KPMG

cutting through complexity™

Mac OS X Forensik

- ein Überblick -

KPMG Forensic Technology

Alexander Geschonneck

Nadja Kickinger

Mac OS X Forensik - Agenda

- Situation heute - Herausforderungen
- Sicherung des Datenträgers
- Partitionsschema
- Dateisystem HFS+
- Werkzeugunterstützung
- Benutzerspuren und Artefakte
- Analyse des laufenden Systems

Forensische Analyse von Mac OS X

Situation heute

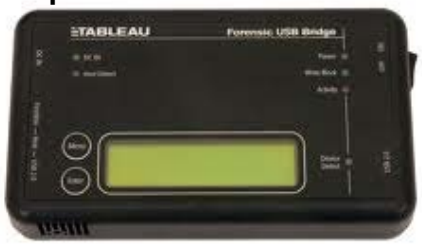
- Immer häufiger Computer von Apple im Unternehmensumfeld im Einsatz.
- Dadurch auch relevanter im Rahmen von Betrugs- und Korruptionsbekämpfung oder der Aufklärung von IT-Sicherheitsvorfällen.
- Bei forensischen Analysen daher Fachkenntnisse gefordert hinsichtlich Besonderheiten der Apple Computer.

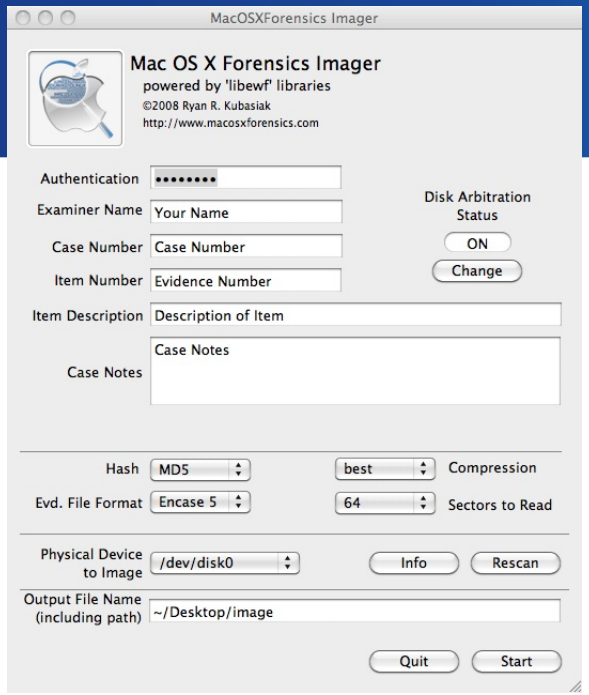
Herausforderungen und Unterschiede

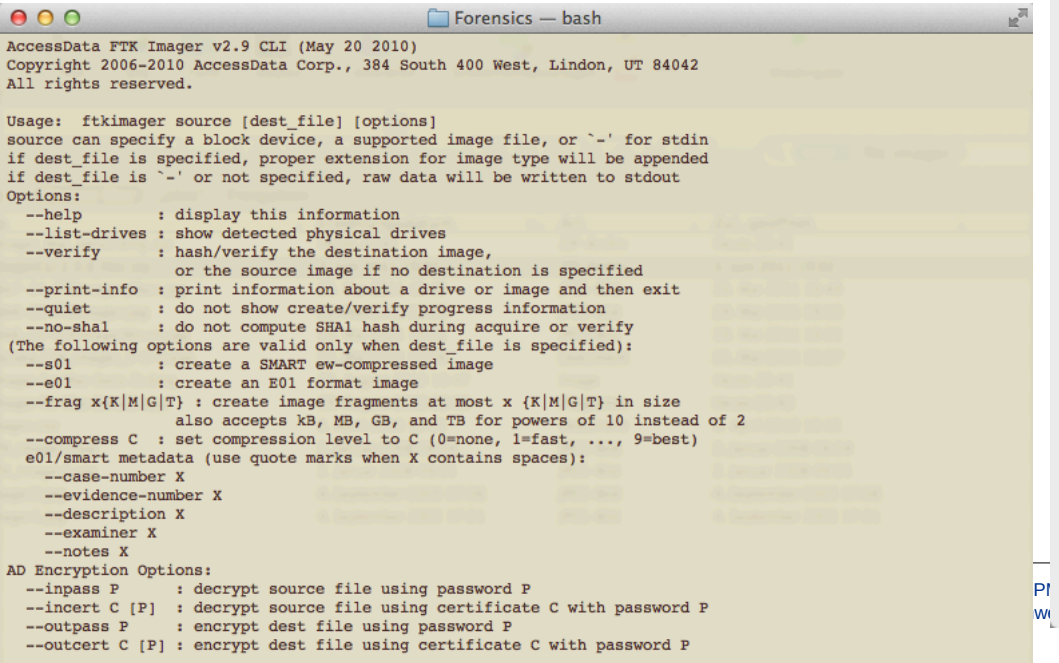
- Spezielles Dateisystem HFS+ erfordert Software-Unterstützung bei herkömmlichen Forensik-Tools
- Physischer Zugriff auf Datenträger unter Umständen schwierig
- Keine „zentrale“ Datenbank (vgl. Windows Registry), sondern verteilte Speicherung von benutzerbezogenen Einstellungen, Historien und anderen relevanten Informationen.

