ECHTHEITSPRÜFUNG VON VIDEOS

MIT BEISPIELEN AUS DER IBIZA-AFFÄRE

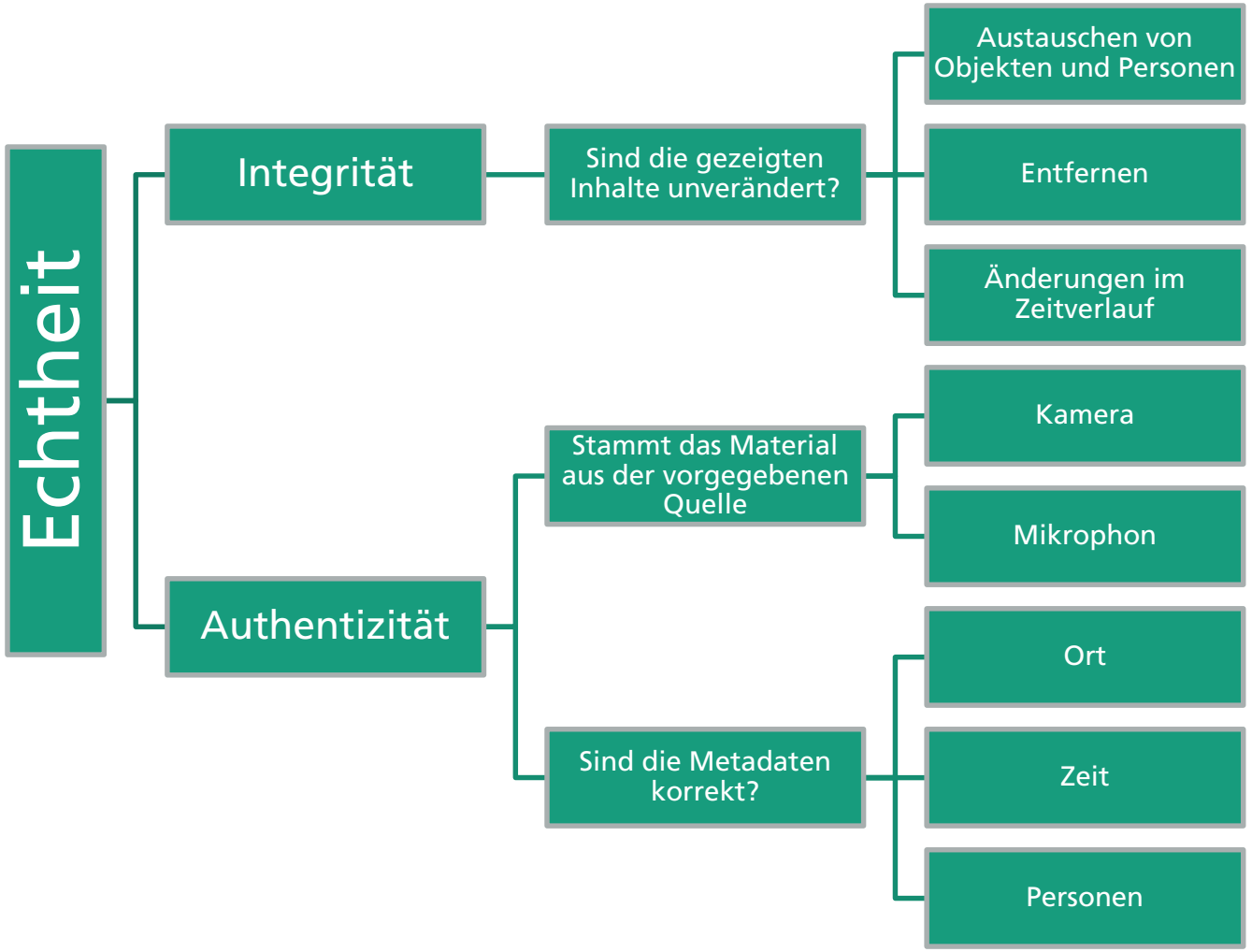
Martin Steinebach

Fraunhofer SIT

Lernlabor Cybersicherheit

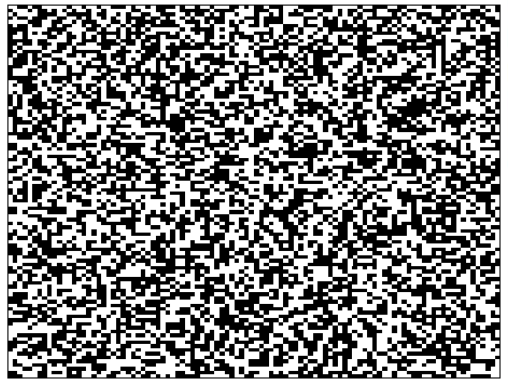
CRISP
Nationales Forschungszentrum für angewandte Cybersicherheit

