Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences & Forensic Medicine
المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي
https://journals.nauss.edu.sa/index.php/AJFSFM

Adapting Metadata as Supporting Evidence within Digital Forensic Investigations: A Proposed Model

تطويع الميتاداتا كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي: نموذج مقترح

أروى نصار الميلبي*

قسم علم المعلومات، جامعة الملك عبدالعزيز، جدة، المملكة العربية السعودية

Arwa Nassar Almailub*

Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Received 1 Feb. 2021; Accepted 10 Nov. 2021; Available Online 30 Dec. 2021

Abstract

In the globalized world that we are witnessing today, technology is part of the daily activities of many people, specifically forensic investigators who have come to obtain information that integrates with the investigation process through the Internet through many tools that integrate in different and varied forms to make technology applicable in the judicial system, and the digital forensic investigation process becomes more effective.

The current study gains its importance from the metadata that contributes to the digital forensic investigation, and achieves the integrative link between informational evidence, investigators, and the digital forensic investigation process, and how to deal with informational evidence to avoid its misuse to obstruct criminal investigations and to reveal the role of the EXIF Viewer Pro program in the process of extracting information through metadata. In a way that achieves promising justice. The study aims to clarify the importance of metadata in digital criminal investigation, and accordingly relied on the descriptive analytical approach, and used the EXIF Viewer Pro program to extract metadata

Keywords: Forensic Science, Metadata, Metadata Extraction Software, EXIF, EXIF Viewer Pro, Exchangeable Image File Format, Digital Images, Digital Forensics.

المستخلص

في عالم العولمة الذي نشهده اليوم، تعد التكنولوجيا جزءًا من الأنشطة اليومية للعديد من الأشخاص، وعلى وجه التحديد المحققون الجنائيون الذين أصبحوا يستقون المعلومات التي تتكامل مع عملية التحقيق من خلال شبكة الإنترنت عن طريق العديد من الأدوات التي تتكامل بأشكال مختلفة ومتنوعة لتجعل التكنولوجية قابلة للتطبيق في النظام القضائي، وتصبح عملية التحقيق الجنائي الرقمي أكثر فاعلية.

وتكتسب الدراسة الحالية أهميتها من الميتاداتا التي تسهم في التحقيق الجنائي الرقمي، وتحقق الترابط التكاملي بين الأدلة المعلوماتية والمحققين وعملية التحقيق الجنائي الرقمي، وكيفية التعامل مع الأدلة المعلوماتية لتفادي سوء استعمالها لعرقلة التحقيقات الجنائية والكشف عن دور برنامج EXIF Viewer Pro في عملية استخلاص المعلومات من خلال الميتاداتا بشكل يحقق العدالة الواعدة. وتهدف الدراسة إلى توضيح أهمية الميتاداتا في التحقيق الجنائي الرقمي، وبناءً على ذلك اعتمدت على المنهج الوصفي التحليلي، واستعانت في التطبيق ببرنامج EXIF Viewer

الكلمات المفتاحية: علوم الأدلة الجنائية، البيانات الوصفية، برمجيات استخراج الميتاداتا، EXIF Viewer Pro ، EXIF ، نماذج لملفات الصور القابلة للتبديل، الصور الرقمية، التحقيق الجنائي الرقمي.

* Corresponding Author: Arwa Nassar Almailub
Email: arwanassar.j@gmail.com

doi: 10.26735/FPFI3820

Pro لاستخراج الميتاداتا من الصور الرقمية. كما استطاعت الدراسة وضع توصيات لما يجب أخذه بعين الاعتبار، سواء من الباحثين عند تصميم حلول مماثلة، أو من المسؤولين عند التخطيط لاستخدامها، بحيث تكون فعالة للغاية.

أهم ما توصلت إليه الدراسة: تسهم برمجيات كشف الميتاداتا مثل EXIF Viewer Pro في توفير تحليل ودليل قوي يمنح اليقين والموثوقية بإصدار الأحكام بشأن القضايا الجنائية، بالإضافة لكون البرمجيات الحديثة مثل EXIF Viewer Pro لاستخراج الميتاداتا تُجيب عن الأسئلة (مَن، متى، كيف) للمحقق الجنائي، واستغنت البرمجيات الحديثة للكشف عن الميتاداتا عن عنصر الموقع الجغرافي؛ نظرًا لسوء استخدامها، وبالتالي لا تستطيع الإجابة بدقة عن التساؤل (أين) للمحقق الجنائي.

from digital images in the application. The study was also able to develop recommendations for what should be taken into consideration, whether from researchers when designing similar solutions, or from officials when planning to use them, so that they are very effective.

The most important findings of the study: Metadata detection software such as: EXIF Viewer Pro contributes to providing strong analysis and evidence that gives certainty and reliability in passing judgments on criminal cases, in addition to the fact that modern software for metadata extraction answers the questions (who, when, how) For forensic investigators, modern software dispense to detect metadata from the geolocation element; Due to its misuse, it cannot accurately answer the question (where) of the criminal investigator.

1. مقدمة

أصبح التحقيق الجنائي الرقمي موضوعًا مهمًّا في صلب الأبحاث القانونية؛ نظرًا لما يمثله من طبيعة مختلفة عن نظيره التقليدي، ولا سيما في طرق جمعه للأدلة الرقمية، والتزايد المطرد في التقنيات الحديثة المعتمدة على الحاسب بشكل أساسي؛ إذ يكاد في هذا العصر لا يخلو أي تحقيق جنائي دونما جمع المعلومات والبيانات الرقمية من الحواسيب أو الأجهزة النقالة أو وسائط التخزين (إسخيطة، 2019) وتتضمن الخطوة الحاسمة في أي تحليل للتحقيق الجنائي الدليل المعلوماتي القائم على جمع المعلومات وتحديد مصداقيتها، وكيف يمكن لهذه المعلومات أن تضيف قيمة في التحقيق الجنائي من حيث القرار الذي يمكن استنتاجه. وبشكل عام يجب أن يتضمن معلومات مثل: مَن فعل؟ وماذا؟ ومتى؟ وأين؟ (Salama, 2012).

لقد غيرت الثورة الصناعية الرابعة طرق التعامل في البيئة الرقمية، وفرضت البيانات الوصفية (الميتاداتا) دورًا فعالًا جديدًا في الأدلة المعلوماتية الرقمية باعتبار أنها توفر كمًّا ضخمًا من المعلومات للمحقق الشرعي عن الملفات التي يتم التحقيق بها، بالإضافة للفائدة التي تقدمها تلك البيانات الوصفية (الميتاداتا) في حل النزاعات الجنائية القضائية، ويمكن من خلالها إثبات أو دحض الأدلة الأخرى المقدمة (Alanazi & Jones, 2015)، ووفقًا للهيئة العامة للمحكمة العليا في المملكة العربية السعودية؛ فقد صدر القرار برقم 34 بتاريخ 1439/4/24هـ «بأن الدليل الرقمي حجة معتبرة في الإثبات متى سلم من العوارض، ويختلف قوةً وضعفًا حسب الواقعة وملابساتها وما يحيط بها من قرائن» وعليه يجب أن تُراعى الدقة أثناء التعامل مع الميتاداتا لاتخاذ القرارات؛ لأنها في معظم الأحيان معرضة للتلاعب، ويمكن تعديلها عمدًا وتأطير بياناتها من قبل أطراف أخرى (Bhangale, 2020).

أوضح هاينسون (heinson, 2015) أن الدلائل الرقمية والتحقيق الجنائي هما المستقبل القريب لعمليات البحث الجنائي في ضوء التغير الكبير في سلوكيات الأفراد تجاه استعمال التكنولوجيا في مناحي العمل والحياة كافة، ومن هنا أدرك التحقيق الجنائي الرقمي أهمية الميتاداتا؛ وعليه يمكن أن تكون الميتاداتا مفيدة للغاية في الإجابة عن بعض الأسئلة الأساسية للتحقيق الجنائي الرقمي؛ مثل: من فعل شيئًا لملف؟ ومتى فعل ذلك؟ وأين كان القيام به؟ وفي التحقيق الجنائي الرقمي تُستخدم المعلومات التي جُمِعت لتحليل الأحداث التي هي موضوع التحقيق (Salama, 2012).

1. 1 مشكلة الدراسة

تركزت مشكلة الدراسة في التعرف على إمكانات الميتاداتا ودورها الفعّال في إثبات الأدلة الرقمية أو رفضها في التحقيق الجنائي الرقمي؛ حيث سخرت الميتاداتا رؤية مختلفة للمحقق الشرعي في إعادة كتابة الأحداث المعينة بالتحقيق الجنائي الرقمي، بالإضافة لفاعلية الدليل المعلوماتي لارتباطها بالميادين المعقدة في القضاء؛ لأن الميدان الجنائي - كما وضح (إسخيطة، 2019)- مرتبط ارتباطًا وثيقًا بتحسين جودة الحياة، ويمكن صياغة مشكلة الدراسة في التساؤل الآتي: ما دور برمجيات EXIF Viewer Pro في استخراج الميتاداتا في التحقيق الجنائي الرقمي؟

1. 2 أهمية الدراسة

تستمد هذه الدراسة أهميتها من أهمية الدليل المعلوماتي الرقمي

الذي اكتسب أهمية بالغة إبان السنوات الأخيرة في عالم التقنيات الحديثة من أجل تسخير تلك الأدلة؛ لخدمة الميادين الأكثر حساسيةً واحتياجًا لتطويع برمجيات استخلاص الميتاداتا التي تساعد بشكل مباشر في إعادة كتابة الأحداث الجنائية؛ إذ تحولت الأدلة المعلوماتية المعتمدة على الميتاداتا في الأجهزة الذكية من أدلة غير مقبولة قضائيًا إلى أدلة يُدان بها، حتى أصبح يمكن الاعتماد عليها بما يكفي للوقوف في المحكمة وإقناع القاضي بالحجة. ومن هنا برزت أهمية الميتاداتا في إثبات صحة الأدلة المعلوماتية الرقمية؛ إذ تعدُّ عاملًا مهمًّا وأساسًيا في الحكم على صحة الدليل الجنائي، وعدّه دليلًا صحيحًا مكتمل الأركان.

1. 3 هدف الدراسة وتساؤلاتها

تهدف الدراسة إلى تسليط الضوء على إمكانات الميتاداتا في التحقيق الجنائي الرقمي، وتبيان دورها الفيصل في فض النزاعات الجنائية القضائية والقدرة من خلال الميتاداتا على إثبات الدليل المقدم أو دحضه؛ وذلك بواسطة برنامج لاستخلاص الميتاداتا من الأدلة الرقمية، وتسعى الدراسة للإجابة عن التساؤلات الآتية:

1. هل يوفر برنامج EXIF Viewer Pro لاستخراج الميتاداتا المصادقة على الصور الرقمية؟
2. ما مدى مساعدة برنامج EXIF Viewer Pro لاستخراج الميتاداتا المحقق الشرعي على إعادة كتابة الأحداث الجنائية بناءً على التساؤلات (مَن، متى، أين، كيف)؟

1. 4 مصطلحات الدراسة

- الميتاداتا Metadata

«مجموعة من البيانات التي تساعد في وصف الكيان، وتساعد على استرجاعه بأقل جهد ووقت ممكن في الشبكة العنكبوتية وفقًا لمعايير محددة مسبقًا» (الجهني، 2020).

- إخفاء البيانات Steganography

«استخدام طرق مختلفة يُراد بها إخفاء المعلومات عن طريق تضمين البيانات داخل الوسائط المتعددة (النص - الصورة - الفيديو) بطرق لا تثير شك المحقق الجنائي» (Dalal, 2020).

- التحقيق الجنائي الرقمي Digital Forensic Investigation

«استخدام التقنيات الحديثة لاستخراج أنواع البيانات من الأجهزة المختلفة وتحليلها والتي يفسرها المتخصصون بعد ذلك لتكون بمثابة دليل قانوني» (Vacca, 2005).