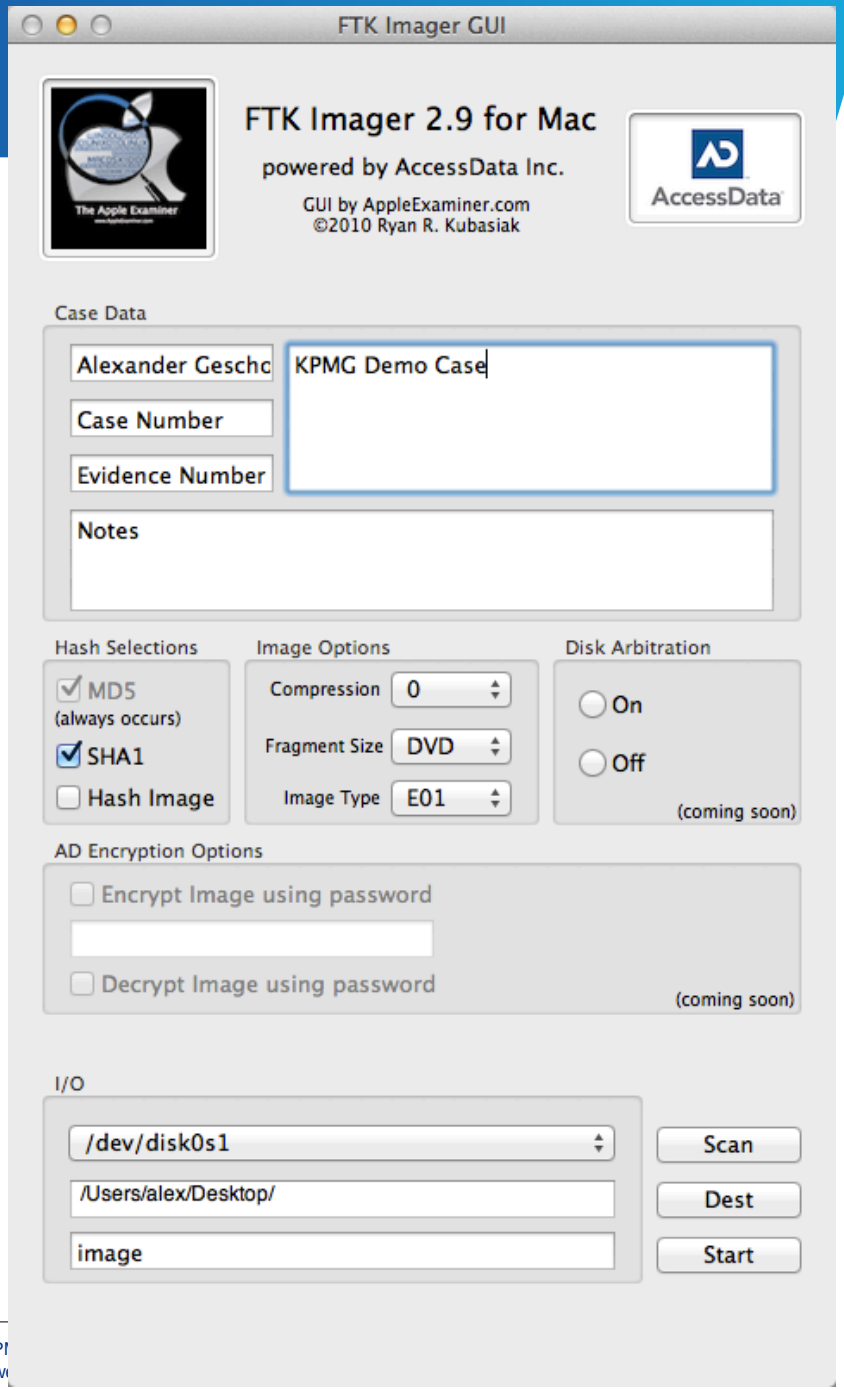
Sicherung des Datenträgers - Basics

- Grundsatz der forensischen Untersuchung: korrektes Sicherstellen der Festplattendaten ohne Beeinträchtigung der Beweismittelkette und ohne Veränderungen am Original.
- Abzug der Festplattendaten und Speicherung in Form eines 1:1 Abbildes / Images mit geeigneter Hard- und Software.
- Hardware-Writeblocker unterbinden sicher die Weiterleitung von Schreibbefehlen, hierzu ist der Ausbau der Festplatte erforderlich.
- Software-Writeblocker stellt Verhalten in Software nach, aber kein vollständiger Schutz vor Veränderung garantiert.
- Kompakte Bauweise von Apple Geräten (z.B.: MacBooks, iMacs) erschwert oder verhindert jedoch physischen Zugriff auf Festplatte.
  - Detaillierte, bebilderte Anleitungen für den Ausbau zum Beispiel auf www.ifixit.com

