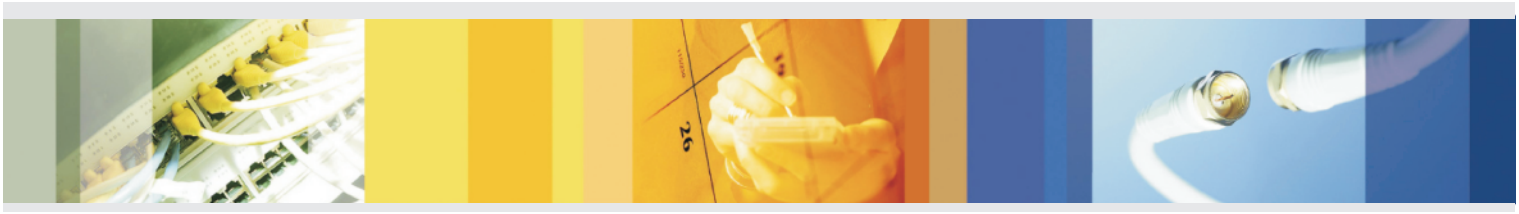
C|HFI Computer Hacking Forensic INVESTIGATOR

# Sunworks Services

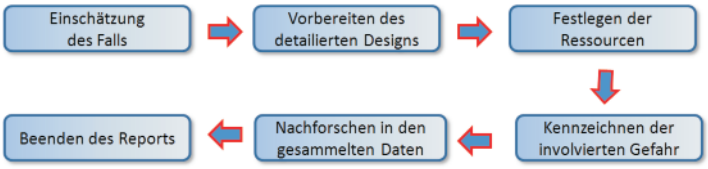
## Digital Forensics, Computer Hacking Forensics



## Warum Forensische Analysen?

Forensische Analysen werden nach Einbrüchen in IT-Systemen durchgeführt, um herauszufinden, ob Angreifer erfolgreich waren, welche Wege genommen wurden und durch welche Systemlücken der Einbruch ermöglicht wurde. Da sich heute meistens nicht mehr die Frage stellt, ob Unternehmen attackiert wurde, sondern wie ein Unternehmen mit einem Einbruch oder einer Notsituation umgehen kann.

In einer Forensischen Analyse wird aufgezeigt, wie Ihr Unternehmen richtig und effizient auf Sicherheitsvorfälle reagieren kann. Prozesse und Methoden zur Auffindung und Sicherung von Beweisen werden analysiert und digitale Beweise, welche der Angreifer hinterlassen hat, korrekt gesammelt. Egal ob Sabotage, Hackerangriff oder Industriespionage, mit einem korrekten Incident Handling lassen sich Schäden deutlich reduzieren.



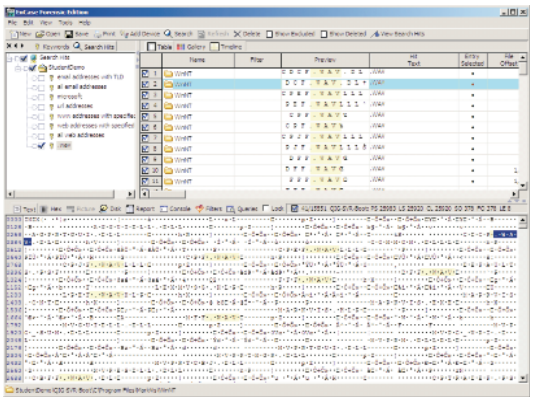

## Wo werden Forensische Analysen eingesetzt?

IT-Forensik kann in verschiedenen Situationen eingesetzt werden. Mit IT-Forensik sind Sie in der Lage, Angriffe (Interne und Externe) zu identifizieren und sich gegen weitere Angriffe, zu schützen. Mittels einer Analyse der Datenträger- oder der Netzwerkanbindung kann auch nachgewiesen werden von wo der Angriff stattgefunden hat oder auf welche Seiten oder Server der Benutzer zugegriffen hat, oder welche Daten er auf seinen PC heruntergeladen, hat auch wenn die Beweise dazu schon gelöscht wurden.

Sunworks bietet dabei Dienste für folgende Situationen an:
- Richtige Spurensicherung am Tatort
- Umgang mit digitalen Beweismitteln
- Analyse von Windows-Rechnern
- Analyse von Datenträgern
- Anomalien im Netzwerkverkehr entdecken
- Verwertung gewonnener Daten

## Initieren einer Forensischen Analyse

Im Initieren einer Forensischen Analyse beginnt die Analyse schon bevor das System physikalisch involviert wird. Da beim ersten Zugriff schon Beweise verändert werden können (Logs, Chache-Files, Internet-Verbindungen, ...) ist gerade in diesem Punkt ein sehr pragmatisches Vorgehen absolute Bedingung.
Danach wird ein Bit-Stream-Image des Datenträgers (Festplatte, USB-Stick, Magnetband, ...) erstellt, um mit der Analyse die Ergebnisse nicht zu verändern. Das gewonnene Abbild wird dann mit Forensischen Werkzeugen durchsucht und analysiert.



## Auswertung /Report

Sunworks erstellt einen Bericht zu den Ergebnissen der Untersuchungen und wird Massnahmen zur Verhinderung weiterer Angriffe vorschlagen.

## Forensics- Abonnemente

Neben einmaligen Aufträgen für eine Forensische Analyse, bietet Ihnen Sunworks auch Abos für regelmässige Tests Ihrer ICT-Umgebung an um die Sicherheit auch gegenüber veränderten Gefahren zu überprüfen.

Sunworks weist folgende Forensic-Zertifizierungen auf:
- Certified Ethical Hacker
- Certified Hacking Forensics Investigator