1. 5 المنهجية

فرضت طبيعة الدراسة الاعتماد على المنهج الوصفي التحليلي، لوصف واقع استخدام البرمجيات الحديثة لاستخلاص الميتاداتا؛ مثل: EXIF Viewer Pro وأهميتها في رفع كفاءة التحقيق الجنائي الرقمي، والاعتماد عليها كدليل معلوماتي مساند من خلال إعادة كتابة الأحداث التي وقعت، وتعدُّ هذه العملية الفيصل في التحقيق لاستخلاص استنتاجات موثوقة مستندة إلى الميتاداتا؛ وبناءً على ذلك اعتمدت الدراسة في التطبيق على برنامج EXIF Viewer Pro لاستخراج الميتاداتا من الصور الرقمية.

2. الإطار النظري

لقد غيرت الثورات الأربع المتتالية في الوقت الذي نعيشه اليوم طرق التعامل في البيئة الرقمية، وفرضت عددًا من القيود والاشتراطات، وهذا ما أدى إلى تغير حياة البشر وعملهم بطريقة فعالة، وذلك بمساعدة الكمبيوتر؛ بالإضافة إلى الجانب المظلم من تلك الأجهزة؛ إذ يستخدمها بعض الأشخاص لتنفيذ الهجمات الخبيثة التي تتراوح ما بين الاحتيال وسرقة الهوية إلى القرصنة والاختلاس وعدد لا يستهان به من الجرائم المعلوماتية، وقد حدثت الجرائم المعلوماتية الرقمية على مدار ما يقارب خمسين عامًا؛ حيث ظهرت بالتزامن مع الإنترنت وأجهزة الكمبيوتر التي سهلت بشكل أو آخر تحصيل الأدلة المعلوماتية من خلالها والمستندة إليها، والتي لا تختلف عن أشكال الأدلة الأخرى (Sivaprasad, 2012), ولكن هذا الدليل المعلوماتي في بداياته لم يلقَ اهتمامًا؛ إذ يثير الإثبات من خلال الدليل المعلوماتي، أو من خلال الوسائل الحديثة بالمقارنة مع طرق الإثبات القديمة عددًا من المشكلات التي نبعت بالأصل من طبيعة المجال التكنولوجي المعقد، الذي يمتاز بالتطور السريع والمستمر، ويجعل القضاء في مواجهة ميادين متجددة عما سبق في بقية وسائل الإثبات.

ويمكن تعريف الدليل المعلوماتي informational evidence على النحو الآتي:

أي مكون رقمي لتقديم المعلومات في مختلف الأشكال نتيجة التطور التكنولوجي، على أن تكون مخزنة في أجهزة الحاسوب أو الملحقات به، مثل: الأقراص أو وسائل الحفظ الحديثة التي تهدف إلى تجميع الدليل المعلوماتي وإتاحته للتحليل عبر برامج وتطبيقات متخصصة؛ بهدف إثبات وقوع الجريمة ونسبتها لمرتكبيها (فرغلي، 2007).

وحتى تتبلور الصورة بشكل أوضح؛ يمكن القول بأن خصائص الدليل المعلوماتي تتمثل في (ولاد مؤمن، 2019):

أ- يمكن عدُّه دليلًا علميًّا: لكونه عبارة عن بيانات ومعلومات ذات

طبيعة غير ملموسة لا تدرك من خلال القدرات البشرية العادية، وإنما يتطلب الأمر الاستعانة بأجهزة ومعدات متخصصة بهذا الشأن، وهو يخضع لقواعد الحاسب وتحليل المعلومات، وعليه فمن الضروري أن يتم تحليلها بشكل سليم حتى تصبح دليلًا مقبولًا قضائيًا.

ب- حداثة الدليل المعلوماتي: بوصف الدليل المعلوماتي ولد مع ظهور التكنولوجيا الحديثة، وظهر نتيجة التطور على الصعيدين التقني والمعلوماتي؛ وهذا ما يجعل التعامل معه مختلفًا عما سبقه من الأدلة العادية والتقليدية.

ج- ذو طبيعة متغيرة: يمكن تقديم الدليل المعلوماتي في عدد من الصيغ المختلفة في القراءة مع ثبات المحتوى في كل تلك الصيغ المقدمة، ومن الممكن أن تكون الصيغة صعبة القراءة لغير المتخصص، أو سهلة القراءة، وفي كلتا الحالتين لا يتغير مضمون ذلك الدليل بأي شكل كان.

وباعتبار أن الأدلة المعلوماتية الرقمية قائمة على الميتاداتا بشكل أساسي؛ فيمكن القول بأن تعريف الميتاداتا وفقًا لدراسة (Alanazi & Jones, 2015) أنها: المعلومات المستخدمة لتصنيف الأدلة الرقمية وتنظيمها وفهمها، وبالتالي القدرة على الحكم من خلالها، وتنبع أهمية الميتاداتا من حقيقة أنها توفر الكثير من المعلومات الإضافية حول الأدلة الجنائية، وغالبًا ما يكون الدليل الأكثر أهمية غير مرئي؛ وبالتالي حريٌّ استخدام برمجيات متخصصة دقيقة كتلك المستخدمة في استخراج الميتاداتا وتحليلها والتثبت من صحة البيانات لإثبات شيءٍ ما أو دحضه، ومن هذا المنطلق برزت أهمية استخدام الميتاداتا كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي، وشاع استخدامها في عدد من الميادين الحيوية (Sharma, 2016).

2. 1 التحقيق الجنائي الرقمي

يدور التحقيق الجنائي الرقمي في الأصل حول الأدلة المستمدة من أجهزة الكمبيوتر التي يمكن الاعتماد عليها بما يكفي للوقوف في المحكمة وإقناع القاضي بالحجة، وهو علم تحديد الموقع؛ عن طريق استخراج أنواع البيانات من الأجهزة المختلفة وتحليلها، والتي يفسرها المتخصصون بعد ذلك لتكون دليلًا قانونيًا، ويمكن العثور على الدليل الرقمي في الأقراص الصلبة للكمبيوتر، والهواتف المحمولة، والكاميرات الرقمية، والأقراص المدمجة، والأقراص البصرية، والأقراص المرنة، وشبكات الكمبيوتر، والإنترنت... إلخ (Vacca, 2005).

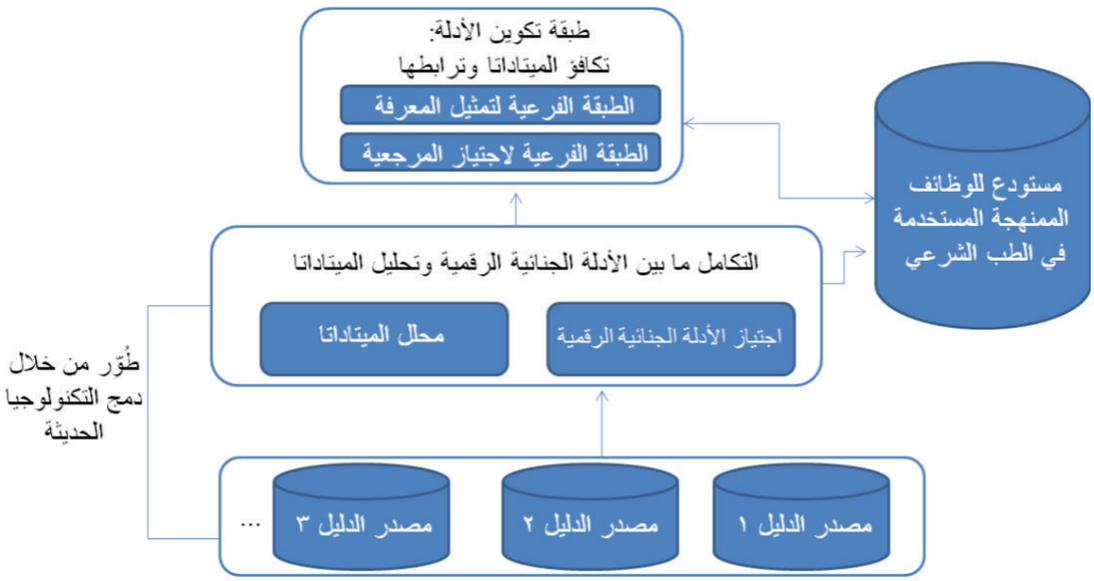
وتركز الأدلة الجنائية الرقمية في الأصل للعثور على الدليل الرقمي الذي يهتم بصفة أساسية بتحليل المعلومات الموجودة داخل أنظمة الكمبيوتر وأجهزة الكمبيوتر التي أُنشئت باستخدام تلك الأنظمة، التي تهدف إلى التعرف إلى: ماذا حدث؟ ومتى حدث؟ بصورة دقيقة، ويتقصى عن كيفية حدوث الجريمة الجنائية، وأخيرًا تبيان الأطراف المشاركة؛ وذلك بوصف التحقيق الجنائي الرقمي هو عملية التحقيق في نظام الكمبيوتر لتحديد سبب الحادث.

ويمكن للكمبيوتر أن يؤدي أحد الأدوار الثلاثة في جرائم الكمبيوتر (Agarwal, 2011):

1. يمكن أن يكون الكمبيوتر هدفًا للجريمة.
2. يمكن أن يكون أداة الجريمة.
3. يمكن أن يكون بمثابة مستودع أدلة لتخزين المعلومات القيمة حول الجريمة.

2. 2 أطر تحديد ارتباطات الأدلة الرقمية باستخدام الميتاداتا

أصبح من الضروري تطويع إمكانات الميتاداتا، ولا سيما في مواجهة تحديات التضخم والتنوع الذي تشهده البيانات؛ نتيجة للتراكم المعلوماتي، ومن أجل تحقيق أعلى استفادة ممكنة يجب أن تكون أدوات التحليل الجنائي الرقمي قادرة على دعم الوظائف المعيارية كافة، وتحديد بنية شاملة لتسهيل الإجراءات القضائية، تقوم معظم أدوات التحليل الجنائي وتحليل المحتوى باستخدام كلٍّ من تقنية: تصفية الكلمات الرئيسة وتصنيف السمات؛ وبذلك يحتاج المحقق الجنائي عادةً إلى تصفية المحتويات بناءً على كلمات رئيسة مختلفة، أو تصنيف الملفات والمعلومات بناءً على سمات متنوعة أثناء التحليل لتحديد نمط وقوع الجريمة، وأثناء الممارسة الفعلية لعملية التحليل، يتعامل المحققون بشكل أساسي مع هذه التقنيات، وإذا لم تُحدَّد الكلمات المفتاحية والسمات الصحيحة في هذه الحالة من الممكن إضاعة النمط المطلوب لاستكمال التحقيق الجنائي، كما يمكن دمج بعض من السمات المعنية في قضية ما أثناء التصنيف، وغالبًا ما يكون ذلك بالتسلسل؛ إذ إن الطريقة الأكثر شيوعًا -كما ذكر بوتيل (Boutell, 2005)- هي الجمع بين الطوابع الزمنية ومالك تلك الملفات واسم المستخدم لملفات الأدلة، وأخيرًا عنوان الـ IP. وهذه الطريقة عادة ما تترك الميتاداتا والسمات المتبقية غير مستخدمة، ومن ذلك المنطلق صمم راغافان (Raghavan, 2014) نموذجًا قائمًا يمكن من خلاله تحديد الارتباطات المستندة إلى الميتاداتا بطريقة غير مقيدة، سواء داخل مصدر بيانات واحد؛ مثل: ملفات موجودة على وسائط تخزين جنائية، أو من خلال العديد من المصادر؛ مثل: الصور الجنائية والسجلات وغيرها، ويوضح الشكل رقم (1): النموذج المقترح لتأطير ارتباط الأدلة الرقمية باستخدام الميتاداتا.