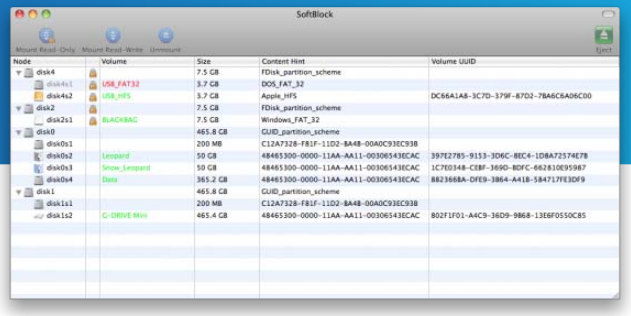



MacOSXForensics Imager
Mac OS X Forensics Imager
powered by 'libewf' libraries
©2008 Ryan R. Kubasiak
http://www.macosxforensics.com
Authentication
Examiner Name
Your Name
Case Number
Case Number
Item Number
Evidence Number
Item Description
Description of Item
Case Notes
Case Notes
Disk Arbitration Status
ON
Change
Hash
MD5
Compression
best
Evd. File Format
Encase 5
Sectors to Read
64
Physical Device to Image
/dev/disk0
Info
Rescan
Output File Name (including path)
~/Desktop/image
Quit
Start


Forensics — bash
AccessData FTK Imager v2.9 CLI (May 20 2010)
Copyright 2006-2010 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.
Usage: ftkimager source [dest_file] [options]
source can specify a block device, a supported image file, or `-' for stdin
if dest_file is specified, proper extension for image type will be appended
if dest_file is `-' or not specified, raw data will be written to stdout
Options:
--help : display this information
--list-drives : show detected physical drives
--verify : hash/verify the destination image,
or the source image if no destination is specified
--print-info : print information about a drive or image and then exit
--quiet : do not show create/verify progress information
--no-sha1 : do not compute SHA1 hash during acquire or verify
(The following options are valid only when dest_file is specified):
--s01 : create a SMART ew-compressed image
--e01 : create an E01 format image
--frag x{K|M|G|T} : create image fragments at most x {K|M|G|T} in size
also accepts kB, MB, GB, and TB for powers of 10 instead of 2
--compress C : set compression level to C (0=none, 1=fast, ..., 9=best)
e01/smart metadata (use quote marks when X contains spaces):
--case-number X
--evidence-number X
--description X
--examiner X
--notes X
AD Encryption Options:
--inpass P : decrypt source file using password P
--incert C [P] : decrypt source file using certificate C with password P
--outpass P : encrypt dest file using password P
--outcert C [P] : encrypt dest file using certificate C with password P


FTK Imager GUI
FTK Imager 2.9 for Mac
powered by AccessData Inc.
GUI by AppleExaminer.com
©2010 Ryan R. Kubasiak
AccessData
Case Data
Alexander Geschc
KPMG Demo Case
Case Number
Evidence Number
Notes
Hash Selections
MD5
(always occurs)
SHA1
Hash Image
Image Options
Compression
0
Fragment Size
DVD
Image Type
E01
Disk Arbitration
On
Off
(coming soon)
AD Encryption Options
Encrypt Image using password
Decrypt Image using password
(coming soon)
I/O
/dev/disk0s1
Scan
/Users/alex/Desktop/
Dest
image
Start

Sicherung des Datenträgers – cont.



Alternativen zum Festplattenausbau

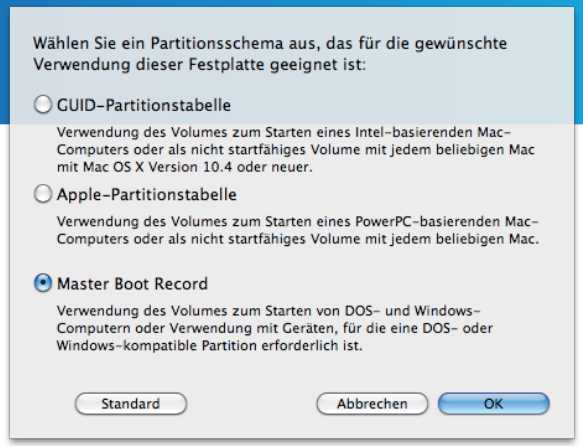
- Einsatz von Live-CDs mit forensischen Werkzeugsammlungen dank Intel-basierter Hardware möglich, zum Beispiel *DEFT*, *Caine* oder *Helix 3*.
- Diese stellen Software-“Writeblocker“ (`mount -ro`) und Werkzeuge für das Erstellen von forensischen Abbildern zur Verfügung:
  - Werkzeuge wie z.B. *Guymager* beherrschen die Image-Erstellung, Hash-Berechnung und Verifizierung von einem oder mehreren Quelldatenträgern und arbeiten diese wahlweise sequentiell oder parallel ab.
- Speicherung des Abbildes auf einem externen Datenträger
  - Problem USB 2.0 Schnittstelle: niedrige Übertragungsrate und dadurch langwieriger Sicherungsprozess
  - Wenn möglich Verwendung von Firewire, Thunderbolt oder derzeit nur Erweiterungskarten (eSATA oder USB 3.0).

