Verdeckte Online-Durchsuchung aus der Sicht der IT-Forensik

Chemnitzer Linuxtage 2008

dn Systems

Dr. Böttger
IT_Beratung + Projektmanagement

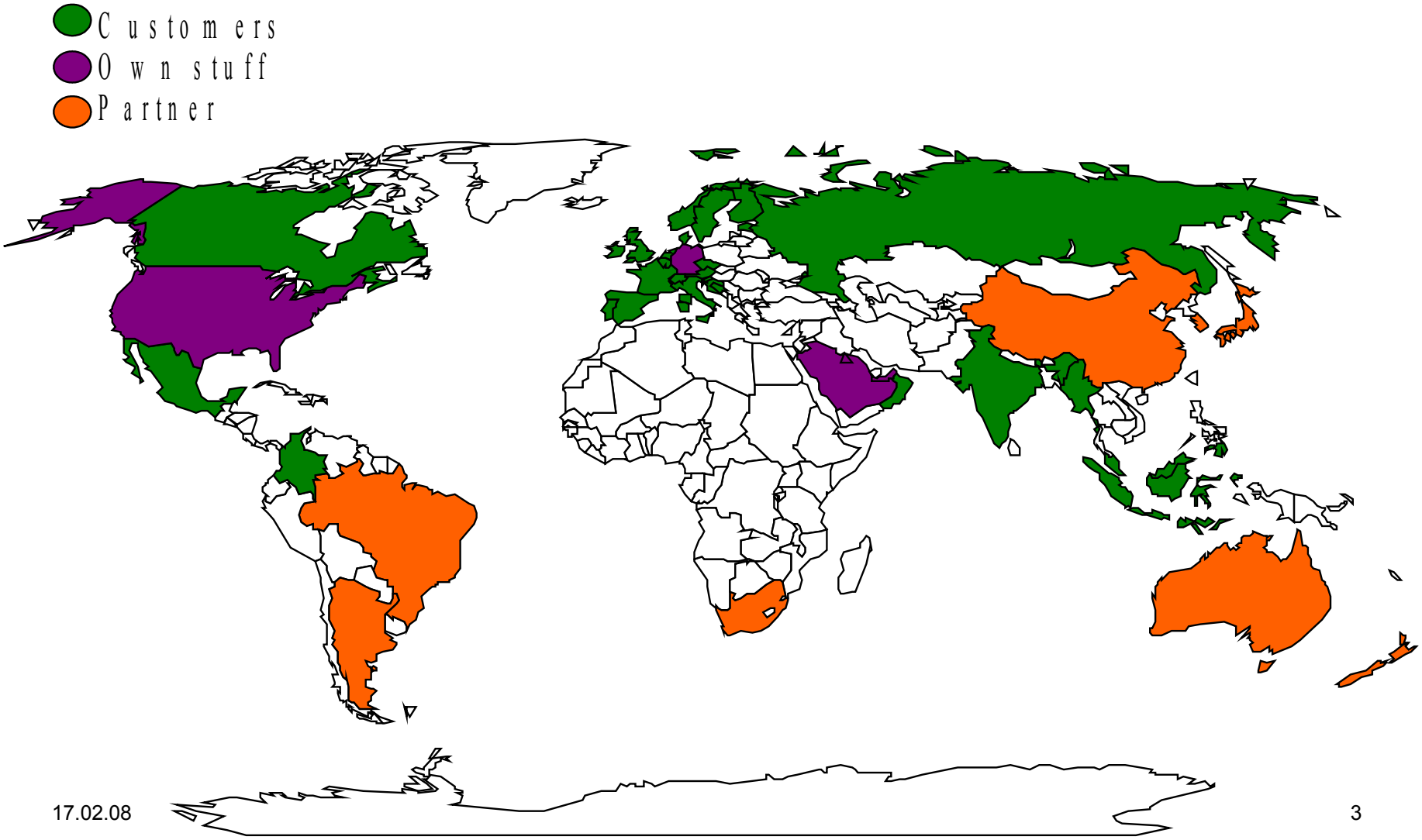
Dr. Christian Böttger
Senior Consultant

Dr. Böttger dn Systems
IT_Beratung + Projektmanagement

Über DN-Systems

- Globales Beratungs- und Technologie-Unternehmen
  - Planung
  - Evaluierung
  - Audit
  - Eigenes Rechner- / Netzwerk- Labor
  - Projektmanagement
  - Integrale Sicherheit (nicht nur IT)
  - Investigation / digitale Forensik / LI

