

# Seminar

# Forensic Investigation

2-Tages Seminar für Forensiker und Ermittler  
2./3. Februar 2012 in Jona (Schweiz)



---

Wie analysiert man Spuren von Hackerattacken oder Computer Missbrauch? Wie bereitet man diese Indizien für das Gericht oder eine interne Ermittlung auf? Erfahren Sie die Details in diesem praktischen Forensik Seminar mit Fokus Computer- und Netzwerk (Malware) Analyse.

---

# Forensic Investigation

Stellen Sie sich vor; Ein Erpresserbrief droht mit der Veröffentlichung von Kreditkarten und Firmengeheimnissen. Trotz Data Leak Prevention wurden Sie Opfer einer Hacker Attacke. Wie reagieren Sie? Welche Fragen ergeben sich, juristisch oder technisch? Die Compass Security AG hat hierzu diesen Kurs entwickelt, welcher

diesen „Fall“ von A-Z durchspielt. Dazu gehören juristische Grundüberlegungen, aber auch Web Log Analysen, OSX File Carving, Windows Trojaner Suche, Spuren auf dem Datenbank Server, iPhone und Social Media Ermittlungen.

## Programm

- Einführung in die Ermittlung
- Chain of Evidence
- Grundlagen Filesystem
- Slack Space
- Office Dokumente
- Windows Systeme - Spuren
- Beweismittel Sicherung
- Beweismittel Transport
- Post Mortem Analyse
- OSX DD Image Analyse
- OSX USB Disk Insertion Analyse
- Netzwerk Forensik
- Traffic Visualisierung
- Malware Hunting
- Advanced Persistent Threat
- iPhone Ermittlung
- iPhone und iTunes Spuren (Sync)
- Life Response Malicious Prozess

## Referenten



**Stephan Rickauer**  
stephan.rickauer@csnc.ch  
+41 (0)55 214 41 65

**Security Analyst**

Stephan Rickauer schloss 1997 die Berufsausbildung zum Elektroniker, Fachrichtung Sicherheitstechnik, ab. Seitdem war er in verschiedenen Unternehmen als Unix Engineer im Netzwerk-, Security- und Infrastruktur-Umfeld tätig. Zuletzt leitete er die IT am Institut für Neuroinformatik an der ETH Zürich. Stephan ist der Kopf bei Compass bezüglich Forensischen Untersuchungen.



**Jens von der Haar**  
jens.vonderhaar@csnc.ch  
+41 (0)55 214 41 77

**Security Analyst**

Jens von der Haar absolvierte an der Hochschule Furtwangen (DE) den Bachelor im Bereich Computer Networking. Die dazugehörige Abschlussarbeit über forensische Möglichkeiten in Bezug auf Windows-Systeme schrieb er im 2010 bei der Compass Security. Seither hat er sich zum Security Analyst für Forensik und Penetration Testing Aufgaben spezialisiert.

## Unterlagen & Sprachen

Die Unterrichtssprache während dem Kurs ist **Deutsch**. Alle Unterlagen und Aufgaben im Hacking-Labor sind in **Englisch**. Sie erhalten einen Ordner mit allen Kursfolien und Zusatzangaben, den Sie während des Kurses mit Notizen ergänzen. Parallel stellen wir die Unterlagen auch als PDF bereit.

---

## Kursort

Der Kurs wird bei der Compass Security AG in Jona (Schweiz) durchgeführt. Der Schulungsraum befindet sich 3 Gehminuten vom Bahnhof Jona und nur 30 Minuten mit der S5 oder S15 vom Hauptbahnhof Zürich entfernt.



Compass Security AG  
Werkstrasse 20  
CH-8645 Jona

---

## Zielgruppe

Dieses Compass Security Seminar richtet sich an Personen, die sich mit CIRT und Incident Response beschäftigen. Es geht in diesem Kurs darum, die Zusammenhänge bei einer Bedrohung zu erkennen, ruhigen Kopf zu behalten und Entscheide über das Vorgehen zu treffen. Mitunter wird an einem Fallbeispiel von A-Z der Incident durchgespielt und dabei werden wichtige Erkenntnisse erarbeitet. Der Kurs wurde erstmals im November 2011 in Berlin durchgeführt und hat grossen Anklang gefunden. Sehr empfehlenswert!