I – ÜBERBLICK ECHTHEITSPRÜFUNG VON VIDEOS



Multimedia Forensik am SIT

- Wiedererkennung von Mediendateien
  - Bild, Video, Audio – Robustes Hashing
  - Bildmontage-Erkennung
- Erkennung von Manipulationen
  - Deepfake-Erkennung
  - Framework zur Erkennung von Bildmanipulationen
  - Deep Learning zur Bildverarbeitungserkennung
- Steganalyse
- Medien-File-Carving
- Datenschutzbewahrende Medienforensik



Forensische Bildanalyse

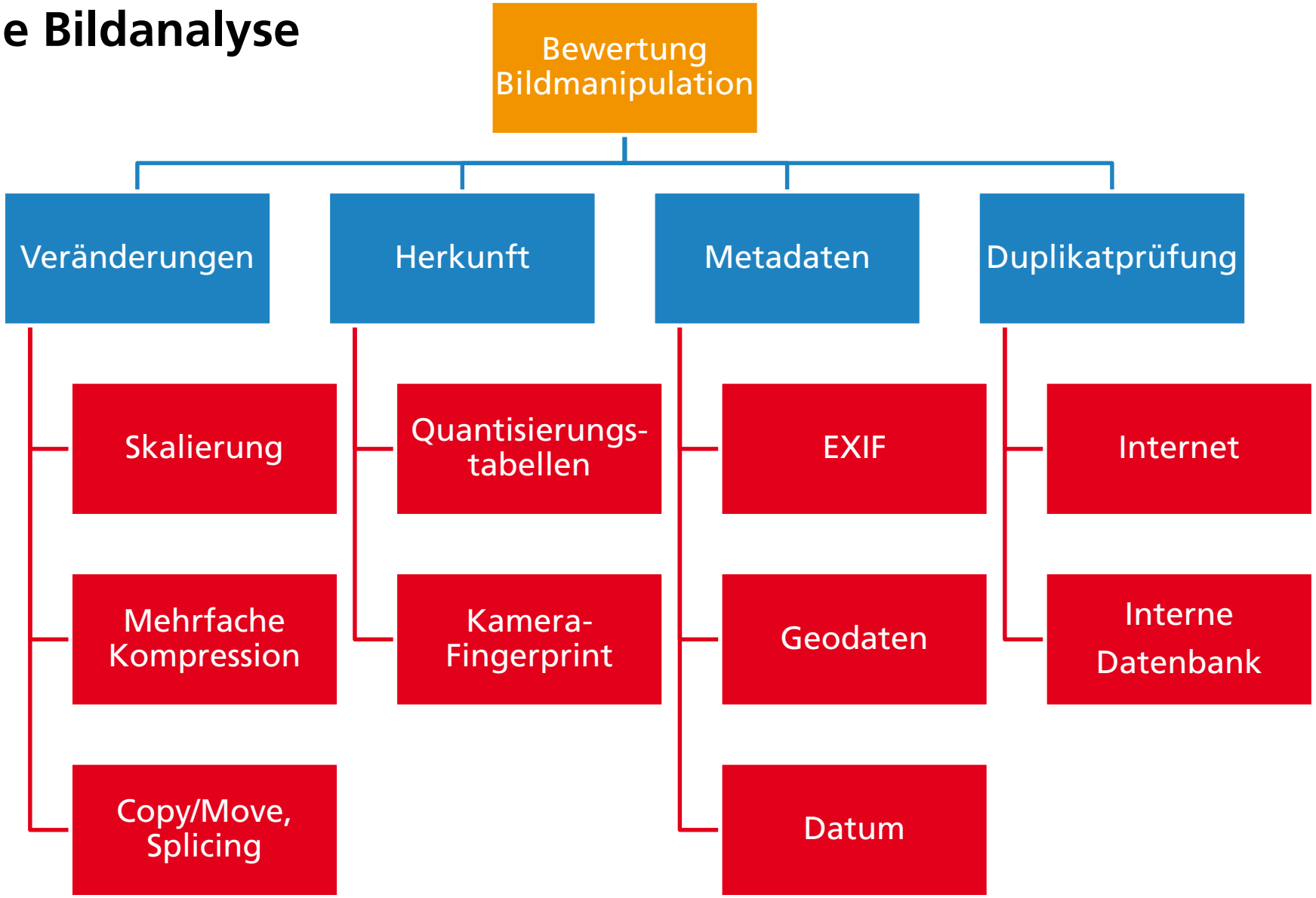
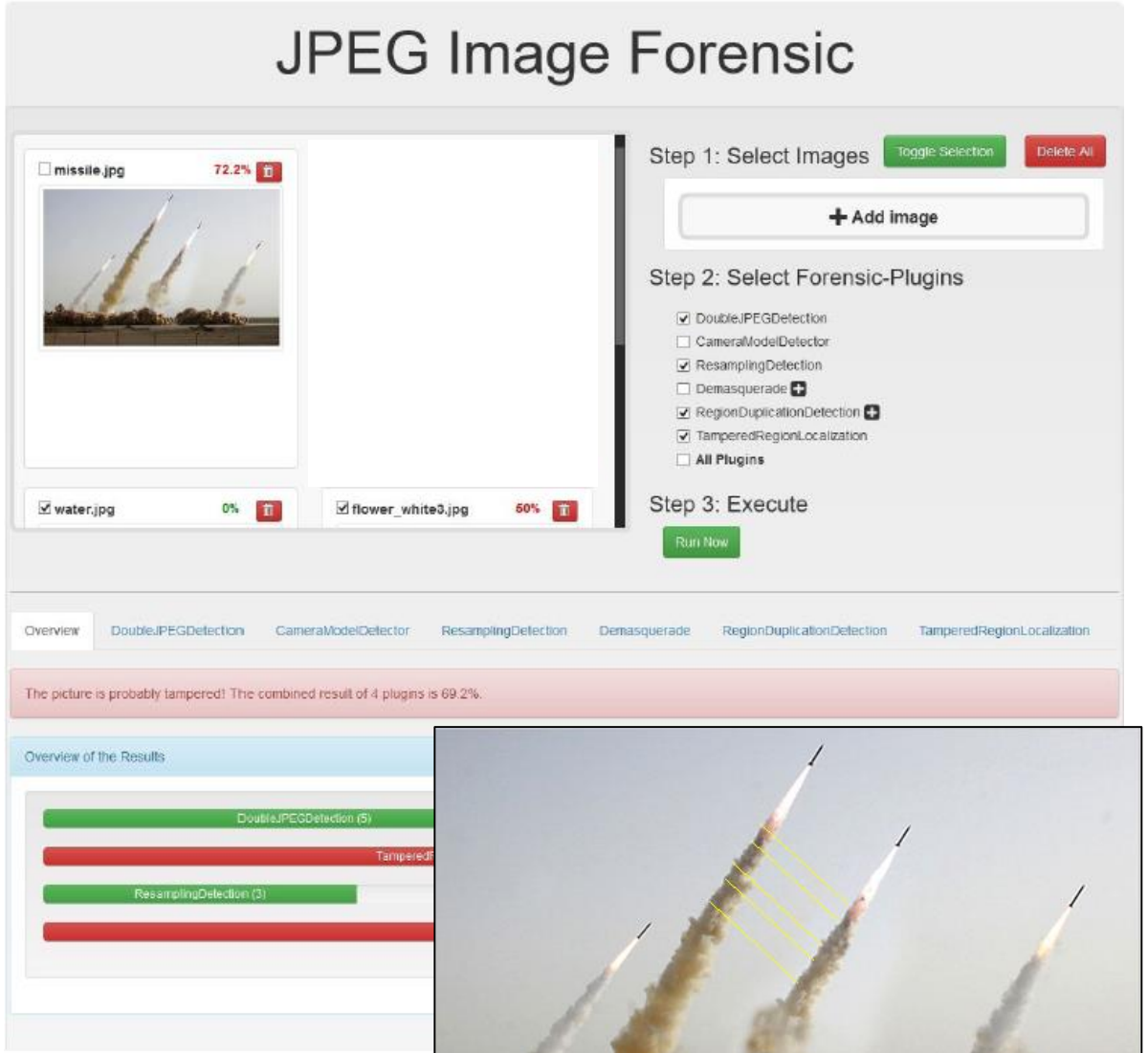