Sicherung des Datenträgers

Alternativen zum Festplattenausbau

- Target Disk Mode:
  - Spezieller Startmodus von Apple Geräten ohne Booten des Betriebssystems der Systempartition
  - Bereitstellung der internen Festplatte über Firewire/Thunderbolt als „externer Datenträger“ für zweiten Analyse-Rechner
  - Beim Booten „T“-Taste gedrückt halten
  - Voller Lese- und Schreibzugriff
  - Aber: nur erste interne ATA-Festplatte ansprechbar

Partitionsschema

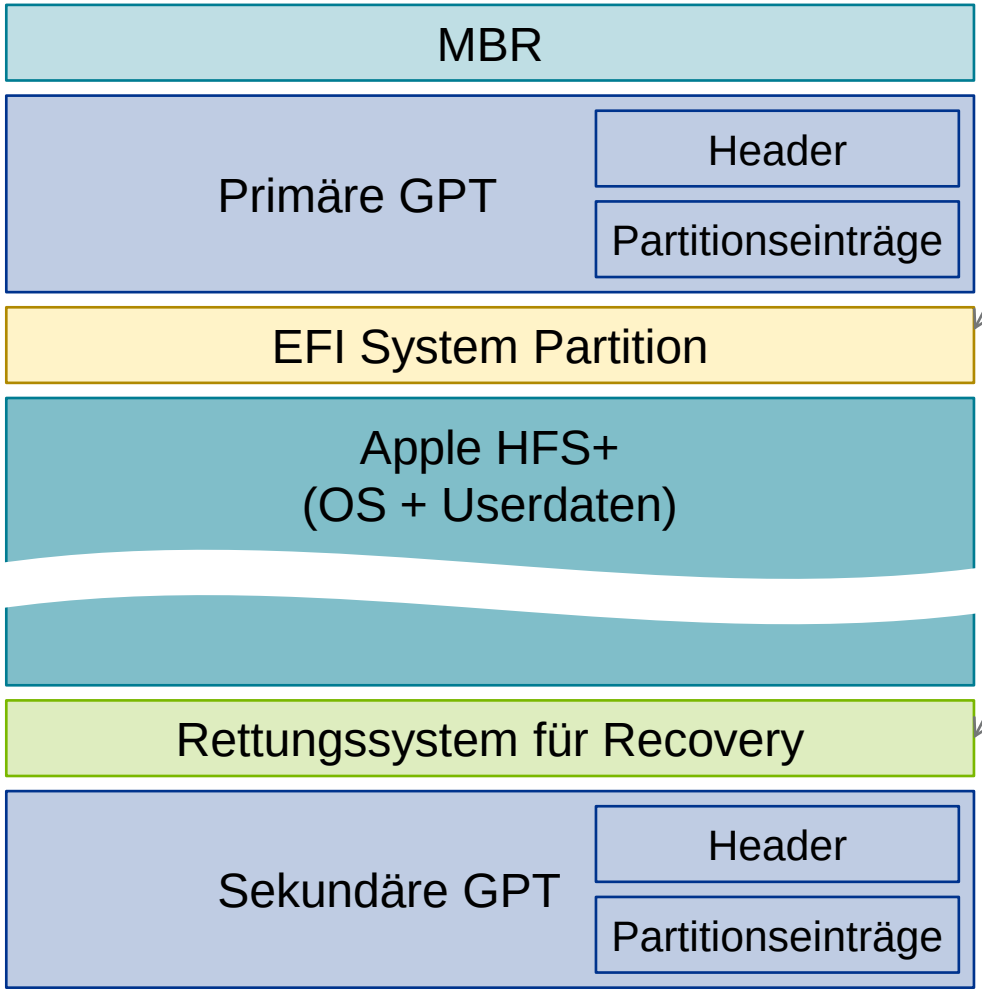


GUID Partition Table (GPT)

- Standard-Partitionstabelle von Intel-basierten Macs.
- Teil der (U)EFI-Spezifikation
- Auch von Windows 7 für Festplatten größer als 2 TB verwendet
- GPT besteht aus Header und Partitionseinträgen
- Einteilung des Datenträgers in Master Boot Record, primäre GPT und sekundäre GPT
  - MBR aus Kompatibilitätsgründen mit einer einzelnen Partition vom Typ 0xEE über den ganzen Datenträger, verhindert Änderungen durch GPT-inkompatible Werkzeuge (z.B. fdisk).
  - Sekundäre GPT am Ende der Platte als Sicherungskopie für den Fehlerfall

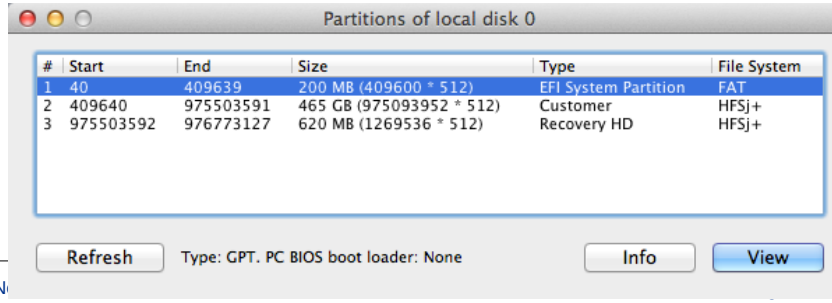
Partitionsschema

Besonderheiten der Partitionierung unter Apple



Erste Partition mit 200 MB für die zukünftige Verwendung durch EFI-Treiber.

