MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE JULI 2023
IT-FORENSIK VON BILDERN UND VIDEOS

ANALYSE VON BILDERN UND DOKUMENTEN

IT-Forensik hat in der heutigen Strafverfolgung einen hohen Stellenwert. Wir zeigen auf, wie Bilder und Dokumente als Beweise in Rechtsstreitigkeiten verwendet werden können.

ANALYSE VON VIDEOS

Ein weiterer wesentlicher Aspekt der IT-Forensik ist die Videoanalyse. Wir erklären anhand eines aktuellen Beispiels wie man unter anderem ein Deep Fake Video erkennt.

Bildquelle: https://unsplash.com/de/fotos/ct10qdGv1hQ

Juli 2023: Angst als schlechter Berater

Forensik im elektronischen Bereich findet nicht selten unter grösster Hektik statt. Nämlich dann, wenn eine Kompromittierung entdeckt wurde, die Quelle derer und ihre Auswirkungen schnellstmöglich identifiziert werden müssen. Unter Hochdruck, weil der Betrieb gestört und dadurch der Umsatz eingeschränkt ist.

Es gibt verschiedene unumstössliche Grundlagen in der Forensik: Wohlüberlegtes Handeln, systematisches Vorgehen, exaktes Arbeiten. Das alles ist erforderlich, um keine Fehler zu machen. Denn Fehler sind genau das, was das Vorhaben gefährden kann. Vielleicht wird etwas übersehen. Oder, noch viel schlimmer, es werden versehentlich Beweise zerstört.

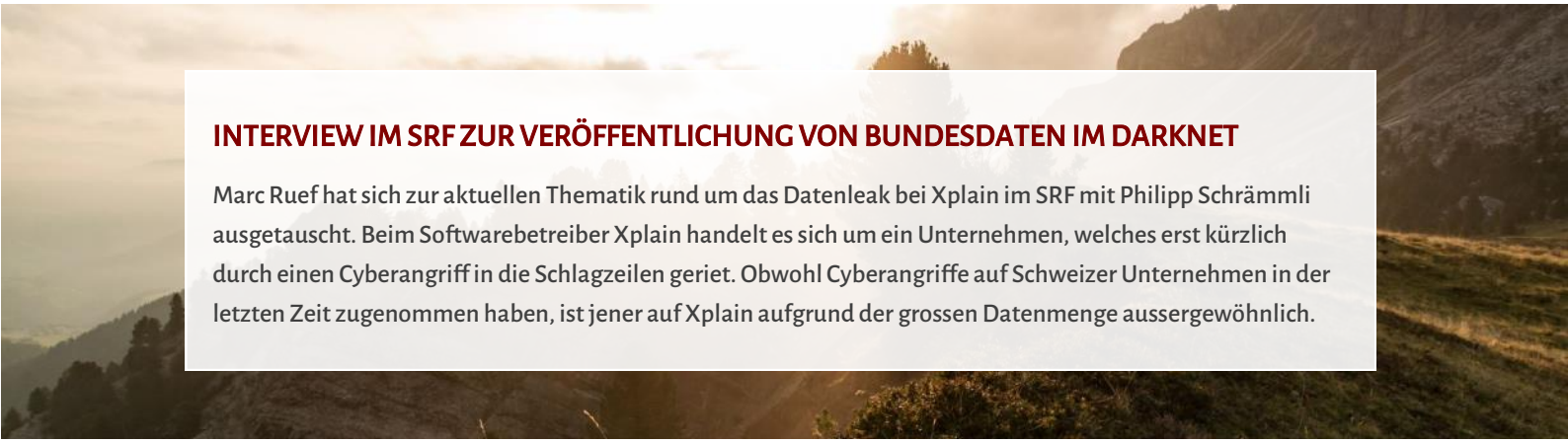
Den Forensikern ist dieses Spannungsfeld bewusst. Sie agieren darin und versuchen die ideale Lösung zu erarbeiten. Die betroffenen Kunden können aber in diesem Momentan nicht klar denken. Eine schier unendliche Hektik prasselt dann auf die Forensiker nieder, die dadurch gleich an mehreren Fronten mental kämpfen müssen. Jeder, der schon einmal in einer solchen Situation war, sehnt sich diese nicht so schnell wieder herbei. Das gilt sowohl für Forensiker als auch für die Opfer.

