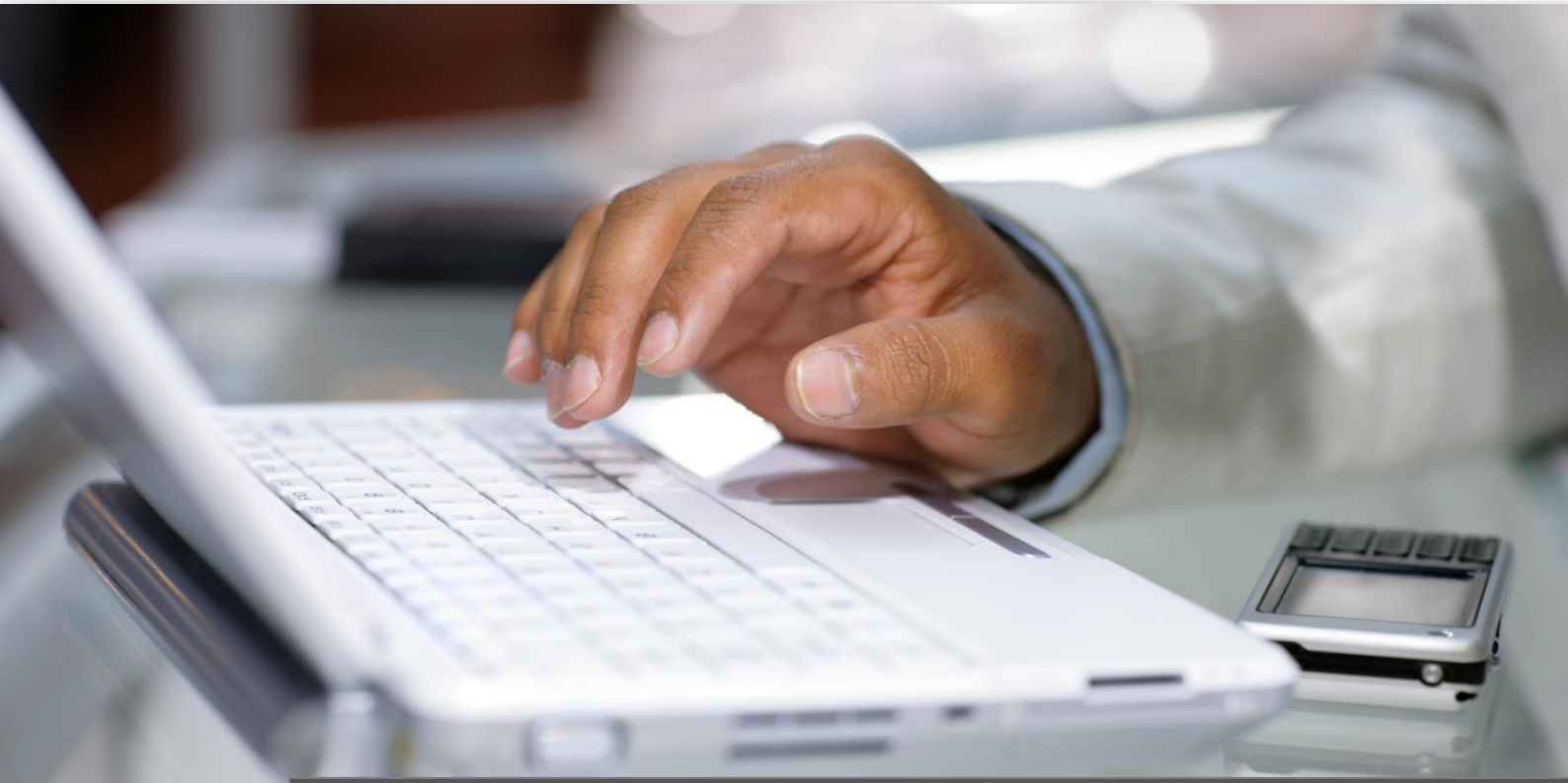
# Certified PC Forensic Professional

Online-Training | Examen CPFP



## Ausbildungsinhalte

ITKservice

# Technische Trainings

## Certified PC Forensic Professional

Ausbildungspfad | Certified Forensic Expert


CPFP → CNFP → CFE Certified Forensic Expert

Nach dieser Ausbildungsreihe haben Sie die Möglichkeit durch „Aufklärung eines Real World Szenarios“ eine sehr praxisorientierte Zertifizierungsprüfung zum *Certified PC Forensic Professional* abzulegen.