الشكل رقم 1 - النموذج المقترح لتأطير ارتباط الأدلة الرقمية باستخدام الميتاداتا

Figure 1- *proposed model for identifying associations in digital evidence using metadata*

إن الطبقة الفرعية المعنية بالمرجعية مسؤولة بشكل أساسي عن المحتوى المرجعي؛ بما في ذلك الميتاداتا داخل مصادر الأدلة الجنائية الرقمية وعبرها؛ إذ يقع على عاتق هذه الطبقة مسؤولية استخدام المؤشرات التي توفرها طبقة "تمثيل المعرفة" لتحديد الارتباطات على المصدر الجنائي نفسه؛ وذلك عبر عدد من المصادر ذات الصلة؛ نظرًا إلى أن طبقة تمثيل المعرفة تستخلص كل مصدر من خلال الأدلة الجنائية الرقمية والميتاداتا المرتبطة بها؛ فإن الطبقة الفرعية لاجتياز المرجعية تصل كل الأدلة ببعضها من خلال الميتاداتا، وتحدد القيم المتطابقة عبر الأدلة الجنائية الرقمية؛ بغض النظر عن نوع الأداة المستخدمة؛ إذ صُمِّمت الطبقة الفرعية لاجتياز المرجعية بطريقة حيادية ومقبولة تقنيًا؛ وذلك من أجل التوسع عبر مجموعات عشوائية من مصادر الأدلة الجنائية الرقمية؛ كما يمكنها أيضًا الوصول الممتد إلى البيانات الموجودة في المستودع الرقمي من عدة مصادر غير متجانسة من المحتمل أن تكون مرتبطة بالتحقيق الجنائي الرقمي، وتتكون من خوارزميات تساعد في اكتشاف الارتباطات.

أما الطبقة الفرعية المسؤولة عن «تمثيل المعرفة» فتُعنى بالاستدلال المنطقي للأدلة الرقمية بناءً على الارتباطات المكتشفة؛ إذ إن مسؤولية هذه الطبقة الفرعية يتمثل بشكل رئيس في تحديد العلاقات السببية بين واحد أو أكثر من التأكيدات التي يمكن إنشاؤها بناءً على الأدلة الجنائية الرقمية؛ إذ يمكن أن تساعد على إنشاء علاقات سببية منطقية بين الكائنات في تحديد الأدلة ذات الصلة لإعادة بناء الأحداث بوصفها جزءًا من التحليل الجنائي الرقمي.

ويتطلب الأمر النظر في الأدلة عبر مصادر غير متجانسة وربطها لتحديد السببية والتطابق أثناء التحقيق الجنائي الرقمي للتثبت من الأدلة المعلوماتية؛ إذ تدمج طبقة "تمثيل المعرفة" روابط الميتاداتا النحوية ومدى تكافؤ علاقات الميتاداتا عبر الأدلة لاشتقاق الاستدلالات الدلالية على مجموعة الأدلة الرقمية ذات الصلة، فعلى سبيل المثال:

1. إذا كانت ملفات الصور الرقمية في الدليل الجنائي متطابقة مع واحدة أو أكثر من الميتاداتا التقنية مثل: EXIF (نماذج لملفات الصور القابلة للتبديل)؛ فيمكن للمختص أن يستنتج أن الصور كانت صورًا رقمية التُقطِت بالجهاز وطراز الكاميرا الرقمية نفسه.
2. إذا كانت سجلات متصفح الويب تشير إلى تنزيل ملف تتطابق الميتاداتا الموجودة فيه مع ملف في محرك الأقراص الثابتة للمستخدم، فيمكن للمختص أن يستنتج أن الملف لم يؤلَّف بواسطة المدعى عليه.

2. 3 معايير الميتاداتا المعنية بالتحقيق الجنائي الرقمي

نستعرض بإيجاز معايير الميتاداتا الرئيسة التي تصف معلومات الميتاداتا المضمنة في كائنات رقمية مختلفة، مثل: الصور والمستندات. وبشكل عام الميتاداتا هي بيانات حول محتوى البيانات، وقد تتضمن أيضًا بيانات حول حاويات البيانات. ومن الممكن تصنيف الميتاداتا إلى

أنواع مختلفة بناءً على ما يوصف وكيفية استخدامه، ويمكن أن يكون هناك أيضًا تداخل بين هذه الأنواع؛ إذ يمكن أن توجد بعض المعلومات الشائعة في أكثر من نوع واحد من الميتاداتا.

مع الاعتبار أن الأنواع الثلاثة من الميتاداتا شائعة في الاستخدام، وتُستخدم الميتاداتا الوصفية لإنشاء مجموعة من الكائنات الرقمية وإدارتها، مثل: الميتاداتا التي أُنشئت بواسطة منشئ النظام الأصلي، وتحتوي هذه الميتاداتا الوصفية عادةً على معلومات حول الكائن الرقمي، مثل: العنوان والمؤلف والمنظمة وتاريخ الإنشاء والكلمات الرئيسة، وتصف الميتاداتا الهيكلية كيفية تجميع الكائنات الرقمية المركبة معًا والعلاقة بين الأجزاء، وهذا النوع من الميتاداتا مفيد في عرض الكائن الرقمي والتنقل عبر أجزائه المختلفة. مثال آخر على هذا النوع من الميتاداتا موجود في الوسائط المعتمدة على الوقت، والتي قد تحتوي على سلسلة من الكائنات الرقمية؛ مثل: الفيديو والصوت والنصوص. وتوفر الميتاداتا الهيكلية الوسائل لإدارة العلاقات والتسلسلات الخاصة بالعناصر المختلفة، وتحدد الميتاداتا الإدارية المعلومات الفنية حول العنصر الرقمي؛ مثل: نوع الملف، ومتى أُنشئ؟ وكيف أُنشئ؟ ومن يمكنه الوصول إليه؟ ويُستخدم لتسهيل الإدارة في تتبع استخدام الكائنات الرقمية وإعادته، ويمكن أن تتضمن الميتاداتا الإدارية أيضًا بيانات تعريف إدارة الحقوق التي تتعامل مع حقوق الملكية الفكرية، وبيانات تعريف الحفظ التي تحتوي على المعلومات اللازمة لأرشفة الكائن الرقمي والحفاظ عليه (Riley, 2017).

وبناءً على ما سبق يمكن القول بأن أهم معايير الميتاداتا المعنية في التحليل الجنائي الرقمي متمثلة في (Salama,2012):

1. IPCT Metadata - نموذج تبادل المعلومات.
2. XMP Metadata - المنصة الواسعة للميتاداتا.
3. EXIF Metadata - نماذج لملفات الصور القابلة للتبديل.

2. 4 الميتاداتا وقضايا التحقيق الجنائي الرقمي

عند الشروع في بروتوكولات التحقيق الجنائي الرقمي، يحتاج المحقق -في الغالب- إلى إعادة بناء العديد من الأحداث والإجراءات التي حدثت على النظام، والتي تعدُّ الفاصل في عملية التحقيق لاستخلاص استنتاجات موثوقة مستندة إلى الميتاداتا، وهنالك العديد من الأسئلة الرئيسة التي يجب على المحقق الجنائي الإجابة عنها، وهي (Du & Scanlon, 2019):

أ- مَن (Who)

تعدُّ مسألة «مَن» المسؤول عن إجراءات معينة مسألة مهمة في سياق التحقيق الجنائي الرقمي؛ إذ تستخدم معظم الأنظمة شكلًا من أشكال آلية المصادقة؛ وعادةً ما يتطلب إجراء تسجيل الدخول اسم مستخدم وكلمة مرور لربط المستخدم بعملية أو جلسة. أما التحقيق الجنائي الرقمي فإن المصادقة -على الرغم من أنها ضرورية- ليست كافية.

ولا يهتم المحقق فقط بتحديد مَن قام بإنشاء ملف أو مستند، ولكن أيضًا مَن قام بتعديله والوصول إلى الملف أو المستند، ومن ثَمَّ فإن الميتاداتا المرتبطة بملف أو وثيقة تشير إلى من قام بإنشاء الملف أو المستند أو تعديله أو الوصول إليه تعدُّ حيوية.

بشكل عام فإن الموضوع يصبح أكثر تعقيدًا عندما تأخذ في الاعتبار تدفق المعلومات بين العمليات والمستخدمين. على سبيل المثال، في حالة التفاعل بين عدة مستخدمين (أو عمليات) تؤدي إلى إنشاء مستند، من الصعب تحديد تأثير مستخدم واحد (أو عملية)، ومن ثَمَّ في تقييم السؤال عن (مَن)، فإن الهدف هو جمع أكبر قدر ممكن من الأدلة المفيدة التي يمكن أن تساعد المحقق الجنائي لإجراء مزيد من التحقيقات بدلًا من الخروج بإجابة مؤكدة تمامًا. علاوة على ذلك فإن المعلومات حول (مَن) يجب ربطها بمعلومات الميتاداتا للأنشطة الأخرى ذات الصلة، بالإضافة إلى الوقت الذي نُفِّذت فيه هذه الأنشطة. على سبيل المثال، في EXIF (نماذج لملفات الصور القابلة للتبديل) يعد إشعار حقوق النشر وتعليقات المنشئ والمستخدم بعض حقول الميتاداتا التي قد تكون مفيدة للإجابة عن السؤال الذي يجيب عن (مَن).

ب- أين (Where)

تعدُّ مسألة مصدر مستند، أو ملف معين، أو بشكل عام من أين تأتي بعض المعلومات المحددة أمرًا بالغ الأهمية في التحقيق الجنائي الرقمي، وقد تكون معلومات الأصل أي شيء من عنوان IP ، والرقم التسلسلي للكمبيوتر إلى إحداثيات نظام تحديد المواقع العالمي (GPS)، ويمكن أن تتضمن أيضًا معلومات؛ مثل: الرقم التسلسلي للكاميرا عندما يتعلق الأمر بالصور. وفي هذا الصدد كانت هنالك العديد من المقترحات بما في ذلك مشروع معيار الإنترنت الذي يناقش المعرفات الفريدة عالميًّا (GUID)، وعلى وجه الخصوص معرف عقدة الشبكة والوقت. في حالة التحقيق الجنائي الرقمي، عند التحقيق في مصدر ملف يحتوي على مواد غير قانونية، قد تؤدي نتيجة التحقيق إلى سلسلة التوزيع.

وغالبًا ما تُستخدم هذه المعلومات في نماذج الثقة في تحديد المخاطر المرتبطة بها، ومع ذلك فإن موثوقية هذه المعلومات وما إذا كانت هذه المعلومات هي نفسها عرضة للهجمات هي قضايا يجب أخذها في الاعتبار عند اتخاذ القرار.

ج- متى (when)

معظم أنظمة الحاسب لديها فكرة عن الوقت، وجميع أنظمة الملفات شائعة الاستخدام تربط الطوابع الزمنية بملفاتها، وتشير هذه الطوابع الزمنية إلى وقت التعديل الأخير، وآخر وقت للوصول، بالإضافة إلى وقت الإنشاء. ويشار إلى هذه الطوابع الزمنية أحيانًا بأوقات MAC لأن Mtime هو وقت التعديل الذي يوضح متى غُيِّر محتوى الملف مؤخرًا، وAtime هو وقت الوصول إلى الملف الذي يحدد آخر وقت فُتِح فيه الملف للقراءة، وأخيرًا Ctime هو وقت التغيير. وفي نظام UNIX يسجل الوقت الذي تُغيَّر فيه ميتاداتا معينة للملف، وليس محتوى الملف، أما في نظام Windows فيحدد Ctime الوقت الذي أُنشئ فيه الملف.

على سبيل المثال: في الصور يمكن الكشف عن وقت الإنشاء ووقت التعديل، وعما إذا كانت الصورة قد حُرِّرت باستخدام تقنية إخفاء البيانات (Steganography)، ويشير الإنشاء والتاريخ والوقت المعدَّل أخيرًا من الميتاداتا (Metadata) إلى وقت التقاط الصورة بالضبط، وهما دائمًا متماثلان، في حين يُظهر الوقت الذي أُنشئ على مستوى نظام التشغيل الوقت المحدد لنسخ الصورة إلى الوسائط، ويجب أن يكون تاريخ التعديل على مستوى نظام التشغيل هو نفسه تاريخ الإنشاء وآخر تعديل من الميتاداتا، وفي حالة تعديل هذه الصورة بأي أداة، فإن تاريخ التعديل على مستوى الميتاداتا سيكون مختلفًا عن تاريخ الإنشاء، ويُعتقد بأن هذا سيعطي مؤشرًا على الاستخدام المحتمل لأسلوب إخفاء البيانات (Steganography). من وجهة نظر التحقيق الجنائي، فإن التعريف الواضح لما تعنيه الطوابع الزمنية له أهمية أكبر؛ لأن الطوابع الزمنية تحدد نطاق التحقيق، ويمكن أن تساعد في تحديد المجالات التي يحتاج المحقق إلى التركيز عليها.