Neu seit Mac OS X 10.7: Rettungs-system in 650 MB großer Partition für Wiederherstellung und Neuinstallation.



Dateisystem HFS+

Grundlegende Eigenschaften und Zugriff

- „Hierarchical File System Plus“ alias „Mac OS Extended“
- Von Apple entwickeltes Standard-Dateisystem der Macs
- Journaling-Dateisystem mit Partitions- und Dateigrößen bis zu 8 EiB (1 Exbiyte=2^{60} byte)
- Unterstützt bis zu 255 Zeichen langen Dateinamen, Unicode-Unterstützung, Unterscheidung zwischen Groß- und Kleinschreibung
- Aufbau des Dateisystems ist dokumentiert (!)
- Lesender Zugriff auf HFS+ unter Linux durch Kernel-Modul „hfsplus“ und Werkzeugsammlung „hfsprogs“ möglich.

Dateisystem HFS+

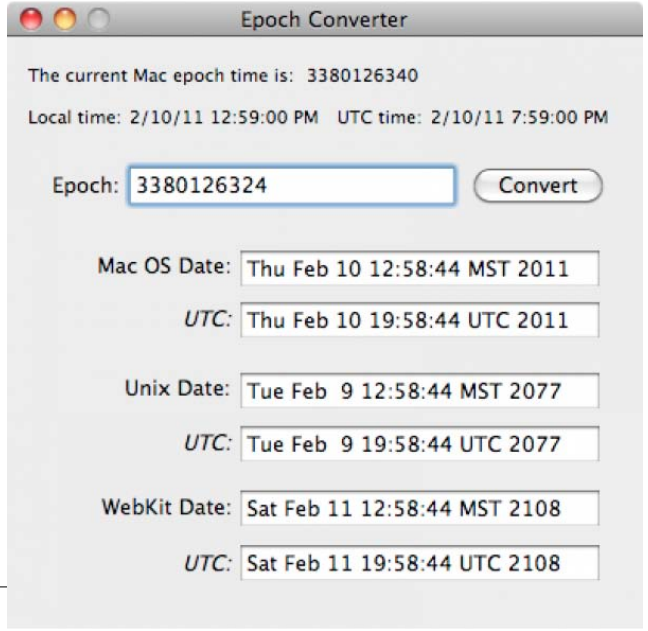
Dateisystem-Strukturen

- Volume Header
  - Grundlegende Verwaltungsinformationen der Partition und Verweise auf die anderen Strukturen
  - Fixe Position am Beginn der Partition nach 1024 reservierten Bytes
  - Sicherungskopie 1024 Byte vor Ende der Partition
- Allocation File
  - Verwaltung belegter Blöcke
- Catalog File
  - Einträge zu allen Dateien und Verzeichnissen
- Weitere Strukturen für Organisation von Metadaten und Attributen

Dateisystem HFS+

Forensisch relevante Eigenschaften

- Löschen einer Datei
  - Entfernen des dazugehörigen Eintrags im Catalog File und Markieren der Datenblöcke im Allocation File als unbelegt.
  - Dateiinhalte verbleiben auf der Festplatte, bis sie durch spätere Schreibaktionen überschrieben werden – grundsätzlich also teilweise oder vollständige Wiederherstellung möglich.
- Zeitstempel
  - Speicherung als 32 Bit-Wert als Anzahl der Sekunden seit 01.01.1904 (erstes Schaltjahr im 20. Jahrhundert) in Zeitzone GMT, Umrechnung auf Lokalzeit dann durch Systemroutinen
  - Vier Zeitstempel: Erstellung der Datei, letzter Zugriff, letzte Änderung des Inhalts und letzte Änderung der Attribute