Marc Ruef
Head of Research

Bildquelle: https://unsplash.com/de/fotos/6p-I-X-sPUY

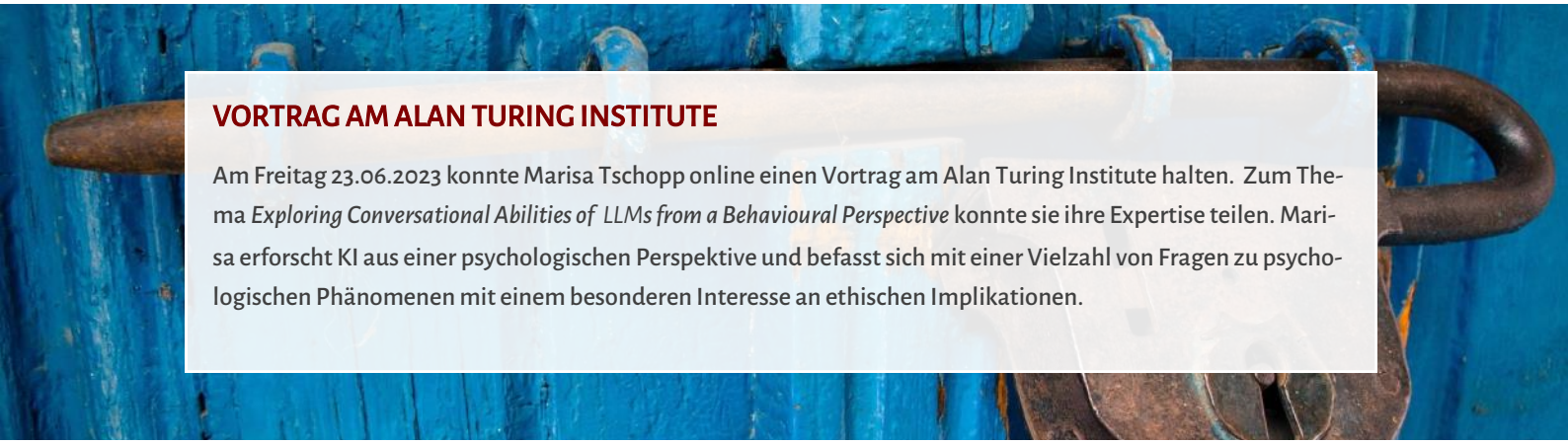
NEWS

WAS IST BEI UNS PASSIERT?



INTERVIEW IM SRF ZUR VERÖFFENTLICHUNG VON BUNDESDATEN IM DARKNET

Marc Ruef hat sich zur aktuellen Thematik rund um das Datenleak bei Xplain im SRF mit Philipp Schrämmli ausgetauscht. Beim Softwarebetreiber Xplain handelt es sich um ein Unternehmen, welches erst kürzlich durch einen Cyberangriff in die Schlagzeilen geriet. Obwohl Cyberangriffe auf Schweizer Unternehmen in der letzten Zeit zugenommen haben, ist jener auf Xplain aufgrund der grossen Datenmenge aussergewöhnlich.



VORTRAG AM ALAN TURING INSTITUTE

Am Freitag 23.06.2023 konnte Marisa Tschopp online einen Vortrag am Alan Turing Institute halten. Zum Thema *Exploring Conversational Abilities of LLMs from a Behavioural Perspective* konnte sie ihre Expertise teilen. Marisa erforscht KI aus einer psychologischen Perspektive und befasst sich mit einer Vielzahl von Fragen zu psychologischen Phänomenen mit einem besonderen Interesse an ethischen Implikationen.

INTERVIEW AUF WATSON ZUM DATENABFLUSS DURCH HACKERBANDE CLOP

Marc Ruef hat sich zum aktuellen Datenklau der Hackerbande *Clop* auf Watson geäussert. Neben Shell und der Universität von Georgia sind hiesige Firmen wie die Schweizerische Krankenkasse ÖVV sowie die Ferienpark-Betreiberin Landal betroffen. *Clop* dürfte dabei kein unbekannter Name mehr sein. Bereits vor einigen Wochen sind die Hackerbande durch einen Ransomware-Angriff in den Schlagzeilen geraten.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

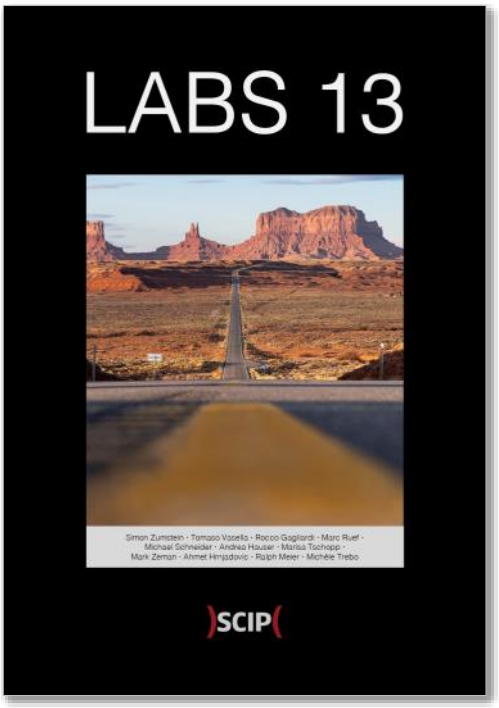
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



IT-FORENSIK ALS DIGITALES BEWEISMITTEL

Bildquelle: https://unsplash.com/de/fotos/fN6K30xtiKE

MICHÈLE TREBO & RALPH MEIER

IT-FORENSIK
ANALYSE VON BILDERN UND DOKUMENTEN

Digitale Forensik oder auch IT-Forensik bezieht sich auf die Anwendung von wissenschaftlichen Techniken und Methoden, um digitale Beweise gerichtsverwertbar zu erheben. Es umfasst die Untersuchung von Daten, die auf digitalen Geräten wie Computern, Mobiltelefonen, Servern, Speicherkarten und anderen digitalen Speichermedien gespeichert sind.

IT-Forensik hat in der heutigen Strafverfolgung einen hohen Stellenwert. Mit der zunehmenden Digitalisierung werden immer mehr Beweismittel in digitaler Form gespeichert. Die IT-Forensik bietet die Möglichkeit, diese digitalen Beweismittel so zu sammeln, zu analysieren und zu bewerten, dass sie vor Gericht verwertbar sind. Die Bedeutung der IT-Forensik geht jedoch weit über die Strafverfolgung hinaus. Unternehmen und Organisationen nutzen IT-Forensik, um Datenverluste, Betrug, Verletzung von Datenschutzrichtlinien und andere Vorfälle zu untersuchen. Die Bild- und Dokumenten-Analyse ist ein wichtiger Aspekt der IT-Forensik, da Bilder beziehungsweise digitale Dokumente oft wichtige Beweise in Fällen von Straftaten, Urheberrechtsverletzungen und anderen Rechtsstreitigkeiten darstellen können. Bei der Analyse von Bildern und Dokumenten werden verschiedene Techniken und Methoden eingesetzt, um die Integrität und Authentizität zu überprüfen und Informationen zu gewinnen.

