تقييم المواد المصوّرة الرقمية مفتوحة المصدر:

دليل للقضاة وجهات تقصي الحقائق

تقييم المواد المصوّرة الرقمية مفتوحة المصدر:

دليل للقضاة وجهات تقصي الحقائق

تقييم المواد المصوّرة الرقمية مفتوحة المصدر:

دليل للقضاة وجهات تقصي الحقائق

Queen Mary University of London – Institute for the Humanities and Social Sciences	OPEN SOCIETY JUSTICE INITIATIVE	TRUE – Trust in User-generated Evidence: Analysing the Impact of Deepfakes on Accountability Processes for Human Rights Violations
Human Rights Centre – University of Essex	Hertie School Centre for Fundamental Rights	MNEMONIC
HUMAN RIGHTS CENTER – UC Berkeley School of Law	University of Oxford – Law – Bonavero Institute of Human Rights	WITNESS – SEE IT FILM IT CHANGE IT

تقييم المواد المصوّرة الرقمية مفتوحة المصدر:

دليل للقضاة وجهات تقصي الحقائق

قائمة المحتويات

عن المؤلفين 6

الاقتباس 6

المقدمة 7

ما هي المعلومات الرقمية مفتوحة المصدر وكيفية تقييمها؟ 9

ما هي السمات التي تميّز المعلومات الرقمية مفتوحة المصدر التي علينا معرفتها؟ 10

القضايا الأساسية التي يجب مراعاتها عند تقييم المعلومات مفتوحة المصدر 11

المعلومات الخاصة بالمحتوى 13

البيانات الوصفية 14

مصدر المعلومات 17

معلومات حول الموقع 18

معلومات خاصة بالوقت 24

الخاتمة 28

قائمة المصطلحات 29

شكر وتقدير 31

عن المؤلفين

تمّ إعداد هذا الدليل عقب ورشة عمل استضافها مركز الحقوق الأساسية في مدرسة هيرتي ببرلين يومي 29-30 حزيران/يونيو 2022 بتمويل من وحدة التحقق الرقمي التابعة لجامعة إسيكس. فقام الأشخاص الآنف ذكرهم بتصميم هذا الدليل وصياغته وتحريره:

البروفيسورة إيفون ماكديرموت ريس، أستاذة في القانون في كليّة هيلاري رودهام كلينتون للحقوق، جامعة سوانسي.

د. دراج موراي ، محاضر أول، في كليّة الحقوق، زميل في معهد العلوم الإنسانية والاجتماعية في جامعة كوين ماري في لندن.

جانا سادلر فورستر، كبيرة مسؤولي التقاضي الاستراتيجي، مبادرة العدالة في المجتمع المفتوح ومحامية في بلاكستون تشامبرز.

راكيل فاسكويز يورينتي، رئيسة قسم القانون والسياسة والتكنولوجيا والتهديدات والفرص في منظمة ويتنيس.

سارة زارمسكي، طالبة دكتوراه ومحاضرة مساعدة في كليّة الحقوق ومركز حقوق الإنسان في جامعة إسيكس.

البروفيسورة باشاك تشالي، مديرة مركز الحقوق الأساسية وأستاذة في القانون الدولي في كليّة هيرتي ورئيسة قسم الأبحاث في معهد بونافيرو لحقوق الإنسان وأستاذة في القانون الدولي في جامعة أكسفورد.

جوزيف فينيرتي، طالب دكتوراه، في مركز الحقوق الأساسية التابع لمدرسة هيرتي.

ليندسي فريمان، مديرة التكنولوجيا والقانون والسياسة، في مركز حقوق الإنسان في جامعة كاليفورنيا، بيركلي، كليّة الحقوق.

الدكتورة أليكسا كونيغ، أستاذة مساعدة ومديرة مشاركة، مركز حقوق الإنسان في جامعة كاليفورنيا، بيركلي، كليّة الحقوق.

ليبي ماكافوي ، مستشارة قانونية، في شركة Mnemonic.

الاقتباس

تقييم المواد المصوّرة الرقمية مفتوحة المصدر: دليل للقضاة وجهات تقصي الحقائق (2024)، منشور على الإنترنت في 2024، https://www.trueproject.co.uk/osguide.

.1

المقدمة

تُستخدم المعلومات الرقمية مفتوحة المصدر – أي المعلومات المتاحة للجمهور العام عبر الإنترنت[1] – بشكل متزايد كأدلّة أمام المحاكم المحلية والدولية، وهيئات حقوق الإنسان، وهيئات تقصي الحقائق،[2] حيث أثبتت قيمتها في مجموعة متنوّعة من السياقات.[3] على سبيل المثال، تمّ تقديم معلومات مفتوحة المصدر كإثبات في عدد من القضايا أمام المحكمة الجنائية الدولية،[4] كما ولعبت مقاطع الفيديو الموجودة على الإنترنت دورًا مهمًا في أوامر الاعتقال التي أصدرتها المحكمة بحق محمود مصطفى بوسيف الورفلي.[5] وفي سابقة هي الأولى من نوعها في المحكمة الأوروبية لحقوق الإنسان، قدّمت الجهات في قضية بونومارينكو وآخرون ضد أوكرانيا وروسيا منصةً رقميةً تفاعليةً لعرض المعلومات مفتوحة المصدر.[6] كذلك، في قضية أوكرانيا وهولندا ضد روسيا تمّت مناقشة كيف تؤخذ المعلومات مفتوحة المصدر بعين الاعتبار.[7] كما وأصبحت الصور ومقاطع الفيديو المنشورة على وسائل التواصل الاجتماعي أساسيةً في عمل بعثات التحقيق التابعة للأمم المتحدة[8] وفي الملاحقة القضائية المحلية للجرائم الدولية.[9]

وقد تكون المعلومات الرقمية مفتوحة المصدر غير مألوفة للعديد من المتخصصين في القانون حيث أنّها شكل جديد نسبيًا من الأدلّة. لذلك، تقدّم هذه الوثيقة نظرةً عامةً حول تقنيات التحقيق الرئيسية في المواد الرقمية المفتوحة المصدر لمساعدة الجهات القضائية وجهات تقصي الحقائق في تقييمها لهذه المعلومات عندما تقدّم من قبل طرف في الدعوى أو من قبل طرف ثالث، أو في حال تمّ الحصول

---

1 تركّز هذه الوثيقة على المواد المصوّرة الرقمية مفتوحة المصدر حيث أنها تشكّل المعلومات التي من المرجّح أن تتلقاها المحاكم في المستقبل القريب، وهي تتضمّن الصور ومقاطع الفيديو، على غرار صور الأقمار الصناعية، أو منشورات وسائل التواصل الاجتماعي، أو مقاطع الفيديو التي يلتقطها الشهود على الهواتف الذكية. للحصول على تعريف كامل للمعلومات مفتوحة المصدر، الرجاء مراجعة مركز حقوق الإنسان في جامعة كاليفورنيا، بيركلي/مكتب المفوض الأعلى لحقوق الإنسان التابع للأمم المتحدة، بروتوكول بيركلي بشأن التحقيقات الرقمية مفتوحة المصدر (يشار إليه في ما يلي باسم "بروتوكول بيركل
https://www.ohchr.org/sites/default/files/2024-01/Berkeley-Protocol_Arabic.pdf .8-5

2 لأغراض هذه الوثيقة، يُستخدم مصطلح "هيئات حقوق الإنسان" بمعناه الواسع وقد يشمل، على سبيل المثال، الهيئات المنشأة بموجب معاهدات حقوق الإنسان، أو الإجراءات الخاصة لمجلس حقوق الإنسان التابع للأمم المتحدة.

3 مراجعة المصادر التالية على سبيل المثال
Sam Dubberley, Alexa Koenig, and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (OUP 2019); Karolina Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands' (2021) 19 *JICJ* 189–211; Sarah Zarmsky, 'Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law' (2021) 19 *JICJ* 213–225; Alexa Koenig and Ulic Egan, 'Power and Privilege: Investigating Sexual Violence with Digital Open Source Information' (2021) 19 *JICJ* 55–84.

4 هذا يشمل مقاطع فيديو: المدعي العام ضد غباغبو وبلي غودي (نص) ICC-02/11-01/15-T-117(7 شباط/فبراير 2017)؛ المدعي العام ضد المهدي (الحكم والعقوبة) ICC-01/12-01/15-171 (72 أيلول/سبتمبر 2016)؛ منشورات على فيسبوك: المدعي العام ضد بيمبا وآخرين. (قرار بشأن "الطلب الخامس للادعاء لقبول الأدلة من المنصة") ICC-01/05-01/13-1524(14 كانون الأول/ديسمبر 2015)؛ المدعي العام ضد بيمبا وآخرين. (الطلب الخامس للادعاء لقبول الأدلة من المنصة) ICC-01/05-01/13-1498(30 تشرين الثاني/نوفمبر 2015)، الفقرات 17-18؛ المدعي العام ضد يكاتوم ونجيسونا (نص) ICC-01/14-01/18-T-023(29 آذار/ مارس2021)، 69؛ الصور: المدعي العام ضد سعيد (نص) ICC-01/04-01/21-T-004 (12 أكتوبر/تشرين الأول 2021)، 17، صور الأقمار الصناعية: المدعي العام ضد الحسن (نص) ICC-01/12-01/18- T-027(21 أيلول/سبتمبر 2020).

5 المدعي العام ضد الورفلي (مذكرة الاعتقال) ICC-01/11-01/17-2 (15 آب/أغسطس 2017)، الفقرات 22-11؛ المدعي العام ضد الورفلي (مذكرة الاعتقال الثانية) ICC-01/11-01/17-13 (5 تموز/يوليو 2018)، الفقرتان 17-18. كذلك، مراجعة
Emma Irving, 'And So It Begins...Social Media Evidence in an ICC Arrest Warrant' (*Opinio Juris*) <http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/>.

6 Ponomarenko and Others v. Russia, المحكمة الأوروبية لحقوق الانسان, المنصة متاحة على: <https://ilovaisk.forensic-architecture.org/>.

7 Ukraine and the Netherlands v. Russia, قرار المقبولية، المحكمة الأوروبية لحقوق الانسان, App. Nos. 8019/16, 43800/14, 28525/20, 30 نوفمبر 2022، § 472.

8 For examples, see Daragh Murray, Yvonne McDermott, and Alexa Koenig, 'Mapping the Use of Open Source Research in UN Human Rights Investigations' (2022) 14 *Journal of Human Rights Practice* 554–581.

9 محكمة الاستئناف في لاهاي، القضية رقم 21-001283/22 (6 كانون الأول /ديسمبر2022)؛ محكمة الاستئناف لغرب السويد، المدعي العام ضد حسن مصطفى المندلاوي والأمين سلطان (الحكم، 30 آذار/ مارس 2016)؛ محكمة منطقة سودرتورن، المدعي العام ضد مهند دروبي (الحكم، 26 شباط/فبراير)؛ محكمة مقاطعة أوريبرو، المدعي العام ضد سعيد (الحكم، 19 شباط/فبراير 2019)؛ محكمة لاهاي المحلية، القضية رقم 19-748012/09 و19-P-748012/09 (الحكم، 29 حزيران/يونيو 2021)؛ محكمة لاهاي المحلية، القضية رقم 19-748001/09 (الحكم، 16 تموز/يوليو 2021).

عليها عن طريق تقرير خارجي.[10] والأهمّ من ذلك، إنّ هذه الوثيقة لا تتناول كيفية إجراء تحقيقات مفتوحة المصدر[11] حيث أنّ الغرض الوحيد من هذا الدليل هو المساعدة في تقييم مصداقية وموثوقية والقيمة الإثباتية الخاصة بالمعلومات مفتوحة المصدر. كذلك، في الدليل شرح لبعض تقنيات التحقيق مفتوحة المصدر، ولكن فقط لتوفير المعرفة حول عملية التحقيق.

يوفّر بروتوكول بيركلي بشأن التحقيقات الرقمية مفتوحة المصدر ("بروتوكول بيركلي") إطارًا يشرح بإسهاب كيفية إجراء التحقيقات الرقمية مفتوحة المصدر[12] ويضع بروتوكول بيركلي المعايير المهنية التي ينبغي تطبيقها في تحديد وجمع وحفظ وتحليل وعرض المعلومات الرقمية مفتوحة المصدر في التحقيقات الجنائية الدولية والتحقيقات الخاصة بحقوق الإنسان. وهو يتضمّن المعايير الدولية للبحث على الإنترنت في الانتهاكات المزعومة للقانون الجنائي الدولي والقانون الإنساني الدولي وقانون حقوق الإنسان. كما ويقدّم إرشادات حول منهجيات وإجراءات جمع المعلومات الرقمية وتحليلها وحفظها بطريقة مهنية وقانونية وأخلاقية.

ويعتمد هذا الدليل على بروتوكول بيركلي لدعم الجهات القضائية وغيرها من جهات تقصي الحقائق في تقييمها للمعلومات مفتوحة المصدر. ونظرًا إلى أهميتها بالنسبة إلى آليات المساءلة والعدالة، يركّز هذا الدليل فقط على المنتجات المصوّرة الرقمية مفتوحة المصدر (أي الصور ومقاطع الفيديو)، وهو يتّبع التعريفات والمبادئ والتقنيات الموضّحة في بروتوكول بيركلي.

