

Christoph Wegener-Bachhuber

KRIMINALHAUPTKOMMISSAR (A11) - LKA HESSEN
CYBERCRIME

@ christoph.wegener-bachhuber@example.de | ☎ +49 611 5524 7186 | 🏠 Wiesbaden, Deutschland
🌐 | 📄 linkedin.com/in/christoph-wegener-bachhuber | 📄 github.com/cwegener-foren6

PROFIL

Kriminalhauptkommissar (A11) im Dezernat Cybercrime des Landeskriminalamts Hessen Wiesbaden. M.Sc. IT-Sicherheit der TU Darmstadt plus B.A. gehobener Polizeivollzugsdienst. 9 Jahre Cybercrime-Ermittlung mit 184 abgeschlossenen Fall-Vorgaengen inkl. 14 Ransomware-Ermittlungen. Mitarbeiter ZIT (Zentrale Stelle zur Bekämpfung der Internetkriminalitaet) Frankfurt. Cybercrime-Spezialkurs DHPol Muenster und FBI Liaison Workshop Quantico.

BERUFSERFAHRUNG

Kriminalhauptkommissar (A11) - Dezernat Cybercrime LKA Hessen 10/2020 - heute
Landeskriminalamt Hessen (LKA Wiesbaden) Wiesbaden, Deutschland

Sachbearbeiter Cybercrime mit Schwerpunkt Ransomware und Krypto-Wallet-Tracking

- Bearbeitung 184 Cybercrime-Vorgaenge in 5 Jahren inkl. 14 Ransomware-Ermittlungen mit StA-Anklage
- Sicherstellung von 24 Servern, 184 mobilen Geraeten und 8,4 Mio. EUR Bitcoin/Monero in 4 Jahren
- Bedienung X-Ways Forensics, EnCase, FTK Imager, Cellebrite UFED 4PC und Oxygen Forensic Detective
- Python-Scripting fuer 24 wiederverwendbare Forensik-Tools, geteilt mit BKA Wiesbaden und LKAs
- Vernehmungen von 184 Verdächtigen, davon 18 mit Cybercrime-Hintergrund auf Russisch B2
- Schnittstelle zur ZIT Frankfurt, BKA Cybercrime SO 4 und Europol EC3 Den Haag
- Mitwirkung am DHPol-Cybercrime-Aufbaukurs als Praxis-Dozent fuer 38 Teilnehmende pro Jahr

Polizeikommissar (A9/A10) - Schutzpolizei und Master-Studium parallel 10/2016 - 09/2020
Polizei Hessen, PI Frankfurt-Nordend Frankfurt am Main, Deutschland

Schutzpolizei mit parallel-Master-Studium TU Darmstadt

- Schutzpolizei-Streifendienst in PI Frankfurt-Nordend, 1.420 Vorgaenge pro Jahr
- Berufsbegleitendes Master-Studium IT-Sicherheit TU Darmstadt mit Note 1,3
- Praktische Master-Thesis 'Forensische Analyse von Ransomware-Krypto-Wallets' in Kooperation mit LKA Hessen

Kriminalkommissar-Anwaerter (gPVD) 09/2013 - 09/2016
Hessische Hochschule fuer Polizei und Verwaltung Wiesbaden, Deutschland

Dualer Bachelor-Studiengang gPVD

- B.A. gPVD mit Note 1,8
- Praktika auf PI Frankfurt-Mitte, KK 12 Wiesbaden und LKA Hessen IT-Beweisstelle
- Bachelor-Thesis 'Beweisverwertung digitaler Spuren bei Cybercrime' mit Note 1,5

PROJEKTE

EG Crypto-Wallet-Tracking Hessen 03/2024 - heute

Verfolgung von Bitcoin- und Monero-Stromen aus Ransomware-Erpressungen, 4 Cluster identifiziert, 8,4 Mio. EUR sichergestellt

Ransomware-Ermittlung Stadtwerke Frankfurt 01/2023 - 06/2023

Cyberangriff auf Stadtwerke Frankfurt, Tatortarbeit IT-Forensik mit X-Ways, Anklage StA Frankfurt 11/2023

PUBLIKATIONEN

Kriminalistik Fachzeitschrift, Heft 9/2024, 14 Seiten 09/2024

AUSBILDUNG

Master of Science IT-Sicherheit 10/2018 - 09/2020
Technische Universitaet Darmstadt - CRISP Darmstadt, Deutschland
IT-Sicherheit 1,3

Studium gehobener Polizeivollzugsdienst (gPVD, B.A.) 09/2013 - 09/2016
Hessische Hochschule fuer Polizei und Verwaltung Wiesbaden, Deutschland
Polizeivollzugsdienst 1,8

Abitur 09/2005 - 07/2013
Goethe-Gymnasium Frankfurt Frankfurt am Main, Deutschland
Allgemeine Hochschulreife GPA: 1,4

FÄHIGKEITEN

Digitale Forensik (X-Ways, EnCase, FTK) Mobile Forensik (Cellebrite UFED, Oxygen)
Open-Source-Intelligence (OSINT) Ransomware-Verfolgung und Kryptowaehrungen
Strafprozessrecht (Paragraph 100a/100b StPO) Python und Forensik-Scripting
Heckler & Koch P30 Vernehmungslehre Cybercrime-Spezifisch

ZERTIFIKATE

GIAC GREM (Reverse Engineering Malware) - SANS 11/2024

FBI Liaison Workshop Cybercrime Quantico (USA) 06/2023

Cybercrime-Spezialkurs (DHPol Muenster) 09/2021

Cellebrite UFED Certified Logical Operator 11/2020

Verbeamtung auf Lebenszeit (Polizei Hessen) 09/2016

SPRACHEN

Deutsch Muttersprache
Englisch C1
Russisch B2
Ukrainisch A2

STÄRKEN

Wissenschaftliche Präzision

Habe in 184 Vorgängen kein Beweis-Verwertungsverbot ausgelöst, 96 Prozent der Asservatensicherungen vor Gericht haltbar

Aktualität IT-Forensik

Lese wöchentlich Bleeping Computer und Krebs on Security, führe interne Schulungen alle 2 Monate für 18 LKA-Kolleg:innen

Verbindung Polizei und Tech-Industrie

Pflege Kontakte zu G DATA, Avira und Bochumer Horst-Goertz-Institut für 4 IT-Forensik-Symposien pro Jahr