Image Forensics: Erkennen von Manipulationen

- Methoden zum Erkennen von Manipulationen von Bildern
  - Kein Original liegt vor
  - Kein Hash des Originals ist bekannt
  - Keine Methode zum Schutz der Integrität im Voraus eingesetzt
- Vorgehensweise
  - Modell eines nicht verändertes Bildes finden
  - Abweichungen vom Modell errechnen
- Beispiele für Methoden
  - Erkennen von identischen Stellen im Bild
  - Erkennen von statistischen Abweichungen
- Erfolg der Methoden sind abhängig vom Angriffstyp



Quelle des untersuchten Bildes:
Sepah News /
Agence France-Presse /
New York Times

Montagenerkennung

- Hier stößt inverse Bildersuche an ihre Grenzen
- Lösungsweg:
  - Lokale Datenbank
  - Über Bild verteilte Merkmale werden gespeichert
  - Abgleich bei neuem Bild: Sind Teile in bekannten Bildern enthalten?
- Erkennung
  - Hintergrund ~ 100%
  - Objekt nach Veränderung ~95%
  - Precision ~99% (TP/(TP+FP))

(a) Montage: newpoliticstoday.com

Source 1: picture-alliance / AP Photo

(c) Source 2: Boston Globe / Getty Images

Deepfake-Erkennung

Welche Gesichter der folgenden Personen wurden nachbearbeitet?

Videoquellen - Rössler et. al: FaceForensics++

rithmus basierend auf Ghost-Artefakten

Deepfake Video
(Ghost-Bild + Video)

II – DIE IBIZA-AFFÄRE

- Erfahrungen und Beispiele

Herausforderungen bei der Durchführungen

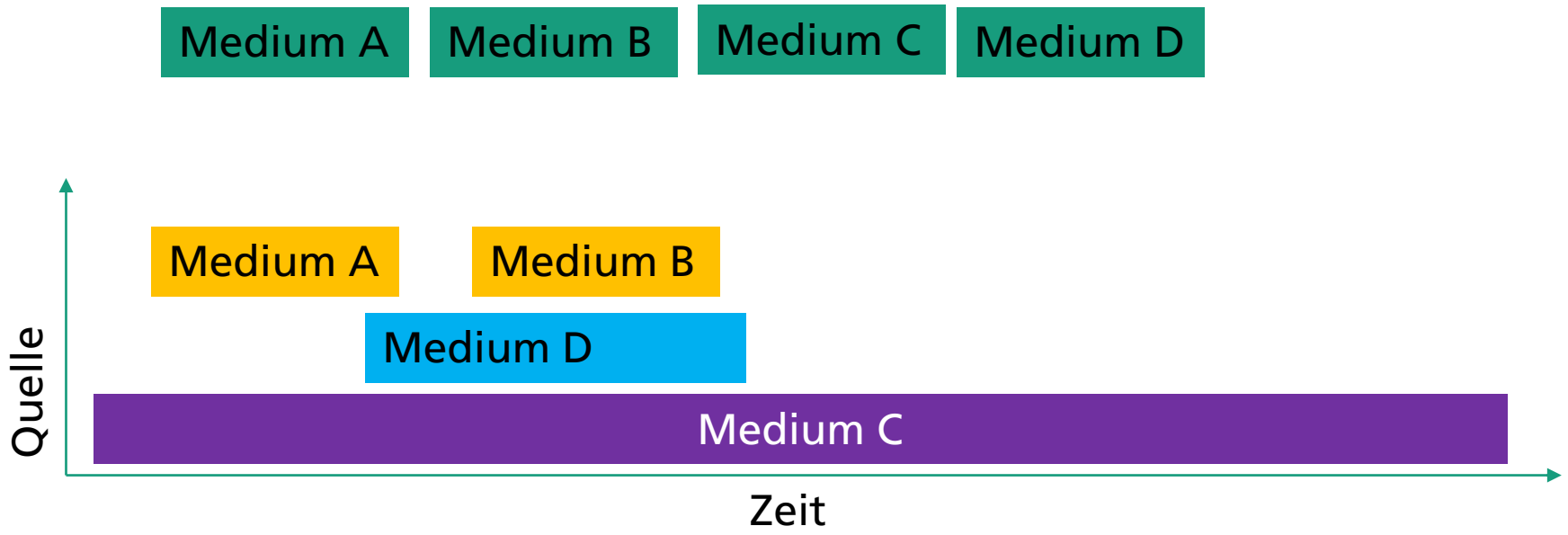
- Sichere Übertragung der Daten
  - Mehre GB Daten
  - Interne File-Hosting-Plattform zu langsam
    - Nutzung öffentlicher Cloud-Lösung
  - Verschlüsselung durch Auftraggeber
  - Schlüsselübertragung via PGP
  - Lokales Speichern in Krypto-Container