وقد تمّ تنظيم هذا الدليل وفقًا لعدد من القضايا الرئيسية التي قد تحتاج المحكمة أو هيئة تقصي الحقائق إلى معالجتها في تقييمها للمعلومات مفتوحة المصدر، بما في ذلك تحديد أصالة الصور الرقمية، وتحليل البيانات الوصفية ذات الصلة والمصدر والموقع والوقت. ولكلّ مسألة، يحدّد الدليل المصطلحات والتقنيات ذات الصلة، ويقدّم أمثلةً لإرشاد القضاة ومتقصي الحقائق في عمليّة التقييم. وفي كلّ قسم مربع "رسائل رئيسية" يلخص أهمّ المعلومات لتسهيل مراجعتها. كما ويتضمّن الدليل مسردًا للمصطلحات الفنية ذات الصلة، وقد زُوّدت المصطلحات المدرجة في المسرد برابط تشعبي أو hyperlink ووُضعت بخط عريض.

تختلف قواعد المقبولية باختلاف الولايات القضائية كما وإنّ كلّ ولاية قضائية تختلف عن الأخرى في ضرورة تقديم أدلة من قبل خبراء وفي نوع الخبرة المطلوبة. وتعتمد هذه الأمور أيضًا وبشكل كبير على وقائع كلّ قضية على حدة.
يهدف هذا الدليل إلى المساعدة في تقييم أي مادة مقدّمة، بحيث تتمكن آليات المساءلة من الاستفادة من الإمكانات الكاملة للمعلومات الرقمية مفتوحة المصدر. ونحن نعتقد أنّ المعلومات مفتوحة المصدر لها قيمة لا تقدر بثمن في السعي لتحقيق المساءلة. وهدف الدليل أن يكون توضيحيًا وليس شاملاً. فهو يتناول أهم التقنيات المستخدمة في التحقيقات مفتوحة المصدر، ولكنّ تقنيات جديدة تظهر باستمرار.

الرسالة الرئيسية: يهدف هذا الدليل إلى مساعدة القضاة وصناع القرار الآخرين في تقييمهم للمعلومات مفتوحة المصدر، من خلال شرح بعض تقنيات التحقيق في المصادر المفتوحة الأكثر شيوعًا. وهو ليس دليلاً حول كيفية إجراء التحقيقات مفتوحة المصدر.

10 لأغراض هذا الدليل، سوف يُستخدم مصطلحي "الأدلة الرقمية مفتوحة المصدر" و"الأدلة مفتوحة المصدر" بالتبادل، وذلك فقط لغايات تسهيل عمليّة القراءة. ومع ذلك، يركّز الدليل بصراحة على الأدلة الرقمية القائمة على المواد المصوّرة مفتوحة المصدر.

11 لنظرة عامة حول تقنيات التحقيق، مراجعة : Dubberley et al., supra note 3 ولدورات أو معلومات حول التحقيقات مفتوحة المصدر، مراجعة: منظمة العفو الدولية، "دورة عبر الإنترنت حول التحقيقات مفتوحة المصدر في مجال حقوق الإنسان" < https://advocacyassembly.org/en/partners/amnesty؛ ومعهد التحقيقات الجنائية الدولية، "دورة التحقيقات مفتوحة المصدر" https://iici.global/course/open-source-investigation-foundational/ .

12 لقد تمّ تطوير بروتوكول بيركلي من قبل مركز حقوق الإنسان، جامعة كاليفورنيا بيركلي والمفوضية العليا لحقوق الإنسان، وقد تضمّن ذلك سلسلة من المشاورات مع خبراء دوليين.

ما هي المعلومات الرقمية مفتوحة المصدر وكيفية تقييمها؟

يُعرّف بروتوكول بيركلي المعلومات مفتوحة المصدر بأنها "المعلومات التي يمكن لأي فرد من الجمهور العام مراقبتها أو شراءها أو طلبها، من دون الحاجة إلى صفة قانونية خاصة أو من دون أن يُعتبر النفاذ إلى هذه المعلومات غير مصرّح به".[13] والمعلومات الرقمية مفتوحة المصدر هي "معلومات متاحة للجمهور بشكل رقمي، ويتم الاستحصال عليها عمومًا من الإنترنت".[14] في سياق المساءلة، تتكوّن المعلومات الرقمية مفتوحة المصدر بشكل خاص من المنشورات على وسائل التواصل الاجتماعي والصور ومقاطع الفيديو والمستندات والتسجيلات الصوتية المنشورة على الإنترنت وصور الأقمار الصناعية والبيانات المنشورة من قبل الحكومات.

ويأخذ القضاة أو غيرهم من جهات تقصي الحقائق، عوامل عدّة في الاعتبار عند تقييم القيمة الإثباتية للمعلومات الرقمية مفتوحة المصدر. وتشير عبارة" التحقق" إلى تقييم جميع المعلومات المتاحة المرتبطة بالمادة. وتتضمّن عملية التحقق من المعلومات مفتوحة المصدر مجموعةً من التقنيات المختلفة، مثل تحديد الموقع الجغرافي وتحديد الموقع الزمني وتحليل البيانات الوصفية [15] ولا تقتصر على تقنية واحدة فقط. وعند تقييم المعلومات مفتوحة المصدر، من المهمّ دراسة منهجية التحقيق المستخدمة.

الرسائل الرئيسية: يتمحور تقييم المعلومات مفتوحة المصدر حول ضمان إجراء عملية التحقق المناسبة. وتختلف تقنيات التحقق المستخدمة باختلاف الحالة. قد يكون من المفيد أن نتذكّر أنّ كل تقنية هي جزء من الفسيفساء المستخدمة لتأكيد المعلومات ويقع على عاتق المحققين استبعاد الاحتمالات البديلة.

13 بروتوكول بيركلي , § 1.

14 بروتوكول بيركلي , § 1.

15 تناقش هذه التقنيات بمزيد من التفصيل أدناه في القسم 4.

.3

ما هي السمات التي تميّز المعلومات الرقمية مفتوحة المصدر التي علينا معرفتها؟

في معظم الأحيان، ينبغي التعامل مع الصور الرقمية مفتوحة المصدر كأي شكل آخر من أشكال الأدلة، وفحص العوامل الموجودة مثل تأكيد المعلومات وموثوقيّة المصدر. ومع ذلك، هناك بعض الاعتبارات الرئيسية الإضافية التي لا بدّ من أخذها في الحسبان:

- أولاً، قد لا تتضمّن الصور مفتوحة المصدر مؤشرات تقليدية على أصالتها، على غرار معلومات عن الشخص الذي سجّل المادة المصوّرة أو عن الجهاز الأصلي الذي تم تسجيل اللقطات عليه. والأهم من ذلك، قد يقوم أي مستخدم بنشر محتوى لم يسجّله بنفسه.
- ثانيًا، كما هي الحال غالبًا في الحسابات على وسائل التواصل الاجتماعي، قد يكون الفرد (الأفراد) المرتبط بالحساب مجهولاً أو غير معروف. على سبيل المثال، لا تفرض بعض منصات الوسائط الاجتماعية من المستخدمين تسجيل أسمائهم الحقيقية، وقد تسمح للمستخدمين بتغيير اسم المستخدم الخاص بهم بشكل متكرر، و/أو قد يقوم عدة أفراد بالنشر تحت حساب واحد.
- ثالثاً، تسمح طبيعة البيئات الرقمية بانتشار كميات كبيرة من المواد بشكل سريع وقد يكون الشخص الذي نشر المادة لأول مرّة غير معروف.
- رابعًا، وكما يظهر في القسم ٤، قد يكون المحتوى غير أصيل بطرق عدّة. فقد أصبحت أدوات إنشاء المحتوى أو تعديله الآن متاحةً أكثر ويمكن استخدامها من دون تدريب احترافي أو برامج معقّدة. وعلى عكس الأدلة المادية، قد يتمّ التلاعب بالمحتوى الرقمي عن بعد.

الرسائل الرئيسية: بشكل عام، ينبغي التعامل مع المعلومات الرقمية مفتوحة المصدر كأي شكل آخر من أشكال الأدلة. ومع ذلك، هناك عدد من السمات الفريدة التي لا بدّ من التنبّه لها. وعلى الجهات التي تقدّم الأدلّة الإجابة عن الأسئلة التي قد تنشأ حول الطرق التي تختلف بها المعلومات مفتوحة المصدر عن أشكال الأدلة الأخرى.

القضايا الأساسية التي يجب مراعاتها عند تقييم المعلومات مفتوحة المصدر

يحدّد هذا القسم القضايا الرئيسية التي يجب مراعاتها عند تقييم أصالة وموثوقية المعلومات الرقمية مفتوحة المصدر. في سياق التحقيقات مفتوحة المصدر، يعرّف التحقق على أنّه العملية التي يتمّ من خلالها تقييم دقة وصحة المعلومات. وتعتبر الصور الرقمية أصليةً وموثوقةً إذا تم إثبات أنها تمثّل فعليًا ما تدعي أنّها تمثله. وعند تقييم كيفية التحقق من الصور الرقمية ومن أصالتها، لا بدّ من التفكير في ما إذا كان تحليل المحقق يقيّم التالي وكيف: (أ) محتوى الصور نفسها، (ب) البيانات الوصفية، (ج) المصدر، (د) الموقع، (هـ) الوقت.

وهناك مجموعة واسعة من الأسباب التي بفعلها لا يكون المحتوى عبر الإنترنت ما يزعم تمثيله.[16] ويشمل هذا، على سبيل المثال لا الحصر، ما يلي:

- الإسناد الخاطئ للمكان أو الوقت أو عدم الإشارة إلى السياق: على الرغم من أنّ المحتوى قد يصوّر أحداثًا حقيقية، فمن الممكن أن يتم إسناد وقت أو مكان خاطئ للصورة أو الفيديو أو قد يؤخذ المحتوى خارج سياقه. على سبيل المثال، في العام ٢٠١٩ تمّ تداول مقطع فيديو يُزعم أنه يصوّر الهجمات التركية في شمال سوريا وانتشر الفيديو على العديد من وسائل الإعلام الرئيسية. ولكن بعد فترة وجيزة، تبيّن أنّ الفيديو كان في الواقع مصوّر في حقل رماية في ولاية كنتاكي في الولايات المتحدة الأمريكية.[١٧]

- المحتوى المُعدّل (التزييف الخفيف): في بعض الحالات، قد يتمّ تقديم الصور أو مقاطع الفيديو المُعدّلة على أنّها أصليّة. وقد يكون قد تمّ قصها، أو وضُعت عليها مرشحات (فلاتر)، أو تمّ إضافة أو حذف بعض العناصر منها، أو تمّ تسريع المشاهد الفيديو أو إبطاؤها (يُعرف هذا باسم "التزييف الخفيف" shallow-fakes).[١٨] ومثال على ذلك مقطع فيديو أصلي لنانسي بيلوسي، رئيسة مجلس النواب في الولايات المتحدة الأمريكية، تمّ تعديله ليظهر وكأنّها في حالة سكر وتتلعثم في كلماتها. وقد تمّ فضح تزييف الفيديو لاحقًا.[١٩]

- **البيانات الوصفية المعدّلة:**

  - البيانات الوصفية التي يتمّ تعديلها أو حذفها تلقائيًا: قد يتمّ تعديل البيانات الوصفية

16 Claire Wardle, 'Fake news. It's complicated.' (*First Draft News*, 16 February 2017) <https://firstdraftnews.org/articles/fake-news-complicated/>.

17 Heather Murphy, 'ABC Apologizes for Showing Video from U.S. Gun Range in Report on Syria' (*The New York Times*, 14 October 2019) <https://www.nytimes.com/2019/10/14/business/media/turkey-syria-kentucky-gun-range.html>.

18 Ashley Stoll, 'Shallowfakes and Their Potential for Fake News' (*Washington Journal of Law*, Technology & Arts, 13 January 2020) <https://wjlta.com/2020/01/13/shallowfakes-and-their-potential-for-fake-news/>.

19 Hannah Denham, 'Another fake video of Nancy Pelosi goes viral on Facebook' (*Washington Post*, 3 August 2020) <https://www.washingtonpost.com/technology/2020/08/03/nancy-pelosi-fake-video-facebook/>.

المرفقة بالمحتوى تلقائيًا من قبل بعض المنصات عند التحميل. على سبيل المثال، يقوم تطبيق واتساب - على غرار معظم وسائل التواصل الاجتماعي ومنصات التواصل الرقمية - بإزالة كافة البيانات الوصفية من المحتوى الذي يتمّ تحميله على المنصة.

» البيانات الوصفية المعدّلة أو المحذوفة يدويًا: قد يتمّ تعديل البيانات الوصفية المرفقة بالمحتوى، عن قصد أو عن غير قصد، فتظهر موقعًا أو جهاز تسجيل أو ختمًا زمنيًا غير صحيح. وقد يتمّ أيضًا محوها كليًا أو جزئيًا. ويمكن إجراء التعديل من خلال برنامج لتعديل البيانات الوصفية أو من خلال وظيفة مدمجة في أنظمة تشغيل معيّنة، وذلك لأغراض مختلفة.[٢٠]

- **المحتوى الملفّق**: قد يتم تلفيق المحتوى باستخدام ممثلين ومواقع تصوير السينما أو التلفزيون. ومثال على ذلك ما حدث في العام ٢٠١٤ في ما يتعلّق بالنزاع في سوريا، حيث انتشر مقطع فيديو لصبي صغير ينقذ فتاةً تحت القصف- بعنوان "Syrian Hero Boy" :الصبي السوري البطل"وقد عُرض في البداية على أنّه حقيقي[٢١] ليتمّ الكشف لاحقًا على مجموعة من صانعي الأفلام يقفون وراء الفيديو الذي لم يكن في الواقع من الصراع في سوريا بل تمّ تصويره مع ممثلين في موقع تصوير في مالطا.