## Forensic Investigation



## Ihr Vorteil

Der **Praxisteil** des Seminars basiert auf dem Hacking-Lab. Dabei entdecken Sie vorhandene Sicherheitslücken und versuchen diese auszunutzen (Exploit). Sie erhalten ein Gefühl für den Angriff und die Konzeption der Abwehr. Zusätzlich erhalten Sie über das Hacking-Lab Fragen zu den Security-Challenges. Über die Solution- und Management-Anwendung des Hacking-Lab erklären Sie die Schwachstelle und schlagen geeignete **Gegenmassnahmen** vor. Ihre Teacher bewerten die eingereichten Lösungen und vergeben Punkte. Im Hacking-Lab haben Sie stets den Überblick über die gelösten Aufgaben und Ihr Skill-Level, das Ihnen auch später als Leistungsmerkmal zur Verfügung steht.

Kennen Sie das? Manchmal benötigen Sie etwas mehr Zeit um alle Varianten eines Angriffs oder Tools ausgiebig zu testen. Kein Problem! Sie erhalten im Anschluss mit unserer Hacking-Lab LiveCD **einen Monat kostenlosen Zugang** zum Hacking-Lab um alle Kursübungen nochmals zu vertiefen.

---

## Certified Hacking-Lab Forensic Investigator (I)

Dieser Kurs ist die ideale Vorbereitung zum Certified Hacking-Lab Forensic Investigator (I)



## Kosten

### Normaltarif

- CHF 2'300.--

### ISACA Mitglieder

- CHF 1'950.--

### ISSS Mitglieder

- CHF 1'950.--

Es gelten die AGB gemäss folgendem URL

<http://www.csnc.ch/de/securitytraining/agbde.pdf>

## Forensic Investigation Leistungen

### Die Kursgebühr beinhaltet:

- Vermittlung von Theorie durch unsere erfahrenen Referenten
- Nutzung Hacking-Lab Infrastruktur
- Hands-On Übungen
- Theorie-Unterlagen auf Papier und PDF
- 30 Tage Zugang zum Hacking-Lab nach der Schulung
- LiveCD für das Hacking-Lab (Zertifizierung)
- Kurszertifikat / ISACA Punkte
- Pausen- und Mittagsverpflegung

**Kurszeiten** • 09:15 bis 17:15 Uhr

## Compass Security Trainings

Interesse an weiteren Compass Trainings? Als führendes Penetration Testing und Ethical Hacking Unternehmen in der Schweiz und Deutschland können Sie sich in weiteren Themen bezüglich Hacking und Defense ausbilden lassen. Alle Kurse basieren auf dem bewährten Konzept mit 50% Theorie und 50% Labor im Hacking-Lab. Die Seminare sind auch On-Site in Ihrem Unternehmen erhältlich.

- Web Security Basic
- Web Security Advanced
- Network Analysis
- Penetration Testing
- iPhone® & iPad® Security
- Wireless & Mobile Security

## Anmeldung

Bitte melden Sie sich über die Web Registrierung unter <http://www.csnc.ch/training> oder per E-Mail an [team@csnc.ch](mailto:team@csnc.ch) unter Angabe von folgenden Informationen an:

Name: \_\_\_\_\_ Titel des Kurses: „Forensic Investigation“  
Vorname: \_\_\_\_\_ Firma: \_\_\_\_\_  
E-Mail: \_\_\_\_\_ Rechnungsadresse: \_\_\_\_\_  
Geb. Datum: \_\_\_\_\_ Position: \_\_\_\_\_  
Hacking-Lab Nickname: \_\_\_\_\_ Vereinszugehörigkeit: \_\_\_\_\_  
(falls vorhanden) (ISSS, ISACA, SGRP)

Die Anmeldefrist läuft bis 4 Wochen vor der Kursdurchführung. Sie erhalten nach dem Eingang Ihrer Anmeldung eine Anmeldebestätigung per Mail. Die finale Teilnahme ist mit der Bezahlung der Teilnahmegebühr wirksam.