WAHRUNG DER INTEGRITÄT VON DIGITALEN BEWEISMITTELN

Bevor die Analyse von digitalen Beweismitteln beginnen kann, muss eine sichere Konservierung durchgeführt werden. Eine sichere Konservierung ist notwendig, damit vor Gericht die Unversehrtheit (Integrität) und Echtheit (Authentizität) von digitalen Bildern und Dokumenten bewiesen werden kann. Dabei wird das gesamte Speichermedium physisch ausgelesen und entweder in Form eines Images oder ein Teilbereich in Form von logischen Dateien wie Dokumente, Emails von einem Email-Server, Auszüge aus spezifischen Programmen, Datenbanken oder Netzwerklaufwerken (Liste nicht abschliessend) geklont. Nach dem Klonen wird ein Hashwert der gesicherten Datenbestände errechnet und gespeichert. Dabei werden meistens Hash-Algorithmen wie MD5, SHA1 oder SHA256 eingesetzt. Wobei MD5 und SHA1 nicht mehr eingesetzt werden sollten, da diese Hash-Funktionen nicht

mehr als kollisionsresistent gelten. Um die Integrität und Unveränderlichkeit des ursprünglich sichergestellten Beweismittels zu gewährleisten, finden die forensischen Analysen der Daten ausschliesslich auf dem Klon statt. Durch die Arbeit auf einem Klon werden potenzielle Veränderungen oder Manipulationen vermieden, die bei direkter Analyse des Originals auftreten könnten. Der Klon dient als Arbeitskopie, auf der verschiedene Techniken und Tools angewendet werden können, ohne das Original zu beeinträchtigen. Dadurch wird sichergestellt, dass die Ergebnisse der forensischen Analyse verlässlich und vor Gericht verwertbar sind, während das originale Beweismittel unverändert bleibt.

BILDANALYSE

Die Analyse von Bildern ist ein wichtiger Bestandteil der IT-Forensik und erfordert spezielle Kenntnisse und Fähigkeiten. Der Einsatz von verschiedenen Technologien wie die Metadatenanalyse, die forensische Bildanalyse, die Gesichtserkennung, die teilweise mit Deep-Learning verbessert wird, unterstützen dabei die Beweismittelsicherung. Wichtig zu beachten ist, dass die Verwendung von Bildern als Beweismittel in der IT-Forensik bestimmte Richtlinien und Protokollen folgen muss, um sicherzustellen, dass die Integrität des Beweismittels nicht beeinträchtigt wird. Dies beinhaltet nebst der oben erwähnten sicheren Konservierung auch die Gewährleistung der Kette der Beweismittelführung und die Einhaltung von Best Practices für die Beweismittelaufbewahrung. Üblicherweise stellen die Behörden zuerst die elektronischen Beweismittel in geeigneter Form sicher. Dies kann durch Beschlagnahme von Geräten, Festplatten, USB-Sticks oder anderen Speichermedien erfolgen. Es wird ein Protokoll erstellt, das detaillierte Informationen über den Fund, den Zustand des Beweismittels, den Ort und die beteiligten Personen enthält. Dieses Protokoll dient als Nachweis für die ordnungsgemässe Sicherstellung. Die elektronischen Beweismittel werden anschliessend sicher und kontrolliert transportiert, um Verlust oder Beschädigung zu vermeiden. Dies kann durch den Einsatz spezialisierter Transportmittel oder verschlüsselter Speichermedien erfolgen. Nach der Sicherstellung werden die Beweismittel versiegelt, um sicherzustellen, dass sie während der Aufbewahrung nicht manipuliert werden. Dies kann durch den Einsatz von Siegeln, Sicherheitsetiketten oder digitaler Ver-

siegelungstechnologie erfolgen. Bei der sicheren Aufbewahrung der Beweismittel werden Massnahmen ergriffen, um unbefugten Zugriff, Beschädigung oder Verlust zu verhindern.

METADATENANALYSE

Metadaten sind Informationen über eine Datei, die in der Datei selbst gespeichert sind. Durch die Analyse von Metadaten können Informationen wie der Erstellungszeitpunkt, je nach Datei der Standort und das verwendete Gerät abgerufen werden. Wenn zum Beispiel ein Bild nach dessen Aufnahme bearbeitet wurde, kann dies ebenfalls in den Metadaten der Datei ersichtlich sein, sofern diese Informationen nicht gezielt entfernt wurden. Eine Einführung in EXIF-Tags ist im Artikel Technische Bild-Forensik zu finden. Die gesetzten EXIF-Tags werden vom Kamera- beziehungsweise Gerätehersteller bestimmt. Dies hängt von den Möglichkeiten der Kamera und der Konfiguration des Benutzers ab. Bei der Analyse eines mit dem iPhone geschossenen Bildes kamen folgende interessante EXIF-Tags zum Vorschein:

- Camera Model Name : iPhone 11 Pro
- Software : 16.3.1
- Lens Model : iPhone 11 Pro back triple camera 4.25mm f/1.8

Es kam auch ein etwas skurriler EXIF-Tag hervor, mit welchem nicht gerechnet wurde:

- Run Time Since Power Up : 13 days 17:06:35

Hier wurde die Laufzeit des Geräts seit dem letzten Neustart, die sogenannte Uptime, zum Zeitpunkt der Fotoaufnahme in die EXIF-Informationen des Fotos hineingeschrieben. Mit dieser Information haben wir während der Recherche zu EXIF-Tags nicht gerechnet, da sie sich sehr unterscheidet zwischen Fotoapparaten und Smartphones. Wir konnten bis auf zusätzliche Information für eine möglichen Reparatur an keine weiteren Use-Cases denken. Ein gängiges Tool für die Extraktion von EXIF-Informationen ist das exiftool.