- المحتوى الذي يتم إنشاؤه أو التلاعب به بواسطة الذكاء الاصطناعي (التزييف العميق أو المواد السمع-بصرية الاصطناعية) SynthMedia: نظرًا إلى أنّ تكنولوجيا الذكاء الاصطناعي أصبحت متاحةًعلى نطاق أوسع، قد يتم إنشاء مقاطع صوتية أو صور ومقاطع فيديو رقمية مفتوحة المصدر أو تعديلها بواسطة الذكاء الاصطناعي.[٢٢] وتُعد الصور المنشأة بواسطة تقنيّة التزييف العميق Deepfakes مثالاً على التقنيات التي تستخدم الذكاء الاصطناعي لتوليد المواد السمع-بصرية الاصطناعية. وهي شكل جديد من أشكال التلاعب السمعي البصري الذي يسمح للأشخاص بإنتاج محاكاة واقعية لوجه شخص ما أو صوته أو حركاته. على سبيل المثال، تمّ تداول مقطع فيديو مزيّف للرئيس الأوكراني زيلينسكي يدعو قواته إلى الاستسلام في العام ٢٠٢٢ على وسائل التواصل الاجتماعي.[٢٣] وتتيح تقنيّة إنشاء المحتوى الاصطناعي أيضًا للمستخدمين إضافة أغراض أو إزالتها بسهولة، أو تعديل الخلفية، أو إنتاج صورة لشخص غير موجود، أو إنتاج صورة لحدث أو غرض بناءً على وصف نصي، من بين ميزات أخرى.[٢٤] وقد يكون من الصعب اكتشاف المحتوى الذي يتم إنشاؤه أو تحريره بواسطة الذكاء الاصطناعي حيث قد يتطلّب ذلك تحليلاً من قبل خبير في الإنتاج عبر الذكاء الاصطناعي أو خبير في الأدلة الجنائية للمواد السمع-بصرية. ولكنّ الأدوات التي تدّعي رصد التزييف العميق ليست دائمًا دقيقةً ولا ينبغي الاعتماد عليها فقط عند فحص أي محتوى مشبوه حيث ينبغي أيضًا النظر في السياق والطرق الأخرى لتأكيد المعلومات.[٢٥] ويمكن أن يؤدّي تحديد وقت إنشاء المحتوى الرقمي إلى

---

20 قد يتم إجراء التعديل لأغراض التضليل أو لأسباب أخرى؛ ففي بعض الحالات، على سبيل المثال، قد تكون هناك حاجة إلى حجب بعض البيانات الوصفية لمنع التعرّف على هوية الأشخاص. للحصول على معلومات حول عمليات تعديل البيانات الوصفية، الرجاء مراجعة Casey Schmidt, 'Revamp your information with these unique metadata editors' (***Canto***, 2 February 2021) <https://www.canto.com/blog/metadata-editor/>; Mauro Huculak, 'How to edit image metadata on Windows 10' (*Windows Central*, 10 January 2017) <https://www.windowscentral.com/how-edit-picture-metadata-windows-10>. >.

21 BBC News, '#BBCTrending: Syrian 'hero boy' video faked by Norwegian director' (*BBC News*, 14 November 2014) <https://www.bbc.com/news/blogs-trending-30057401>.

22 WITNESS, *Deepfakes* (2022), available online at <https://www.mediafire.com/file/421ov54c77t04tq/Backgrounder_Deepfakes_2022.pdf/file>.

23 Bobby Allyn, 'Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn' (*NPR*, 16 March 2022) <https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia?t=1660657155956>.

24 Open AI, 'DALL·E: Creating Images from Text' (***OpenAI***, 5 January 2021) <https://openai.com/blog/dall-e/>.

25 Sam Gregory, 'The World Needs Deepfake Experts to Stem This Chaos' (*Wired*, 24 June 2021) <https://www.wired.com/story/opinion-the-world-needs-deepfake-experts-to-stem-this-chaos/>.

إعطاء فكرة عن أدوات إنشاء أو تعديل المحتوى التي كانت متوفرةً في ذلك الوقت.

ومع ذلك، قد تبقى للمحتوى المعدّل أو غير الأصيل قيمة إثباتية.[26] كما وقد يتمّ التلاعب بالمحتوى من دون وجود نيّة في التضليل. على سبيل المثال، قد يتمّ قص مقطع فيديو وضمّه إلى فيديو آخر، من دون أن تكون نيّة الشخص الذي قام بالتعديل أن يبيّن أنّ المقطع الثاني يلي المقطع الأوّل بالتسلسل. أو، حتى لو كان القصد هو التضليل، فقد تظلّ لبعض جوانب الصورة أو الفيديو قيمة إثباتية، على غرار تاريخ أو وقت تسجيل اللقطات، أو المحتوى نفسه إذا كان من الدعاية السياسية. وقد يشير المحتوى أيضًا إلى عوامل أخرى مثل الركن المعنوي للجريمة. وينبغي بالطبع التعامل مع هذا النوع من المعلومات بحذر. وعلى المحققين تطبيق الاعتبارات العادية لتحليل المعلومات الرقمية مفتوحة المصدر على النحو المبيّن في بروتوكول بيركلي من أجل تحديد القيمة المناسبة، إن وجدت، للصور الرقمية المشكوك في أصالتها.

الرسائل الرئيسية: قد لا تصوّر المواد البصرية المفتوحة المصدر على الإنترنت دائمًا ما تزعم تصويره لأسباب متعدّدة، بما في ذلك: الإسناد الخاطئ؛ التعديل؛ تعديل البيانات الوصفية؛ التلفيق واستخدام الذكاء الاصطناعي لإنشاء المحتوى أو التلاعب به. ويمكن كشف الكثير منها باستخدام تقنيات التحقق المناسبة. وقد تظلّ للمواد الرقمية غير الأصلية قيمة إثباتية.

المعلومات الخاصة بالمحتوى

على الرغم من أنه قد يتمّ تقديم المعلومات مفتوحة المصدر بطريقة مختلفة عن الأشكال التقليدية من الصور أو مقاطع الفيديو، إلا أنه يجب تحليل المحتوى (أي المعلومات التي تعطيها الصورة أو الفيديو) بالطريقة نفسها. وعند تقييم تقرير المحقق، ينبغي النظر في عنصرين:

أولاً، العمليّة التي اتبعها المحقق في فحص المحتوى. فعلى المحقق اتباع المعايير المهنية لجمع وتحليل وحفظ الأدلة مفتوحة المصدر على النحو الوارد في بروتوكول بيركلي . كما وعليه أيضًا أن يتحلّى بالشفافية في ما يخص أي تحيّزات أو قيود معروفة موجودة في عمله، ومحاولة موازنة التحيزات المعرفية والتقنية حيثما أمكن ذلك.[27] كذلك، على المحقق أن يذكر ما إذا كان قد اختبر فرضيات بديلة أو فكّر في طرق أخرى لتفسير عمله أو الطعن فيه.

ثانيًا، لا بدّ من التأكّد ممّا إذا كانت تحليلات المحقق ونتائجه متوافقةً مع مجال خبرته. على سبيل المثال، في بعض الحالات قد يكون من الضروري للمحقق استشارة خبير تقني أو خبير في الموضوع أو خبير في إحدى الصناعات (مثل خبراء في المباحث الجنائية أو في علم النبات أو خبراء في الطب أو الأسلحة أو الأمور العسكرية أو الجغرافيا المكانية). في حالات أخرى، قد يكون من الضروري أن يقوم المحقق باستشارة أفراد يتمتّعون بمعرفة خاصة بالسياق، حيث أنّ المحققين الذين ليس لديهم خبرة في السياق أو الموضوع الوارد في الصور - كالمحققين الذين ليسوا على دراية شخصية بالمنطقة المزعوم تصويرها - قد يفوتون أدلّةً تتعلّق بالسياق قد تدحض النتائج أو قد لا يقومون بطرح التساؤلات حول التحيّزات أو الافتراضات أو المعلومات الخاطئة والمضلّلة. وعلى من يقدّم الأدلة استشارة الخبراء عند الضرورة وعدم تقديم ادعاءات حول ما يراه في المواد المصوّرة إذا لم يكن ذلك من ضمن مجال خبرته. وفي حال كانت لغة المصدر الأصلي تختلف عن لغة التقرير، لا بدّ من التحقق من دقة الترجمة.

26 انظر على سبيل المثال، المدعي العام ضد ناهيمانا وباراياغويزا ونغيزي ، الحكم الصادر عن المحكمة الجنائية الدولية لرواندا، القضية رقم ICTR-99-52-T، 3 ديسمبر/كانون الأول 2003، الفقرة 274.

27 Yvonne McDermott, Alexa Koenig, and Daragh Murray, 'Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations' (2021) 19 *JICJ* 85–105.

الرسائل الرئيسية: لا بدّ من تحليل المحتوى المصوّر مفتوح المصدر كما يتمّ تحليل الصور أو مقاطع الفيديو التقليدية، مع ضرورة التدقيق في نقطتين مهمتين. أولاً، لا بدّ من تقييم طريقة عمل المحقّق للتأكّد من أنّه مارس العناية الواجبة عند تحليل المحتوى. ثانياً، يجب أن تكون النتائج التي يتوصّل إليها المحقق تتوافق مع مجال معرفته وخبرته.

البيانات الوصفية

البيانات الوصفية هي البيانات التي تصف وتقدّم معلومات حول محتوى معيّن، مثل الصور أو مقاطع الفيديو التي يتم تقييمها.[28] هناك مجموعتان رئيسيتان من البيانات الوصفية المحتملة لكلّ محتوى: البيانات الوصفية التي تُنتج تلقائيًا عند الإنشاء أو التعديل أو النشر؛ والبيانات الوصفية التي يضيفها المحققون كجزء من عملية التحليل أو الحفظ. ويمكن لكلّ من هاتين المجموعتين توفير معلومات مختلفة.[29]

البيانات الوصفية المنتجة عند إنشاء المحتوى أو تعديله أو نشره

يمكن أن تشمل البيانات الوصفية المنتجة عند إنشاء المحتوى الرقمي وقت وتاريخ وموقع التقاط الصورة أو الفيديو، بالإضافة إلى معلومات مثل نوع الجهاز الذي تم إنشاء المحتوى عليه. ويختلف إنتاج البيانات الوصفية باختلاف نوع الجهاز الذي أنشئ المحتوى عليه، ويعتمد إلى حد كبير على تكوين الجهاز(configuration)، أو ما إذا كانت المنصّة التي تم تحميله عليها "تزيل" البيانات الوصفية تلقائيًا أم لا.

ويمكن لعدد من العوامل أن تؤدي إلى اختلافات في البيانات الوصفية، مثل:

A. الطابع الزمني: قد يتأثّر الطابع الزمني بما إذا كان الجهاز موضوع على إعداد المنطقة الزمنية "الافتراضية" أم لا(default' time zone)؛

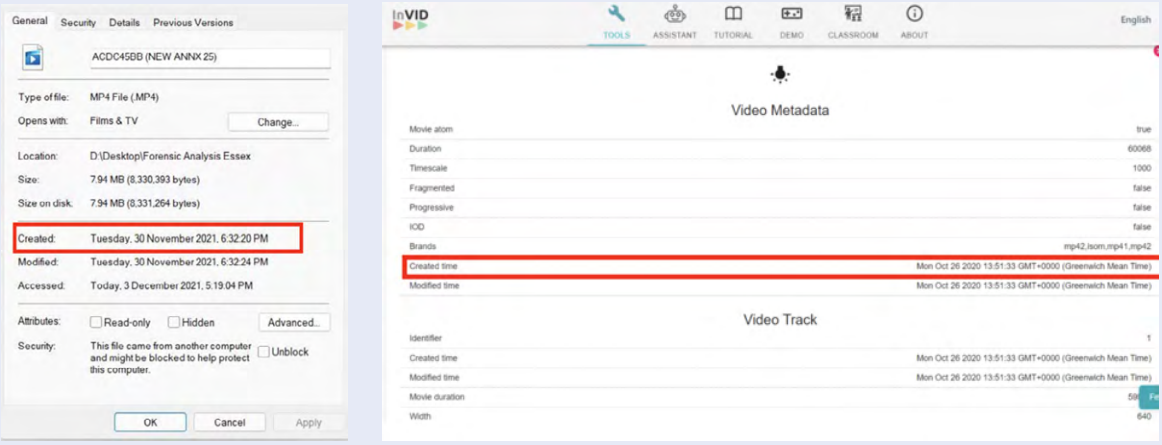
B. إحداثيات نظام تحديد المواقع العالمي (GPS) التقريبية: قد تتأثّر هذه الإحداثيات بعوامل مختلفة على غرار عدد وموقع الأبراج الخلوية الموجودة في الجوار، أو مستوى تغطية شركة الاتصالات في المنطقة؛

C. قراءة البيانات الوصفية المشتقة: على سبيل المثال، تفسّر بعض الهواتف المحمولة الارتفاع عن سطح البحر على أساس نقاط بيانات وصفية أخرى.