Herausforderungen bei der Durchführungen

- Sichere Nutzung der Daten
  - Wie kann sichergestellt werden, dass möglichst wenige digitale Spuren der Daten verbleiben
  - GIT, lokale Ordner, Fileserver, … erzeugen alle Back-ups
  - Strategie:
    - Container lokal kopieren
    - Daten nur dort nutzen
    - Ergebnisse direkt in Container oder
      in vom Back-up ausgeschlossenen lokalen Ordnern speichern

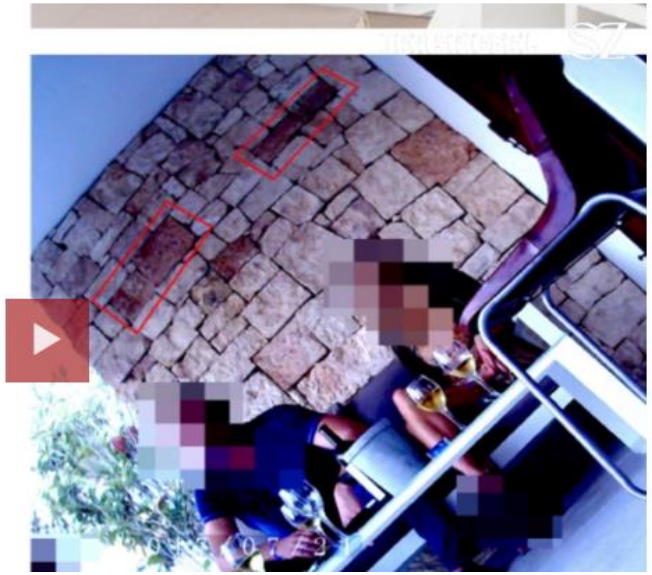
Ergebnisse, die öffentlich bekannt sind

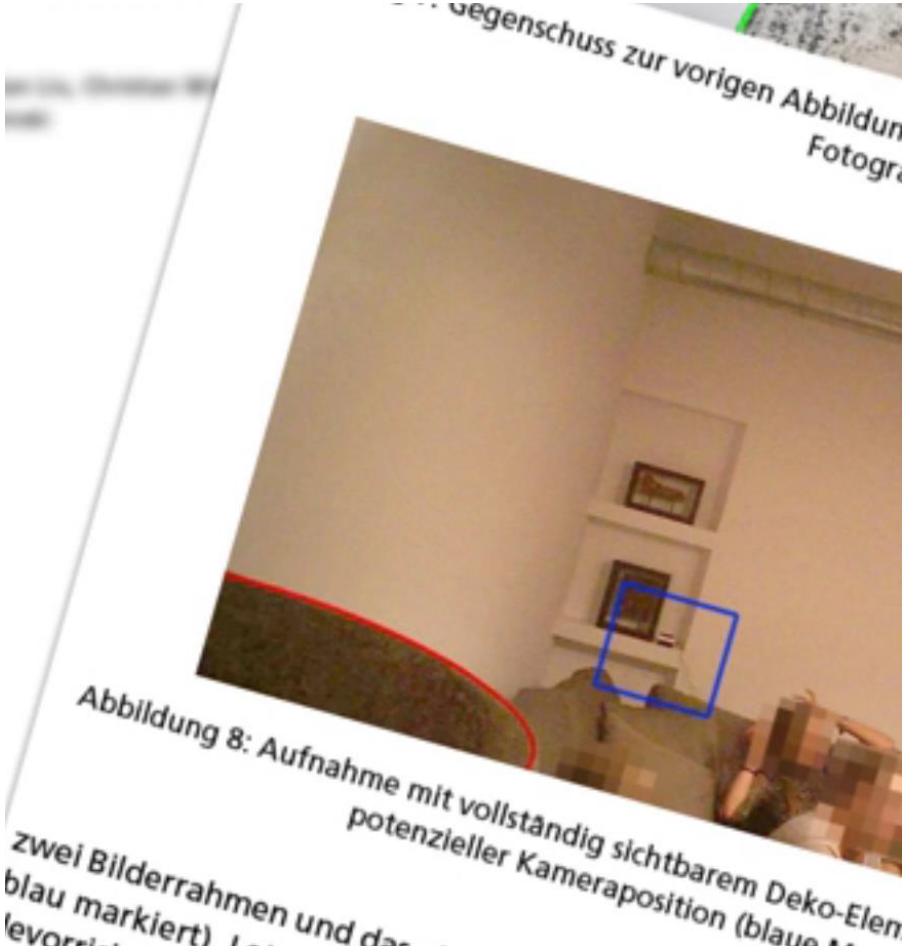
- Prüfung der Metadaten
  - Passen Videos zueinander, sind sie also von der gleichen Kamera in Folge gefilmt worden?
  - Passen verschiedene Perspektiven zueinander, stimmen die Tonspuren überein?



Ergebnisse, die öffentlich bekannt sind

- Prüfung des Orts der Aufnahmen
  - Vergleich von Referenzfotos und Videoaufnahmen
  - Nachvollziehen von Kamerawinkeln





https://www.spiegel.de/video/strache-video-oesterreich-gutachter-prueften-der-aufnahmen-video-99027197.html

Ergebnisse, die öffentlich bekannt sind

- Prüfung von Hinweisen auf Manipulation
  - Test auf wiederkehrende Frames
  - Copy-Angriffe zum Synthetisieren von Szenen

