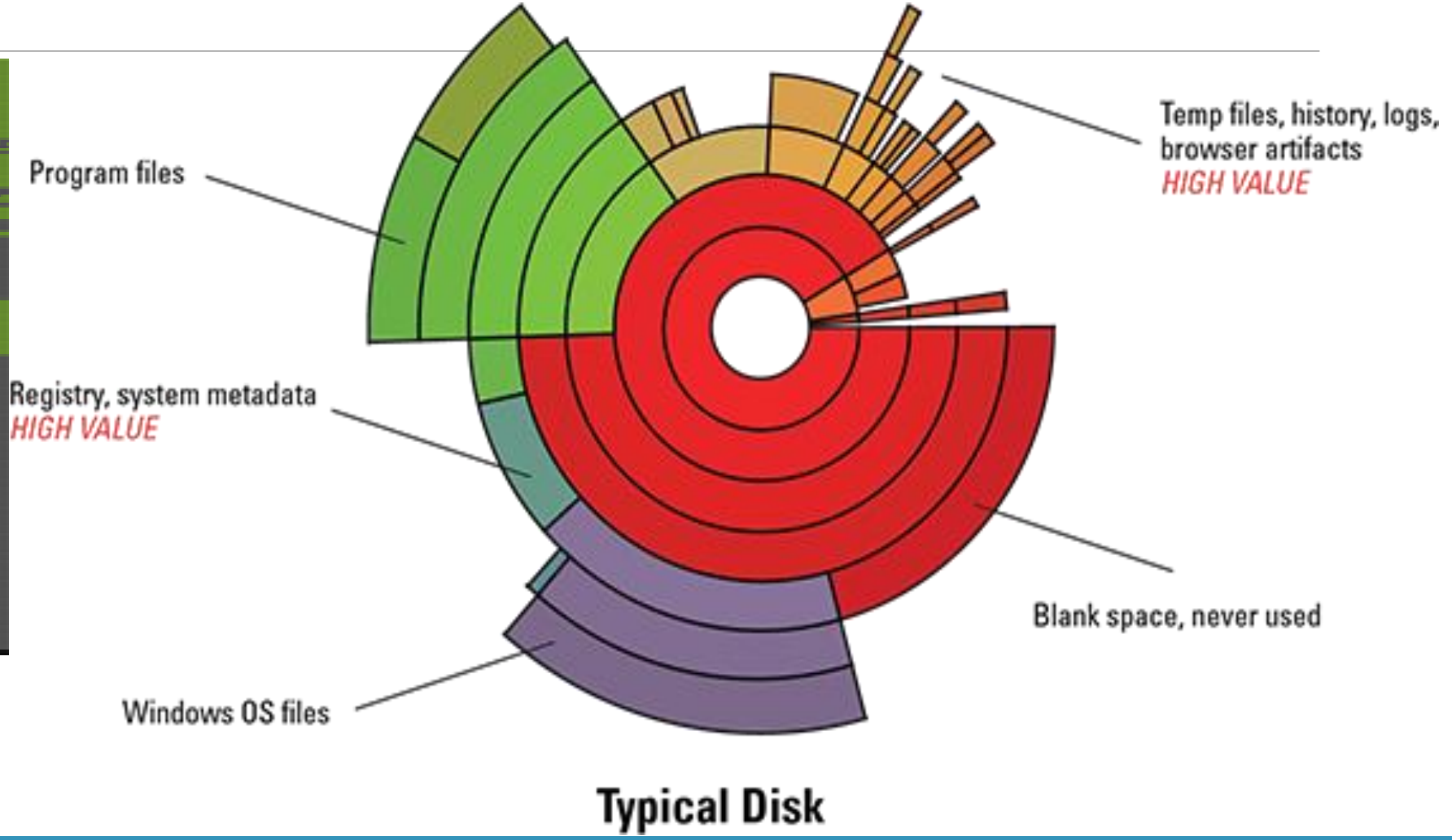
- الاستيلاء على الوسائط.
- اكتساب الوسائط؛ أي تكوين صورة جنائية للوسائط لفحصها.
- تحليل صورة الادلة الجنائية للوسائط الأصلية .يضمن ذلك عدم تعديل الوسائط الأصلية أثناء التحليل ويساعد في الحفاظ على القيمة الإثباتية للأدلة.