د- كيف (How)

تعدُّ الطريقة التي تُنفَّذ بها العملية على ملف أو كيفية إنشاء الملف ذات أهمية أيضًا للمحقق الجنائي، من خلال معرفة البرامج التي استُخدمت لإجراء العمليات على الملف وبأي تسلسل أُجريت، ويكون المحقق قادرًا على إعادة بناء سلسلة الأحداث والتغييرات في الملف، ويمكن استخدام هذه المعلومات بعدة طرق، على سبيل المثال: يمكن استخدام هذه المعلومات لإنشاء توقعات هجوم يمكن أن تساعد بدورها في التعرف إلى الجاني، وتوفر العديد من الأنظمة شكلًا من أشكال آليات التدقيق التي تسجل البرامج التي استُدعيت، ومتى؟ ومن قام بها؟ ويجب تأكيد أهمية حماية موثوقية وأمن هذه الميتاداتا، فعلى سبيل المثال: من الأفضل حماية معلومات سجل التدقيق من التعديل غير المصرح به، كما أنه من المهم أيضًا ضمان وجود آليات تمنع آليات التدقيق من عدم تجاوزها، وعلاوة على ذلك فإن الطبيعة الفعلية لتعديل الملف مهمة أيضًا. ومن ناحية أخرى أكثر شمولًا فإن سلسلة التعديلات الكاملة من إنشاء الملف حتى حالته الحالية مهمة، وعادةً ما يحتوي تاريخ المستند ومسارات المراجعة على معلومات قيمة في عملية التحقيق الجنائي الرقمي.

2. 5 الميتاداتا في التصوير الرقمي لأغراض التحقيق الجنائي

الميتاداتا هي بشكل مبسط بيانات حول البيانات، على سبيل المثال قد تحتوي الميتاداتا على اسم المؤلف وتواريخ إنشاء/ تعديل المستند، كما قد تحتوي الميتاداتا على معلومات مفيدة للمحقق، وبشكل أكثر تحديدًا قد تحتوي صور الكاميرا الرقمية على رأس معلومات الملف الموسع (EXIF - نماذج لملفات الصور القابلة للتبديل) الذي يحفظ معلومات حول الكاميرا التي التقطت الصورة، ونشأ تنسيق EXIF بواسطة جمعية تطوير الصناعة الإلكترونية اليابانية، ويُشار إليه على أنه تنسيق الصورة المفضل للكاميرات الرقمية، ويستخدم رؤوس EXIF، ويُخزَّن هذا الرأس في جزء محدد من ملف JPEG ، أو كعلامات معرفة بشكل خاص في ملف TIFF، وهذا يعني أن JPEG أو TIFF للصور الرقمية تحتفظ بالميتاداتا بتنسيق قياسي يمكن أن تقرأه التطبيقات التي تظهر الميتاداتا من معيار EXIF (Alvarez, 2004)، ويوجد أدناه الجدول رقم (1) لنموذج EXIF (بتنسيق يمكن للبشر قراءته).

في عصرنا الحالي تحظى الصور الرقمية بشعبية كبيرة بشكل مطرد في الاستخدامات؛ بسبب التوفر العالي للكاميرات الرقمية في الهواتف المحمولة، أما عند بعض الأشخاص؛ فقد تكون الصورة غير مهمة أو للمتعة فقط، ولكن عند الآخرين؛ مثل: المحققين الشرعيين؛ فقد تمثل دليلًا يمكن استخدامه لتوضيح الحقائق للآثار القانونية أو المدنية أو الإدارية أو الجنائية أيضًا؛ وعليه يمكن أن يكون للصورة الرقمية تأثير غير متوقع في سير عملية التحقيق الجنائي، ويمكن أن تكون أكثر تمثيلًا بكثير من الوصف الشفهي أو الكتابي للأحداث لدى المحاكم، ولا سيما مع التقدم التكنولوجي.

ووفقًا للقانون الصادر برقم 34 وتاريخ 1439/4/24 من الهيئة العامة للمحكمة العليا بموجب القانون السعودي؛ يمكن عدُّ الصورة الرقمية دليلًا مهمًّا، ولكن يجب إثبات أن الصورة أصلية ولم تُحرَّر أو تُحوَّل. واستخدم جانجوار وباثانيا (Gangwar & Pathania,2018) منهجية جديدة لمصادقة الصورة الرقمية، يعتمد على الميتاداتا ل

الجدول 1- نموذج EXIF (بتنسيق يمكن للبشر قراءته)

Table 1- *EXIF Metadata -Human-readable format- (Alvarez,2004)*

NO	Forms	Examples / أمثلة	النماذج	رقم
1	File name	jpg.0805-153933	اسم الملف	1
2	File size	bytes 463023	حجم الملف	2
3	File date	21:02:04 2001:08:12	تاريخ الملف	3
4	Camera make	Canon	نوع الكاميرا	4
5	Camera model	Canon PowerShot S100	طراز الكاميرا	5
6	Date/Time	15:39:33 2001:08:05	التاريخ / الوقت	6
7	Resolution	x 1200 1600	الدقة	7
8	Flash used	No	استخدام الفلاش	8
9	Focal length	(5.4mm (35mm equivalent: 36mm	البعد البؤري	9
10	CCD Width	5.23mm	أداة استشعار الكاميرا	10
11	Exposure time	(s (1/10 0.100	وقت الحدث	11
12	Aperture	f/2.8	الفجوة	12
13	Focus Dist	1.18m	مسافة التصوير	13
14	Metering Mode	center weight	وضعية القياس	14
15	Jpeg process	Baseline	معالجة الصيغة	15

EXIF (نماذج لملفات الصور القابلة للتبديل) وخصائص فك تشفير الصور الرقمية، كما أكده فرانسيسكو رودريغيز-سانتوس وآخرون (Rodríguez-Santos et al, 2015) بتطبيق منهجية عملية لمصادقة الصور الرقمية باستخدام تقنيات التحقيق الجنائي، وخلصت النتائج إلى أن الميتاداتا والصورة المصغرة وآثار الكاميرا والبيانات المخفية الموجودة في الصور الرقمية توفر تحليلًا ودليلًا قويًّا يمنح اليقين والموثوقية بإصدار الأحكام بشأن القضايا الجنائية. ويمكن توضيح حاويات الميتاداتا من خلال الشكل (2) (Orozco et al, 2015):

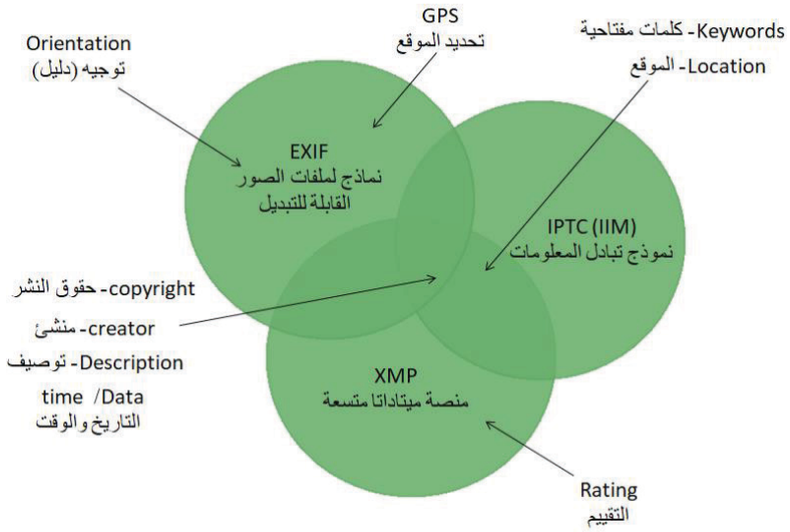
تُعرف الميتاداتا بأنها «بيانات حول البيانات»؛ أي إنها المعلومات المكملة للمحتوى الرئيس للمستند الرقمي؛ لأن هذه الميتاداتا قادرة بشكل فعال على التنظيم والبحث في فحوى الصور الرقمية؛ إذ تُخزَّن الصور الرقمية بتنسيقات مختلفة، مثل: TIFF أو JPEG أو PSD أو RAW، وكل تنسيق له قواعده واشتراطاته فيما يتعلق بتخزين الميتاداتا بالملف نفسه.

إن من أشهر حاويات الميتاداتا المعنية بالصور على سبيل المثال: IFDs Exif / TIFF وAdobe XMP وIPTC-IMM، وإن كل نوع من هذه الحاويات لها نسقها الخاص الذي يشير إلى خصائص الميتاداتا المخزنة داخلها؛ بالإضافة إلى ترتيب الميتاداتا داخل الحاوية ومدى دقتها، وتختلف تلك المعايير الدلالية للحاويات وفقًا للامتيازات لكل حاوية على حدة.

تنقسم المجموعات الدلالية لخصائص أكثر دقة في بيانات الميتاداتا المتفردة؛ لأن كل خاصية تحتوي على بيانات محددة مرتبطة ببعضها، مثل: السلاسل، أو الأرقام المرتبطة بالصورة، وبعض الخصائص تمتاز بتوضيح اتجاه الصورة والبعد البؤري، واستشعار الكاميرا، علمًا بأن هذه الخصائص شديدة الدقة، وليست شائعة في معظم حاويات الميتاداتا، ويمكن أن تخزن حاويات الميتاداتا المعلومات الأساسية التي تساعد في تحري الدقة، مثل: حقوق النشر، الوصف، الموقع بشكل دقيق، تاريخ التقاط الصورة ووقته، وأخيرًا منشئ هذه الصورة الرقمية.

2. EXIF 6 ومصادقة الصور الرقمية لأغراض التحقيق الجنائي

من خلال المصادقة على نموذج EXIF (نماذج لملفات الصور القابلة للتبديل) ومراجعته، يمكن استرجاع بعض المعلومات القيمة للمحلل



الشكل 2 - حاويات الميتاداتا

Figure 2- Metadata containers (Orozco et al,2015)

الجنائي؛ ويمكن من خلال الميتاداتا استرجاع تواريخ إنشاء الملفات ووقتها، بالإضافة إلى وقت التقاط الصور؛ مع الأخذ بالاعتبار أن تاريخ التقاط الصور أو وقته لن يتغير، وقد يساعد استخراج نماذج EXIF من ملفات JPEG المحققين على إثبات الجرائم بواسطة برمجيات الميتاداتا وإخفاء البيانات من خلال استخراجها بواسطة برامج التحليل الجنائي التي تعدُّ أسهل في عملية المصادقة الرقمية من استخراج الصور المعنية وتحليلها باستخدام أداة قائمة بذاتها؛ ويوضح (Gangwar, 2018) بأن الشكلين (3 و 4) أمثلة للميتاداتا المستخرجة بواسطة البرامج المعنية في مصادقة الصور الرقمية لأغراض التحقيق الجنائي:

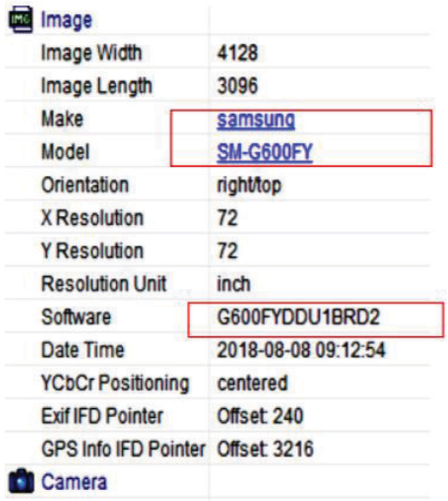
ويتضح من الشكلين رقم (3 و 4) أنه يمكن التحقق من أصالة الصورة الرقمية من خلال تحليل الميتاداتا المختلفة من EXIF (نماذج لملفات الصور القابلة للتبديل) والعمل على فك خصائص التشفير باستخدام أدوات برمجيات متنوعة لأغراض المصادقة للصور الرقمية، ويمكن التعرف إلى البرنامج المستخدم لتحرير/ تحويل الصورة والتاريخ الأصلي والوقت والتاريخ والوقت الذي حُرِّرت فيه الصورة، والتقصي حول منشئ هذه الملفات أو الصور الرقمية، وإثبات ملكية الملفات لأصحابها، وتحديد الموقع والبيانات المخفية كافة التي تحتويها تلك الصور الرقمية باستخدام أدوات مخصصة للتحليل الجنائي من خلال الميتاداتا التي يمكن استنباطها للتحليل الجنائي الرقمي وإقامة الحجة.