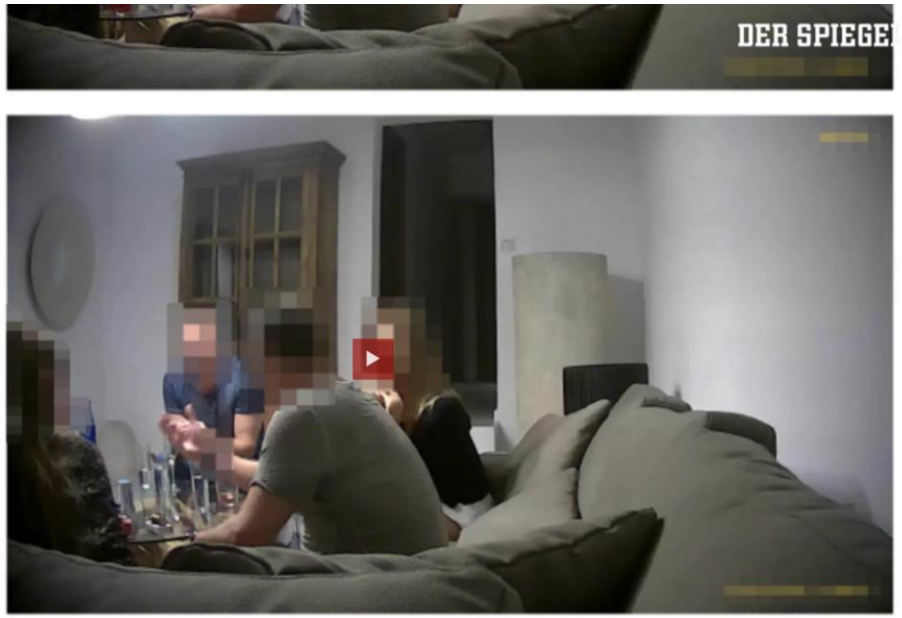
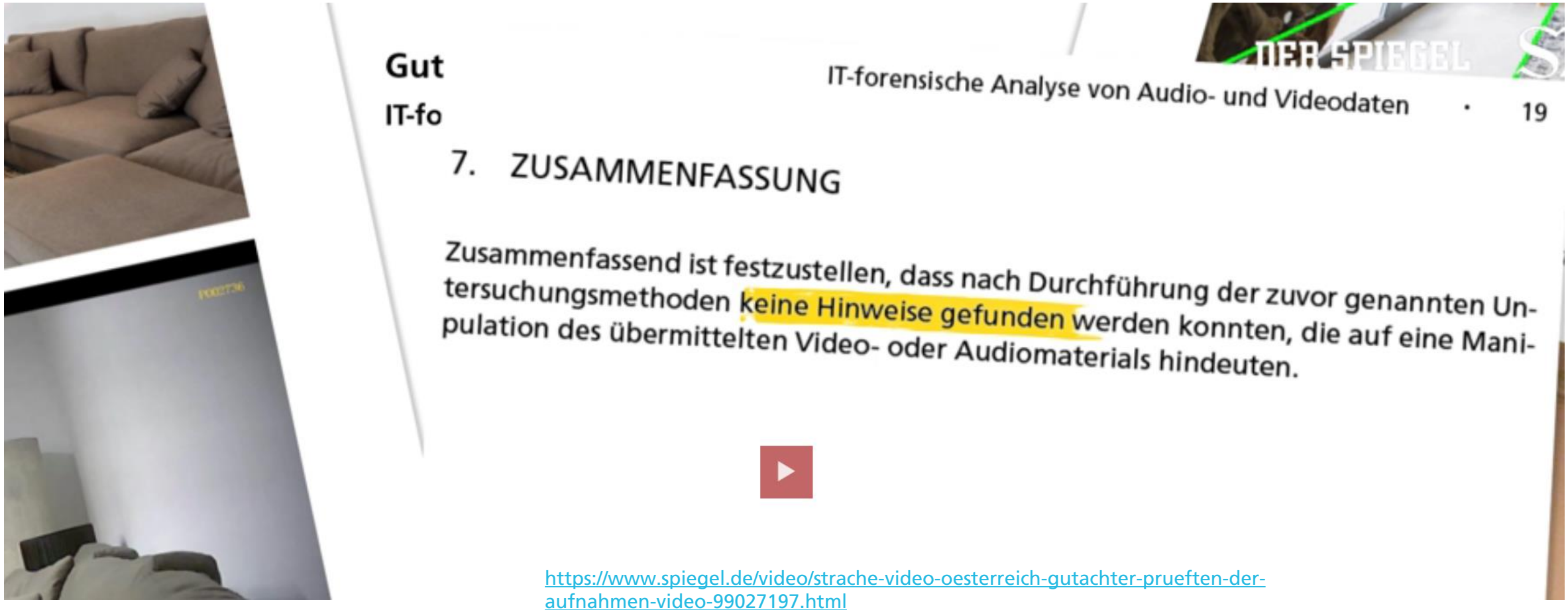


Abbildung 1: Verschiedene Beispielbilder mit identischem robusten Hash (abgebildete Personen wurden nachträglich verpixelt)

https://www.spiegel.de/video/strache-video-oesterreich-gutachter-prueften-der-aufnahmen-video-99027197.html

Vielen Dank!



https://www.spiegel.de/video/strache-video-oesterreich-gutachter-prueften-der-aufnahmen-video-99027197.html

Kontakt

Prof. Dr. Martin Steinebach

Rheinstrasse 75, 64295 Darmstadt, Germany

Phone: +49 6151 869-349, Fax: +49 6151 869-224

martin.steinebach@sit.fraunhofer.de

www.sit.fraunhofer.de

Lernlabor Cybersicherheit

- https://www.academy.fraunhofer.de/de/weiterbildung/information-kommunikation/cybersicherheit.html
- https://www.academy.fraunhofer.de/de/weiterbildung/information-kommunikation/cybersicherheit/fachkraefte--und-anwenderschulungen/multimedia-forensik_fuer_ermittlungsverfahren.html