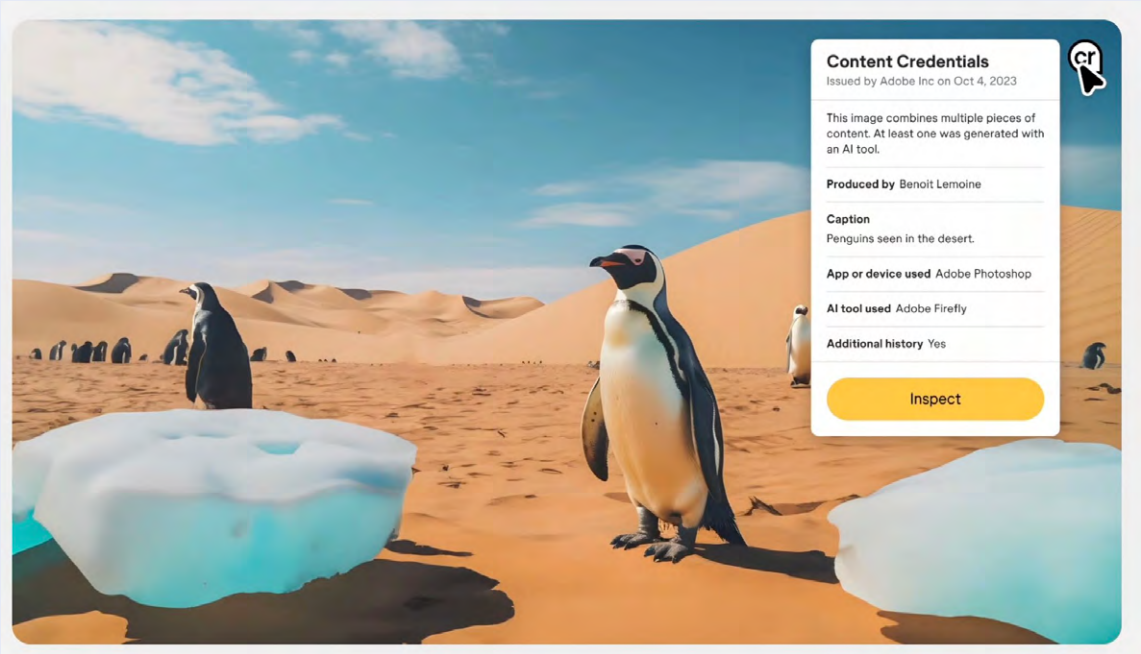
بالإضافة إلى ذلك، لا بدّ من فحص البيانات الوصفية عادةً باستخدام برنامج لعرض البيانات الوصفية لاستخراجها وتفسيرها. ووفقًا لبرنامج عرض البيانات الوصفية المستخدم، قد تختلف النتائج قليلاً، كما توضّح الأمثلة التالية (الشكل أ). بالنسبة إلى المحتوى الذي يتمّ إنشاؤه أو تعديله بواسطة الذكاء الاصطناعي، قد تقوم بعض أدوات الذكاء الاصطناعي بتضمين تفاصيل حول البرنامج الذي أنشأ الصورة أو المقطع الصوتي أو عدّله، أو نموذج الإنشاء الذي تمّ استخدامه (الشكل ب).

28 Berkeley Protocol, § 184.

29 تجدر الإشارة إلى أنه يمكن أيضًا تعديل البيانات الوصفية أو إنشاؤها بطرق أخرى. على سبيل المثال، قد يتمّ تعديل البيانات الوصفية عمدًا بعد إنشائها، بهدف التلاعب بوقت التسجيل، وما إلى ذلك. كذلك، قد تتمّ إضافة البيانات الوصفية تلقائيًا إذا تم تعديل المحتوى باستخدام حزم تعديل الصور أو الفيديو.



الشكل أ: لقطات شاشة لنتائج برنامجي عرض البيانات الوصفية مأخوذة من وحدة التحقق الرقمي في جامعة إسيكس للتحقق من مقطع فيديو يصوّر حدثًا في Lekki Tollgate في نيجيريا. تُظهر الصورة العلوية البيانات الوصفية المستخرجة باستخدام Microsoft File Explorer، والتي تدرج تاريخ ووقت الإنشاء وهما 30 تشرين الثاني/ نوفمبر 2021 في الساعة 6:32 مساءً فيما تُظهر الصورة السفلية البيانات الوصفية المستخرجة باستخدام صندوق أدوات InVid، والتي تبيّن أنّ تاريخ إنشاء والوقت هما 26 تشرين الأول/أكتوبر 2020 في الساعة 13:51. ويعزو الباحثون هذا التناقض إلى أنّ البيانات الوصفية لـ Microsoft File Explorer (أي 30 تشرين الثاني/نوفمبر 2021) تمثّل الوقت الذي تمّ فيه تحميل الملف على الكمبيوتر، في حين أنّ البيانات الوصفية التي يظهرها InVid (أي 26 تشرين الأول/ أكتوبر 2020) هي الوقت الفعلي الذي تمّ فيه تسجيل مقطع الفيديو.



الشكل ب: مثال على بيانات المحتوى التي تشرح الطرق المستخدمة لإنشاء صورة باستخدام الذكاء الاصطناعي. المصدر؛
https://blog.adobe.com/en/publish/2023/10/10/new-content-credentials-icon-transparency

وتعتمد دقة البيانات الوصفية أيضًا على إعداد المستخدم لأجهزة مثل كاميرات للمراقبة (CCTV)، حيث يجب إدخال الوقت يدويًا ممّا قد يؤدي بسهولة إلى ورود الأخطاء.

ومن التحديات الأخرى التي تواجه الباحثين في المصادر المفتوحة البيانات الوصفية غير الموجودة، حيث أنه غالبًا ما يتمّ "حذف" البيانات الوصفية من المحتوى عند نشرها على مواقع التواصل الاجتماعي أو إرسالها عبر تطبيقات الرسائل على غرار واتساب. ونظرًا إلى أنّ يتم استحصال الكثير من المحتويات المذكورة في هذا الدليل من وسائل التواصل الاجتماعي، فمن المحتمل ألا نجد البيانات الوصفية الأصليّة مرفقةً بأي تقارير مقدمة من الباحثين أو الجهات الفاعلة الأخرى.

البيانات الوصفية المنتجة عند التحميل أو خلال التواجد على الإنترنت

على الرغم من أنّ البيانات الوصفية للملف الأصلي غالبًا ما تتمّ إزالتها أثناء عملية التحميل، إلا أنّه يمكن إضافة بيانات وصفية مفيدة عند التحميل وأثناء التواجد على الإنترنت. وكما هو موضح في القسمين الفرعيين د و ه أدناه، يمكن أن توفّر التفاصيل المتعلّقة بالوقت والموقع المسجّلة خلال عمليّة التحميل للمحققين أدلةً إضافيةً لتقييمهم لهذه المعلومات الأساسية. إضافةً إلى ذلك، فإنّ التفاعلات عبر الإنترنت مع المحتوى - مثل التعليقات والمشاركات وغيره - قد تعطي المحققين معلومات مفيدة.

وفي السنوات القليلة الماضية، ظهرت العديد من الأدوات التي تقوم بدمج البيانات الوصفية بالصور. ويمكن للمعايير المتعلّقة بمصدر هذه المقاطع تعقّب طريقة صنعها، والتعديلات التي قد تكون قد خضعت لها، بطريقة تجعل من الصعب جدًا التلاعب بتوقيع التشفير من دون ترك أدلّة على ذلك. ولأغراض التحقق، فإنّ الأدوات الأكثر قيمةً هي تلك التي تدمج البيانات الوصفية التي يتمّ تجزئتها hashed بشكل مشفّر عند الجمع، وليس في مرحلة لاحقة (حيث كان من الممكن التلاعب بالصورة خلال هذه الأثناء). وغالبًا ما يُشار إلى هذه الأدوات باسم "تكنولوجيا الالتقاط المضبوط" controlled-capture technology. وقد يختلف تصميم هذا البرنامج ولا ينبغي اعتبار سلامة البيانات الوصفية الخاصة به أمرًا مفروغًا منه. وبالمثل، فإنّ افتقار الصور إلى بيانات وصفية مجزأة بشكل مشفّر لا يعني أنّ المحتوى غير موثوق به أو لا يمكن التحقق منه عبر وسائل أخرى.

البيانات الوصفية التي يضيفها المحققون

يمكن أيضًا للمحققين إضافة البيانات الوصفية، بعد حصولهم على المحتوى، كجزء من عملية التحليل أو الحفظ. على سبيل المثال، قد يضيف المحققون بعض المعلومات إلى الحزمة الرقمية تمثل تفسيراتهم للمحتوى، مثل بيانات جديدة حول طبيعة الحدث (أي "ضربة جوية" أو "عمليّة تعذيب"). وكجزء من عملية الحفظ، يمكن للمحققين أيضًا إضافة بيانات وصفية مثل الختم الزمني (يشير إلى متى تلقى المحقق البيانات أو تقديرًا لوقت الحدث) أو قيمة التجزئة. وقيمة التجزئة hash value هي شكل فريد من أشكال التعريف الرقمي (سلسلة أبجدية رقمية) تؤكّد، من خلال استخدام التشفير، أنّ المحتوى الذي تمّ جمعه لم يخضع للتعديل منذ وقت احتساب قيمة التجزئة.[30] وقد يتمّ تعيين قيم التجزئة لمحتوى ما للمساعدة في إثبات عدم التلاعب به منذ وقت تطبيق التجزئة إلى لحظة تقديمه إلى المحكمة أو إلى أي هيئة أخرى لتقصي الحقائق. وفي حال تمّ تعديل الصورة الرقمية ولو بشكل طفيف، فسيؤدّي ذلك إلى قيمة تجزئة جديدة تمامًا.

العلامات المائية watermarks غير المرئية

بالنسبة إلى المواد السمعية البصرية الاصطناعية، يتمّ تضمين علامات مائية غير مرئية على مستوى البيكسل في المواد المرئية أو يتم تشفيرها في الترددات الصوتية. وهي غير مرئية بالعين أو مسموعة

30 بروتوكول بيركلي, § 155(h).

بالأذن البشرية، ولكن يمكن رصدها بواسطة برامج مدرّبة على اكتشافها. ويتطلّب تعديلها أو إزالتها دراية فنية. وقد يتمكّن محلّل الصور الجنائي من تأكيد ما إذا كان الفيديو أو الصورة قد تم إنشاؤها باستخدام الذكاء الاصطناعي .

الرسائل الرئيسية: ينبغي النظر إلى البيانات الوصفية كجزء من صورة أكبر تسعى إلى تأكيد أصالة المحتوى. ويمكن أن تكون البيانات الوصفية مفيدةً في بناء الفرضيات الخاصة بوقت وموقع التقاط الصورة أو الفيديو، أو ما إذا كان المحتوى قد تمّ تعديله ولكن لا بدّ من إخضاع هذه البيانات للاختبار. إنّ البيانات الوصفية غير الصحيحة أو غير الموجودة لا تعني بالضرورة أنّ المحتوى غير موثوق به. بالنسبة إلى المحتوى الاصطناعي، يمكن أن تساعد العلامات المائية غير المرئية أدوات الكشف المدربّة بشكل مناسب على توفير المزيد من السياق حول الصورة.

مصدر المعلومات

تقليديًا، يشهد الشهود على مصدر الصورة أو الفيديو. ولكن، نظرًا إلى الطبيعة المميّزة للبيئة الرقمية، قد لا يكون هذا ممكنًا في حال الصور الرقمية مفتوحة المصدر الموجودة على الإنترنت. على سبيل المثال، قد يجعل حجم المحتوى الرقمي من المستحيل إحضار شهود لكلّ صورة أو لكلّ مقطع فيديو، أو قد يكون القائم بتحميل المحتوى أو مشاركته مجهولاً أو متوفيًا. والأهمّ من ذلك، أنّ معظم تقنيات التحقيق الموضّحة في هذا القسم لا تؤكّد هوية مصدر الصورة أو الفيديو بل هي مفيدة في تحديد خصائص المصدر الرئيسية (مثل الانتماءات السياسية المحتملة، أو الموقع المحتمل الظاهر، أو العلاقة المنتظمة بحدث ما، وما إلى ذلك) ممّا من شأنه تسهيل تقييم موثوقيّة هذا المصدر.

ولا بدّ من أخذ دور العديد من الجهات الفاعلة في الاعتبار عند تقييم مصدر الصورة الرقمية، بما فيه من أنشأ الصورة (أي من سجّل المحتوى الأصلي)، ومن قام بالتحميل (من نشر المحتوى على الإنترنت)، ومن شارك المحتوى (من قام بتوزيع المحتوى إما عبر الإنترنت أو من خلال مجموعات الدردشة)، ومن قام بالجمع أو التعديل (من قد يكون قد جمع مقاطع فيديو متعددة في مقطع فيديو واحد أو قام بتعديل المحتوى بطريقة ما) وقد تتداخل هذه الأدوار. فعلى سبيل المثال، قد يكون من أنشأ المحتوى هو من قام أيضًا بالتحميل.

وفي بعض الحالات، قد تكون هناك مؤشرات تتعلّق بهويّة من قام بالتحميل. فعلى سبيل المثال، قد تصنّف بعض حسابات وسائل التواصل الاجتماعي على أنها موثوقة أي تمّ التحقق منها "verified"،[31] ممّا يشير إلى الهوية المحتملة لمن قام بالتحميل، على الرغم من أنّ مستوى التحقّق الخاص بمنصات الوسائط الاجتماعية المتعددة قد يختلف بشكل كبير. وتدلّ إشارة "تمّ التحقق منه" هنا إلى من قام بالنشر وليس إلى المحتوى بحدّ ذاته. ولا ينبغي الافتراض أنّ المحتوى المنشور بواسطة حساب "تم التحقق منه" هو في الواقع ذو مصداقية أو موثوق به.