2. 7 حماية حقول الميتاداتا من التلاعب

نظرًا لكون الميتاداتا هي «بيانات حول البيانات» فتتضمن نوعين من الحقول، نوع يمكن لمعظم المستخدمين رؤيته مثل: اسم الملف ونوعه وتاريخ آخر فتح للملف وآخر تعديل، وأما الأخير فهي الحقول المخفية لمعظم المستخدمين والتي تُستخرج بواسطة برمجيات متخصصة دقيقة، مثل: من أنشا الملف أو عدله؟ وما الذي قام بتغييره؟ ومتى؟ ومن خلال أي جهاز تمت تلك العملية؟ في حين أنه من الممكن تغيير بعض حقول الميتاداتا، مثل العنوان والموضوع والمؤلفين، ولا يمكن تغيير حقول مثل تاريخ الإنشاء والجهاز المستخدم لإنشاء الملف (Bhangale, 2020). لذلك فإن الحقول القابلة للتعديل والتلاعب لا يمكن الاستعانة بها كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي، لأنه يشوبها الشك وبالتالي من الممكن أن تعرقل عملية إعادة كتابة الأحداث الجنائية بالاستعانة بالميتاداتا.

وتتطلب معايير فحص الميتاداتا أن يقوم الفاحص المختص باتباع بروتوكولات معينة أثناء عملية التحقيق الجنائي الرقمي. والهدف الرئيسي منها هو تحديد الأدلة المحتملة عن طريق عملية تُدعى «المصادرة والبحث والاسترجاع» مع الحفاظ على «سلامة البيانات» للملفات الأصلية أو المشبوهة. ومن الممارسات الجيدة إجراء تجزئة لـ «الوسائط المشبوهة» قبل البدء في تحليل الميتاداتا. وينبغي تصدير نسخة خالية من عوامل التشويش وأن تكون سليمة بشكلها الرقمي. و يُعرف هذا باسم «وسائط الإثبات». ومن ثم بمجرد اكتمال عملية التحليل، يتم بعد ذلك إجراء تجزئة أخرى ضد ملفات الأدلة الأخرى لضمان استمرار وجود تطابق تام مع الوسائط المشبوهة.

إن الغرض الفعلي من قيمة التجزئة «hash value» هو التحقق



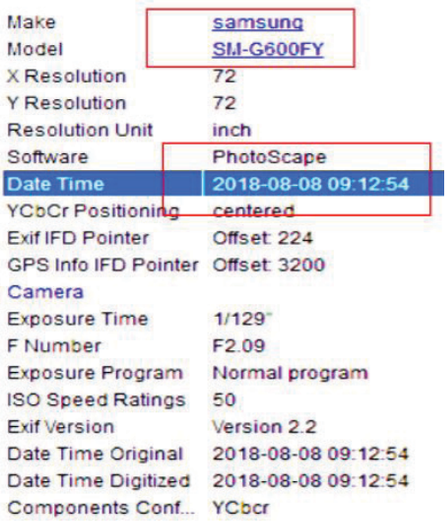
الشكل 3 - يوضح نوع الكاميرا وطرازها والبرامج المستخدمة في تحرير الصور

Figure 3- Shows the make and model of the camera & Software used in image editing (Gangwar,2018)

من صحة وسلامة الملفات أو الصور باعتبارها نسخة طبق الأصل من الوسائط الأصلية. وتعتبر قيم التجزئة مهمة جدًا للمحقق الشرعي ومحلل الميتاداتا، خاصة عند قبول الأدلة في المحكمة، وذلك لأن أي تغيير حتى ولو كان أصغر جزء من البيانات سيولد قيمة تجزئة جديدة تمامًا. وعلى سبيل المثال: عند إنشاء ملف جديد أو تحرير ملف موجود بالفعل, فإنه ينشئ قيمة تجزئة جديدة لهذا الملف. قيمة التجزئة هذه وغيرها من عناصر الميتاداتا للملفات أو الصور غير مرئية في شكلها الطبيعي ولكن يمكن لمحلل الميتاداتا الوصول إليها باستخدام برمجيات متخصصة ودقيقة للكشف عنها. وإذا كانت قيم التجزئة لا تتطابق مع القيم المتوقعة، فقد يثير ذلك مخاوف للمحقق الشرعي بأنه تم التلاعب بالأدلة (Granja, 2015).

3. الإطار التطبيقي للدراسة

تزخر الشبكة العنكبوتية بالعديد من البرامج التي تعمل على استخلاص الميتاداتا من الصور الرقمية لأغراض التحقيق الجنائي الرقمي والتي كانت محط اهتمام الباحثين والمحققين الشرعين لإعادة كتابة الأحداث الجنائية, وفي إطار هذه الدراسة سلطت الضوء على معيار EXIF Metadata والتي ركزت دراسة (Alanazi & Jones, 2015) في توضيح أهميتها في إعادة كتابة أحداث التحقيق الجنائي الرقمي وسعيًا ضمن أهداف هذه الدراسة فقد تم اختيار برنامج EXIF Viewer Pro الذي يُعتبر برنامجًا مجانيًا ويركز على تحليل الصور الرقمية لنظام ويندوز Windows. فهو يحلل ويعرض



الشكل 4 - يوضح النظام الأصلي

Figure 4- Shows the original system (Gangwar, 2018)

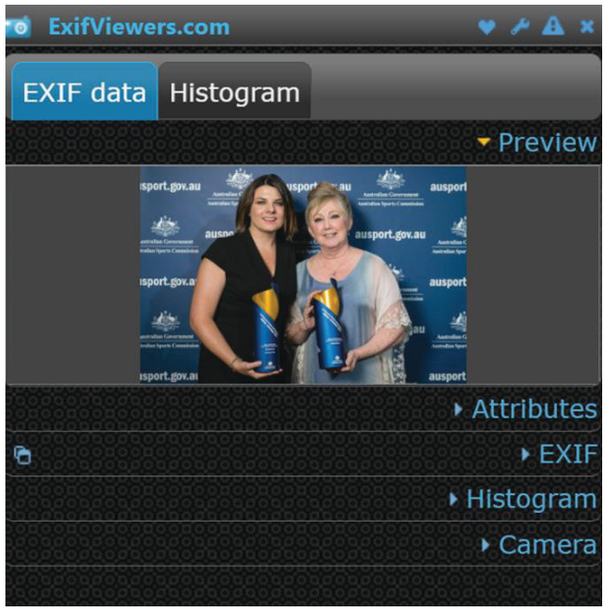
ورؤوس Exif الإجبارية والاختيارية في معظم الصور الرقمية، شكل رقم (5).

وكان التحليل يعتمد على استنباط رؤوس EXIF بواسطة أشهر الكاميرات الرقمية وهي Canon وNikon كما كان تحليل الصورتين بناءً على الاستعانة ببرمجيات مساندة أخرى، فشملت نتيجة التحليل للصورة الرقمية الأولى بالاستعانة ببرنامجين، أحدهما لإضافة عناصر ورؤوس ميتاداتا مثل: برمجيات Opanda IExif 2.3 - على سبيل التمثيل وليس التأكيد - وثانيهما برامج التعديل على الصور Adobe Photoshop. أما نتيجة تحليل الصورة الرقمية الثانية فلم يتم الاستعانة فيها بأي برامج مساندة أو إضافة أي رؤوس وعناصر ميتاداتا، إذ إن التباين في أنواع التحليل من الممكن أن يُعطي نظرة أشمل نحو الموضوع ومعرفة جوانبه المختلفة، ويساعد على تحقيق الفهم نحو دور الميتاداتا الفعّال في التحقيق الجنائي الرقمي.

3. 1 تحليل الصورة الرقمية الثانية مع الاستعانة ببرمجيات مساندة

تم تحليل هذه الصورة الرقمية بواسطة برنامج EXIF Viewer Pro وظهرت نتيجة التحليل كما يمثله الجدول رقم (2) موضحًا اسم الكائن الرقمي ونتيجة الفحص التي ظهرت من خلال برنامج EXIF Viewer Pro.

نستشف من الجدول رقم (2): أنه في تحليل الصورة الرقمية الأولى أظهر برنامج EXIF Viewer Pro عددًا من رؤوس EXIF، وشملت عددًا من عناصر الرؤوس الرئيسة المتمثلة في خمسة عشر



الشكل 5 - *تحليل الصورة الرقمية الأولى في برنامج EXIF Viewer Pro*

Figure 5- *Analysis of the first digital image in EXIF Viewer Pro*

عنصرًا أساسيًا؛ مثل: موقع الصورة، ويُقصد به المكان الذي أُخذت منه الصورة الرقمية؛ ويظهر هذا العنصر جليًا في الصور الرقمية المنشورة على الشبكة العنكبوتية؛ حيث يمكن من خلاله تتبع موقع الصورة بشكل دقيق، يليها عنصر حجم الصورة، ويوضح أبعاد الصورة الرقمية طوليًا وعرضيًا التي تُمكن من معرفة أي تلاعبات تمت على الصورة الرقمية إذا كانت قياساتها تختلف مع طراز الكاميرا، وفيما يليه عنصرا مساحة اللون وأبعاد Pixel X & Y التي تعتبر رؤوسًا مفصلية لمحللي إخفاء البيانات؛ حيث تعتبر أي عملية تشفير تمت من خلال الصورة الرقمية يتم الكشف عنها، لا سيما إذا كانت الأرقام غير منطقية لطراز الكاميرا والبرمجيات المعينة؛ كما أن رؤوس الطوابع الزمنية من أهم العناصر التي ينبغي توافرها؛ مثل: الوقت الأصلي لالتقاط الصورة الرقمية وتاريخ الالتقاط لهذه الصورة؛ ويُضاف عليها تاريخ ووقت النشر الرقمي باعتبار أن الاختلاف وارد بين تاريخ الالتقاط الفعلي ووقت نشرها في الإنترنت، ويليه رؤوس الكيفية؛ حيث تشتمل على وضعية القياس واستخدام الفلاش ونوع الالتقاط، وأخيرًا البعد البؤري، وظهر في تحليل الصورة الرقمية الأولى بأنه لم يتم استخدام الفلاش، ويعتبر حسب تحليل برمجيات EXIF بأنها صورة قياسية، ومن المقاييس المهمة للتثبت من صحة الصورة الرقمية هو عينات Pixel وbit ودقة الصورة؛ وكذلك مؤشر Exif IFDفلكل طراز كاميرا مختلف نسبة متوقعة من عدد لكل عينة من Pixel أو bit وهذا بالطبع يدخل في إطار إخفاء البيانات، فإذا تم تضمين أي بيانات مشفرة على الصورة الرقمية؛ فإنه بشكل تلقائي يتغير عدد Pixel أو bit ومن الممكن أن تدل هذه البيانات المتغيرة للمحقق الشرعي على أن شيئًا ما حدث للصورة الرقمية، أما فيما يختص بمؤشرات Image file directory Exif IFD فهي عدة أرقام وحروف مجتمعة أو متفرقة توضح معلومات إضافية عن حالة الصورة الرقمية، ففي حالة تحليل الصورة الرقمية الأولى على سبيل المثال، كان المؤشر 2676 وفقًا لما تم وصفه في الموقع الرسمي لـ exif tool فهي تدل على وضعية التصوير بشكل أدق، ويقصد بها توازن اللون الأبيض واستخدمت الكاميرا النمط العريض في التصوير (Wide mode) وأن الصورة ضمن التنسيق القديم لصيغة JPEG (old-style) وأخيرًا في الرؤوس الرئيسة عنصر نوع الكاميرا وطرازها الذي يتم من خلاله تبيان من خلال أي كاميرا أو هاتف محمول تم التقاط هذه الصورة، فعلى سبيل المثال في التحليل أعلاه تم التقاطها بواسطة Canon وكان طراز هذه الكاميرا EOS-1D X مما يضفي نوعًا من الموثوقية في الصور الرقمية، كما ذكرت دراسة (Gangwar,2018) حول مخاوف تحيط بالميتاداتا، ومنها إمكانية تسليم الصور الرقمية في أجهزة مختلفة عن الأجهزة الفعلية التي تم من خلالها إثبات ملكية الصورة الرقمية.