FORENSISCHE BILD-/DOKUMENTENANALYSE

Bei der forensischen Bild- oder Dokumentenanalyse werden verschiedene Techniken verwendet, um die Echtheit eines Bildes oder Dokumentes zu überprüfen und um Manipulationen oder Verfälschungen des Inhaltes aufzudecken. Beispiele hierfür sind die Analyse von Pixeln, die Erkennung von Bildkompression, die Analyse von Wasserzeichen und die Überprüfung der Farbbalance des Bildes. Zur Darstellung von unterschiedlicher Farbbalance in einem Bild oder Dokument hilft der Einsatz eines Histogramms oder anderen Farbdarstellungen, um zum Beispiel die Verwendung von zwei unterschiedlichen Stiften bei einer handschriftlichen Unterschrift aufzuzeigen.

FARBANALYSE EINER UNTERSCHRIFT MIT VERSCHIEDENEN STIFTEN

Die linke Farbdarstellung zeigt die Stiftfarbe des Buchstaben “T”, welche sich deutlich von der Stiftfarbe des Buchstaben “e” unterscheidet, dargestellt auf der rechten Farbdarstellung.

GESICHTSERKENNUNG

Gesichtserkennungstechnologien werden immer häufiger bei der Untersuchung von Straftaten eingesetzt. Diese Technologie ermöglicht es, Gesichter auf Bildern mit anderen Aufnahmen zu vergleichen, um die Identität von Personen zu bestimmen. Dabei können bestehende Bilder inklusiv ein Profilfoto der gesuchten Person in ein Gesichtserkennungstool übermittelt werden. Sind keine Bilder vorhanden, sondern beispielsweise eine Videoaufnahme, ist diese zuerst in Bildausschnitte (zum Beispiel alle drei Sekunden ein Bild) zu unterteilen. Die aus dem Video extrahierten Bilder können anschliessend in ein Gesichtserkennungstool übermittelt werden, wo die Bilder nach den darauf erkennbaren Gesichtern gruppiert werden. Eine mögliche Fotoplattform,

auf welcher eine starke Gesichtserkennung freigeschaltet ist, ist Google Photos. Die Gesichtserkennung von Google Photos läuft grössten Teils vollautomatisch ab. Die genauen Details zur Funktionsweise sind jedoch nicht öffentlich bekannt, da Google keine ausführlichen Informationen zu den internen Algorithmen und Technologien preisgibt. Um die Gesichtserkennung von Google Photos nutzen zu können, ist zuerst ein Google-Konto notwendig. Nach der Installation der Google Photos Applikation und der erfolgreichen Anmeldung mit dem Google-Konto, kann der Zugriff auf die auf dem Gerät vorhandenen Fotos gewährt werden. Nach der Aktivierung der Gesichtserkennung in den Einstellungen, läuft die Gesichtserkennung automatisch. Je nach Anzahl der Fotos und der Geschwindigkeit der Internetverbindung kann dieser Vorgang einige Zeit dauern. Indem erkannten Gesichtern ein Name oder eine Identität hinzugefügt wird, kann die Genauigkeit der Gesichtserkennung verbessert werden.

DEEP-LEARNING-TECHNOLOGIE

Die Verwendung von Deep-Learning-Technologien in Form von trainierten künstlichen neuronalen Netzen oder Ansätze basierend auf Convolutional Neural Networks (CNNs) ermöglichen es, grosse Mengen an Daten effektiver zu analysieren und Muster oder Gesichter in Bildern zu erkennen. Durch den Einsatz von grossen Datensätzen mit Gesichtern aus verschiedenen Perspektiven und mit unterschiedlichen Lichtverhältnissen ist es möglich, Gesichter schneller und akkurater zu identifizieren. Durch eine Verlängerung der Trainingsphase, dem Erweitern des Trainingsdatensets oder durch Änderungen der Architektur des neuronalen Netzwerks kann das eingesetzte Deep-Learning-Modell kontinuierlich verbessert werden.

FAZIT

IT-Forensik entwickelt sich stetig weiter, um den Bedürfnissen der sich immerwährenden ändernden digitalen Landschaft gerecht zu werden. IT-Forensiker werden sich anpassen und neue Technologien, Tools und Methoden entwickeln müssen, um effektiv Beweismittel zu sammeln und zu analysieren. So ermöglicht beispielsweise maschinelles Lernen die schnellere Verarbeitung und Analyse grosser Datenmengen. Durch den Einsatz von Algorithmen des maschinellen Lernens können zudem Muster, Anomalien und Zusammenhänge in den Daten erkannt werden, die auf verdächtige Aktivitäten hinweisen können. Dies hilft Forensikern, potenziell relevante Beweise effizienter zu identifizieren und zu analysieren.

Michèle Trebo

Ralph Meier

Ob Angriff, Verteidigung oder Forschung.