ونظراً لطبيعة البيئة الرقمية، قد يكون المصدر مجهولاً أو محجوب بهوية مستعارة. وقد يكون الحساب المحجوب بهوية مستعارة حسابًا يمثّل شبكةً من الأشخاص يقومون بتصوير محتوى ما ومشاركته عادةً في ما يخص قضيةً أو صراعًا معيّنًا. ومن الأمثلة على ذلك مجموعة "الرقة تُذبح بصمت"، وهي مجموعة من النشطاء يحمّلون بانتظام منشورات حول أنشطة داعش في الرقة، سوريا.[32] وفي بعض الحالات، قد

31 عندما يصنّف حساب على إحدى منصات التواصل الاجتماعي على أنّه موثوق أي تم التحقق منه (مثل Facebook أو Twitter أو Instagram أو YouTube)، فهذا يعني أن المنصّة أكدّت (وفقًا لمعاييرها الخاصة) أن الملفّ الشخصي للشخص أو الشركة التي يمثلها هو حقيقي. وتأخذ المنصات في الاعتبار مجموعةً متنوعةً من العوامل عند تحديد ما إذا كان الحساب قد تمّ التحقق منه، بما في ذلك تحديد الهوية باستخدام المعرّف أو عنوان بريد إلكتروني رسمي، والتغطية الإخبارية، وأعداد المتابعين، ونشاط الحساب.

32 على سبيل المثال مراجعة صفحة الفيسبوك "الرقة تذبح بصمت" المتوفّرة على الرابط التالي < https://m.facebook.com/Raqqa.Sl/?__tn__=%2Cg >.

تكون الحسابات المجهولة حسابات مقلّدة (أي حسابات تنتحل شخصية فرد أو كيان مشهور) أو حسابات روبوتية (حسابات تنشئ منشورات بشكل تلقائي). ومن أجل تقييم المصادر المجهولة، من الضروري تحليل سلوك الحساب. على سبيل المثال، ما إذا كان الحساب ينشر بانتظام حول صراع أو قضية ما، وما إذا كان هذا المحتوى متوافق مع السياق العام (على سبيل المثال، يحتوي على معلومات حول مناطق معروفة أو أطراف صراع معروفة)، أو ما إذا كان المصدر يظهر انتماءً سياسيًا أو تحيّزًا ما. ومن المؤشرات الأخرى على الموثوقية ما إذا كانت هناك حسابات أخرى موثوقة وذات مصداقية تتبع هذا الحساب.

من جهة أخرى قد تقوم المصادر التي لا تنشر بشكل منتظم حول وضع ما بنشر قطعة محتوى واحدة فقط تكون ذات موثوقية وأهمّية كبرى. وكانت هذه حال مقطع فيديو يصوّر مقتل امرأتين وطفلين في الكاميرون في العام 2018 تمّ تداوله على نطاق واسع عبر وسائل الإعلام.[33] وأدّى التحقق من هذا الفيديو إلى اعتقال وإدانة الجنود المتورّطين في عمليات الإعدام.[34]

الرسائل الرئيسية: هناك طرق متعددة يمكن من خلالها تقييم مصدر الصور الرقمية. ومع ذلك، نظرًا لطبيعة البيئة الإلكترونية التي تسمح بمشاركة المقاطع وإعادة مشاركتها، ونظرًا إلى أنّ الحسابات قد تكون مجهولة المصدر، قد يكون من الصعب تحديد مصدر الصورة الرقمية أو الفيديو مفتوح المصدر بشكل مؤكّد. ولكن حتى في الحالات التي لا يمكن فيها تحديد المصدر، هذا لا يعني أنّ المحتوى غير موثوق أو ليس له قيمة إثباتية.

معلومات حول الموقع

يستخدم المحققون مجموعةً متنوعةً من التقنيات لتحديد مكان التقاط الصورة أو الفيديو. ويشير تحديد الموقع الجغرافي إلى "تحديد أو تقدير موقع الغرض أو النشاط أو الموقع الذي تمّ فيه إنشاء المحتوى".[35] وتهدف عملية تحديد الموقع الجغرافي إلى تحديد مكان إنشاء المحتوى. ولا بدّ من أن يتضمّن تقرير تحديد الموقع الجغرافي عرضًا شفافًا للمعلومات الدقيقة التي استخدمتُ لتحديد الموقع الجغرافي. وتعتمد الدقّة على عدد من المتغيّرات.

قد تتضمّن البيانات الوصفية الخاصة بالصورة أو الفيديو وسمًا جغرافيًا (إحداثيات GPS)، يمكن استخدامها كنقطة بداية لتقييم مكان التقاط الصورة أو الفيديو. ومع ذلك، قد تكون البيانات الوصفية الأصليّة غير موجودة (خاصةً إذا تمّ نشر صورة أو مقطع فيديو على وسائل التواصل الاجتماعي، حيث يتمّ حذف البيانات الوصفية) أو من الممكن أن يتمّ تغييرها، وبالتالي يجب استخدامها فقط كجزء من الإطار الشامل الذي يؤكد المحتوى.

في أبسط الأشكال، يتطلّب تحديد الموقع الجغرافي مطابقة الخصائص الجغرافية المرئية في الصورة (سواء كانت طبيعيةً أو من صنع الإنسان) مع مكان فعلي، باستخدام صور الأقمار الصناعية أو غيرها من المواد المرجعية المعروفة، على غرار Google Street View. بشكل عام، كلما زادت الخصائص الفريدة الموجودة والتي يمكن مطابقتها مع البيانات المرجعية، كلما زادت الثقة في أنّ الصورة أو الفيديو قد تمّ التقاطه في ذلك الموقع المحدد.

33 Nick Turse, 'Cameroon is a close U.S. ally–and its soldiers carried out a shocking execution of women and children' (*The Intercept*, 26 July 2018) <https://theintercept.com/2018/07/26/cameroon-executions-us-ally/>.

34 BBC News, 'Cameroon soldiers jailed for killing women and children' (*BBC News*, 21 September 2020) <https://www.bbc.co.uk/news/world-africa-54238170>.

35 بروتوكول بيركلي, § 190.

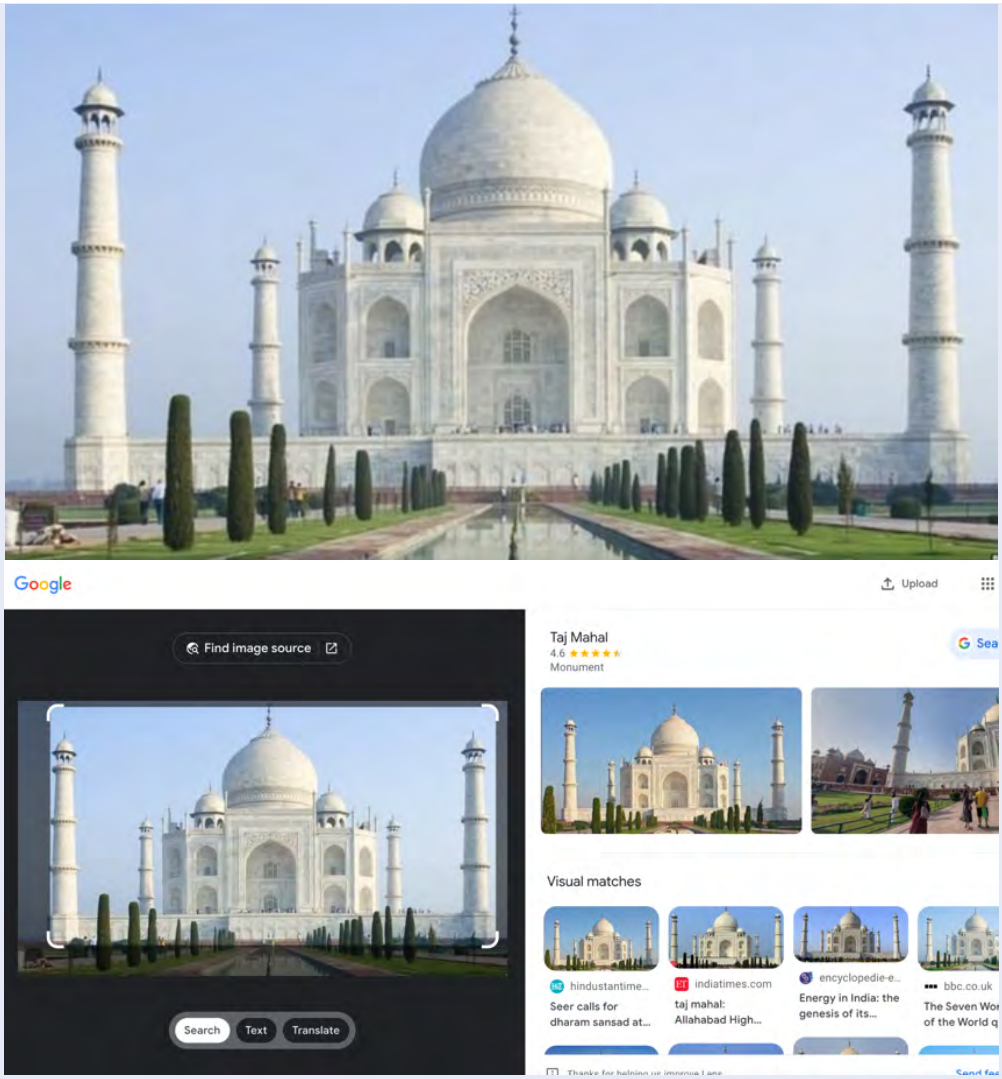
البحث العكسي عن الصور أو مقاطع الفيديو

يتضمّن يتضمّن البحث العكسي تحميل تحميل صورة أو لقطات ثابتة من مقطع فيديو على محرّك بحث، بحيث تتمكّن خوارزمية البحث من التعرّف على نسخ أخرى من الصورة نفسها أو صور مشابهة على الإنترنت. وقد يكشف البحث العكسي عن الصور ما إذا كان قد تمّ نشر صورة أو مقطع فيديو على الإنترنت قبل تاريخ الإنشاء المزعوم. ويمكن أن يثبت هذا أنّ الصورة أو الفيديو ليس ما يدعيه ناشره. ومع ذلك، فإنّ عدم وجود مطابقات مع صور أخرى لا يثبت بشكل قاطع أنّ الصورة تتمتّع بالمصداقية. فعلى سبيل المثال، قد يكون قد تمّ إزالة الصور السابقة عن الإنترنت، أو ربما لم يتمّ تحميلها.

ومن محدوديات البحث العكسي عن الصور أنه يقوم بالبحث فقط في قاعدة بيانات محرّك البحث وهي لا تحتوي إلا على نسبة صغيرة من المحتوى الموجود على الإنترنت. وهي لا تتضمّن، على سبيل المثال، المواد التي تُحمّل علىشبكة الإنترنت العميقة (التي لا يتم ربطها بمحركات البحث) أو شبكة الإنترنت المظلمة (وهي جزء من الإنترنت لا يمكن الوصول إليه إلا من خلال برامج متخصصة، مثل متصفح تور). من الممكن ألا يؤدّي البحث العكسي عن الصور في وقت التحقيق إلى أي نتائج، فيما قد تؤدّي عمليّة البحث نفسها إلى نتائج إذا تمّت في وقت لاحق - مثل وقت إجراءات المحاكمة. وتشهد قواعد البيانات التابعة لمحركات البحث تزايدًا مستمرًا في المحتوى، وقد يختلف المحتوى الذي تتمّ فهرسته بشكل كبير من محرك إلى الآخر. وقد يؤثر ازدياد حجم المحتويات السمعية البصرية الاصطناعية على الإنترنت على الأرشيفات السمعية والبصرية ممّا يؤدي إلى تغيير النتائج. وعلى عكس ذلك، قد تعطي المحتويات التي يتمّ إنشاؤها أو تعديلها بواسطة الذكاء الاصطناعي نتائج عند القيام ببحث عكسي عن الصور.

وفي بعض الحالات، يمكن أن يؤدي البحث العكسي عن صورة أو مشهد رئيسي من مقطع فيديو إلى تطابق مباشر مع موقع معيّن. ويحدث هذا بشكل أساسي عندما تتضمّن الصورة شارعًا أو معلمًا معروفًا أو أي بنية أخرى يمكن التعرّف عليها بسهولة.

وفي النهاية، يمكن استخدام البحث العكسي لمحتوى تمّ اكتشافه على الإنترنت لتقييم ما إذا كانت الصورة أو الفيديو الذي يحلله المحقق هي الصورة أو الفيديو المنشور للمرة الأولى على الإنترنت. ويمكن أيضًا استخدام عمليات البحث العكسي عن الصور لاستبعاد مواقع معيّنة إذا ظهرت الصورة سابقًا في إحدى قواعد البيانات وتمّ التأكيد على أنها تمثّل موقعًا مختلفًا عن الموقع قيد التحقيق.



الشكل ج: صورة لتاج محل ولقطة شاشة للبحث العكسي عن الصور باستخدام غوغل. تم تحميل الصورة لإجراء بحث باستخدام ميزة "البحث من خلال الصور" في غوغل فأسفرت عن النتيجة أعلاه التي أعطت اسم المعلم.