تحديد مناطق القرص التي قد تحتوي على أدلة

تنتج أدوات الحصول على القرص التقليدية صورة قرص تكون نسخة بت مقابل بت من الوسائط الأصلية .لذلك، إذا كان حجم قطعة الوسائط التي تم الحصول عليها 2 تيرابايت، فسيكون حجم صورة القرص المنتجة أيضًا 2 تيرابايت .ستتضمن صورة القرص جميع مناطق الوسائط الأصلية، حتى تلك الفارغة أو غير المستخدمة أو غير ذات الصلة بالتحقيق .وسيشمل أيضًا أجزاء كبيرة مخصصة لأنظمة التشغيل) على سبيل المثال ، Windows 10أو Mac OSX وتطبيقات الطرف الثالث والبرامج التي يوفرها البائعون مثل Microsoft أو Apple .

تحديد مناطق القرص التي قد تحتوي على أدلة





تحديد مناطق القرص التي قد تحتوي على أدلة

تم اقتراح أسلوبً جديد يقوم فقط بتصوير مناطق القرص التي قد تحتوي على أدلة .يُطلق عليه الاستحواذ السريع للأدلة الجنائية للوسائط الكبيرة مع جامعي الغربلة (الفرز) Sifting Collectors، يتخطى تطبيق البرنامج هذا المناطق التي تحتوي حصريًا على تطبيقات جهات خارجية غير معدلة ، وبدلاً من ذلك ، أصفار في المناطق التي تحتوي على البيانات والأدلة الأخرى

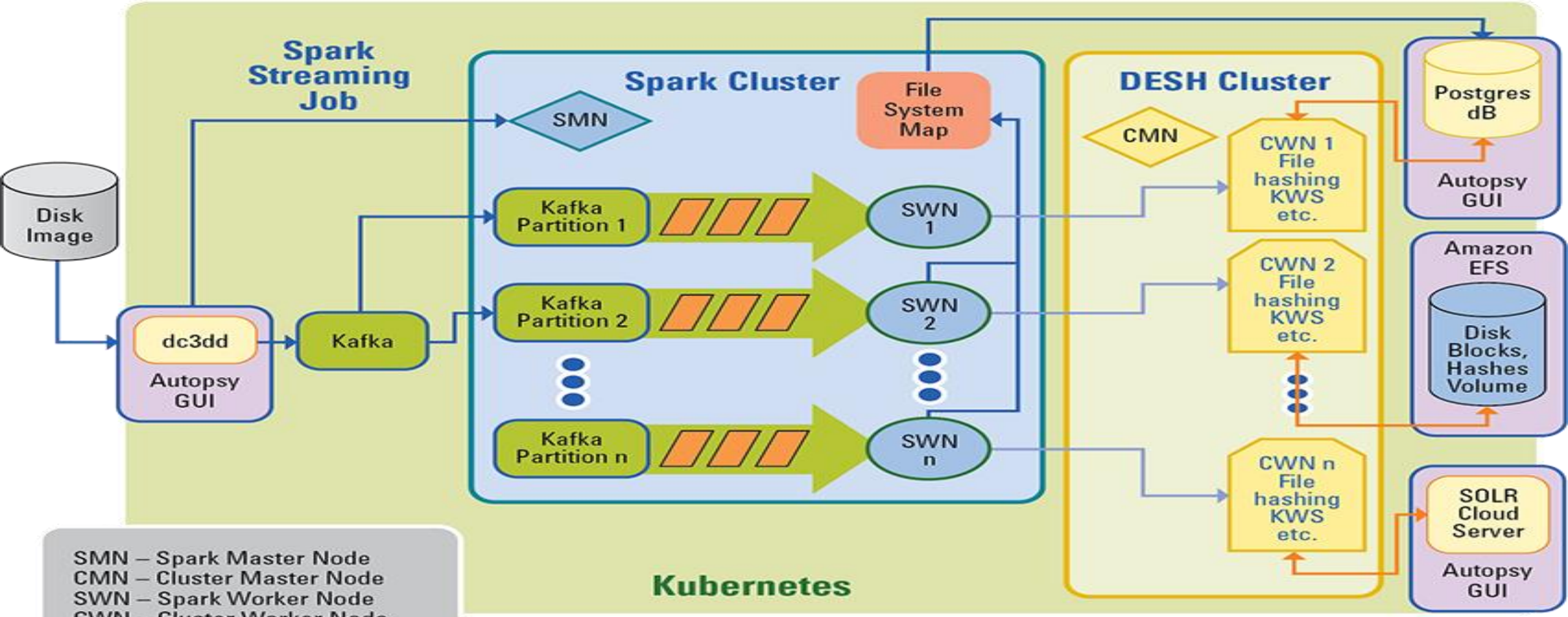
يمكن تكوين البرنامج بسهولة لتجميع تطبيقات الجهات الخارجية عند الضرورة لأنواع معينة من الحالات.