Weltweiter Service



Unsere Kunden

- RZ- und Datacenter-Betreiber
- Internet-Service-Provider und Backbone-Betreiber
- Telekommunikations-Konzerne
- Supply-Chain-Betreiber
- Transport und Logistik
- International tätige Konzerne
- Banken und Finanznetz-Betreiber (Kreditkarten-Clearing)
- Produzenten von Sicherheits-Hard- und Software
- Behörden und Staaten

Vorstellung Person

- Freiberuflicher IT-Berater seit Mai 2006
- Vorher Projektmanager und Teamleiter bei einem Systemhaus
- Seit 1996 beruflich in der EDV
- Seit 1994 im WWW
- Seit ca 1987 im Internet
- Ausbildung: promovierter Physiker
- Seit Ende der '90er freier Autor für *iX* (Heise Verlag)
- Auslandsaufenthalte: Australien, Oman, EU

Themen

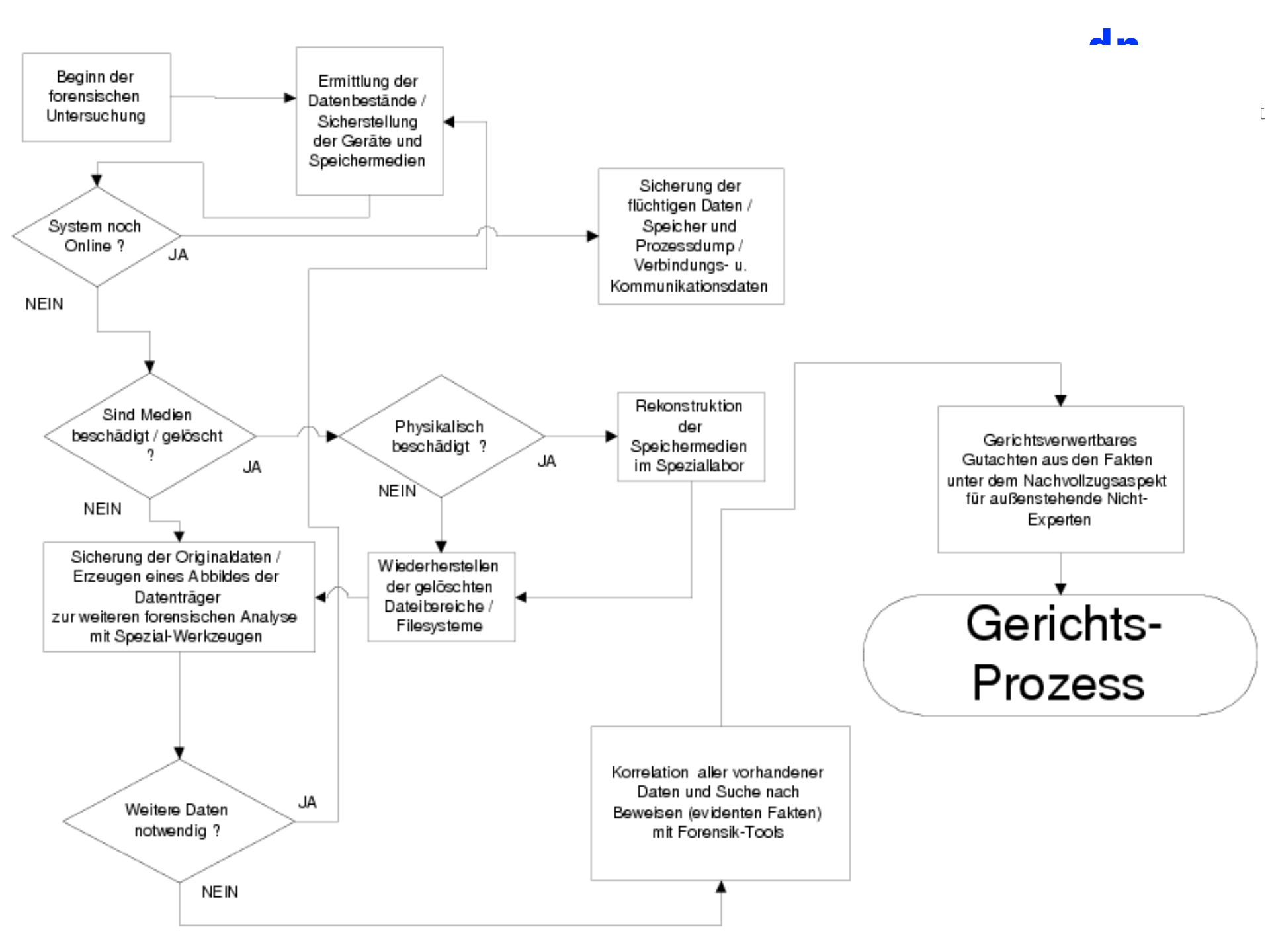
- EDV-Strategie
- Projektmanagement
- Internet und Netze
  - WWW
  - Mail, Anti-SPAM, Sicherheit
- Linux
- Open Source
- Groupware
- IT-Security, LI

Die Aufgabe

- Es müssen
  - be- und entlastende Beweise gefunden werden.
- Dies gelingt durch *dokumentiertes* und *nachvollziehbares* Auffinden von evidenten Daten.

Die Aufgabe

- Das wird sichergestellt durch
  - logische Analysen
  - physikalische Analysen
  - Datenintegritätsanalysen
  - Täterprofile / Zugrifsanalysen
- Sicherheit bei einem Gerichtsverfahren durch:
  - Nachvollziehbares Vorgehen
  - Absicherung gegen den Vorwurf der Manipulation an Beweismitteln


Beginn der forensischen Untersuchung
Ermittlung der Datenbestände / Sicherstellung der Geräte und Speichermedien
System noch Online ?
JA
NEIN
Sicherung der flüchtigen Daten / Speicher und Prozessdump / Verbindungs- u. Kommunikationsdaten
Sind Medien beschädigt / gelöscht ?
JA
NEIN
Physikalisch beschädigt ?
JA
NEIN
Rekonstruktion der Speichermedien im Speziallabor
Gerichtsverwertbares Gutachten aus den Fakten unter dem Nachvollzugsaspekt für außenstehende Nicht-Experten
Sicherung der Originaldaten / Erzeugen eines Abbildes der Datenträger zur weiteren forensischen Analyse mit Spezial-Werkzeugen
Wiederherstellen der gelöschten Dateibereiche / Filesysteme
Gerichts-Prozess
Weitere Daten notwendig ?
JA
NEIN
Korrelation aller vorhandener Daten und Suche nach Beweisen (evidenten Fakten) mit Forensik-Tools

Terminologie

- (verdeckte) Online-Durchsuchung
  - Analog Hausdurchsuchung: einmalige Durchsuchung und Auswertung des Datenbestands aus der Ferne
  - Strafverfolgung, Strafprozeßordnung (BMJ)
- (verdeckte) Online-Überwachung
  - Laufende Überwachung der Kommunikation inkl. verschlüsselten Inhalten (z.B. Skype, E-Mails)
  - Prävention, Quellen-TKÜV (BMI)

Die Online-Durchsuchung

- Verdeckte Einbringung von Durchsuchungs-Software („Bundes-Trojaner“) durch:
  - manipulierte E-Mails
  - manipulierte Webseiten
  - manipulierte Datenträger
  - „man-in-the-middle“-Angriffe
  - klassischen Einbruch

Die Online-Durchsuchung

- Folgerungen für den „Bundes-Trojaner“
  - darf nicht erkannt werden
    - auch nicht von Virenscanner und SPAM-Abwehr
  - darf nicht analysiert werden
    - alles ganz geheim
    - muss nach Beendigung der Durchsuchung wieder gelöscht werden
    - aber: was ist mit removeable devices und Backups?
  - Die Zielperson muss „dumm genug“ sein (?)