Wir beraten Dich in Sachen Cybersicherheit.

MICHÈLE TREBO & RALPH MEIER

IT-FORENSIK ANALYSE VON VIDEOS

Die digitale Forensik, auch bekannt als IT-Forensik, bedient sich wissenschaftlicher Verfahren und Methoden, um digitale Beweise zuverlässig zu erfassen, damit sie vor Gericht verwendet werden können. Sie beinhaltet die Untersuchung von Daten, die auf verschiedenen digitalen Geräten wie Computern, Mobiltelefonen, Servern, Speicherkarten und anderen Speichermedien gespeichert sind.

Die Bedeutung der IT-Forensik erstreckt sich über die Strafverfolgung hinaus und nimmt aufgrund der wachsenden Digitalisierung in anderen Bereichen ebenfalls zu. Unternehmen und Organisationen nutzen IT-Forensik, um Vorfälle wie Datenverluste, Betrug und Verstösse gegen Datenschutzrichtlinien zu untersuchen und aufzudecken. Durch die Anwendung von IT-Forensik können digitale Beweismittel gesammelt, analysiert und bewertet werden, um vor Gericht verwendet werden zu können. Die forensische Analyse von Bildern und Dokumenten ist ein Hauptbestandteil von IT-Forensik. Eine Einführung und dazugehörige Techniken können im vorherigen Artikel gelesen werden: IT-Forensik Analyse von Bildern und Dokumenten Ein weiterer wesentlicher Aspekt der IT-Forensik ist die Videoanalyse, die dazu beiträgt, die Authentizität von Videoaufnahmen zu überprüfen und wertvolle Informationen aus den Videos zu extrahieren. Dabei werden verschiedene Techniken und Methoden angewendet.

VIDEOANALYSE

Die Analyse von Videos ist ein wichtiger Bestandteil der IT-Forensik und erfordert spezielle Kenntnisse und Fähigkeiten. Wichtig zu beachten ist, dass die Verwendung von Videos als Beweismittel in der IT-Forensik bestimmte Richtlinien und Protokollen folgen muss, um sicherzustellen, dass die Integrität des Beweismittels nicht beeinträchtigt wird. Dies beinhaltet die Gewährleistung der Kette der Beweismittelführung und die Einhaltung von Best Practices für die Beweismittelsicherung und -aufbewahrung. In der Regel werden elektronische Beweismittel von den Behörden zunächst in angemessener Form sichergestellt. Dies erfolgt durch die Beschlagnahme von Geräten wie Festplatten, USB-Sticks oder anderen Speichermedien. Dabei wird ein Protokoll erstellt, das detaillierte Informationen über den Fund, den Zustand des Beweismittels, den Ort und die beteiligten Personen enthält. Dieses Protokoll dient als

Nachweis für die ordnungsgemässe Sicherstellung. Die elektronischen Beweismittel werden daraufhin sicher und kontrolliert transportiert, um Verlust oder Beschädigung zu vermeiden. Hierfür können spezialisierte Transportmittel oder verschlüsselte Speichermedien eingesetzt werden. Nach der Sicherstellung werden die Beweismittel versiegelt, um sicherzustellen, dass sie während der Aufbewahrung nicht manipuliert werden. Dies kann durch den Einsatz von Siegeln, Sicherheitsetiketten oder digitaler Versiegelungstechnologie erfolgen. Bei der sicheren Aufbewahrung der Beweismittel werden Massnahmen ergriffen, um unbefugten Zugriff, Beschädigung oder Verlust zu verhindern.

AUTHENTIZITÄTSANALYSE

Die Authentizitätsanalyse von digitalen Inhalten spielt eine immer wichtigere Rolle in einer Zeit, in der Manipulationen und Fälschungen von Informationen und Medien weit verbreitet sind. Besonders im Bereich der forensischen Untersuchungen und der Medienanalyse ist die Überprüfung der Echtheit von grosser Bedeutung, um die Integrität von Beweismitteln und die Vertrauenswürdigkeit von Informationen sicherzustellen. Die Authentizitätsanalyse befasst sich mit der Überprüfung von Merkmalen und Eigenschaften eines digitalen Objekts, um festzustellen, ob es tatsächlich das ist, was es vorgibt zu sein, und ob es während des gesamten Erstellungs-, Übertragungs- und Speicherungsprozesses unverändert geblieben ist. Dieser Prozess beinhaltet die Untersuchung verschiedener Faktoren wie Metadaten, Datenstrukturen, Dateiformate, digitale Signaturen und andere charakteristische Merkmale des digitalen Objekts.

METADATEN

Metadaten spielen eine zentrale Rolle bei der Authentizitätsanalyse, da sie Informationen über den Ursprung, die Erstellung und die Bearbeitung des digitalen Objekts liefern können. Beispielsweise enthalten Bilddateien Metadaten wie Aufnahmedatum, Kameramodell, GPS-Koordinaten und möglicherweise den Namen des Fotografen. Durch die Analyse und Überprüfung dieser Metadaten können Unregelmässigkeiten, Widersprüche oder Manipulationen festgestellt werden. Eine mögliche Manipulation könnte beispielsweise darin bestehen, dass ein

Foto mit einem späteren Datum versehen wurde, um eine bestimmte Geschichte zu unterstützen.