الشكل التوضيحي 2 عبارة عن تصور لمناطق القرص تم إنشاؤه بواسطة حزمة تشخيص .Sifting Collectors تمثل المناطق الخضراء الملفات التي أنشأها المستخدم وتمثل المناطق السوداء أجزاء من الوسائط لم يتم استخدامها مطلقًا.

يمتلك المنخلون القدرة على الحد بشكل كبير من تراكم الأعمال الجنائية الرقمية والحصول بسرعة على أدلة قيمة للأشخاص الذين يحتاجون إليها .في الاختبارات المعملية ، سرع من عملية التصوير ثلاث إلى 13 مرة بينما لا يزال ينتج 95 إلى 100 بالمائة من الأدلة.

الأكاديمية العربية الدولية
Arab International Academy

تسريع تحليل الأدلة الجنائية الرقمية



SMN – Spark Master Node
CMN – Cluster Master Node
SWN – Spark Worker Node
CWN – Cluster Worker Node
KWS – Key Word Search

تسريع تحليل الأدلة الجنائية الرقمية

كل عام ، يزداد الوقت المستغرق لإجراء تحقيقات الادلة الجنائية الرقمية مع استمرار زيادة حجم محركات الأقراص الثابتة .بدعم من معهد NIJ ، طورت مؤسسة RAND تطبيقًا مفتوح المصدر لمعالجة الأدلة الجنائية الرقمية مصممًا لتقليل الوقت المطلوب لإجراء تحليلات جنائية سليمة للبيانات المخزنة على أجهزة الكمبيوتر

يستفيد التطبيق ، المسمى Digital Forensics Compute Cluster (DFORC2) ، من قدرة المعالجة المتوازية للخوادم المستقلة عالية الأداء أو بيئات الحوسبة السحابية على سبيل المثال ، تم اختبارها على سحابة Amazon Web Services