| | Online-Training | Dauer | Examen |
|---|---|---|---|
| | Certified PC Forensic Professional | 20 UE | CPFP |

Sie erlernen unter anderem gelöschte Dateien wiederherzustellen, einen Aktivitätsindex zu erstellen, E-Mails, Binärcodes, die Registry und Datenbanken zu analysieren, versteckte Bereiche aufzudecken, Password Recovery, Angriffe gegen Bitlocker und vieles mehr.
Auch rechtliche Aspekte und die Durchführung von forensischen Sicherungen inklusive verschiedenen Sonderfällen (z.B. RAID oder SSD-Speichermedien) sind Bestandteil der Ausbildungsreihe.

| | Unterrichtseinheit | UE 01 | CPFP |
|---|---|---|---|
| | Einführung und Hintergründe<br>✓ Geschichte der Computer Forensic<br>✓ Erfolge der Computer Forensic<br>✓ Ein Thema für jeden?<br>▪ Privatpersonen<br>▪ Unternehmen<br>▪ Öffentlicher Dienstag<br>✓ Unterstützende Gesetze<br>▪ IT-Sicherheitsgesetz<br>▪ Bundesdatenschutzgesetz<br>▪ Strafgesetzbuch<br>✓ Forensic im Internet<br>▪ Forensic Tools in diesem Training<br>▪ OSForensics<br>▪ Volatility<br>▪ Sonderfall: Mobile Device Forensic<br>✓ Formen der Computer Forensic<br>▪ Live Response<br>▪ Post Mortem | | |

| Unterrichtseinheit | UE 02 | CPFP |
|---|---|---|

Cybercrime – Zahlen , Fakten und Fallbeispiele

- ✓ Cyberkriminalität in Deutschland (2010 – 2015)
- ✓ Schäden durch Cyberkriminalität
- ✓ Forensische Methoden im Unternehmen
- ✓ Grundsätzliches
- ✓ Erstmaßnahmen treffen
- ✓ Szenario
  - Hackerangriff I - IV
  - Hackerangriff Website
  - Hackerangriff Mitarbeiter (HeimPC)
  - Hackerangriff Ransomware
  - CEO Fraud
  - CEO Fraud II
  - Erpressung

| Unterrichtseinheit | UE 03 | CPFP |
|---|---|---|

Forensische Verfahren im Überblick – Live Response

- ✓ Einführung
- ✓ Vorbereitung
- ✓ Vorbereitung II
- ✓ Analyse des betroffenen Systems
- ✓ Vorteile des Speicherdumps
- ✓ Live Response mit OS Forensics
- ✓ Beispiel
  - Prozess und Speicheranalyse
  - Gelöschte Dateien lokalisieren
- ✓ Schnellüberblick

| Unterrichtseinheit | UE 04 | CPFP |
|---|---|---|

Forensische Verfahren im Überblick – Post Mortem Forensik

- ✓ Einführung
- ✓ Vorbereitung
- ✓ Vorbereitung II
- ✓ Vorbereiten für Post Mortem Forensiken
- ✓ Erstellung eine forensischen Kopie
- ✓ Integration von forensischen Kopien
- ✓ Erste Schritte am forensischen Image
- ✓ Schnellüberblick

| Unterrichtseinheit | UE 05 | CPFP |
|---|---|---|

Einführung: OSForensics

- ✓ Hintergrund
- ✓ Drei Phasen Anwedung
- ✓ Weitere Features:
  - Hash-Set Unterstützung
  - Rainbow Tables
- ✓ Trainings und Zertifizierungen
- ✓ Zusammenfassung

| Unterrichtseinheit | UE 06 | CPFP |
|---|---|---|

Forensische Datenträgersicherung
- ✓ Grundlagen
- ✓ Methode
  - Physikalische Kopie
  - Physikalische Kopie – Writeblocker
  - Logische Kopie – Bordmittel
  - Logische Kopie – Bordmittel II
- ✓ Verifikation einer Forensischen Kopie
- ✓ Abhängigkeit vom Betriebssystem
- ✓ DEFT Linux
  - Überblick
  - Forensische Kopie mit Guymager
- ✓ Forensische Kopie mit OSForensics
- ✓ Image-ing Special: .E01 nach VMDK
- ✓ Sonderfall: Mobile Endgeräte
- ✓ Beispiel: Elcomsoft Phone Password Breaker