وفي المقابل هناك برمجيات مختلفة لإضافة البيانات الوصفية (الميتاداتا) أو حذفها؛ مثل: برنامج Opanda IExif 2.3 ففي التحليل أعلاه تم إضافة بعض الرؤوس (الاختيارية) متمثلة في اثني عشر عنصرًا التي لا يشكل عدم وجودها أي تعطيل لعملية التحقيق الجنائي الرقمي القائم على الدليل المعلوماتي، فعلى سبيل المثال، إضافة عنصري ارتفاع وعرض الصورة الرقمية، بالإضافة لوصف الصورة الرقمية، كأن تحمل تعبيرًا ووصفًا لسبب التقاط الصورة، وكذلك عنصرا مصدر الصورة وعنوانها يصفان ما يسعى عنصر الوصف لتوضيحه، والمعلومات العامة عن الكاميرا؛ مثل: طراز العدسة ورقم العدسة التسلسلي، هي عبارة عن رؤوس إضافية تغطي الرؤوس الرئيسة مثل عنصريّ نوع وطراز الكاميرا المطلوب من الميتاداتا، وكذلك رؤوس بيانات ملكية الصورة الرقمية وإدراجها مثل: ملتقط الصورة وحقوق النشر والبرمجيات المساندة التي تم استخدامها لإخراج الصورة الرقمية، وأخيرًا هناك عنصر الموقع الجغرافي، وهو غير دقيق وتم إضافته باعتبار أن هنالك تحفظات من قبل بعض برمجيات استخراج الميتاداتا بالمحافظة على خصوصية الموقع الجغرافي، وتعتبر إضافة مثل هذه الرؤوس الاختيارية بمثابة حفظ لحقوق الملكية الرقمية للصورة الرقمية، ولا سيما إذا نُشرت في الإنترنت، فبواسطة الميتاداتا والبيانات المخفية يستطيع صاحب الصورة نسبها لنفسه. وهذا ما حاولت دراسة (Bhangale, 2020) وصفه بأهمية التتبع وفحص رؤوس الكائنات

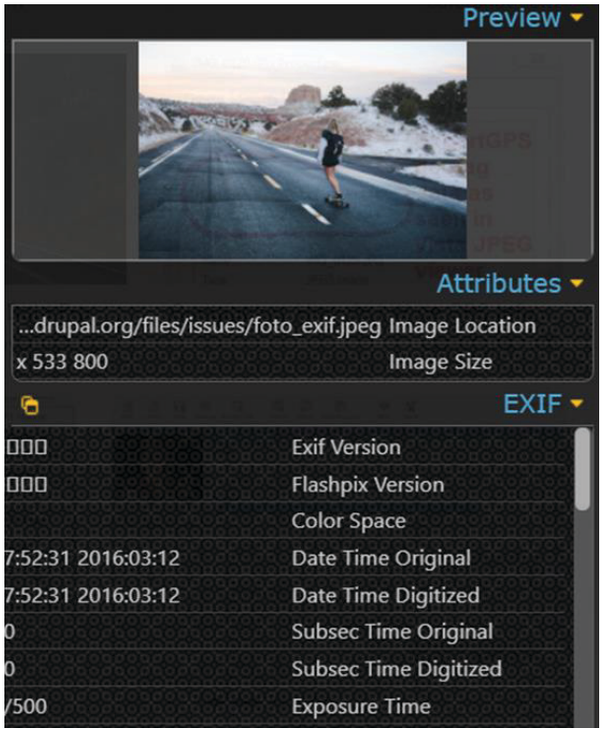
تم تحليل هذه الصورة الرقمية بواسطة برنامج EXIF Viewer Pro وظهرت نتيجة التحليل كما يمثله الجدول رقم (2) موضحًا اسم الكائن الرقمي ونتيجة الفحص التي ظهرت من خلال برنامج EXIF Viewer Pro.

NO	digital objects	Result / نتيجة الفحص	الكائنات الرقمية	رقم
1	Image Location	https://www.sportaus.gov.au/__data/assets/image/0009/681894/ASC_Media_Awards_2017_768x512.jpg	موقع الصورة	1
2	Image Size	x 512 768	حجم الصورة	2
3	Image Width	2700	عرض الصورة	3
4	Image Height	1800	ارتفاع الصورة	4
5	Color Space	1	مساحة اللون	5
6	Pixel X Dimension	768	أبعاد X Pixel	6
7	Pixel Y Dimension	512	أبعاد Y Pixel	7
8	Date/Time Original	22:11:31 2018:02:01	التاريخ / الوقت الأصلي	8
9	Date Time Digitized	22:11:31 2018:02:01	التاريخ / الوقت الرقمي	9
10	Exposure time	1/160	وقت الحدث	10
11	Metering Mode	Center Weighted Average	وضعية القياس	11
12	Flash	Flash did not fire, compulsory flash mode	استخدام الفلاش	12
13	Focal length	50	البعد البؤري	13
14	Scene Capture Type	Standard	نوع التقاط المشهد / الصورة	14
15	Exif IFD Pointer	2676	مؤشر Exif IFD	15
16	BitsPerSample	3	عينة bit	16
17	SamplesPerPixel	3	عينة لكل بكسل	17
18	Resolution Unit	2	الدقة	18
19	Date/Time	13:03:12 2018:09:10	تاريخ / وقت نشر الصورة الرقمية	19
20	Image Description	AUSTRALIAN SPORTS COMMISSION: ASC Media Awards 2017 February 1, 2018. Daltone House, Hyde Park, Sydney, NSW, Australia. Photo: Narelle Spangher, Australian Sports Commission	وصف الصورة	20
21	Camera make	Canon	نوع الكاميرا	21
22	Camera model	Canon EOS-1D X	طراز الكاميرا	22
23	LensInfo	0/0 0/0 70/1 24/1	معلومات عن العدسة	23
24	LensModel	EF24-70mm f/2.8L II USM	طراز العدسة	24
25	LensSerialNumber	2920004167	رقم العدسة التسلسلي	25
26	Software	(Adobe Photoshop CC (Windows	برمجيات مساندة	26
27	Artist	Narelle Spangher	ملتقط الصورة	27
28	Copyright	Â© 2018 Narelle Spangher/Australian Sports Commission. .All Rights Reserved	حقوق النشر	28
29	City	Sydney	موقع الصورة	29
30	Credit Photo	Narelle Spangher, Australian Sports Commission	مصدر الصورة	30
31	Headline	ASC Media Awards 2017 February 1, 2018	العنوان	31

الرقمية والتثبت من كون المعلومات لم يتم العبث بها أو تغييرها وتفادي سوء استعمالها لعرقلة التحقيقات الجنائية.

3. 2 تحليل الصورة الرقمية الثانية بدون الاستعانة ببرمجيات مساندة

تم تحليل هذه الصورة الرقمية بواسطة برنامج EXIF Viewer Pro ، شكل رقم (6)، وظهرت نتيجة التحليل كما يمثله الجدول رقم (3) موضحًا اسم الكائن الرقمي، ونتيجة الفحص التي ظهرت من خلال برنامج EXIF Viewer Pro.



الشكل 6- *تحليل الصورة الرقمية الثانية في برنامج EXIF Viewer Pro*

Figure 6- *Analysis of the second digital image in EXIF Viewer Pro*

نستشف من الجدول رقم (3) أنه في تحليل الصورة الرقمية الثانية أظهر برنامج EXIF Viewer Pro عناصر الرؤوس الرئيسة في EXIF، مثل: موقع الصورة ويُقصد بها المكان الذي أُخذت منه الصورة الرقمية، ويكون هذا العنصر مفعلًا فقط في الصور الرقمية المنشورة على الشبكة العنكبوتية (الإنترنت) ويمكن من خلال هذا العنصر تتبع موقع الصورة بشكل دقيق، يليها عنصر حجم الصورة، ويوضح أبعاد الصورة الرقمية طوليًا وعرضيًا، حيث يستطيع المحقق الشرعي الرقمي معرفة أي تلاعبات تمت على الصورة الرقمية؛ إذ كانت قياساتها تختلف مع طراز الكاميرا، أما الرؤوس المفصلية في عملية التحقق من صحة الصورة الرقمية فهما عنصرا مساحة اللون وأبعاد Pixel X & Y حيث تعتبر أي عملية تشفير تمت من خلال الصورة الرقمية يتم الكشف عنها لا سيما إذا كانت الأرقام غير منطقية لنوع الكاميرا وطرازها، كما أن رؤوس الطوابع الزمنية (التاريخ والوقت الأصلي والرقمي، بالإضافة لتاريخ ووقت نشر الصورة الرقمية) يعتبر من أهم العناصر التي ينبغي توافرها والتحقق من تواجدها لإعادة كتابة الأحداث والإجابة عن تساؤل متى ويليه رؤوس الكيفية؛ حيث تشتمل على وضعية القياس واستخدام الفلاش ونوع الالتقاط، وأخيرًا البعد البؤري، وظهر في تحليل الصورة الرقمية الأولى أنه لم يتم استخدام الفلاش ويعتبر حسب تحليل EXIF بأنها صورة رقمية تم تصويرها بشكل مباشر، ولم تمر بأي برمجيات مساندة لإخراجها، ومن المقاييس المهمة للتثبت من صحة الصورة الرقمية هو عينات Pixel وbit ودقة الصورة وكذلك مؤشر Exif IFD (Image file directory)، فلكل طراز كاميرا مختلف نسبة متوقعة من عدد لكل عينة من Pixel أو bit ولذلك فإن أي تضمين لبيانات مشفرة على الصورة الرقمية يسهم بشكل تلقائي بتغيير عدد Pixel أو bit ومن الممكن أن تدل هذه البيانات المتغيرة للمحقق الشرعي بأن شيئًا ما حدث للصورة الرقمية، أما فيما يختص بمؤشرات Exif IFD كما أسلفنا في التحليل السابق، فهي عدة أرقام وحروف مجتمعة أو متفرقة توضح معلومات إضافية عن حالة الصورة الرقمية، ففي حالة تحليل الصورة الرقمية الثانية على سبيل المثال كان المؤشر 188 وفقًا لما تم وصفه في الموقع الرسمي لـ exif tool فهي تدل على وضعية التصوير بشكل أدق، ويقصد بها أن الكاميرا الرقمية أعلاه استخدمت الضوء القياسي بدرجة (B) ولم يتم أثناء الالتقاط - نظرًا لطبيعة الضوء- استخدام الفلاش، وكذلك أن الصورة ضمن تنسيق الصيغة JPEG وأخيرًا في الرؤوس الرئيسة عنصر نوع الكاميرا وطرازها الذي يتم من خلاله تبيان من خلال أي كاميرا أو هاتف محمول تم التقاط هذه الصورة وما إصدارها، فعلى سبيل المثال في التحليل أعلاه تم التقاطها بواسطة NIKON CORPORATION وكان طراز هذه الكاميرا NIKON D7100 وباعتبار أن بعض عناصر الرؤوس تعتبر معلومات شخصية وحساسة وتتعلق بأصحابها، كما أوضحته دراسة (Khobragade, 2019) وأكدته دراسة (Bhangale, 2020) بأنه في العقد الماضي تم استخدام عنصر الموقع الجغرافي بطريقة خاطئة كما حدث لبعض المنشورات الرقمية التي تَتبع من خلالها اللصوص المنازل وسرقتها والحادثة التي حصلت في عام 2017 عندما تم تحديد أربع طائرات هليكوبتر تابعة للجيش الأمريكي من طراز أباتشي، وذلك بمساعدة الميتاداتا (البيانات الوصفية) التي تحمل إحداثيات الموقع الجغرافي، وتم تسريب الميتاداتا (البيانات الوصفية) من خلال

تم تحليل هذه الصورة الرقمية بواسطة برنامج EXIF Viewer Pro وظهرت نتيجة التحليل كما يمثله الجدول رقم (3) موضحًا اسم الكائن الرقمي، ونتيجة الفحص التي ظهرت من خلال برنامج EXIF Viewer Pro.