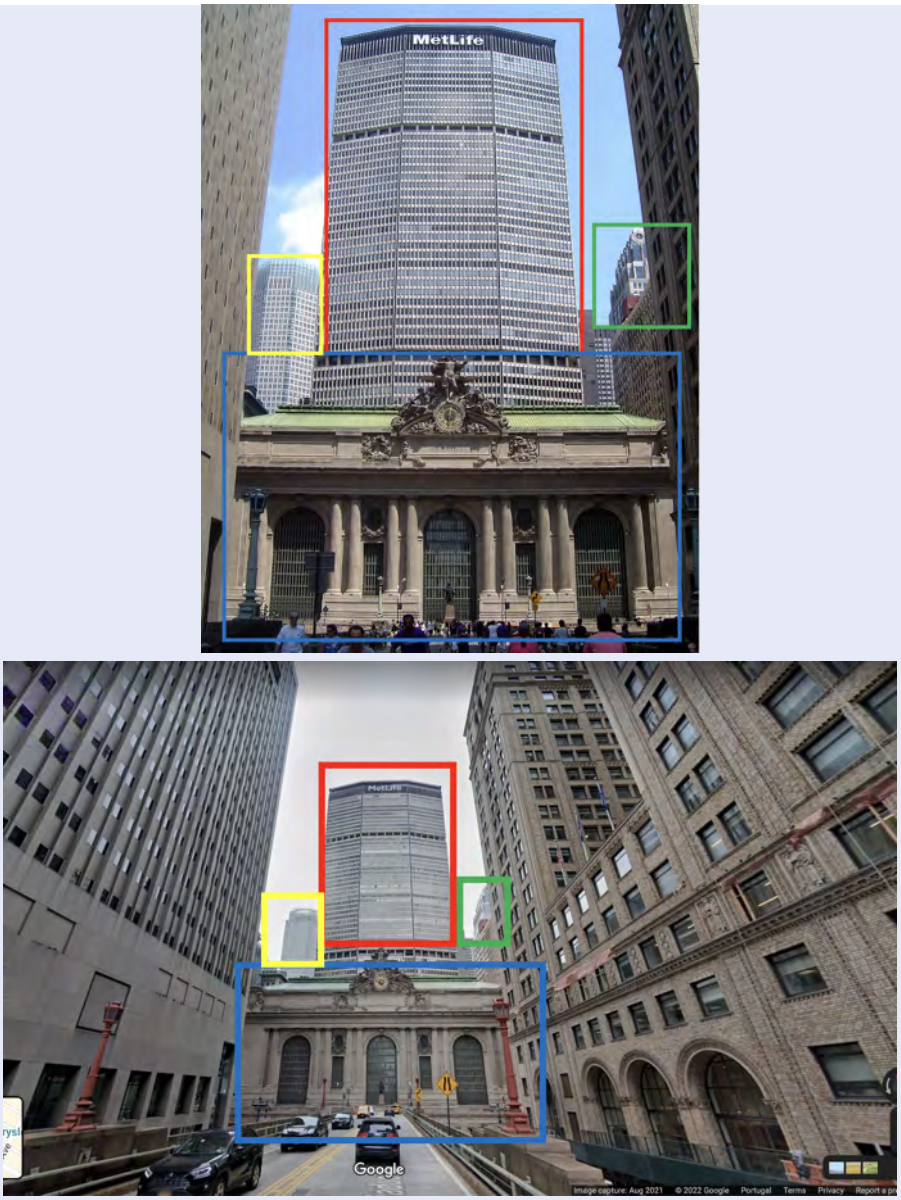
استخدام الدلائل الموجودة في الصور

لتحديد مكان التقاط الصورة الرقمية، تتضمّن الصور أحيانًا دلائل يمكن استخدامها كمعلومات رئيسية. ويمكن البحث عن التفاصيل الظاهرة في الموقع مثل المتاجر وأسماء الشوارع. وقد تشير معلومات ظاهرة أخرى أيضًا إلى الموقع مثل لوحات ترخيص السيارات التي تختلف من موقع إلى آخر، والزي الرسمي للشرطة أو الجيش، وشكل مصابيح الشوارع. وقد يساعد هذا النوع من المعالم الموجودة في الصورة أو الفيديو في تضييق نطاق الاحتمالات المعقولة لمكان إنشاء المحتوى.

وغالبًا ما يقوم المحقق بوضع تعليقات على لقطة الشاشة التابعة لصورة أو لمقطع فيديو ما باستخدام مربّعات ملونة لتسليط الضوء على معالم معيّنة، مثل المباني أو الأشجار المميّزة أو سلاسل الجبال المرئية، والتي تُستخدم كجزء من التحليل. وبعد تحديد هذه المعالم، يمكن للمحققين مطابقتها مع الموقع باستخدام تقنية أو أكثر من التقنيات التالية:

التجوّل الافتراضي Street view أو الخرائط ثلاثية الأبعاد

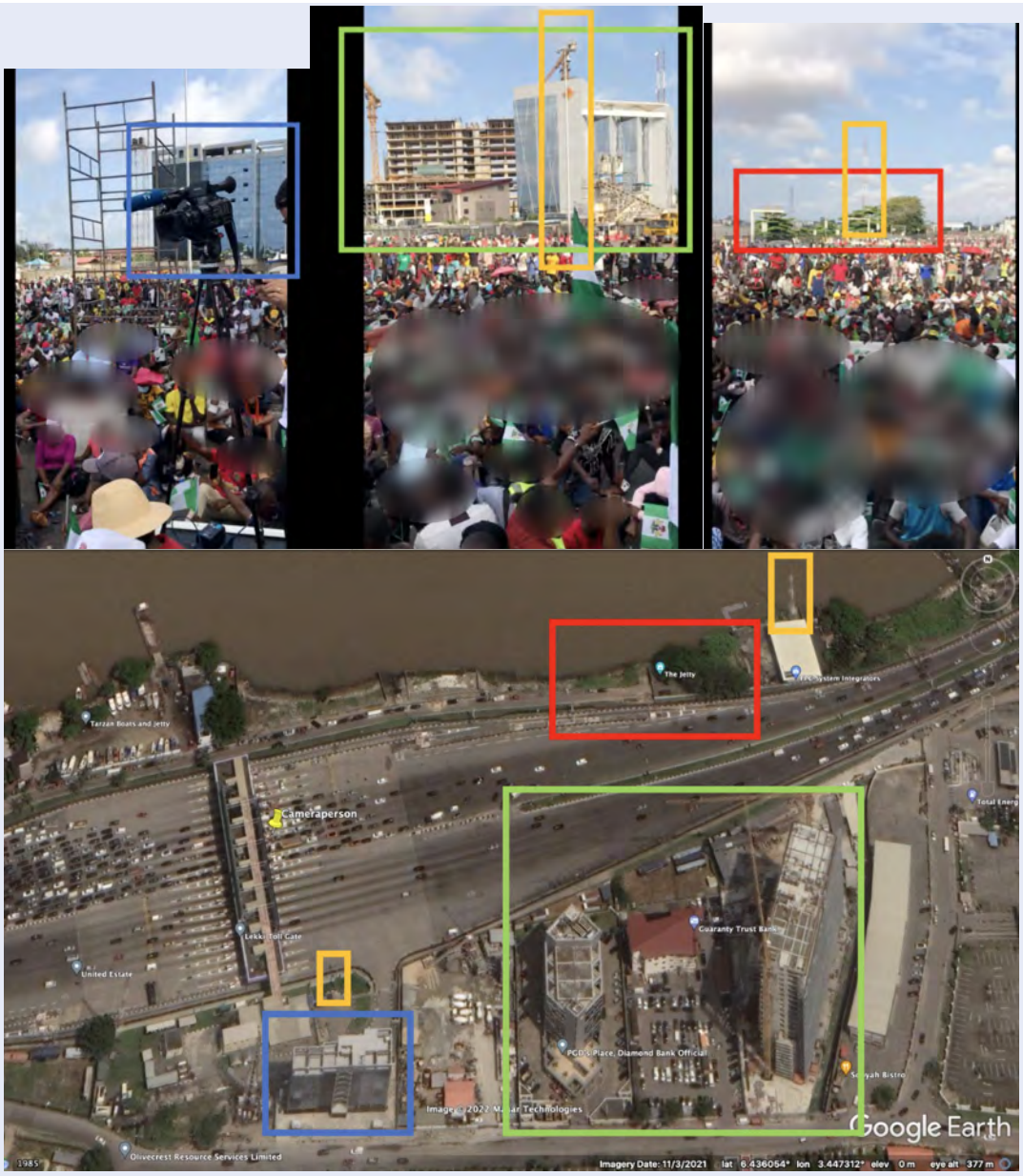
يمكن استخدام التجوّل الافتراضي أو رؤية الشارع Street view أو الخرائط ثلاثية الأبعاد الأخرى لمطابقة المعالم حيثما أمكن وقد يكون مفيدًا أن تكون المباني أو المعالم معنونة من قبل



الشكل د: مثال على استخدام ميزة التجوّل الافتراضي لمطابقة صورة من Google Images لمحطة Grand Central Station في مدينة نيويورك (الصورة العلوية) مع صور التجوّل الافتراضي على خرائط Google (الصورة السفلية).

صور الأقمار الصناعية

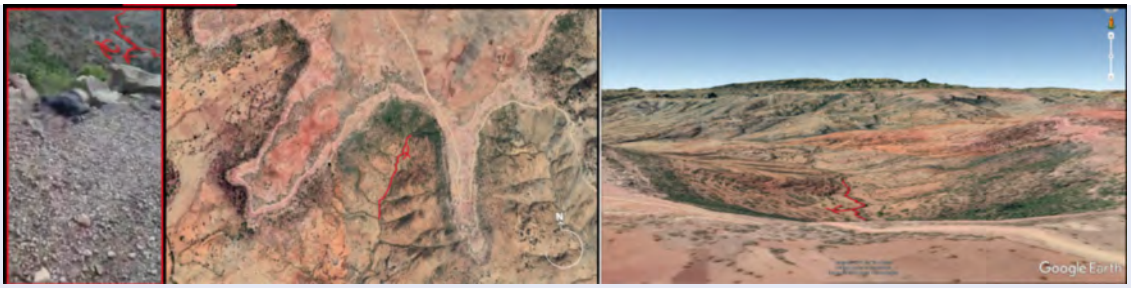
يمكن استخدام صور الأقمار الصناعية لمطابقة المعالم من زاوية علوية. يتم ذلك عادةً باستخدام علامات، مثل المربّعات الملونة، لإبراز البنى الظاهرة في الصورة أو الفيديو التي تتطابق مع النقاط الموجودة على صور الأقمار الصناعية.



الشكل هـ: تحديد الموقع الجغرافي لمقطع فيديو لحادث وقع في Lekki Tollgate في نيجيريا، أجرته وحدة التحقق الرقمي في جامعة إسيكس. قام المحققون بوضع التعليقات على الصور باستخدام مربعات ملوّنة للإشارة إلى المكان الذي تبدو فيه البنى التي تظهر في الفيديو مفتوح المصدر متطابقة مع البنى الظاهرة في صور القمر الصناعي من Google Earth Pro.

رسم خرائط التضاريس

يتضمّن رسم خرائط التضاريس البحث عن المعالم الطبوغرافية مثل سلاسل الجبال ومطابقتها مع صور الأقمار الصناعية، وهذا يعدّ مفيدًا في حال عدم توفّر التجوال الافتراضي أو في حال كانت هناك بنى قليلة من صنع الإنسان ظاهرة في الصور الملتقطة، أو في حال لا تتوفر سوى الصور السيئة الجودة.



الشكل واو: مثال لرسم خريطة التضاريس مأخوذ من تحديد الموقع الجغرافي في مختبر أدلة المواطنين التابع لمنظمة العفو الدولية لمقطع فيديو لحادث وقع في ماهبيري ديغو في إثيوبيا. وقد تمّت مطابقة الجبال المحددة بخطوط حمراء في خلفية الفيديو مع صور الأقمار الصناعية من Google Earth Pro.

مشاكل تحديد الموقع الجغرافي

غالبًا ما يستغرق تحديد الموقع الجغرافي وقتًا طويلاً وقد يكون في غاية الصعوبة. لذلك فمن المهمّ أن نفهم محدوديته. وعلى تقرير التحقيق المصاحب لتحديد الموقع الجغرافي تفسير المنهجية المعتمدة بشكل واضح وشرح القيود التي تحدّ التحليل.

على سبيل المثال، عادةً ما يتضمّن تحديد الموقع الجغرافي مقارنة المحتوى بصور الأقمار الصناعية التي قد تختلف من حيث توفّرها وجودتها. فوفقًا للنقطة على الأرض، قد تكون صور الأقمار الصناعية أقلّ جودةً بسبب وجود بعض القيود (على سبيل المثال، عندما تمنع الحكومات شركات صور الأقمار الصناعية من توفير صور عالية الدقّة لمناطق معيّنة، وهو ما حدث سابقًا في غزة).[36] كذلك قد يحجب الغطاء السحابي صور الأقمار الصناعية، كما قد تقوم بعض الحكومات بالتعتيم على بعض المناطق (على سبيل المثال، عند كتابة هذا التقرير، كانت الصين تحجب مناطق في منطقة شينجيانغ على خرائط بايدو).[37] وإذا كانت اللقطات مصوّرة في الداخل، قد يكون تحديد الموقع الجغرافي عبر المقارنة مع صور الأقمار الصناعية مستحيلًا؛ وفي هذه الحال لا بدّ من استخدام طرق أخرى مثل البحث العكسي عن الصور والبحث القائم على الدلائل. وبسبب عامل واحد أو أكثر من هذه العوامل، أو ببساطة بفعل غياب أي خصائص محددة في اللقطات (على سبيل المثال، مقطع فيديو تم تصويره في البحر من دون أي معالم ظاهرة)، قد يكون تحديد الموقع الجغرافي صعبًا جدًا أو مستحيلًا. وفي الحالات التي لا يكون فيها تحديد الموقع الجغرافي ممكنًا، من المهمّ أن يقدّم المحقق شرحًا لسبب عدم تمكنّه من تحديد الموقع الجغرافي للمحتوى.

الرسائل الرئيسية: هناك طرق متعدّدة يمكن للمحققين استخدامها عند تحديد مكان التقاط الصورة أو الفيديو، بما في ذلك على سبيل المثال لا الحصر: تحليل البيانات الوصفية، والبحث العكسي عن الصور والفيديو، واستخدام الدلائل الموجودة في الصورة، ومطابقة المعالم مع صور الأقمار الصناعية، ورسم خرائط التضاريس. ولكلّ هذه الطرق محدودياتها. ولا بدّ لأي من عمليات تحديد الموقع الموثوقة أن تراعي وتستخدم طرقًا متعدّدة للتحليل.