| Unterrichtseinheit | UE 07 | CPFP |
|---|---|---|

Forensic Discovery
- ✓ Angriffe gegen Bitlocker Medien
  - Zwingende Voraussetzung
  - Problematik
  - Angriffsszenarien
  - Notwendige Tools
- ✓ Live Demo: Elcom Forensic Disk Decrypter
- ✓ Verschieden Ziele zur Auswahl
- ✓ Einstieg in die Fonresic Discovery / OS Forensic
  - Suche nach Daten
  - Erzeugen von Verzeichnissignaturen

| Unterrichtseinheit | UE 08 | CPFP |
|---|---|---|

Forensic Discovery
- ✓ Forensische Analyse
  - Real World
- ✓ Einleitend
  - Prüfsummenverifikation
- ✓ Alternativ
  - Prüfsummenverifikation
- ✓ Case für Data Leakage erstellen
- ✓ Zielvorgaben Data Leakage Case

| Unterrichtseinheit | UE 09 | CPFP |
|---|---|---|

Forensic Discovery
- ✓ Realistische Aufwände und Zahlen
- ✓ Special: Mobile Device Forensic
- ✓ Live Demo

| Unterrichtseinheit | UE 10 | CPFP |
|---|---|---|

Forensic Identify – RAID/NAS Recovery
- ✓ Problemsituation: RAID/NAS Recovery
- ✓ Praxisbeispiel
  - LINUX RAID
  - LINUX RAID bei OS Forensics
- ✓ Alternative Lösung
  - R-Studio von RTT
- ✓ Problemlösung
  - FTK Imager & R-Studio = RAID/NAS Recovery
- ✓ Fertiges Image bearbeiten

| Unterrichtseinheit | UE 11 | CPFP |
|---|---|---|

Forensic Identify – Typische Kundenanfrage
- ✓ Vorbereitung/Vorspiel
- ✓ OS Forensic Vorbereitung
- ✓ Suche nach Verborgenen
- ✓ Rekonstruktion nach Graden
- ✓ Ungewöhnliche Dateien finden
- ✓ Gezielte Zeiträume

| Unterrichtseinheit | UE 12 | CPFP |
|---|---|---|

Forensic Identify – Memory Forensic
- ✓ Schnelle Einblicknahme
- ✓ Problematik
- ✓ Volatility Framework
  - Schnellüberblick
  - Hiberfil.SYS Wandlung
  - Im Einsatz
- ✓ Logische Angriffe für Memory Acces
- ✓ Inception – Memory Attacks

| Unterrichtseinheit | UE 13 | CPFP |
|---|---|---|

OS Forensics – Erstellen von Berichten
- ✓ Berichterstellung
- ✓ Memory Forensic
- ✓ OS Forensic
  - Bericht erstellen
  - Integration von Beweisbildern
  - Integration in Bericht
  - Überblick Anpassung OS Forensics Reports

| Unterrichtseinheit | UE 14 | CPFP |
|---|---|---|

OS Forensics – Password Breaking
- ✓ Knacken von Passwörtern mit OS Forensics
- ✓ Integrierte Möglichkeiten
  - Password
  - Keys
- ✓ Windows Kennwörter
  - Lokal
  - Domain
- ✓ Rainbow Tables mit OS Forensics erzeugen
- ✓ Rainbow Tables
  - Downloaden
  - Einsetzen
- ✓ Dateien im OS Forensics knacken
- ✓ Kommerzielle Recovery Tools
- ✓ NIST National Software Reference Library (NSRL)
- ✓ NSRL im Überblick
- ✓ Integration von RDS nach OS Forensics
- ✓ Einsatz von NSRL (RDS 2.55 Modern Unique)

| Unterrichtseinheit | UE 15 | CPFP |
|---|---|---|

Forensische Malware Analyse
- ✓ Analyse von Malware
- ✓ Kompaktes Malware 1&1
- ✓ Forensischer Ansatz
  - Malware Analyse
- ✓ Online-AV-Scan (oder Filezugriff & Vtotal)
- ✓ Offline-AV-Scan (Virtualisierung des Images)
- ✓ Offline-AV-Scan (AV Scan innerhalb VM)
- ✓ Memory Forensik (Anti Malware Methoden)
- ✓ Einsatzgebiete