NO	digital objects	Result / نتيجة الفحص	الكائنات الرقمية	رقم
1	Image Location	https://www.drupal.org/files/issues/foto_exif.jpeg	موقع الصورة	1
2	Image Size	x 533 800	حجم الصورة	2
5	Color Space	1	مساحة اللون	5
6	Pixel X Dimension	2272	أبعاد X Pixel	6
7	Pixel Y Dimension	1704	أبعاد Y Pixel	7
8	Date/Time Original	07:52:31 2016:03:12	التاريخ / الوقت الأصلي	8
9	Date Time Digitized	07:52:31 2016:03:12	التاريخ / الوقت الرقمي	9
10	Exposure time	1/500	وقت الحدث	10
11	Metering Mode	Directly photographed	وضعية القياس	11
12	Flash	Flash did not fire, auto mode	استخدام الفلاش	12
13	Focal length	35	البعد البؤري	13
14	Scene Capture Type	Standard	نوع التقاط المشهد / الصورة	14
15	Exif IFD Pointer	188	مؤشر Exif IFD	15
16	BitsPerSample	5	عينة bit	16
17	SamplesPerPixel	5	عينة لكل بكسل	17
18	Resolution Unit	2	الدقة	18
19	Date/Time	14:22:51 2016:10:18	تاريخ / وقت نشر الصورة الرقمية	19
20	Image Description	Found no description meta tag	وصف الصورة	20
21	Camera make	NIKON CORPORATION	نوع الكاميرا	21
22	Camera model	NIKON D7100	طراز الكاميرا	22

الصور المنشورة على شبكة الإنترنت من قبل جنود غير مدركين لأهمية وخطورة البيانات الوصفية (الميتاداتا)، وبعد تلك الحوادث المتكررة اكتفت بعض الكاميرات الرقمية فقط بحذف عنصر الموقع الجغرافي لخصوصيتها وعدم استخدامها للأسباب الخاطئة وتجنبت حذف بقية عناصر البيانات الوصفية (الميتاداتا) لكونها تفيد في التحقيقات الجنائية.

4. الخاتمة

بمراجعة الدراسات المنشورة التي انطلقت من سياق التقصي حول دور الميتاداتا وإخفاء البيانات في التحقيق الجنائي الرقمي، لوحظ أن مسألة الإثبات من خلال الدليل المعلوماتي تبدو واعدة، ولكنها من أصعب ما يواجه القضاء؛ نتيجة للطبيعة التقنية وغير المادية التي تمتاز بها تلك الأدلة؛ وهذا ما يشكل عقبة في التحقيق الجنائي؛ لأن الوسائل التقليدية المستخدمة في جمع الأدلة غير كافية لإثباته وإدانته، فيتعين استخدام الوسائل الحديثة؛ مثل: تحديد المستخدم وتاريخ الإنشاء، وماذا حدث للمواد الرقمية -إن أمكن- وتمييز الأصوات، وإظهار البيانات المخفية في الأدلة الرقمية، مثل: الفيديو والصور التي تشمل معلومات من الممكن أن تؤدي إلى تيسير السبل القضائية في إحقاق الحق.

4. 1 نتائج الدراسة

- تُجيب البرمجيات الحديثة؛ مثل: EXIF Viewer Pro لاستخراج الميتاداتا عن الأسئلة (مَن، متى، كيف) للمحقق الشرعي.

- تسهم برمجيات كشف الميتاداتا، مثل: EXIF Viewer Pro في توفير تحليل ودليل قوي يمنح اليقين والموثوقية بإصدار الأحكام بشأن القضايا الجنائية.
- توفر برمجيات EXIF Viewer Pro لاستخراج البيانات الوصفية (الميتاداتا) عددًا من الطوابع الزمنية التي تؤطر نطاق التحقيق، ويمكن أن تساعد في تحديد المجالات التي يحتاج المحقق إلى التركيز عليها.
- تساعد برمجيات EXIF Viewer Pro لاستخراج الميتاداتا المحقق الشرعي في كتابة الأحداث المتوقعة لاستخلاص استنتاجات موثوقة مستندة إلى الميتاداتا.
- أن برمجيات EXIF Viewer Pro لاستخراج الميتاداتا تسهم في إثبات المصادقة الرقمية التي يستطيع من خلالها المحقق الشرعي التثبت من منشئ الملفات والصور الرقمية والطوابع الزمنية وغيرها من المعلومات التي تحتوي عليها عناصر رؤوس الميتاداتا.
- استغنت البرمجيات الحديثة EXIF Viewer Pro للكشف عن الميتاداتا عن عنصر الموقع الجغرافي؛ نظرًا لسوء استخدامها؛ وبالتالي لا تستطيع الإجابة بدقة عن التساؤل (أين) للمحقق الشرعي.

2.4 التوصيات

وفي ضوء ما سبق توصي الدراسة بالتوسع في الاستفادة من إمكانات الميتاداتا في تحليل الأحداث الجنائية، وتسهيل عملية البحث التي تساعد في صنع القرار المناسب للقضية المعنية. وذلك نتيجة ما حدث في الآونة الأخيرة من انتشار استخدام الميتاداتا والتزايد الملحوظ في نموها بالميادين الحيوية، وكان الغرض الفعلي منها هو توصيف البيانات لسهولة العثور على المواد الرقمية في فضاء الإنترنت؛ حيث ظهرت الميتاداتا بالتزامن مع انتشار المواد الرقمية بمختلف أشكالها، ولا نخص بالحديث الصور الرقمية فقط، فهنالك العديد من معايير الميتاداتا التي تُعنى بتوصيف أي مصدر حسب شكله أو نوعه وجميعها تصب في مسار واحد، وهو سهولة العثور. ولكن نتيجة لزيادة الجريمة الرقمية منذ ظهور الإنترنت، لم تَعد الأدلة المادية وحدها كافية، وحازت المعلومات والبيانات الموجودة بالأجهزة اهتمام المحققين الشرعيين؛ وذلك نتيجة لتسخير العلماء التقنيات والبرمجيات التي تسهم بشكل فعال للاستفادة من إمكانات الميتاداتا، وتُحقق غايات التحقيق الجنائي الرقمي، باعتبار أن الميتاداتا هي أدلة مساندة لمختلف الأدلة الجنائية المادية منها والرقمية؛ حيث تساعد المحقق الشرعي على إعادة كتابة الأحداث الجنائية بالإضافة لكونها تساعده في الإجابة عن تساؤلات المحقق الشرعي حول: مَن فعل؟ ومتى قام به؟ وكيف تم ذلك؟ وأخيرًا يعتبر الاستناد إلى الميتاداتا كدليل مساند يُساعد على توسيع مدارك المحقق واكتشاف طرق جديدة ومعلومات بالغة في الأهمية تجعل عملية التحقيق أكثر سلاسة.

كما أن استغلال التقنيات الحديثة التي تفجرت من الثورة الصناعية الرابعة أصبحت مطلبًا أساسيًا لمواكبة الجرائم المعلوماتية التي تُستحدث؛ نتيجة لهذه التطورات واستغلال تلك التقنيات؛ مثل: برمجيات استخلاص الميتاداتا التي تساعد المحقق الشرعي في التوصل للإجابات المهمة، وعليه ظهرت أهمية الميتاداتا كدليل مساند وأهمية استخدام الميتاداتا في تحليل الأحداث الجنائية بغية للتوصل لنتائج تُساعد على حل قضية معينة.

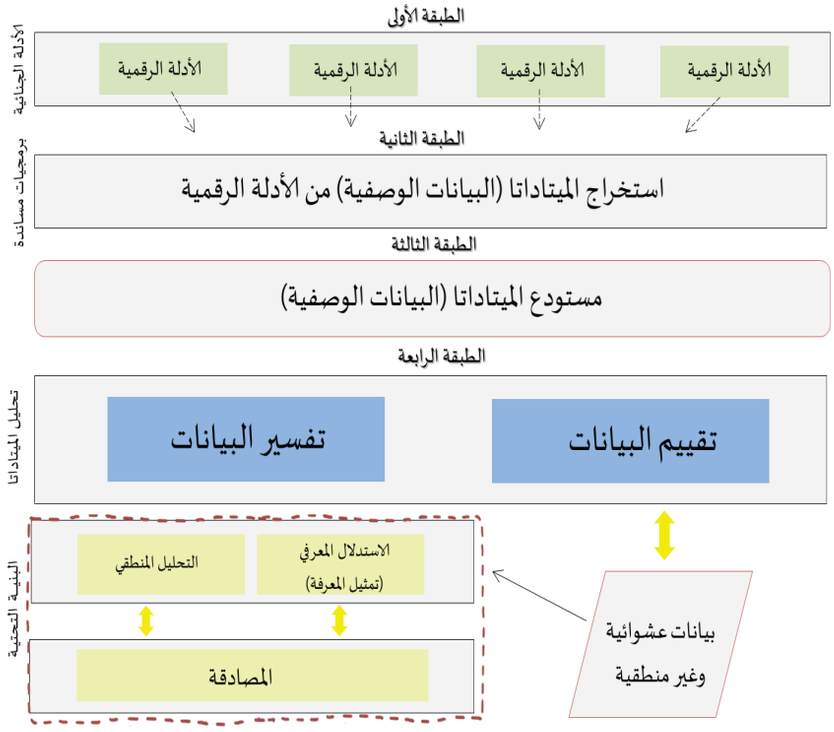
ونتيجة لهذه الأهمية البالغة للميتاداتا؛ وسعيًا لتحقيق الاستفادة القصوى من توصية الدراسة تقدم الباحثة نموذجًا مقترحًا يساعد على تطويع الميتاداتا كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي، يهدف لتعزيز دور الأدلة المساندة القائمة على الميتاداتا وتفعيل دورها من خلال نموذج عمل لسير العملية منذ البداية حتى النهاية مرتبة في أربع مراحل أو طبقات تحت مظلة التحقيق الجنائي الرقمي ويوضح الشكل رقم (7) طريقة تطويع الميتاداتا كدليل مساند في عملية التحقيق الجنائي الرقمي.

تمر عملية تطويع الميتاداتا كدليل مساند للتحقيق الجنائي الرقمي من خلال أربع مراحل أساسية تتمثل بالآتي:

1. الأدلة الرقمية.
2. استخراج الميتاداتا (البيانات الوصفية) بواسطة برمجيات مساندة.
3. مستودع الميتاداتا (البيانات الوصفية).
4. تحليل الميتاداتا (البيانات الوصفية).