TECHNISCHE ANALYSEN

Technische Analysen von digitalen Inhalten können vielversprechende Hinweise auf Manipulationen liefern. Bei Bildern können beispielsweise Artefakte auftreten, die auf das Entfernen oder Hinzufügen von Objekten oder auf die Veränderung von Pixeln hinweisen. Bei Videos kann die Analyse der Bildrate, der Bewegungsmuster und der Audiowiedergabe Hinweise auf Bearbeitungen oder Synchronisierungsprobleme geben. Diese technischen Analysen erfordern oft spezialisierte Softwaretools und Fachkenntnisse.

DIGITALE SIGNATUREN ODER ZERTIFIKATE

Ein weiterer wichtiger Aspekt der Authentizitätsanalyse ist die Überprüfung von digitalen Signaturen oder Zertifikaten. Digitale Signaturen dienen dazu, die Echtheit und Integrität eines digitalen Objekts zu gewährleisten. Sie werden häufig verwendet, um digitale Dokumente oder Transaktionen zu verifizieren. Durch die Überprüfung der digitalen Signatur kann festgestellt werden, ob das Objekt seit der Unterzeichnung unverändert geblieben ist und ob der Unterzeichner vertrauenswürdig ist.

AUTOMATISIERTE METHODEN

Die Entwicklung von künstlicher Intelligenz und Deep-Learning-Algorithmen hat auch Auswirkungen auf die Authentizitätsanalyse. Es werden zunehmend automatisierte Methoden und maschinelle Lernalgorithmen eingesetzt, um Manipulationen in Bildern und Videos zu erkennen. Diese Techniken ermöglichen es, Veränderungen in Pixeln, Artefakte von Bildbearbeitungssoftware und unübliche Muster zu identifizieren. Maschinelle Lernalgorithmen können trainiert werden, um anhand von Beispielen zu lernen, welche Merkmale auf eine Manipulation hindeuten. Dies kann dazu beitragen, den Prozess der Authentizitätsanalyse effizienter zu gestalten und potenzielle Fälschungen schnell zu identifizieren.

ANWENDUNGSBEREICHE

Die Authentizitätsanalyse findet in verschiedenen Bereichen Anwendung. In der forensischen Untersuchung von Straftaten können digitale Beweismittel wie Bilder, Videos oder Dokumente überprüft werden, um sicherzustellen, dass sie nicht manipuliert wurden und vor Gericht verwendet werden können. Im Journalismus und in den Medien ist die Überprüfung der Authentizität von entscheidender Bedeutung, um vertrauenswürdige Informationen bereitzustellen und Fehlinformationen oder gefälschte Inhalte zu vermeiden. In der Sicherheitsbranche werden Authentizitätsanalysen verwendet, um Manipulationen von Überwachungsvideos oder anderen sicherheitsrelevanten Aufnahmen aufzudecken. Es ist jedoch wichtig anzumerken, dass die Authentizitätsanalyse nicht immer eindeutige Ergebnisse liefert. Manchmal können Manipulationen so geschickt durchgeführt werden, dass sie schwer zu erkennen sind. Darüber hinaus können einige Techniken zur Fälschung von digitalen Inhalten dazu führen, dass sie als authentisch eingestuft werden, selbst bei sorgfältiger Analyse. Es ist daher ratsam, verschiedene Analysemethoden zu kombinieren und eine umfassende Bewertung vorzunehmen, um die Wahrscheinlichkeit einer erfolgreichen Authentizitätsanalyse zu erhöhen.

FRAME-BY-FRAME-ANALYSE

Die Frame-by-Frame-Analyse ist eine Methode, die in verschiedenen Bereichen wie der IT-Forensik, der Videoüberwachung und der Filmindustrie eingesetzt wird, um detaillierte Informationen aus Einzelbildern eines Videos zu extrahieren, Beweise zu sammeln oder wertvolle Erkenntnisse zu gewinnen. Bei dieser Art der Analyse wird jedes Einzelbild sequenziell betrachtet und auf mögliche Merkmale, Ereignisse oder Muster untersucht. Der Prozess der Frame-by-Frame-Analyse beginnt damit, dass das Video in seine Einzelbilder aufgeteilt wird. Dies kann mithilfe spezialisierter Software oder Tools erfolgen. Jedes Bild wird dann einzeln analysiert und detailliert untersucht. Diese Analyse kann manuell oder mithilfe automatisierter Techniken wie maschinelles Lernen und Bildverarbeitungsalgorithmen durchgeführt werden, um bestimmte Merkmale oder Ereignisse automatisch zu erkennen. Diese Algorithmen werden mit grossen Mengen an Trainingsdaten trainiert,

um bestimmte Muster oder Objekte im Video zu identifizieren. Während der Frame-by-Frame-Analyse können verschiedene Aspekte des Videos untersucht werden. Dies umfasst die Identifizierung von Personen, Fahrzeugen oder Objekten, die Bewegungsmuster, die Identifizierung von Gesichtern, Gesten oder Aktionen, die Analyse von Texten oder Symbolen im Video, die Erkennung von Veränderungen im Hintergrund oder das Auffinden von Beweisen für kriminelle Handlungen oder Unfälle. Jedes einzelne Frame wird sorgfältig betrachtet, um mögliche Hinweise oder Beweise zu finden, die für den jeweiligen Kontext relevant sein können. Die Dokumentation der Analyseergebnisse ist entscheidend, um die Integrität der gefundenen Beweise zu gewährleisten und die Ergebnisse später nachvollziehen zu können.