| Unterrichtseinheit | UE 16 | CPFP |
|---|---|---|

Spearphishing Angriff im Detail
- ✓ Überblick
- ✓ Einführung Testumgebung
- ✓ Forensische Analyse

| Unterrichtseinheit | UE 17 | CPFP |
|---|---|---|

Darknet Activität am Arbeitsplatz
- ✓ Überblick
- ✓ Einführung Testumgebung
- ✓ Schritte im Detail
- ✓ TOR Konfigurationsdateien
- ✓ Forensische Analyse
  - Memory Forensik
  - Post Mortem Forensik
- ✓ Forensik Remount
  - VM-gestützter Zugriff

| Unterrichtseinheit | UE 18 | CPFP |
|---|---|---|

Forensische Berichterstattung: Anforderung & Special: AntiForensik
- ✓ Forensische Analyse erschweren
- ✓ Verschleierung von Informationen
- ✓ Verschlüsselung von Informationen
- ✓ Manipulation von Zeitinformationen (Win)
- ✓ Komplette Zerstörung von Informationen
- ✓ Szenario
  - Schlagwortsuche
  - Malwareanalyse
- ✓ Ausgang einer Forensik
- ✓ Rechtsstreit
- ✓ Beweis in der Forensik
- ✓ Mitarbeiter als Täter – zu beachten
- ✓ Ermittlungsmethoden gegen Mitarbeiter
- ✓ 1&1: Was tun bei illegalen Datenfund?

| Unterrichtseinheit | UE 19 | CPFP |
|---|---|---|

Forensische Berichterstattung: Ausführung und Umsetzung
- ✓ Dokumentation im Überblick
- ✓ Deckblatt
- ✓ Inhaltsverzeichnis
- ✓ Executive Summary
- ✓ Forensische Sicherung
  - Wann/wo durchgeführt?
  - Wer war anwesend?
  - Welche Tools wurden eingesetzt?
  - Welche Beweisstücke wurden eingesetzt?
  - Fotos der Beweisstücke
- ✓ Definition der Untersuchungsmethoden

| | Unterrichtseinheit | UE 20 | CPFP |
|---|---|---|---|
| | Forensische Berichterstattung: Ausführung und Umsetzung<br>✓ Dokumentation im Überblick<br>✓ Ereignis: Funde nach Schlagwortliste<br>✓ Special: Beispiel Memory Forensik<br>✓ Abschlussnotiz<br>✓ Einblick Netzwerk-Forensik | | |

# Weitere wichtige Informationen

## Ihr Trainer: Herr Thomas Wittmann

Der Trainer dieser exklusiven Online-Ausbildungsreihe ist Herr Thomas Wittmann. Er ist ca. 20 Jahren im Bereich IT-Security aktiv und als *Senior Security Specialist* für innoSec | Schweiz tätig. Er ist einer der erfahrensten Sicherheitsexperten Deutschlands!

Neben einer umfangreichen Praxiserfahrung trägt er unter anderem die Titel *Professional Security Analyst Accredited Certification (OPSA)*, *Professional Security Tester Accredited Certification (OPST)* und *Offensive Security Certified Professional (OSCP)*. Zudem ist er als Oracle Datenbank-Spezialist, System-administrator und Datenschutzbeauftragter aktiv. Hierüber hinaus verfügt er über sehr viel Erfahrung als national und international tätiger Penetrationstester und dies auch in hochkritischen Bereichen wie beispielsweise regierungsnahen Umgebungen.

Als „Ex-Hacker“ gab er 2012 dem Handelsblatt ein Interview, in dem er die Bedrohungslage für Start-ups aufzeigte. 2016 nahm er im WDR Stellung zum Hackerangriff auf die Telekom.

## Optimale Prüfungsvorbereitung

Etwa ein zwei Tage vor der Prüfung zum *Certified PC Forensic Professional* erhalten Sie alle notwendigen Prüfungsunterlagen und eine detaillierte Anleitung, wie Sie die Prüfung ablegen können und was das Ziel Ihres Angriffs ist.

## Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 13:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.FORENSIC

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

## Copyrights und Vertragsbedingungen



## Kontaktdaten | Impressum

ITKservice GmbH & Co. KG
Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60
Telefax: 09526 95 000 63

www: ITKservice.NET
E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).
Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizensiert.
Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.