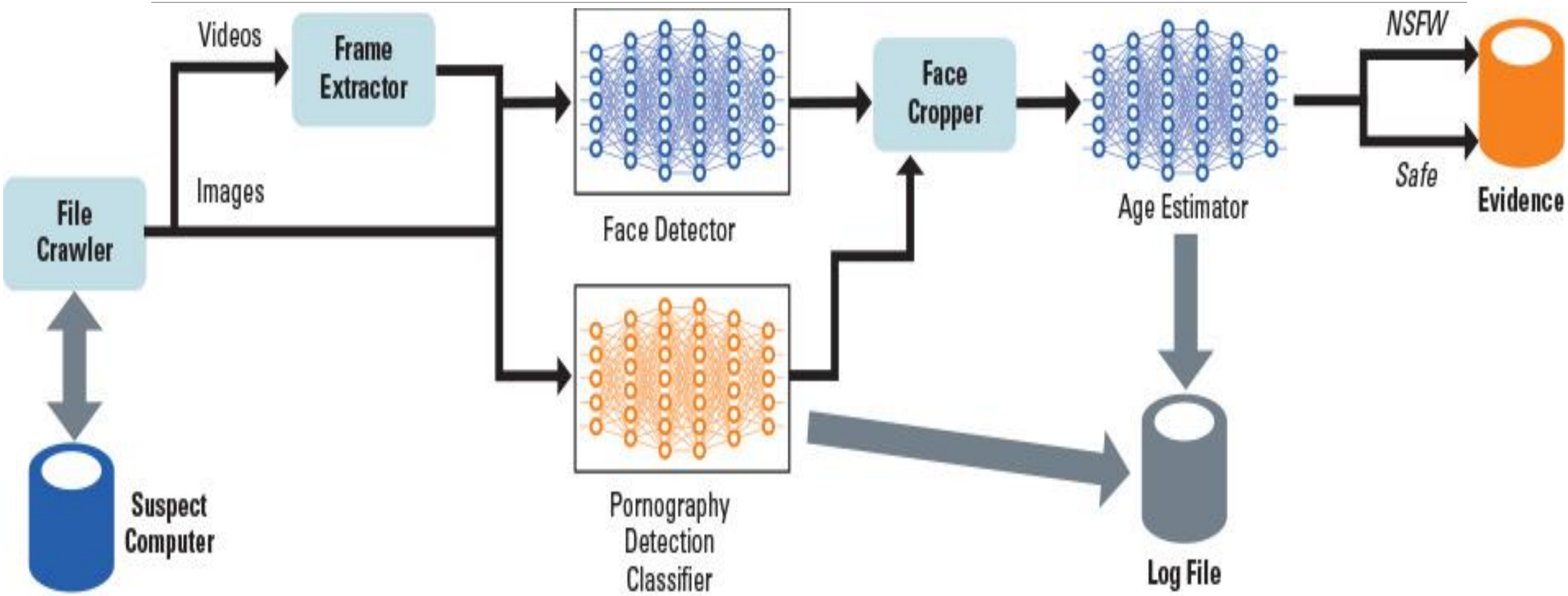
DFORC2 هو مشروع مفتوح المصدر .ويستخدم حزم برامج مفتوحة المصدر مثل التطبيقات:
(dc3dd, Apache Kafka, Apache Spark, Kubernetes Cluster Manager)