IT-FORENSIK

In der IT-Forensik kann die Frame-by-Frame-Analyse verwendet werden, um Beweise zu sammeln. Dies kann die Identifizierung von Verdächtigen anhand ihres Aussehens oder Verhaltens, die Verfolgung von Bewegungen vor, während und nach einem Verbrechen oder die Rekonstruktion eines Unfallszenarios umfassen. Die detaillierte Untersuchung jedes einzelnen Frames kann dazu beitragen, wichtige Informationen zu gewinnen, die bei der Identifizierung von Tätern oder der Rekonstruktion von Ereignissen von entscheidender Bedeutung sind.

VIDEOÜBERWACHUNG

In der Videoüberwachung wird die Frame-by-Frame-Analyse eingesetzt, um verdächtige Aktivitäten zu erkennen, Sicherheitsverletzungen zu identifizieren oder ungewöhnliche Ereignisse zu überwachen. Durch die genaue Betrachtung jedes Frames können Abweichungen von normalen Mustern oder Verhaltensweisen erkannt werden. Dies kann die Erkennung von Einbrüchen, Vandalismus, Diebstahl oder anderen unerwünschten Ereignissen erleichtern.

FILMINDUSTRIE

In der Filmindustrie wird die Frame-by-Frame-Analyse verwendet, um visuelle Effekte zu erstellen, spezielle Aufnahmen zu bearbeiten oder Szenen zu verbessern. Durch die Untersuchung jedes Frames

können visuelle Elemente wie Hintergrunddetails, Farbkorrekturen, Bildstabilisierung oder die Integration von CGI-Effekten (Computer Generated Imagery Effekte werden oft verwendet, um realistische visuelle Darstellungen von Fantasiewelten, ausserirdischen Kreaturen, Spezialeffekten, Explosionen, virtuellen Umgebungen und anderen Dingen zu erzeugen) angepasst werden. Dies ermöglicht eine präzise Kontrolle über das visuelle Erscheinungsbild eines Films und sorgt für eine nahtlose Integration von Effekten oder Änderungen in einer bestimmten Szene.

HERAUSFORDERUNGEN

Es gibt jedoch auch einige Herausforderungen bei der Frame-by-Frame-Analyse. Die genaue Betrachtung und Auswertung grosser Mengen an Videomaterial erfordert viel Zeit und Ressourcen. Zudem kann die Qualität des Videos, wie beispielsweise Auflösung, Bildrauschen oder Komprimierung, die Genauigkeit der Analyse beeinflussen. Darüber hinaus können Bewegungsunschärfe, schnelle Bewegungen oder unklare Aufnahmen die Erkennung und Analyse von Details erschweren.

ZEITLICHE ANALYSE

Die zeitliche Analyse ist ebenfalls ein wichtiger Teil der forensischen Untersuchung von Videos. Sie befasst sich mit der Überprüfung der Bildrate, der Bewegungsmuster, der Synchronisierung von Audio und Video sowie der Zeitstempel, um Manipulationen und Unregelmässigkeiten aufzudecken. Die Analyse hilft, die Authentizität von Videos zu bestätigen und den genauen zeitlichen Ablauf von Ereignissen zu rekonstruieren. Maschinelles Lernen und künstliche Intelligenz unterstützen auch hier zunehmend automatisierte Analysen. Die zeitliche Analyse kann jedoch herausfordernd sein. Um genaue Ergebnisse zu erzielen und die Integrität von Videos sicherzustellen, braucht es Fachwissen und spezialisierte Ausrüstung.

STIMMFORENSIK

Die Stimmforensik ist ein Fachgebiet, das sich mit der wissenschaftlichen Analyse stimmlicher Eigenschaften befasst. Sie wird verwendet, um die Identität einer Person anhand ihrer Stimme zu bestätigen oder stimmliche Manipulationen zu erkennen. Die

Stimmforensik spielt eine wichtige Rolle in der Strafjustiz, der Abhörabwehr und der Medienanalyse. Durch die Analyse von Tonhöhe, Timbre und anderen stimmlichen Merkmalen können forensische Experten Rückschlüsse ziehen und genaue Ergebnisse erzielen. Es ist jedoch wichtig zu beachten, dass die Stimmforensik gewisse Grenzen hat und Manipulationen immer auch hier nicht auszuschliessen sind.

ERKENNUNG VON DEEPFAKES

Deepfakes sind trainierte Deep-Learning-Modelle, mit welchen es ein Leichtes ist ein Gesicht einer Drittperson mit einem Gesicht in einem beliebigen Video auszutauschen. Im Artikel Deepfakes eine Einführung gibt Andrea eine Einführung in das Thema. Bereits darin erwähnt sie das erste forensische Tool der US Defense Advanced Research Projekt Agency (DARPA) um Deepfakes identifizieren zu können. Im Jahr 2021 wurde das Paper Exposing Manipulated Photos and Videos in Digital Forensics Analysis zusammen mit einem vielversprechenden Autopsy Plugin veröffentlicht: Photo and video manipulations detector . Wie der Name des Plugins bereits verrät, soll das Plugin Manipulationen unter anderem auch Deepfakes in Fotos und Videos erkennen können. Bei Autopsy handelt es sich um eine Open Source Plattform für forensische Arbeiten mit digitalen Geräten und Dateien.

BEISPIEL – STEHT SELENSKI HIER WIRKLICH MITTEN IN KIEW?

Einen Monat nach der russischen Invasion vom 24. Februar 2022 forderte der ukrainische Präsident Selenski in einem Video alle freien Menschen dieser Erde dazu auf, sich für die Freiheit, den Frieden und damit – so seine Schlussfolgerung – auch für die Ukraine zu positionieren, steht Selenski hier wirklich mitten in Kiew?