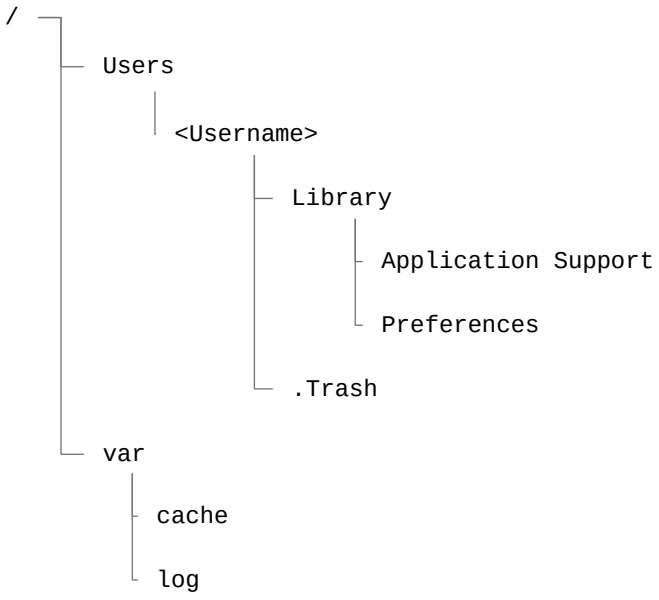
Dateisystem HFS+

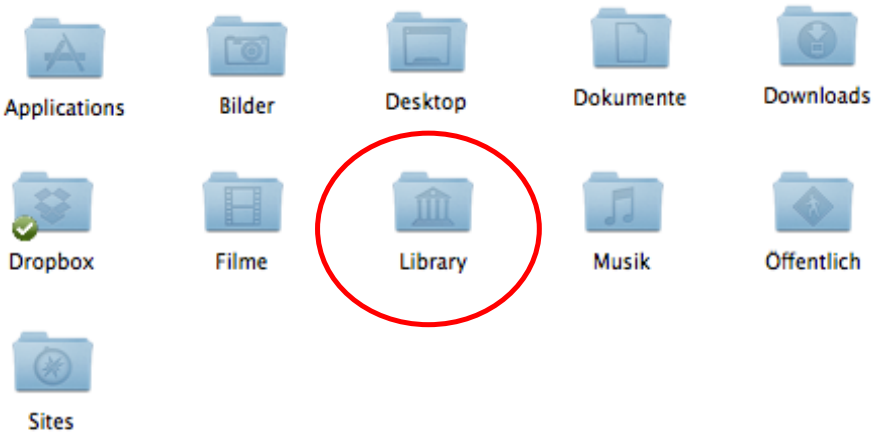
Forensisch relevante Eigenschaften

- Forks
  - Unterscheidung zwischen Data Forks und Resource Forks: Data Forks für den eigentlichen Dateiinhalt, Resource Forks für zusätzliche strukturierte Metadaten in unterschiedlichen Datentypen
  - Resource Forks vergleichbar mit Alternate Data Streams von NTFS, ermöglichen Verschleierung von Daten
- Erweiterte Attribute
  - Zusätzliche Metainformationen durch Anwendungsprogramme speicherbar, z.B.: farbliche Markierung im Finder, aber auch Downloadzeitpunkt einer Datei
- Beim Kopieren auf Nicht-HFS+ Dateisysteme werden Forks und erweiterte Attribute in zusätzlichen Dateien nach dem Schema „._Dateiname“ gespeichert.

Benutzerspuren und Artefakte

- Nutzung von Mac OS X hinterlässt genauso wie unter Windows Benutzerspuren
- Interessante Verzeichnisse unter OS X:





Benutzerspuren und Artefakte

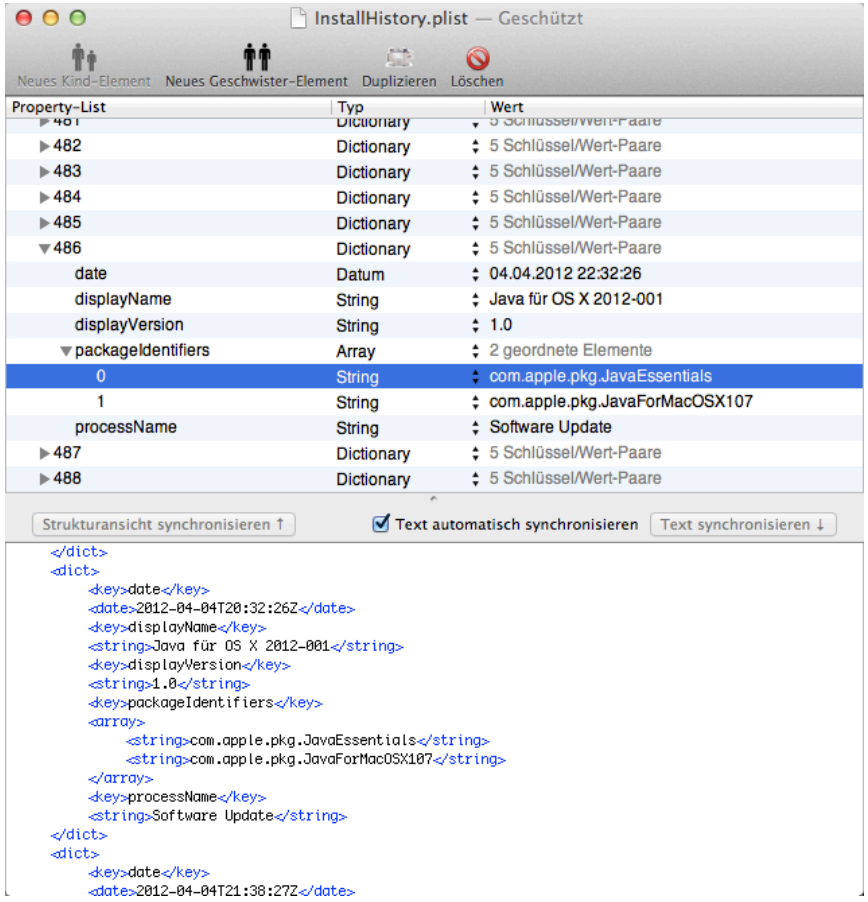
Papierkorb

- Persönlicher Papierkorb im Verzeichnis `.Trash` im Benutzerordner
- „Einfaches“ Löschen einer Datei = Verschieben in persönlichen `~/.Trash` mit Original-Dateiname (z.B. im Gegensatz zu Windows 7)
- Für Funktion „Zurücklegen“ Speicherung des Ursprungpfads in versteckter Datei `~/.Trash/.DS_Store` seit OS X 10.6 – davor keinerlei Metadaten abgelegt
- Original-Zeitstempel (Erstell- und Änderungsdatum) werden weder beim Löschen noch beim „Zurücklegen“ verändert

Benutzerspuren und Artefakte

Property Lists (.plist)

- Kein Pendant zur „zentralen“ Windows Registry unter Mac OS X
- Speicherung von Programmeinstellungen, Historien, Verläufen und Systemkonfigurationen stattdessen in Property Lists
- Property Lists zur strukturierten Datenspeicherung basierend auf XML
- Bearbeitung / Ansicht mit z.B. Property List Editor (Teil der Apple Entwicklerwerkzeuge)



Benutzerspuren und Artefakte (forensisch relevante Property Lists.plist) – Wo starten?

Dateiname	Inhalte
`/private/var/log/OSInstall.custom (10.5)` `/private/var/db/.AppleSetupDone (10.6)`	Installationsdatum des Betriebssystems (Enthält auch die bei der Installation eingegebenen Registrierungsdaten)
`/System/Library/CoreServices/SystemVersion.plist (OS X Client)` `/System/Library/CoreServices/ServerVersion.plist (OS X Server)`	OS Version
`/Library/Receipts/InstallHistory.plist` `/Library/Preferences/com.apple.SoftwareUpdate.plist`	Verlauf der installierten Anwendungen und Update Letztes Software Update

`/etc/localtime (Linkfile zur aktuellen Zeitzone)`
`oder`
`/Library/Preferences/.GlobalPreferences.plist`
	Aktuell konfigurierte Zeitzone

`/Library/Preferences/com.apple.loginwindow.plist`	Auto-Login und Last Login User Info
`/Library/Preferences/com.apple.preferences.accounts.plist`	Gelöschte Benutzer

Benutzerspuren und Artefakte (forensisch relevante Property Lists.plist) – Wo starten? cont.

Dateiname	Inhalte
`/Users/username oder ~/`	die Benutzerverzeichnisse
`~/Library/Preferences/com.apple.recentitems.plist`	Die jeweils letzten 10 geöffneten Dokumente, gestarteten Anwendungen und verbundenen Netzwerkfreigaben
`~/Library/Preferences/com.apple.loginitems.plist` `~/Library/Preferences/loginwindow.plist`	Automatisch beim Login des Benutzers gestartete Anwendungen oder Skripte
`/Users/username/Library/Preferences/com.apple.sidebarlists.plist`	Angeschlossene Laufwerke
`/Library/Preferences/SystemConfiguration/com.apple.smb.server.plist`	Verbundene Laufwerke

`/Users/username/Library/Application Support/MobileSync/Backup`
 	
`~/Library/Preferences/com.apple.iPod.plist`
	iPhone/iPod/iPad - Syncverzeichnis
	
	Synchronisierung mit iPods und iPhones inklusive Zeitstempel, Seriennummer und IMEI

`/Users/username/Library/Application Support/MobileSync/Backup/UUID/Info.plist`	Informationen über jedes synchronisierte i-Device. Modification Time der Datei ist der letzte Synczeitpunkt

Benutzerspuren und Artefakte (forensisch relevante Property Lists.plist) – Wo starten? Netzwerkeinstellungen

Dateiname	Inhalte
/Library/Preferences/com.apple.alf.plist /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist /Library/Preferences/SystemConfiguration/com.apple.nat.plist **/Library/Preferences/SystemConfiguration/com.apple.network.identification.plist** /Library/Preferences/SystemConfiguration/com.apple.NetworkInterfaces.plist /Library/Preferences/SystemConfiguration/com.apple.preferences.plist	Firewall-Einstellungen Airport-Einstellungen Internet Sharing Einstellungen **Verlauf der TCP/IP-Einstellungen mit Zeitstempeln** onBoard Netzwerkgeräte Netzwerkkonfiguration der Netzwerkgeräte
/Users/username/Library/Application Support/Screen Sharing	Screen Sharing
/Library/Preferences/com.apple.Bluetooth.plist	Bluetooth Verlauf