تسريع تحليل الأدلة الجنائية الرقمية

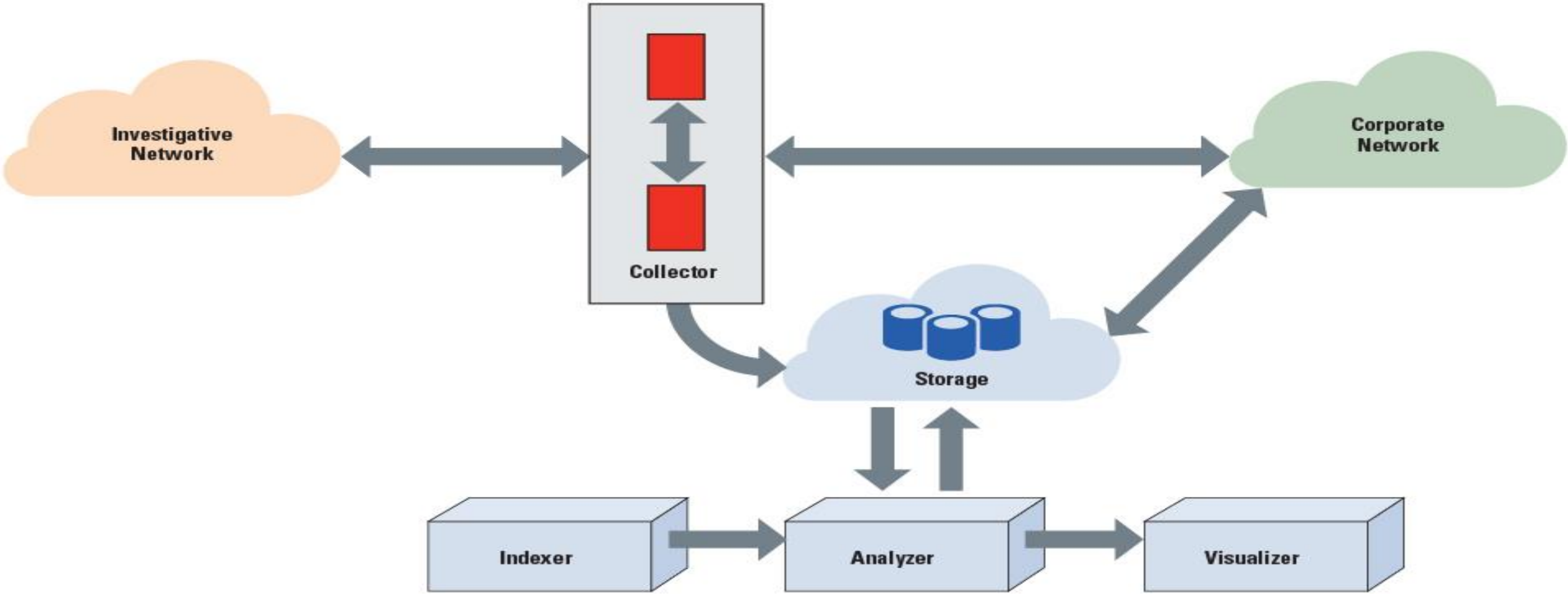
- التطبيق dc3dd الذي أنشأه مركز الجرائم الإلكترونية التابع لوزارة الدفاع ، قادر على تجزئة الملفات وكتل الأقراص "بشكل سريع جداً" أثناء قراءة القرص. يمكن تنزيل التطبيق على SourceForge
- Apache Kafka هي منصة معالجة تدفق مفتوحة المصدر توفر منصة موحدة وعالية الإنتاجية ومنخفضة الكمون للتعامل مع خلاصات البيانات في الوقت الفعلي.
- يوفر Apache Spark واجهة لبرمجة مجموعات كاملة مع توازي البيانات الضمني والتسامح مع الأخطاء.
- Kubernetes Cluster Manager عبارة عن نظام أساسي مفتوح المصدر يعمل على أتمتة نشر التطبيقات وتوسيع نطاقها وتشغيلها على مجموعات الحوسبة.

الأكاديمية العربية الدولية
Arab International Academy

اتمتة الكشف عن الصور



معالجة شبكات الكمبيوتر واسعة النطاق WAN



خلاصة

تشير المعلومات الأساسية إلى أنه على الرغم من أن مجال الأدلة الرقمية جديد نسبيًا، إلا أنه يتطلب التحقق من الصحة والاختبار باعتباره تخصصًا في الادلة الجنائية .غالبًا ما توفر الأدلة الرقمية رؤية أعمق للتحقيق في جريمة أو الدفاع عن الجاني المزعوم .تعكس التجارب ووجهات النظر تطور الأدوات والبيانات الرقمية في ارتكاب الجرائم، الأمر الذي تطلب تطوير أدوات التحقيق لجمع الأدلة الرقمية وتفسيرها والمصادقة عليها .تمت ملاحظة أن الأدلة الرقمية ركزت في البداية على أجهزة الكمبيوتر باعتبارها الجهاز الأساسي لتخزين ونقل الأدلة الرقمية المتعلقة بالجرائم وبالتالي التحقيقات؛ ومع ذلك، فقد تطورت الأجهزة الرقمية لتشمل الأجهزة المحمولة باليد وغيرها من الأجهزة المحمولة التي قد تقدم أدلة تتعلق بالموقع، ومقاطع الفيديو ، والصور .تضمنت التجارب أيضًا تطوير أدوات التحقيق والمعايير والتدريب والاعتماد في علم الادلة الجنائية وإنفاذ القانون الناتج عن الأنشطة الإجرامية المتطورة التي تنتج شكلاً من أشكال الأدلة الرقمية.

الأكاديمية العربية الدولية
Arab International Academy

شكراً لحضوركم

آمل ان تكونوا قد حققتم الفائدة