36 Christopher Giles and Jack Goodman, 'Israel-Gaza: Why is the region blurry on Google Maps?' (*BBC News*, 17 May 2021) < https://www.bbc.co.uk/news/57102499>.

37 Alison Killing, Megha Rajagopalan, and Christo Buschek, 'Blanked-Out Spots On China's Maps Helped Us Uncover Xinjiang's Camps' (*Buzzfeed News*, 27 August 2020) <https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps>.

معلومات خاصة بالوقت

عادةً ما يكون تحديد وقت التقاط الصورة أو مقطع الفيديو أصعب من تحديد مكان التقاطها، على الرغم من أنّ عملية التحقيق تتّبع أساليب مماثلة. عند تقييم وقت إنشاء صورة أو مقطع فيديو ما، عادةً ما ينظر المحقق أولاً في البيانات الوصفية لتحديد ما إذا كانت تحتوي على ختم زمني يحدّد تاريخ الإنشاء. ومع ذلك، في كثير من الحالات، تكون البيانات الوصفية إمّا غير دقيقة أو غير موجودة. لذلك يحتاج المحقّقون إلى استخدام تقنيات أخرى لتحديد الموقع الزمني للصورة أو الفيديو. ويشير تحديد الموقع الزمني إلى "تأكيد تاريخ ووقت الأحداث الواردة في معلومة ما عادةً ما تكون موادًا بصرية".[38] في ما يلي بعض تقنيات تحديد الموقع الزمني الشائعة:

تحميل الختم الزمني بالوقت والتاريخ
قد يكون الختم الزمني الذي يشير إلى وقت وتاريخ وضع المنشورات على الإنترنت مفيدًا لتحديد الموقع الزمني، وهو يوضع دائمًا مع المنشور على مواقع التواصل الاجتماعي. والأهمّ من ذلك، أنّ الختم الزمني أي ختم الوقت والتاريخ يشير إلى الوقت الذي قام فيه هذا الحساب المحدّد بتحميل المحتوى، وليس إلى وقت إنشاء المحتوى. لذلك، يمكن استخدام ختم الوقت والتاريخ كمؤشر على الإطار الزمني للحدث، وقد يشكّل نقطة بداية مفيدةً لتحديد الموقع الزمني، ولكن لا يمكن الاعتماد عليه لمعرفة الوقت الفعلي لوقوع هذا الحدث بشكل قاطع.

بالإضافة إلى ذلك، قد يختلف الختم الزمني وفقًا للمنصة التي نُشر المحتوى عليها، حيث تعمل مواقع التواصل الاجتماعي المختلفة في مناطق زمنية مختلفة أو تتّبع بروتوكولات مختلفةً للأختام الزمنية. على سبيل المثال، قد تعرض بعض المنصات منشورات في الوقت والتاريخ التابعين للمنطقة الزمنية المحلية للمشاهد، أو للمنطقة الزمنية التي تقع فيها الشركة، وليس وفقًا للمنطقة الزمنية للموقع الذي تمّ فيه التقاط الصورة أو الفيديو في الأصل.

تحديد الدلائل في الصورة

تتضمّن الصور أحيانًا دلائل قد تساعد في تحديد تاريخ أو وقت التقاط الصورة أو الفيديو. وقد كانت هذه هي الحال دائمًا ولكنّ النفاذ إلى هذه الدلائل قد يكون الآن أسهل. على سبيل المثال، إذا كانت هناك تفاصيل مؤقتة على غرار ملصقات موجودة في خلفية الصورة، قد تساعد الصور القديمة المتوفّرة الآن في خاصية التجوّل الافتراضي في تحديد الوقت التي تمّ فيه وضع تلك الملصقات. حدث ذلك عندما اتُهم مساعد ترامب السابق، جورج بابادوبولوس، بمغادرة البلاد خلال فترة خضوعه للتحقيق من قبل مكتب التحقيقات الفيدرالي بعد أن نُشرت له صورة في لندن.[39] وتمكّن الصحفيون من إثبات أنّ الصورة لم تُؤخذ في الوقت المزعوم بسبب الدلائل الموجودة في خلفية الصورة، بما في ذلك ملصق موضوع على عمود إنارة وقد تبيّن في النهاية أنّ الصورة عمرها أربع سنوات وليست جديدة.[40] وقد تساعد دلائل أخرى موجودة في الصورة أو الفيديو، على غرار زينة عيد الميلاد، في تحديد الموسم الذي تمّ فيه إنشاء المحتوى. ولكن بطبيعة الحال، يمكن التلاعب بهذه التفاصيل حيث من الممكن إضافتها إلى المحتوى أو حذفها منه.

تحليل الظلّ

يُبنى تحليل الظلّ على أنّه بإمكان الظلال التي تلقي بها الأغراض والأفراد أن تشير إلى موقع الشمس عند

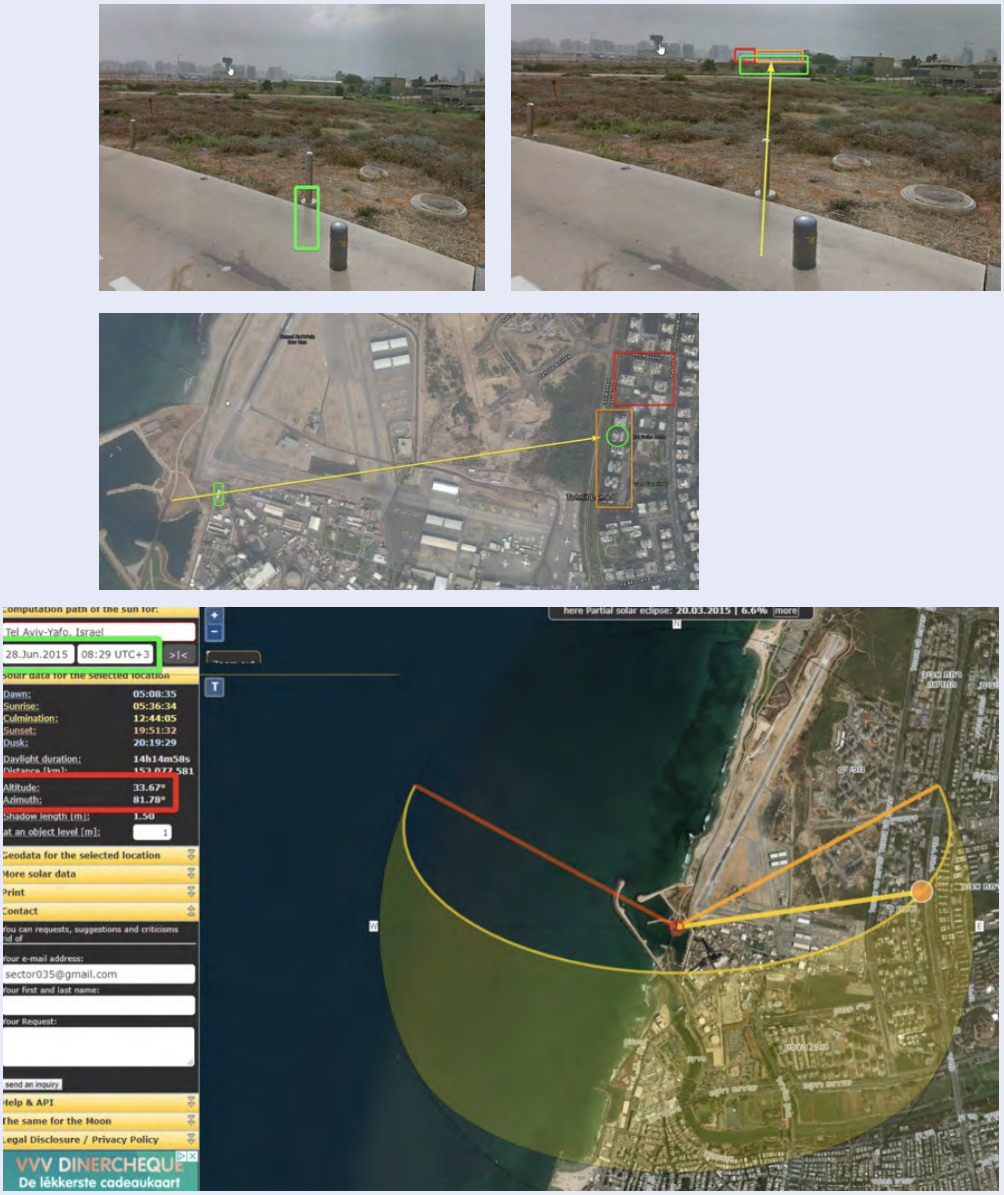
---

38 بروتوكول بيركلي, § 191.

39 George Bowden and Jack Sommers, 'London Photo Of George Papadopoulos Was Taken At Least Four Years Ago' (*HuffPost*, 31 October 2017) <https://www.huffingtonpost.co.uk/entry/george-papadopoulos-twitter-donald-trump-london-picture_uk_59f8793ae4b09b5c2568ff4c>.

40 المرجع نفسه.

التقاط الصورة . وإذا كان الموقع والتاريخ معروفين، فإنّ بمقدور طول واتجاه الظلّ الذي تنتجه أشعّة الشمس والظاهر في الصورة أن يشير إلى الوقت التقريبي الذي تمّ فيه التقاط الصورة أو الفيديو. وتقوم برامج حساب الظلّ بحساب طول الظل التقريبي واتجاهه بشكل مستقل وذلك بالنسبة إلى البنى ذات الأحجام المختلفة وبناءً على موضع الشمس في الموقع والتاريخ والوقت التقريبي الذي يدخله الباحث.[41] ومع ذلك، فإنّ تحليل الوقت باستخدام هذه الأدوات غير دقيق. وعندما يكون من الممكن تحليل الظلّ فهو يعطي المحقق من خلال الفحص البصري أفضل تقدير للنافذة الزمنية التي تمّ فيها التقاط صورة أو مقطع فيديو، ولكنه لا يعطيه حسابًا دقيقًا.



الشكل ز: تحديد الموقع الزمني قام به Sector035 لصورة تمّ التقاطها على المسار الوطني الإسرائيلي في تل أبيب. في الصورة الأولى تم تحديد الظل ثم تم تمديد طوله ليتوافق مع المباني الموجودة في الخلفية (الصورتان الثانية والثالثة). ثم تمّ استخدام SunCalc لتقدير الوقت الموافق لذلك.
https://medium.com/quiztime/lining-up-shadows-2351ae106cec

41 Youri van der Weide, 'Using the Sun and the Shadows for Geolocation' (*Bellingcat*, 3 December 2020) <https://www.bellingcat.com/resources/2020/12/03/using-the-sun-and-the-shadows-for-geolocation/>.

التحليل التاريخي للطقس

يمكن استخدام تقارير الطقس التاريخية لتأكيد وقت التقاط الصورة أو مقطع الفيديو، بشكل عام من خلال إظهار أنّ الطقس الظاهر في الصور يتوافق مع الطقس المبلّغ عنه في التقارير في التاريخ المفترض. ومع ذلك، قد يكون التحليل التاريخي للطقس غير موثوق به، حيث يمكن في يومنا هذا تغيير الظروف الجوية في الصور أو مقاطع الفيديو مع توفر تقنية الخوارزميات والتزييف العميق.[42]

البحث العكسي عن الصور أو مقاطع الفيديو

يمكن أيضًا استخدام البحث العكسي عن الصو لتحديد الموقع الزمني. وقد يكون البحث العكسي عن الصور مفيدًا لاختبار الفرضيات المتعلّقة بوقت إنشاء الصورة أو الفيديو. على سبيل المثال، إذا كان التعليق التوضيحي لصورة ما يدّعي أنه تم التقاطها في تاريخ محدد (على سبيل المثال، كانون الأول/ديسمبر 2017)، ولكن البحث العكسي عن الصورة يظهر أنها كانت موجودة على الإنترنت في وقت سابق (على سبيل المثال شباط/فبراير 2014)، فهذا يشير إلى أنّ الصورة لم يتم التقاطها فعليًا في التاريخ المزعوم. ومع ذلك، إذا لم يسفر البحث العكسي عن الصور عن أي نتائج، فهذا لا يعني أنّ المحتوى لم يكن موجودًا من قبل، حيث أنّ المعلومات الموجودة على قواعد بيانات البحث لا تمثل سوى نسبة صغيرة من المعلومات الموجودة على الإنترنت. بشكل عام، عندما تسفر عمليات البحث العكسي عن الصور عن نتائج فهي تقدّم معلومات مفيدةً تسمح باختبار فرضيات الباحثين، ولكن إذا لم تسفر عن أي نتائج، لا ينبغي افتراض أنّ الصورة أو الفيديو لم يكن موجودًا من قبل.

مقارنة صور الأقمار الصناعية

يمكن مقارنة صور الأقمار الصناعية لتحديد الموقع الزمني عندما تكون هناك تغييرات ظاهرة في صور الأقمار الصناعية طرأت على المنطقة مع مرور الوقت. على سبيل المثال، يمكن استخدام صور الأقمار الصناعية التاريخية لتضييق الإطار الزمني الذي تمّ فيه تشييد المباني أو تدميرها.[43] فمن خلال عرض صور من فترات زمنية مختلفة، يمكن للمحللين معرفة متى ظهرت معالم جديدة أو اختفت. على سبيل المثال، قد تشير صور الأقمار الصناعية إلى الوقت الذي تمّ فيه حرق مبنى ما أو تدنيس معلم ثقافي ما،[44] أو قد تظهر تربةً مقلوبةً ممّا قد يشير إلى وجود مقبرة جماعية. ومع ذلك، فمن المهمّ أن نعرف أنّ صور الأقمارالصناعية (خاصةً تلك المتوفرة للجمهور العام صور مثل Google Earth Pro) لا تحتوي عادةً على صور تاريخية.