أولًا: الأدلة الرقمية

يتم في بداية الأمر تجميع الأدلة الرقمية ذات الصلة بقضية ما مع الإحاطة بأن كل نوع من أنواع المواد الرقمية تختلف طبيعتها، وبالتالي طبيعة استخراج الميتاداتا منها، بالإضافة لاختلاف المعايير وفقًا لطبيعة المادة الرقمية، وينبغي أن يتم تجميعها وفقًا لنوع المادة، حتى يَسهل على محلل الميتاداتا التعامل مع الاختلافات المتباينة بين الأنواع المختلفة، فعلى سبيل المثال: المعيار الخاص بالملفات الرقمية مثل: المستندات وغيرها لا تحمل عنصر طراز ونوع الكاميرا باعتبار أن طبيعة تلك المواد لا تخضع لمعيار EXIF المعني بالصور الرقمية، وعليه يمكن قياس جميع الاختلافات بين هذه المواد الرقمية، ومن



الشكل 7- *تطويع الميتاداتا كدليل مساند في عملية التحقيق الجنائي الرقمي*

Figure 7- *employing metadata as supporting evidence in digital forensics*

أشهر معايير الميتاداتا المستخدمة في إعادة كتابة الأحداث المعتمدة على الميتاداتا هي:

- IPCT Metadata - نموذج تبادل المعلومات.
- XMP Metadata - المنصة الواسعة للميتاداتا.
- EXIF Metadata - نماذج لملفات الصور القابلة للتبديل.

ثانيًا: استخراج الميتاداتا (البيانات الوصفية)

إذا اعتبرنا أن معايير الميتاداتا هي الجزء غير المرئي أثناء تبادل الملفات الرقمية أو التقاط الصور الرقمية، فإن العملية الفيصل هُنا هي استخدام التقنية المناسبة لاستخراج الميتاداتا (البيانات الوصفية) من تلك الأدلة الرقمية، على اعتبار أن الميتاداتا في الأصل تمتاز بطبيعة تقنية ديناميكية ولا يمكن توقعها؛ وذلك بسبب تضخم المواد الرقمية وظهور عدد من معايير الميتاداتا لكل نوع من أنواعها، وأيضًا الميتاداتا ذات طبيعة غير ملموسة لا تدرك من خلال القدرات البشرية العادية، وإنما يتطلب الأمر الاستعانة بأجهزة ومعدات متخصصة بهذا الشأن، ويُراعى في هذه النقطة الاختلاف الجوهري بين برمجيات استخراج الميتاداتا التي تختلف حسب إمكاناتها وما يمكنها الخروج به من نتيجة فعّالة من الممكن أن تُساعد المحقق الشرعي في إعادة كتابة الأحداث، وحري استخدام برمجيات عالية الدقة لاستخراج الميتاداتا من الأدلة الرقمية ومراعاة التباين بين المواد الرقمية، فليس جميع البرمجيات تعمل مع ذات المواد، على سبيل المثال: البرمجيات لاستخراج الميتاداتا الخاصة بالصور الرقمية تختلف جذريًّا عن البرمجيات المعنية بالملفات الرقمية وغيرها من الأنواع، ومن الممكن الدمج بين البرمجيات والخروج بأكبر كمية ممكنة من الميتاداتا عبر عدد من الأدلة مختلفة الأنواع، ويتم تخزينها في المستودع الرقمي الخاص بالميتاداتا حتى يتم تفسيرها، وبالتالي الاستفادة منها في عملية إعادة كتابة الأحداث وفقًا لقضية ما.

ثالثًا: مستودع الميتاداتا (البيانات الوصفية)

إن مستودع الميتاداتا من العمليات الفيصل في تطويع الميتاداتا ضمن عمليات التحقيق الجنائي الرقمي؛ وذلك باعتبار أن عملية الحفظ الدائم من أهم العوائق التي تقف حاجزًا ضد الاستفادة القصوى من الدليل المعلوماتي؛ وذلك لأنه كما أسلفنا بأن الميتاداتا قابلة للتزوير والتلاعب من طرف ثالث؛ فإن عملية تخزين جميع

البيانات المستخرجة من البرمجيات المساندة من أهم العمليات؛ تفاديًا للتزوير أو التعديل الذي من الممكن أن يحدث مستقبلًا للمادة الرقمية؛ بالإضافة لإمكانية رجوع المحقق الشرعي إليها وقت الحاجة دون أن يتطلب الموضوع القيام بعملية الاستخراج مجددًا، وأن تدور العملية في حلقة مُفرغة؛ لذلك فإن توافر بيئة جيدة وآمنة للحفظ تسمح بالاستفادة القصوى من جميع إمكانات الميتاداتا لدعم التحقيق الجنائي الرقمي.

رابعًا: تحليل الميتاداتا (البيانات الوصفية)

تعتبر من أهم العمليات التي يبني على أساسها المحقق الشرعي الأحداث التي حصلت للمادة الرقمية، بمختلف جوانبها الزمنية والكيفية وغيرها؛ حيث تنقسم هذه العملية لقسمين مهمين؛ هما: تقييم البيانات وتحليل البيانات؛ وذلك باعتبار أنه ليس جميع البيانات قابلة للتقييم، وبالتالي التحليل؛ حيث يَعترض البيانات موجة من التلوث ويُقصد بها: أن تحمل البيانات طابع الفوضوية والتكرار التي تحول دون الوصول لنتيجة ممكنة في التحقيق الجنائي الرقمي؛ ومن أهم العمليات الفرعية لتحليل الميتاداتا:

- تقييم البيانات

وتعتبر من أولى عمليات تحليل الميتاداتا؛ حيث إن تقييم البيانات المستخلصة من مستودع الميتاداتا يتم وفقًا لأهميتها، ويساعد ذلك على التفسير واستخدامها بشكل يتناسب مع طبيعة القضية، وبالتالي تُقسم البيانات إلى ثلاثة أقسام وهي: مهم جدًا، مهم، غير مهم. ويكون ذلك بناءً على درجة أهميتها بالنسبة للقضية، وتختلف التقسيمات حسب طبيعة المادة الرقمية في المقام الأول.

- تفسير البيانات

تعتمد هذه الخطوة بشكل رئيس على التقييم لدرجة أهمية البيانات؛ حيث يأتي تفسيرها وربط تلك البيانات بعضها ببعض للخروج باستدلالات مناسبة تساعد المحقق الشرعي على إعادة كتابة الأحداث؛ ومن أهم العمليات لتفسير البيانات ما يلي:

- الاستدلال المعرفي (تمثيل المعرفة)

يقصد بها الطريقة التي يستخدمها محلل الميتاداتا لتمثيل المعرفة من مصادرها المختلفة للمساعدة في معالجة البيانات داخل مستودع الميتاداتا؛ والغرض من ذلك هو الاستدلال المنطقي للأدلة الرقمية بناءً على العلاقات السببية والتشابه عبر المصادر المختلفة وغير المتجانسة للقضية، وبالتالي إمكانية إعادة بناء الأحداث باعتبار أنها جزء من التحقيق الجنائي الرقمي.

- التحليل المنطقي

يتم من خلال هذه المرحلة التحقق من أي تلاعب محل شك لمحلل الميتاداتا؛ حيث إنه يركز بشكل أساسي على الأرقام والتحليل المنطقي لها، فإذا كان حجم الملف أكبر من الطبيعي ومحتوى الملف لا يُتوقع منه هذا الحجم، وبهذه الحالة يتحقق المحلل من وجود أي ملفات أو نصوص مخفية في الملف أو الصورة الرقمية، وهذه الخطوة من الممكن أن تكون مفيدة في عملية التحقيق الجنائي الرقمي، بالإضافة للتزوير الذي يمكن أن يحصل للمواد الرقمية إذا كانت الأرقام المستخرجة من البرمجيات المساندة غير منطقية لمحلل الميتاداتا، فإذا استشف المحلل أي مكون من مكونات البيانات غير منطقي، ولا يمكن أن يحمل الملف أو الصورة هذا الكم الهائل، فهنا يتم التدقيق خلف تلك المواد الرقمية والتثبت منها.

وخلال عمليتي الاستدلال المعرفي (تمثيل المعرفة) والتحليل المنطقي تتم مصادقة الأدلة المستندة إلى الميتاداتا، وإعادة كتابة الأحداث الجنائية بعد المصادقة على تلك العمليات التي مر بها الدليل المعلوماتي، حتى يسلم من العوارض، ويتم الاستناد إليه كدليل ثانوي؛ وذلك بغرض فض النزاعات الجنائية القضائية، ويتمكن المحقق الشرعي من خلال الميتاداتا من إثبات الدليل المقدم أو دحضه.

وأخيرًا توصي الدراسة بمتابعة مستجدات الميتاداتا في مجالات الإثبات الجنائي المختلفة من خلال عقد المؤتمرات وورش العمل المحلية، والاشتراك في المؤتمرات الخارجية، وتبادل الخبرات في هذا المجال.

قائمة المراجع والمصادر

1. إسخيطة، رضوان حسان. (2019). التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية. مجلة الندوة للدراسات القانونية: قارة وليد، ع26.
2. الجهني، أروى نصار. (2020). ميتاداتا مواقع البوابات الوطنية لدول مجلس التعاون الخليجي: دراسة تطبيقية. Cybrarians Journal: البوابة العربية للمكتبات والمعلومات، ع58.
3. فرغلي، عبد الناصر محمد، المساري، محمد عبيد. (2007). الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة). جامعة نايف العربية للعلوم الأمنية.
4. ولاد مومن، نزار. (2019). الدليل المعلوماتي في الميدان الزجري وسؤال نجاعة: وسائل البحث والتحقيق مجلة العلوم الجنائية: المركز المغربي للدراسات والاستشارات القانونية وحل المنازعات، ع6، 5.
5. Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic

15. Khobragade, N. (2019). Study Of Assessment Of Image Integrity Using Metadata Circulated Online Over Social Media Platforms. Advance and Innovative Research, 263.
16. Orozco, A. L. S., González, D. M. A., Villalba, L. J. G., & Hernández-Castro, J. (2015). Analysis of errors in exif metadata on mobile devices. Multimedia Tools and Applications, 74(13), 4735-4763.
17. Raghavan, S. (2014). A framework for identifying associations in digital evidence using metadata (Doctoral dissertation, Queensland University of Technology).
18. Riley, J. (2017). Understanding metadata. Washington DC, United States: National Information Standards Organization, 23.
19. Rodríguez-Santos, F., Delgado-Gutierréz, G., Palacios-Luengas, L., & Medina, R. V. (2015). Practical implementation of a methodology for digital images authentication using forensics techniques. Advances in Computer Science: an International Journal, 4(6), 179-186.
20. Salama, U., Varadharajan, V., & Hitchens, M. (2012). Metadata based forensic analysis of digital information in the web. In Annual Symposium of Information Assurance and Secure Knowledge Management, Albany, NY (pp. 9-15).
21. Sharma, P. C. P. D. B.(2016). Meta Data as a Part of Digital Forensic Investigation. IJSRD Journal.
22. Sivaprasad, A., & Jangale, S. (2012). A complete study on tools & techniques for digital forensic analysis. In 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET) (pp. 881-886). IEEE.
23. Vacca, J. R. (2005). Computer forensics: computer crime scene investigation (pp. 35-36). Hingham, MA: Charles River Media.

investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), 118-131.
6. Alanazi, F., & Jones, A. (2015). The value of metadata in digital forensics. In 2015 European Intelligence and Security Informatics Conference (pp. 182-182). IEEE.
7. Alvarez, P. (2004). Using extended file information (EXIF) file headers in digital evidence analysis. International Journal of Digital Evidence, 2(3), 1-5.
8. Bhangale, R. (2020). Securing Image Metadata using Advanced Encryption Standard (Doctoral dissertation, Dublin, National College of Ireland).
9. Boutell, M., & Luo, J. (2005). Beyond pixels: Exploiting camera metadata for photo classification. Pattern recognition, 38(6), 935-946.
10. Dalal, M., & Juneja, M. (2020). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications, 1-49.
11. Du, X., & Scanlon, M. (2019). Methodology for the automated metadata-based classification of incriminating digital forensic artefacts. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).
12. Gangwar, D. P., & Pathania, A. (2018). Authentication of digital image using exif metadata and decoding properties. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 3(8), 335-341.
13. Granja, F. M., & Rafael, G. D. R. (2015). Preservation of digital evidence: application in criminal investigation. In 2015 Science and Information Conference (SAI) (pp. 1284-1292). IEEE.
14. Heinso,Dennis.(2015).IT-Forensik.-Mohr Siebeck.