

Forensische Echtheitsprüfung für Digitalfotos und -videos

Praxisnahes Training, um manipuliertes Bildmaterial und „Fakenews“ selbst zu erkennen

Erlernen Sie praxisorientierte Methoden zur Echtheitsprüfung von Bild- und Videodaten. Der Kurs behandelt Bildforensik, Signalforensik und die Analyse von Metadaten, um Manipulationen wie Deepfakes zu erkennen. Perfekt für Forensiker, Ermittler und Journalisten.

Digitale Bild- und Video-Forensik: Manipulationen erkennen und analysieren

Das Seminar zur Echtheitsprüfung von Bild- und Videodaten vermittelt praxisorientiertes Wissen zur Erkennung von Manipulationen in digitalen Medien.

Teilnehmende lernen, wie Bildmaterial durch Software oder Deepfake-Technologien verfälscht werden kann und wie diese Manipulationen identifiziert werden. Es wird gezeigt,

dass auch unverändertes Bildmaterial in einem anderen Kontext irreführend sein kann. Der Kurs behandelt verschiedene Methoden der Bildforensik, einschließlich der Analyse von Metadaten und Pixel-Daten, und erläutert den Lebenszyklus von Bildmaterial. Praktische Übungen und Forensik-Software werden bereitgestellt, um die erlernten Techniken anzuwenden.

Kursdetails auf einen Blick

- Für **IT-Forensiker*innen, Fachjournalist*innen**
- **Offenes Format** oder **Inhouse Training**
- Dauer: **3 Tage**
- Format: **Online**
- Kosten: 1.400,00 Euro (zzgl. MwSt)

Praxisnahe Bild- und Video-Forensik: Echtheit sicher prüfen und analysieren

Das Seminar ist besonders relevant für IT-Forensikerinnen, Ermittlerinnen, Journalisten, Schadensregulierer und technik-affine Interessierte, die die Echtheit von Bild- und Videodaten sicher überprüfen möchten.

Nach dem Seminar sind die Teilnehmenden in der Lage, Methoden zur Echtheitsprüfung von Bildern und Videos anzuwenden, Limitierungen der Bildforensik zu erkennen und Software-Werkzeuge zur Analyse auszuwählen. Ein weiterer Schwerpunkt liegt auf der Anwendung freier und kommerzieller Software sowie der Diskussion aktueller akademischer Forschung.

Inhalte des Seminars umfassen unter anderem die Analyse von JPEG-Daten, Deepfakes, Signalforensik, OSINT und die Beweiskraft von Bildforensik. Teilnehmende erhalten Einblicke in die neuesten Entwicklungen der Bildforensik und können erlernte Methoden direkt an Beispielen aus der Praxis anwenden.

Nach dem Seminar können Sie:

- **Dateiformate** und den »Lebenszyklus« von Bildmaterial verstehen.
- **Methoden zur Prüfung** der Echtheit digitaler Bilder verstehen und anwenden.
- **Limitierungen** der Bildforensik einschätzen.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Metadata-Analysis>

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- Das JPEG-Format: Kompressionsverfahren, Speicherformat (als Web-based Training zur Vorbereitung, Dauer ca. 1h)
- Schutzziele Integrität versus Authentizität
- Arten der Bildmanipulation von Deepfakes bis »Cheap Fakes«
- Signalforensik unsichtbarer Spuren in authentischen und veränderten Bilddaten
- modellbasierte versus datengetriebene Forensik-Methoden
- Analyse der Metadaten
- Untersuchung sichtbarer Bildinhalte und OSINT
- Beweiskraft der Bild- und Videoforensik
- verfügbare Software-Werkzeuge (kommerziell und gratis)
- Literaturtipps (Lehrbücher, Konferenzen/Journals)
- PC-Übungen zu Signalforensik und Metadaten-Analyse

Zugangsvoraussetzung:

Allgemeine IT-Kenntnisse.

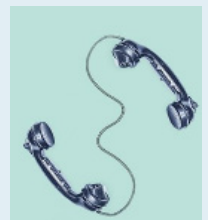
Weitere Informationen:

Inklusivleistung: Sie haben die Gelegenheit nach Veranstaltungsende eine Woche lang die Übungsaufgaben weiterzubearbeiten und Nachfragen zum Kurs an unsere Trainer*innen zu stellen (Betreuung per Forum).

Fachlicher Ansprechpartner am Fraunhofer SIT

Dr. Sascha Zmudzinski
Tel. +49 6151 869-321
sascha.zmudzinski@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt



Lernlabor
Cybersicherheit