42 Samantha Cole, 'Watch an Algorithm Turn Winter Into Summer in Any Video' (*Vice*, 5 December 2017) <https://www.vice.com/en/article/xwvz9a/watch-an-algorithm-turn-winter-into-summer-in-any-video-image-to-image-translation>.

43 Sam Dubberley and Joe Freeman, 'Killings, corruption, land grabs: human rights violations against the Rohingya today' (*Amnesty International*, 25 August 2020) <https://citizenevidence.org/2020/08/25/rohingya-verification/>.

44 Benjamin Strick, 'Geolocation of Infrastructure Destruction in Cameroon: A Case Study of Kumbo and Kumfutu' (*Bellingcat*, 21 November 2018) <https://www.bellingcat.com/resources/case-studies/2018/11/21/geolocation-infrastructure-destruction-cameroon-case-study-kumbo-kumfutu/>; SITU Research, 'ICC Digital Platform: Timbuktu, Mali' <https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali>.

الشكل ح: لقطة شاشة للمنصة الرقمية التي طورتها شركة SITU Research لصالح المحكمة الجنائية الدولية والتي تصوّر تدمير مواقع التراث الثقافي في مالي. وتظهر الصور موقع ضريح الكونتي قبل وبعد التدمير. (http://icc-mali.situplatform.com/).

الرسائل الرئيسية: يمكن للمحققين استخدام طرق متعدّدة لتقدير وقت التقاط الصورة الرقمية، بما في ذلك (على سبيل المثال لا الحصر) تحليل البيانات الوصفية، وتحليل الظل، والدلائل الموجودة في الصورة، والتحليل التاريخي للطقس، وتحليل وقت التحميل وتحليل الختم الزمني، وعمليات البحث العكسي عن الصور والفيديو، ومقارنة صور الأقمار الصناعية. ولكلّ هذه الطرق محدودياتها. ولا بدّ لأي تقييم موثوق يتعلّق بموعد التقاط الصورة الرقمية أن يأخذ في الاعتبار ويستخدم طرق تحليل مختلفة.

.5

الخاتمة

تُستخدم الصور الرقمية مفتوحة المصدر بشكل متزايد من قبل المحاكم والهيئات التابعة لمعاهدات حقوق الإنسان وغيرها من هيئات تقصي الحقائق. ويمكن أن تشكّل مادةً إثباتيةً مهمةً في التقييم الجنائي والقضائي للانتهاكات المشتبه بها للقانون الدولي لحقوق الإنسان وللقانون الإنساني الدولي وللقانون الجنائي الدولي، ويمكن أن يقدّمها كلّ من الادعاء والدفاع في المحاكمات الجنائية لدعم قضيته. ومع ذلك، فإنّ الاستخدام المتزايد للصور ومقاطع الفيديو مفتوحة المصدر كأدلّة ينطوي على مخاطر منها سوء التفسير أو الاعتماد الذي هو في غير محله إمّا على المواد مفتوحة المصدر وإمّا على تحليل المحققين. وقد وُضعت التقنيات والأوصاف الواردة في هذا الدليل بهدف مساعدة القضاة وهيئات تقصي الحقائق عند تقييم المواد الرقمية مفتوحة المصدر. وفي الوقت نفسه، لا بدّ أن يشكّل هذا النوع من المواد جزءًا من مجموعة أكبر من الأدلة المعروضة على المحكمة أو هيئة تقصي الحقائق. ولا بدّ في نهاية المطاف من تقييم المعلومات الرقمية مفتوحة المصدر باستخدام قواعد الإثبات الشاملة نفسها التي تتبعها المؤسسة أو المحكمة، ولا بدّ من أن تخضع للأعباء ولمعايير الإثبات التي تحددها هذه المؤسسة أو المحكمة.

قائمة المصطلحات

الذكاء الاصطناعي (AI) : فرع من علوم الكمبيوتر مخصّص لتطوير برمجيات تسمح للآلات بتعلّم كيفية التفاعل مع متغيّرات غير معروفة والتكيّف مع بيئات جديدة.

تحديد الموقع الزمني : تأكيد تاريخ ووقت الأحداث المصوّرة في معلومة ما، عادةً ما تكون موادًا مصوّرة. على سبيل المثال، قد يكون من الممكن تحديد الوقت الذي تمّ فيه التقاط الصورة عن طريق فحص طول الظلال الناتجة عن ضوء الشمس، بالإضافة إلى مؤشرات أخرى.

الإنترنت المظلمة: جزء من الإنترنت لا يمكن الوصول إليه إلا عن طريق برامج متخصصة، ويسمح للمستخدمين ولمشغلي مواقع الويب بالحفاظ على سرية هويتهم كما ولا يسمح بتعقبهم.

الإنترنت العميقة: جزء من الإنترنت غير مفهرس وبالتالي لا يمكن الوصول إليه عبر محركات البحث.

معلومات رقمية مفتوحة المصدر: معلومات متاحة للجمهور في شكل رقمي يتمّ الحصول عليها عادة من الإنترنت.

تحديد الموقع الجغرافي : تحديد أو تقدير موقع غرض أو نشاط ما أو الموقع الذي تم فيه إنشاء محتوى ما. على سبيل المثال، قد يكون من الممكن تحديد الموقع الذي تمّ التقاط مقطع فيديو أو صورة فوتوغرافية تمّ تنزيلها من الإنترنت باستخدام تقنيات تحديد الموقع الجغرافي. ويمكن أن تشمل هذه التقنيات، على سبيل المثال، تحديد المعالم الجغرافية الفريدة في صورة فوتوغرافية وتحديد موقعها الفعلي على الخريطة.

قيمة التجزئة التشفيرية: عمليات حسابية يمكن تطبيقها على أي نوع من الملفات الرقمية لتوليد سلسلة أبجدية رقمية ذات طول ثابت يمكن استخدامها كدليل على أنّ الملف الرقمي لم يتم تعديله منذ أنّ تم تجزئة هذا المحتوى. وتبقى هذه السلسلة على حالها في كلّ مرة يتم فيها تطبيق العملية الحسابية طالما لم يطرأ أي تغيير على الملف.

البيانات الوصفية: هي بيانات عن البيانات. وهي تحتوي على معلومات حول ملف إلكتروني إمّا مُضمّنة في ملف ما أو مرتبطة به. وغالبًا ما تحتوي البيانات الوصفية على خصائص الملف وتاريخه، غلى غرار عنوانه وحجمه وتاريخ إنشائه وتاريخ تعديله. وقد تصف البيانات الوصفية كيف ومتى ومن قام بجمع الملف الرقمي وإنشائه والنفاذ إليه وتعديله وتنسيقه.

المعلومات مفتوحة المصدر: المعلومات التي يمكن لأي فرد من الجمهور مشاهدتها أو شرائها أو طلبها، من دون الحاجة إلى صفة قانونية خاصة أو نفاذ غير مصرّح به.

حجب الهوية باستخدام هوية مستعارة: معالجة البيانات الشخصية بطريقة لا يمكن فيها نسب المعلومات إلى صاحب بيانات محدد من دون استخدام معلومات إضافية.

البحث العكسي عن الصور/الفيديوهات : يتضمّن البحث العكسي تحميل صورة أو مقطع فيديو على محرك بحث ما لتتمكّن خوارزمية البحث من رصد نسخ أخرى من الصورة نفسها أو صور مشابهة لها على الإنترنت. وتتمثّل محدودية البحث العكسي عن الصور في أنّ محركات البحث تقوم بالبحث في الصور الموجودة فقط في قاعدة البيانات التابعة لها والتي لا تتضمّن إلا نسبةً صغيرةً من المحتوى الموجود

حاليًا على الإنترنت. وهي لا تتضمّن، على سبيل المثال، المواد التي يتم تحميلها علىشبكة الإنترنت العميقة (التي لا يتم ربطها بمحركات البحث) أو شبكة الإنترنت المظلمة (وهي جزء من الإنترنت لا يمكن الوصول إليه إلا من خلال برامج متخصصة، مثل متصفّح تور).

المواد السمعية البصرية الاصطناعية: يُشار إليها أيضًا باسم المواد السمعية البصرية التوليدية، ويتمّ تعريفها على أنها محتويات سمعية أو بصرية أو متعددة الوسائط تم إنشاؤها أو تعديلها بواسطة الخوارزميات (عادةً عبر الذكاء الاصطناعي). وغالبًا ما تكون هذه المخرجات واقعيةً جدًا ولا يمكن للشخص العادي أن يعرف أنها اصطناعية، وقد تحاكي المنتجات المصنوعة يدويًا أو الأشخاص أو الأحداث.

التَحَقّق : يشير إلى عملية التحقق من دقة أو صحة المعلومات التي تمّ جمعها على الإنترنت. ولا بدّ من فحص المصدر والمحتوى والمادة أو الملف الرقمي بشكل جماعي ومقارنتها للتحقّق من تجانسها.

شكر وتقدير

لقد تم تمويل الترجمة والإنتاج من خلال حساب تسريع التأثير ESRC التابع لجامعة سوانسي ومشروع TRUE في جامعة سوانسي، بتمويل منحة الأبحاث UKRI Frontier Research Grant EP/ X016021/1. وحظي هذا العمل أيضًا بدعم معهد العلوم الإنسانية والاجتماعية (IHSS) في جامعة كوين ماري في لندن.

ونودّ أن نشكر الأفراد التالي ذكرهم الذين تقدموا جميعًا بتعليقات مفيدة حول جوانب مختلفة من النص في مراحل مختلفة من عملية الصياغة: **داتو شيامالا ألاجيندرا،** محامي جنائي دولي؛ **هادي الخطيب،** المدير العام لشركة Mnemonic؛ **شوبان ألين،** محامية أولى، الشبكة العالمية للعمل القانوني (GLAN)؛ **شيرين أنلين**، خبيرة تكنولوجية في الوسائط السمعية البصرية، منظمة ويتنس؛ **سعادة القاضية سولومي بوسا**، قاضية في دائرة الاستئناف في المحكمة الجنائية الدولية؛ جاكوبو كاستيلانوس، منسق في منظمة ويتنس؛ **سعادة القاضي سولومي بوسا**، المحكمة الجنائية الدولية؛ **سعادة القاضية مارغريت دي جوزمان**، الآلية الدولية لتصريف الأعمال المتبقية للمحكمتين الجنائيتين؛ **جيف دويتش**، باحث أول في Mnemonic؛ **مايكل السندي**، باحث في المواد مفتوحة المصدر، Mnemonic؛ **جيسيكا غافرون** ، المديرة القانونية للمركز الأوروبي للدفاع عن حقوق الإنسان؛ **الدكتور ماثيو جيليت**، محاضر أول، كليّة الحقوق وحقوق الإنسان، جامعة إسيكس؛ **جوناثان هاك**، المجلس الملكي، **آن هوسكنشت** ، طالبة دكتوراه، مشروع TRUE، جامعة سوانسي؛ بيتر هاينز المجلس الملكي؛ **البروفيسور لورانس ر. هيلفر**، أستاذ في القانون في جامعة ديوك، وعضو لجنة حقوق الإنسان التابعة للأمم المتحدة؛ غابرييلي جودكايت-جرانسكيني، قاضية في المحكمة العليا في ليتوانيا؛ **كوين كلويسن** ، مفتش مباحث ومحقق في المواد المفتوحة المصدر (الجرائم الدولية)، النيابة العامة الهولندية؛ سعادة القاضية جوانا كورنر، المحكمة الجنائية الدولية؛ البروفيسور فيليب ليتش، أستاذ قانون حقوق الإنسان، جامعة ميدلسكس في لندن؛ كاترينا لاتيش، زميلة في الدرسات ما بعد الدكتوراه في MSCA4Ukraine، جامعة فيلنيوس وأستاذة مشاركة في جامعة ياروسلاف مودري للقانون الوطني؛ نيما ميلانينيا، المستشارة الخاصة للسفير الأمريكي لشؤون العدالة الجنائية العالمية؛ ديربلا مينوغ، محامية أولى، الشبكة العالمية للعمل القانوني (GLAN)؛ جودي ميونكي، محامية دفاع، المحكمة الجنائية الدولية، مسؤولة الاتصال لمنطقة أفريقيا، لجنة قانون حقوق الإنسان التابعة لنقابة المحامين الدولية؛ إيفون إنج، مديرة برنامج الأرشيف، منظمة ويتنس؛ **رالوكا راكوسان**؛ **سعادة القاضي كيث رينور**، قاضي إنجلترا وويلز؛ **ياروسلافنا سيشينكوفا**، مستشارة مستقلة؛ **البروفيسور يوفال شاني**، كرسي هيرش لوترباخت للقانون الدولي، الجامعة العبرية في القدس؛ **كونستانتينا ستافرو**، طالبة دكتوراه، جامعة فيينا؛ **بنجامين ستريك**، مركز مرونة المعلومات؛ **هريهوري زوراكيفسكي**، بعثة المساعدة التابعة للاتحاد الأوروبي إلى أوكرانيا.

كما ونتقدّم بالشكر أيضًا من كافة القضاة الحاليين والسابقين الذين تقدموا بتعليقات ولكنّهم لم يرغبوا في الكشف عن هويتهم.

تقييم المواد المصوّرة الرقمية مفتوحة المصدر:
دليل للقضاة وجهات تقصي الحقائق

The Authors, 2024 ©