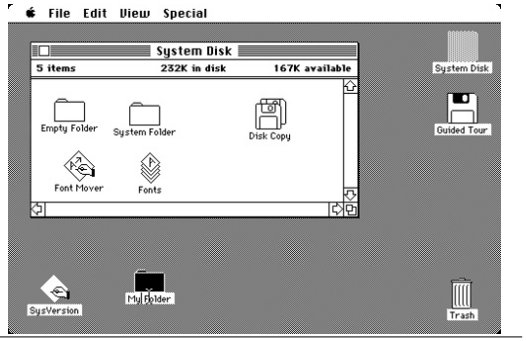
Benutzerspuren und Artefakte (forensisch relevante Property Lists.plist) – Wo starten? Instant Messaging

Dateiname	Inhalte
/Library/Preferences/com.apple.iChat.AIM.plist /Library/Preferences/com.apple.iChat.plist /Library/Preferences/com.apple.iChat.SubNet.plist /Users/username/Library/Preferences/com.aol.aim.plist /Users/username/Library/Preferences/com.adiumX.adiumX.plist /Users/username/Library/Preferences/com.apple.iChat.AIM.plist /Users/username/Library/Preferences/com.apple.iChat.plist /Users/username/Library/Preferences/com.apple.SubNet.plist /Users/username/Library/Preferences/com.skype.skype.plist /Users/username/Library/Preferences/com.yahoo.messenger3.plist /Users/username/Library/Preferences/com.yahoo.messenger3.Users.screenname.plist	Instant Messaging
/Users/username/Library/Safari/Bookmarks.plist /Users/username/Library/Safari/Downloads.plist /Users/username/Library/Safari/History.plist /Users/username/Library/Safari/LastSession.plist	Safari – Bookmarks Safari – Inhalt des Download Fensters Safari – Browser Verlauf Safari – letzte Brwoser Session (Tabs & Fenster)

Benutzerspuren und Artefakte (Protokolldateien)

Protokolldateien

- Aufzeichnungen von Systemdiensten in `/var/log` zeigen Verwandtschaft zu Unix/Linux, zum Beispiel:
  - `/var/log/cups/access.log` enthält Aufzeichnungen zu erfolgreich abgesetzten Druckaufträgen inklusive Zeitstempel und Druckernamen
  - `/var/log/samba/log.nmbd` erlaubt Nachvollziehen der Verbindungen mit (Windows-) Netzwerken
  - `/private/var/log` enthält systemweiten Aufzeichnungen
- Benutzerbezogene Protokolle befinden sich in `~/Library/Logs`
- Befehlshistorie des Terminals in `~/.bash_history` – sofern Bash als Shell genutzt wird
- Sleep File `/private/var/vm/sleepimage`
- Virtual Memory `/private/var/vm/swapfile0`



Benutzerspuren und Artefakte (Mail & iCal)

Apple Mail

- E-Mailkonten in `~/Library/Mail` abgelegt
- Unterordner jeweils für Eingang, Gesendet, Entwürfe usw.
- E-Mail Anhänge im Verzeichnis Attachments bzw. in `~/Library/Mail Downloads`

Kalender

- Daten des Apple Kalender (iCal) unter `~/Library/Calendars` in einzelnen ICS-Dateien abgelegt
- Hier finden sich auch alle synchronisierten Kalender

```
$ ls /Users/XYZ/Library/Calendars/E8386B2F-617A-40C8-021FBE77685995.calendar/Events/
03656DED6F-E079-457F6-91D1-DD0C8FD9D3F288.ics
080AED6891-1F7D-458B7-8E25-0E7734563B82C8.ics
0CA724657D-75F5-4526F-B8FB-0FD2C305664076.ics
0C45DE659C-3885-415BD-9F13-F643C6B4A9C265C.ics
```

Analyse am laufenden System

Live-Forensik

- Auch unter Mac OS X Sicherung des Arbeitsspeichers eines laufenden Systems sinnvoll
- Ermöglicht detaillierte Analyse von Aktivitäten von Benutzern, Prozessen und des Kernels
- Erstellung eines Speicherabbilds unter Mac OS X erfordert Root-Rechte, z.B. mit Mac Memory Reader
- Anschließende Analyse des Speicherabbildes durch beliebiges Forensik-Produkt mittels Datei-Header-Signatursuche oder textuellen Suchen
- Benutzerkennwörter im Klartext, aber schwierig zu finden – Extraktion aller Zeichenketten zur Erstellung einer Wortliste möglich (Wörterbuch-Attacke)
- Spezialisiertes Tool Volafox zum Auslesen von System-, Kernel- und Prozessinformationen

Werkzeugunterstützung

- Werkzeug-gestützte Analyse von Mac-Abbildern erfordert Unterstützung von HFS+
- Beispiele für kommerzielle Produkte mit HFS+ Unterstützung
  - Encase Forensic
  - Forensic Toolkit (FTK)
  - X-Ways Forensics
- Spezialisierte Produkte für Mac-Forensik
  - BlackLight
  - Mac Marshal Forensic Edition
  - MacForensicsLab
- Automatismen der Analyse-Produkte ersetzen jedoch nicht erforderliches Fachwissen über relevante Fundstellen und Systemeigenschaften!

KPMG

cutting through complexity™

KPMG

Alexander Geschonneck

Partner

Forensic Technology

Tel. +49 30 20681520

ageschonneck@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft,
a subsidiary of KPMG Europe LLP