Doch bei der genauen Betrachtung des Videos kommen Zweifel auf, ob Selenski tatsächlich auf offener Strasse von dem Kiewer Regierungsgebäude steht.

Aufgrund der Lichteinstrahlung in Selenskis Gesicht dürfte links von ihm eine helle warm-weisse Lampe (~3300 Kelvin) stehen. Diese müsste Einfluss auf den Schattenwurf des Soldaten im Hintergrund haben. Ein solcher bleibt jedoch aus. Zudem fehlt der Schattenwurf der beiden Lampen, die direkt vor Selenski stehen und anhand der Reflexion in seinen Augen erkennbar sind.

Das im Hintergrund erkennbare Licht, das seine linke Wange streift, hat nicht den erwarteten Einfluss auf seine Barthaare. Das sogenannte volumetrische Schimmern ist nicht ersichtlich. Weiter ist zu sehen, dass bei Minute 03:27 des Videos der Schatten des Soldaten sich bewegt, da er seine Position verändert. Nach dem Cut steht er aber noch immer still an der alten Position. Bei Minute 06:24 fällt ausserdem auf, dass der Soldat im Hintergrund in der gleichen Position verharrt, was bedeutet, dass dieser sogenannte Jump Cut kein echter, sondern lediglich ein nachträglich im Schnitt angefertigter Zoom ist. Zudem hat der Jump Cut den sonderbaren Effekt, dass sich der Hals des Soldaten sofort nach links verschiebt. Das ist nur möglich, wenn der Schnitt aus zwei unterschiedlichen Aufnahmen stammt. Sowohl der Soldat als auch das pulsierende Licht bleiben jedoch ihrer Kadenz treu. Somit handelt es sich beim Hintergrund um dieselbe weitergeführte Aufnahme. Auch interessant sind die fehlenden Umgebungsgeräusche. Dies ist nur möglich, wenn ein Richtmikrofon eingesetzt sowie Noise-Cancelling (Lärmunterdrückung) oder starke Kompression ge-

nutzt wurde. Des Weiteren entspricht der Klangeffekt von Selenskis Stimme, wie etwa der Hall, nicht der weitläufigen Strasse. Möglich ist das nur, wenn ein zielgenaues Richtmikrofon oder ein Ansteckmikrofon verwendet wurde. Beides ist auf dem Video nicht zu sehen. All diese Merkmale weisen auf ein fabriziertes Video und die Verwendung eines Greenscreens hin.

ZUSAMMENFASSUNG

Die Analyse von Videos in der IT-Forensik spielt eine wichtige Rolle bei der Untersuchung digitaler Videodaten. Ziel ist es, relevante Informationen zu extrahieren, Manipulationen zu identifizieren und die Integrität der Beweismittel sicherzustellen. Diese Analyse findet Anwendung in Bereichen wie Strafverfolgung, Gerichtsverfahren, digitaler Forensik und Sicherheitsüberprüfungen. Verschiedene Techniken und Methoden werden eingesetzt, um eine umfassende Videoanalyse durchzuführen. Zunächst erfolgt eine Authentizitätsanalyse, bei der die Echtheit des Videos und das Vorhandensein möglicher Manipulationen überprüft werden. Hierbei werden Metadaten wie Zeitstempel, Kameraeinstellungen und Dateiinformationen untersucht, um eventuelle Unstimmigkeiten oder Abweichungen festzustellen. Des Weiteren spielt die Frame-by-Frame-Analyse eine wichtige Rolle. Dabei werden einzelne Frames des Videos analysiert, um Merkmale wie Kompressionsartefakte, Farbunterschiede, Unregelmässigkeiten in den Kantenstrukturen und Anzeichen von Bearbeitungen aufzudecken. Diese Untersuchungen helfen dabei, Manipulationen zu identifizieren. Die zeitliche Analyse betrachtet die zeitlichen Aspekte des Videos. Hierbei wird die Bildrate überprüft, die Synchronisierung von Audio und Video analysiert sowie Bewegungsmuster untersucht. Abweichungen in diesen Bereichen können ebenfalls Hinweise auf Manipulationen liefern. Ein weiterer wichtiger Aspekt ist die Stimmforensik, die sich auf die Überprüfung der Echtheit von Audioaufnahmen im Video konzentriert. Merkmale der menschlichen Stimme werden analysiert, um Manipulationen oder synthetisch erzeugte Stimmen zu erkennen. Fortgeschrittene Techniken umfassen auch die Erstellung von 3D-Modellen, um Perspektiven, Schatten und Beleuchtung im Video zu analysieren. Dadurch können Anomalien oder Unregelmässigkeiten aufgedeckt werden. Durch den Einsatz spezialisierter Techniken und

Werkzeuge können Forensikexperten Manipulationen identifizieren, die Echtheit von Videos überprüfen und somit zur Gewährleistung der Integrität des Beweismaterials beitragen. Eine besondere Herausforderung besteht darin, dass Manipulationstechniken immer fortschrittlicher werden. Es gibt eine Vielzahl von Werkzeugen und Softwareprogrammen, die es auch unerfahrenen Benutzern ermöglichen, digitale Inhalte zu manipulieren und Fälschungen zu erstellen. Daher ist es wichtig, dass die Methoden der Authentizitätsanalyse ständig weiterentwickelt werden, um mit den neuesten Manipulationstechniken Schritt zu halten.

Michèle Trebo

Ralph Meier

AUCH BEI VIDEOS GILT:
KRITISCH BLEIBEN.

Bildquelle: https://unsplash.com/photos/h-ySkoCRzhs

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch