Computer-Forensik

Forensische Analyse im Detail

F.M. Winter, H. Platzer, R. Riediger

Angewandte Informatik

20. Jänner 2017

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
- Mobiltelefone

Schluss

Problematik

Computersysteme sind oft viel zu schwach gesichert, Angreifer kommen viel zu leicht an wertvolle Informationen.

Motive der Täter:

Problematik

Computersysteme sind oft viel zu schwach gesichert, Angreifer kommen viel zu leicht an wertvolle Informationen.

Motive der Täter:

- sozial
- politisch
- technisch
- finanziell
- staatlich-politisch

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
- Mobiltelefone

Schluss

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
  - Festplatten-Images
    - erstellen
    - auswerten
  - Arbeitsspeicher-Images
    - erstellen
    - auswerten
  - Unix-spezifische Daten
    - spez. Daten (1)
    - spez. Daten (2)
- Windows
- Mobiltelefone

Schluss

Festplatten-Images erstellen

- `dd if=/dev/sda of=/mnt/sdb/test.img`
  Image eines Datenträgers in Datei schreiben
- `ddrescue`
  nützlich bei defekten Datenträgern

Festplatten-Images auswerten

- Sleuthkit
  - Live- oder Image-Analyse
  - Server zum Zugriff auf Images
  - Timeline des Dateisystems
- Testdisk / Photorec
  - Suche nach Dateisystemen / Partitionen
  - Datei-Carving

Arbeitsspeicher-Images erstellen

- LiME (Linux Memory Extractor)
  Kernelmodul zum Speicherzugriff
- Cold Boot - Angriff
  Speichermodule auf anderem System auslesen

Arbeitsspeicher-Images auswerten

- Volatility
  - Python-Framework, Plugin-Support
  - Aufteilung des Speichers nach Prozessen
  - Suche nach Mustern

Unixspezifische Daten

Befehl	Output
`cat /proc/cmdline`	Bootparameter des Kernels
`cat /proc/modules`	Informationen zu Kernelmodulen
`top`	Prozesse sortiert nach CPU / RAM - Verbrauch
`/proc/$PID/...`	Informationen über einen Prozess
`netstat -anp`	Aktive Netzwerkverbindungen / Ports
`netstat -rn`	Routingtabelle
`iptables -L`	Konfiguration des Paketfilters
`mount`	Eingehängte Partitionen
`df`	Auslastung d. Partitionen

Unixspezifische Daten

Befehl	Output
`cat /etc/passwd`	Existierende User
`cat /etc/shadow`	Passwörter d. User
`who`	Angemeldete User
`dpkg -l`	Installierte Softwarepakete
`cat /etc/apt/sources.list`	Paketquellen
`chkrootkit`	Suche nach Rootkits

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
- Mobiltelefone

Schluss

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
  - Vorarbeiten
  - Spezielle Datenträgerbereiche analysieren
    - Spez. Datenträger (1)
    - Spez. Datenträger (2)
    - Spez. Datenträger (3)
  - Fragestellungen an die Windows Registry
    - Fragestellungen (1)
    - Fragestellungen (2)
  - außerdem
- Mobiltelefone

Schluss

Vorarbeiten

- RAM Dump erstellen und weitere Auswertungen machen
- Von den vorhandenen Datenträgern ein forensisches Duplikat erzeugen
- Weitere Schritte:
  - Jegliche Daten wiederherstellen
  - Suchindex und Hashindex erzeugen und verifizierte Daten aussortieren
  - Sortierung nach Kategorien
  - Timeline Analyse

Spezielle Datenträgerbereiche analysieren

- File Slack
- Master File Table (MFT)
- Alternate Data Stream (ADS)
- NTFS Volumen Schattenkopien
- NTFS und Registry Transferprotokolle
- Weitere zu untersuchende Stellen
- Automatisierung mit Tools unter http://computer-forensik.org/tools/

Spezielle Datenträgerbereiche analysieren

File Slack

File Slack wird der freie Platz innerhalb eines Clusters (Blocks) vom Ende der Datei bis zum letzten Sektor des Clusters genannt.

Spezielle Datenträgerbereiche analysieren

File Slack

File Slack wird der freie Platz innerhalb eines Clusters (Blocks) vom Ende der Datei bis zum letzten Sektor des Clusters genannt.

MFT Slack

Der Master File Table beinhaltet die Datenbank mit allen Infos über Verzeichnisse und Dateien auf dem Datenträger. Auch hier gibt es einen überschüssigen Bereich, den MFT Slack.

Spezielle Datenträgerbereiche analysieren

File Slack

File Slack wird der freie Platz innerhalb eines Clusters (Blocks) vom Ende der Datei bis zum letzten Sektor des Clusters genannt.

MFT Slack

Der Master File Table beinhaltet die Datenbank mit allen Infos über Verzeichnisse und Dateien auf dem Datenträger. Auch hier gibt es einen überschüssigen Bereich, den MFT Slack.

NTFS Streams

NTFS Streams sind Daten, welche an Dateien oder Verzeichnisse angehängt werden können.

Spezielle Datenträgerbereiche analysieren

NTFS TxF

Das NTFS Transaktionssystem ermöglicht es, Dateioperationen atomar auszuführen. Veränderungen am Dateisystem werden dementsprechend nur dann vorgenommen, wenn die komplette Transaktion erfolgreich durchgeführt werden konnte.

Spezielle Datenträgerbereiche analysieren

NTFS TxF

Das NTFS Transaktionssystem ermöglicht es, Dateioperationen atomar auszuführen. Veränderungen am Dateisystem werden dementsprechend nur dann vorgenommen, wenn die komplette Transaktion erfolgreich durchgeführt werden konnte.

NTFS Volumen Schattenkopien

Mit dieser Technik werden Volumenvorgänge überwacht und Sicherungskopien von Sektoren erstellt, bevor Änderungen daran vorgenommen werden.

Spezielle Datenträgerbereiche analysieren

NTFS TxF

Das NTFS Transaktionssystem ermöglicht es, Dateioperationen atomar auszuführen. Veränderungen am Dateisystem werden dementsprechend nur dann vorgenommen, wenn die komplette Transaktion erfolgreich durchgeführt werden konnte.

NTFS Volumen Schattenkopien

Mit dieser Technik werden Volumenvorgänge überwacht und Sicherungskopien von Sektoren erstellt, bevor Änderungen daran vorgenommen werden.

Die Windows Registry

Die Registry, die zentrale hierarchische Konfigurationsdatenbank von MS Windows, ist für jeden Forensiker eine unschätzbar wertvolle Quelle.

Fragestellungen an die Windows Registry

- Welche Details über das System gibt es?
- MAC Adressen?
- Nutzerkennungen?
- Welche Programme sind / waren jemals installiert?
- Hardware?

Fragestellungen an die Windows Registry

- Welche Details über das System gibt es?
- MAC Adressen?
- Nutzerkennungen?
- Welche Programme sind / waren jemals installiert?
- Hardware?
- Installierte Gerätetreiber
- Partitionen? Eventuell alte Partitionen?
- Welche Anwendungen wurden wann benutzt?
- Welche Dateisysteme?
- Freigaben?
- Letzte Kommandos des Kommandoprompts?

Fragestellungen an die Windows Registry cont.

- Letzte zugegriffene Dateien?
- Letzte gesetzte Verknüpfungen?
- Welche Geräte waren jemals mit dem Gerät verbunden, samt Seriennummer desselben?
- Welche Programme sind / waren jemals installiert?

Fragestellungen an die Windows Registry cont.

- Letzte zugegriffene Dateien?
- Letzte gesetzte Verknüpfungen?
- Welche Geräte waren jemals mit dem Gerät verbunden, samt Seriennummer desselben?
- Welche Programme sind / waren jemals installiert?
- Verwendete Benutzernamen und Kennwörter?
- Besuchte Websites?
- Gespeicherte Formulardaten?
- Gespeicherte Suchen lokal oder im Web?
- Zeitstempelanalyse - Gibt es hier Inkonsistenzen?
- et cetera.

Weitere zu untersuchende Stellen:

- Registry Virtualisierung.
- Verzeichnis Virtualisierung.
- Windows User Assist Keys.
- Windows Prefetch Dateien.

Weitere zu untersuchende Stellen:

- Registry Virtualisierung.
- Verzeichnis Virtualisierung.
- Windows User Assist Keys.
- Windows Prefetch Dateien.
- Auslagerungsdateien.
- Hibernationsdatei.
- Sonstige versteckte Dateien.
- Systemprotokolle.
- Analyse von Netzwerkmitschnitten.

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
- Mobiltelefone

Schluss

Themenübersicht

Einleitung

Forensische Analyse für

- UNIX
- Windows
- Mobiltelefone
  - Forensische Analyse bei Mobiltelefonen
  - SIM-Karte
    - Wichtige Fragen
    - Informationen auf der SIM-Karte
  - Ablaufschema für Analyse
  - Software für Analyse
  - iPhone Analyzer

Schluss

Forensische Analyse bei Mobiltelefonen

Mobiltelefone rücken immer näher in den geschäftlichen und privaten Alltag.

- immer mehr Straftaten durch und auf Handys

Forensische Analyse bei Mobiltelefonen

Mobiltelefone rücken immer näher in den geschäftlichen und privaten Alltag.

- immer mehr Straftaten durch und auf Handys
- Geräte durch S-A-P-Modell behandeln
  S-A-P = Sicherstellen, analysieren, präsentieren

Forensische Analyse bei Mobiltelefonen

Mobiltelefone rücken immer näher in den geschäftlichen und privaten Alltag.

- immer mehr Straftaten durch und auf Handys
- Geräte durch S-A-P-Modell behandeln
  S-A-P = Sicherstellen, analysieren, präsentieren
- Speicherkarten (FAT-32) analysieren
  FAT-32 = File Allocation Table 32,
  32 Bit Dateisystem-standard

SIM-Karte

- ermöglicht Einsatz in GSM-Netzen. (Global System for Mobile Communication)
  Das Mobiltelefon übernimmt die Funktionen der SIM-Karte direkt. Da in dieser auch Daten abgespeichert werden, kann diese für eine Analyse wichtig sein.

SIM-Karte

- ermöglicht Einsatz in GSM-Netzen. (Global System for Mobile Communication)
  Das Mobiltelefon übernimmt die Funktionen der SIM-Karte direkt. Da in dieser auch Daten abgespeichert werden, kann diese für eine Analyse wichtig sein.
- Von Interesse sind:
  - Transaktionen durch Provider nachvollziehbar machen
  - IMEI-Nummer, macht das Telefon selbst identifizierbar

Wichtige Fragen bei der Analyse

- *Um welches Gerät handelt es sich? (IMEI/IMSI/etc.)*
- *Welche Telefonnummer gehört zu dem Gerät?*
- *Welche Telefonnummern wurden wann gewählt?*
- *Welche zusätzliche Software wurde auf dem Gerät installiert?*
- *Auf welche Zeitzone ist das Gerät eingestellt?*
- *Befinden sich Medien (Fotos/Dokumente) auf dem Gerät?*
- *Welche weiteren Dateien befinden sich auf dem Gerät?*
- *Welche (Internet-)Konfigurationsparameter sind eingegeben worden?*
- ...

wichtige Informationen auf der SIM-Karte

Auf der SIM-Karte befinden sich unter anderem folgende Informationen:

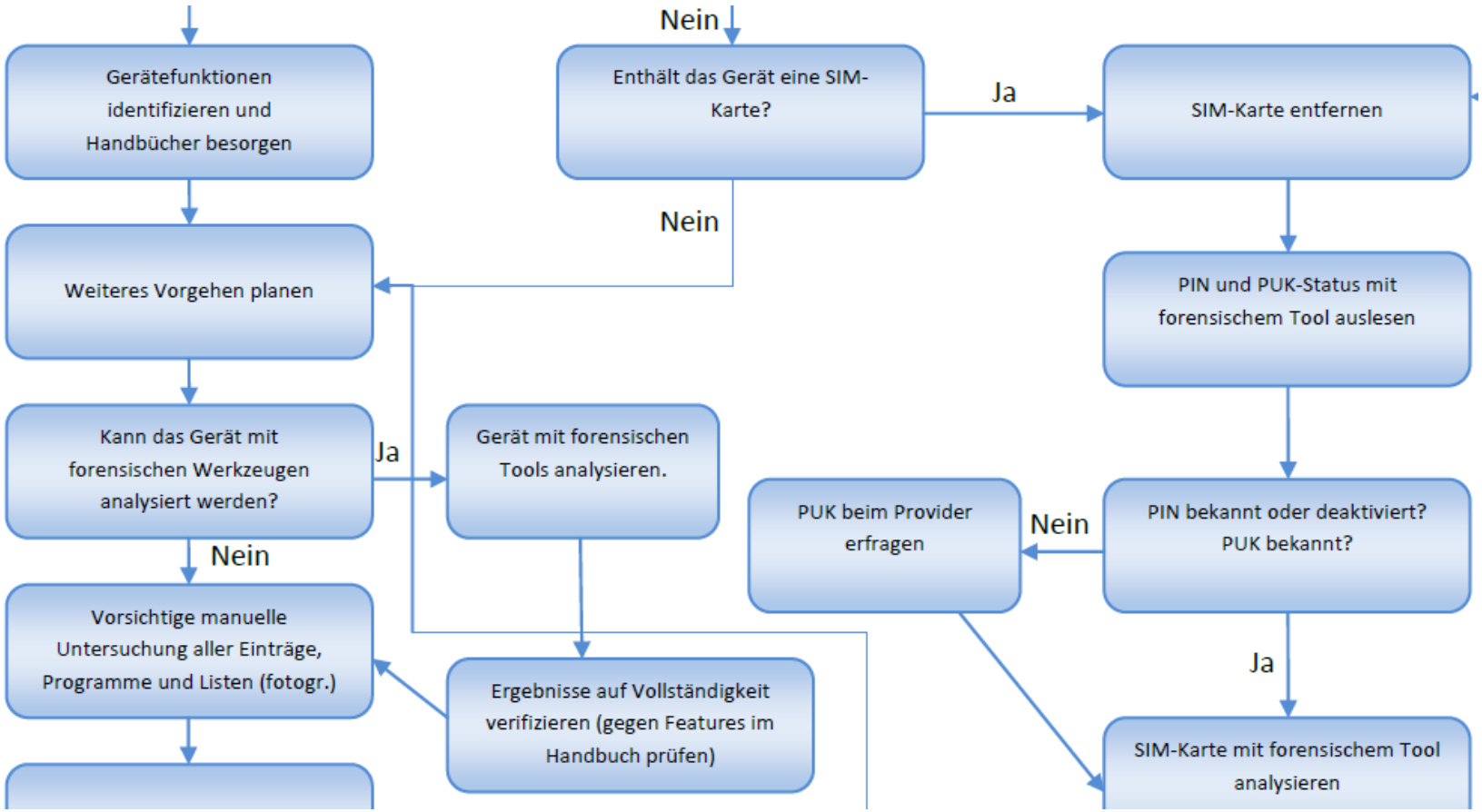
- Informationen über Netzteilnehmer
  - IMSI-Nummer, Identifizierung der SIM
  - MSISDN, Rufnummer

wichtige Informationen auf der SIM-Karte

Auf der SIM-Karte befinden sich unter anderem folgende Informationen:

- Informationen über Netzteilnehmer
  - IMSI-Nummer, Identifizierung der SIM
  - MSISDN, Rufnummer
- SMS, manchmal nach Löschung wiederherstellbar
- gewählte Rufnummern, etwaiger Standort

Analyse-Schema



Programme zur forensischen Analyse

Mit etlichen Tools ist es heutzutage möglich, Mobiltelefone forensisch zu analysieren.

- Software für mobile Geräte:
  - Pdd
  - PDASeizure
  - Oxygen Forensics

Programme zur forensischen Analyse

Mit etlichen Tools ist es heutzutage möglich, Mobiltelefone forensisch zu analysieren.

- Software für mobile Geräte:
  - Pdd
  - PDASeizure
  - Oxygen Forensics
- laufendes Gerät nicht ausschalten!!
- verschlüsselt gespeicherte Daten sind oft unverschlüsselt im Hauptspeicher

Programme zur forensischen Analyse

Mit etlichen Tools ist es heutzutage möglich, Mobiltelefone forensisch zu analysieren.

- Software für mobile Geräte:
  - Pdd
  - PDASeizure
  - Oxygen Forensics
- laufendes Gerät nicht ausschalten!!
- verschlüsselt gespeicherte Daten sind oft unverschlüsselt im Hauptspeicher
- weitere Software für übliche Mobiltelefone:
  - Paraben's Cell
  - Device Seizure
  - Oxygen Forensic Suite
  - XRY
  - iPhone Analyzer

iPhone Analyzer

Der iPhone-Analyzer liest über iTunes auf den Rechner geladene Backups aus und erhält somit folgende Informationen.

- Anruferlisten, SMS, MMS
- Kontakte
- E-Mails
- Kalender, Notizen
- Bilder, Screenshots, Videos
- Musikstücke
- Browser-History, Bookmarks, Cookies
- installierte Apps mit ihren Daten
- Daten aus Google Maps
- GPS-Tracking
- Informationen über Voice-Mails
- Wifi-Konfigurationen
- ...

Danke

Danke für Ihre Aufmerksamkeit!

Quellen
Literatur

Buch:
Computer-Forensik : Computerstraftaten erkennen, ermitteln, aufklären
Verlag:
Heidelberg : dpunkt-Verl.
Ausgabe:
6., aktualisierte und erw. Aufl.
ISBN/ISSN:
978-3-86490-133-1 / 3-86490-133-2

Quellen
Internet

Unix:

- dd, ddrescue: Unix-Manpage der Programme
- Sleuthkit: http://forensicswiki.org/wiki/The_Sleuth_Kit
- Testdisk, Photorec: http://www.cgsecurity.org/wiki
- LiME: https://github.com/504ensicsLabs/LiME
- Cold Boot Angriff: https://en.wikipedia.org/wiki/Cold_boot_attack
- Volatility: http://forensicswiki.org/wiki/Volatility_Framework

Mobile Geräte:

- www.wikipedia.at
- www.itwissen.info
- www.alzomar.com/uploads/XRY.png