Die Online-Durchsuchung

- Rechtliche Vorgabe: der Kernbereich des privaten Lebens des Betroffenen darf nicht berührt werden („Tagebuch“)
  - Wie soll eine Suchsoftware das entscheiden? (Tagebuch.doc kann eine Bombenbauanleitung enthalten)
- Ist es zulässig, angebundene Netzwerklaufwerke zu durchsuchen? Die könnten ja auch (über VPN) z.B. der Firma gehören, bei dem der Mensch arbeitet.

Die Online-Durchsuchung

- Einsatz von versteckter Software
  - Onlinesuche auf dem Datenbestand der Festplatte
  - Speichern von Suchmustern und Schlüsselwörtern auf dem Zielsystem
  - Manipulation am Betriebssystem des durchsuchten Rechners
  - Keine strikten logischen Analysen oder Täterprofile/Zugriffsanalysen mehr möglich
  - Zerstörung der Zeitstempel durch die Suche
  - Suche ist von Unbefugten manipulierbar

Die Online-Durchsuchung

- Probleme beim Trojaner-Einsatz
  - Bemerkbar vom Betroffenen
- Sicherheit / Beweiskraft vor Gericht?
  - Keine nachvollziehbare Vorgehensweise
  - Schwierige / mangelhafte Dokumentation
  - Ermöglicht den Vorwurf der Manipulation an Beweismitteln

Kriterien der Analyse

- Wie wird mit meinen Daten im Analyseprozess umgegangen?
- Wie ist gewährleistet, dass Daten weder vernichtet noch verfälscht werden können?
- Wie ist die Kenntnis und das Know-How des Durchführenden für die spezifische Umgebung?
- Sind Spezialkenntnisse für Forensik-Analysen vorhanden?
- Sind weitere Fertigkeiten wie z.B. Reparatur eines beschädigten Datenträgers nötig?

Die Online-Durchsuchung

- Manipulation und Zerstörung von Beweismitteln
- Mögliche Folgeschäden
  - Verfügbarkeit
  - Integrität
  - Authentizität
  - Verschwiegenheit
  - Geheimhaltung

Die Online-Durchsuchung

Analyse eines Servers

- Sicherstellen der Informationen durch:
- Sicherstellung der Daten von Log- und Zeitservern
- Festplatten lokal und/oder auf NAS / SAN und/oder removeable devices?
- Welche Metadaten können manipuliert sein?
- RAID oder plain disks? evtl. de-striping
- Welche Filesysteme? (NFS, FAT, NTFS, SMB/CIFS, ...)
- Sicherung allgemeiner Betriebsdaten (MAC, CPU-ID, System-ID, ...)

Analyse eines Servers

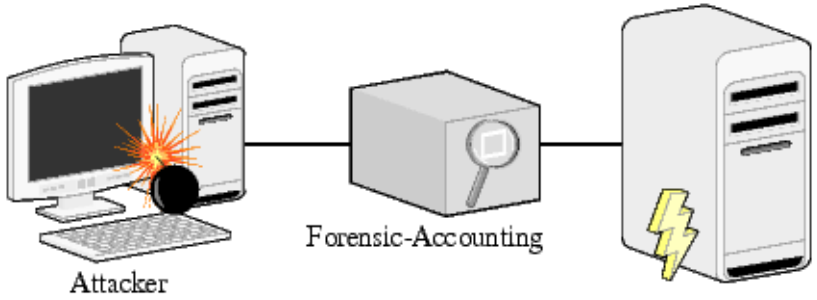
- Sicherstellen der Informationen durch:
- Welche Kommunikationsbeziehungen?
- Physischer Zugriff? Welche Personen?
- ggf. Zuführung zu einer Plattenforensik

Analyse eines Desktops

- Sicherstellen der Informationen durch:
- Sicherstellung der Festplatten und anderer Medien
  - CDRs, CD/DVD, Tapes, Token-Speicher, Online-Festplatten, ...
- Sofortiges Abschalten des Systems, um Löschen temporärer Daten zu verhindern
  - Browser-Cache, E-Mails, Downloads, News-Verzeichnisse, Chat-Logs, ...
- ggf. Zuführen zu einer Plattenforensik

Weitere Analyse

- Sicherstellen der Informationen durch:
- Firewall und IDS-Logs
- Radius/TACAS- und Einwahl-Logs vom ISP
- weitere Zugriffskontroll-Logs



Labor-Analyse

- Begutachtung der Speichermedien
- Medien verschlüsselt oder nicht lesbar?
- Physikalische Rekonstruktion durch Datenrettungslabor
- Erzeugung eines identischen Abbildes inkl. Meta- und Filesystemdaten
- Wiederherstellung gelöschter Dateibereiche auf dem Abbild
- Weitere Analyse ggf. auf einer weiteren Arbeitskopie des Abbildes
- **Dies kann die Onlinedurchsuchung nicht leisten!**

Zu beachten bei der Analyse

- Es gibt eine Vielzahl von Betriebssystemen, Encodings und Dateiformaten
- Oft sind evidente Daten gelöscht oder nur noch bruchstückhaft vorhanden
- Encoding der Daten muss gewandelt werden
  - z.B. ISO-8859-6 zu Iso-Latin-1, Unicode, UCF, UTF. EBCDIC, ...
- RAID- und SAN-Systeme (dump und de-striping, ...)

Analyse-Ebenen

- File system layer
  - Dateinamen, Verzeichnis-Einträge, NTFS Index tree, ...
- Meta-Daten File system layer
  - Unix inodes, NTFS MFT Einträge, ...
- Logical disk layer
  - Logische Blöcke, HD-Cluster, IP-Einkapselung, ...
- Physical layer
  - ATAPI-, SCSI- Zugriffe über Hostadapter oder Ethernet, ...
- Physical media layer
  - Magnetische Aufzeichnungsschicht, Modulation auf dem Netz,...
- **Online-Durchsuchung kann nur File System Layer mit etwas Meta-Daten**

Top-Down Analyse

- Erst mit den Mitteln des Betriebssystems nach dateien im logischen Dateisystem suchen.
- Spezielle Software, die Dateitypen an Hand von „Magic Bytes“ erkennt, hilft schnell, auch gelöschte Datenbestände zu klassifizieren.
- Analyse der Zugriffsberechtigungsdaten (Permissions, ACLs, Filesystem- und Objekt-Rechte)
- Auswertung deŕ verschiedenen Zeitstempel auf den verschiedenen Ebene
- Integritätsanalyse der Meta-Daten, um Maipulationen zu erkennen.
- **Online-Durchsuchung kann nur den ersten Schritt**

Grundsätzliche Aufgaben

- Rekonstruktion
  - Auffinden evidenter Daten
  - Wiederherstellung gelöschter Datenbereiche
- Manipulationssicher die Speichermedien duplizieren ohne Beweise zu verfälschen
- Auswertung von Datenformaten
  - Dokumente, Mail-Folder, Bild-Dateien, Chat-Logs, ...
- **Online-Durchsuchung kann das meiste hiervon nicht.**

Fazit

Mittels verdeckter Online-Durchsuchung ist eine zu verwertbaren Beweismitteln führende forensische Analyse prinzipiell nicht möglich.

- Einbringen von Suchpattern auf das Zielsystem, die false positive Ergebnisse liefern können (ohne diese Tatsache erkennen zu können)
- Zerstören von Informationen und Meta-Informationen, die Indizien liefern (z.B. Zeitstempel)
- Kein Sichern von anderen wichtigen Nicht-Online-Daten (externe Datenträger)
- Manipulation von Beweismitteln (Installation von Software)

Fragen ?

Thank You

Dr. Böttger
IT_Beratung + Projektmanagement

Dr. Christian Böttger
Bentestraße 10
31311 Uetze
Phone: +49.5173.9249744
Mail: c.boettger@boettger-consulting.de
http://www.boettger-consulting.de/

dn Systems

DN-Systems GmbH
Hornemannstr. 11-13
31137 Hildesheim, Germany
Phone: +49-5121-28989-0
Mail: info@dn-systems.de
http://www.dn-systems.de/

DN-Systems International Limited
P.O. Box 285 282
Dubai · U.A.E.
Phone: +971-50-2861299
Mail: info@dn-systems.com