HOCHSCHULE MITTWEIDA
University of Applied Sciences

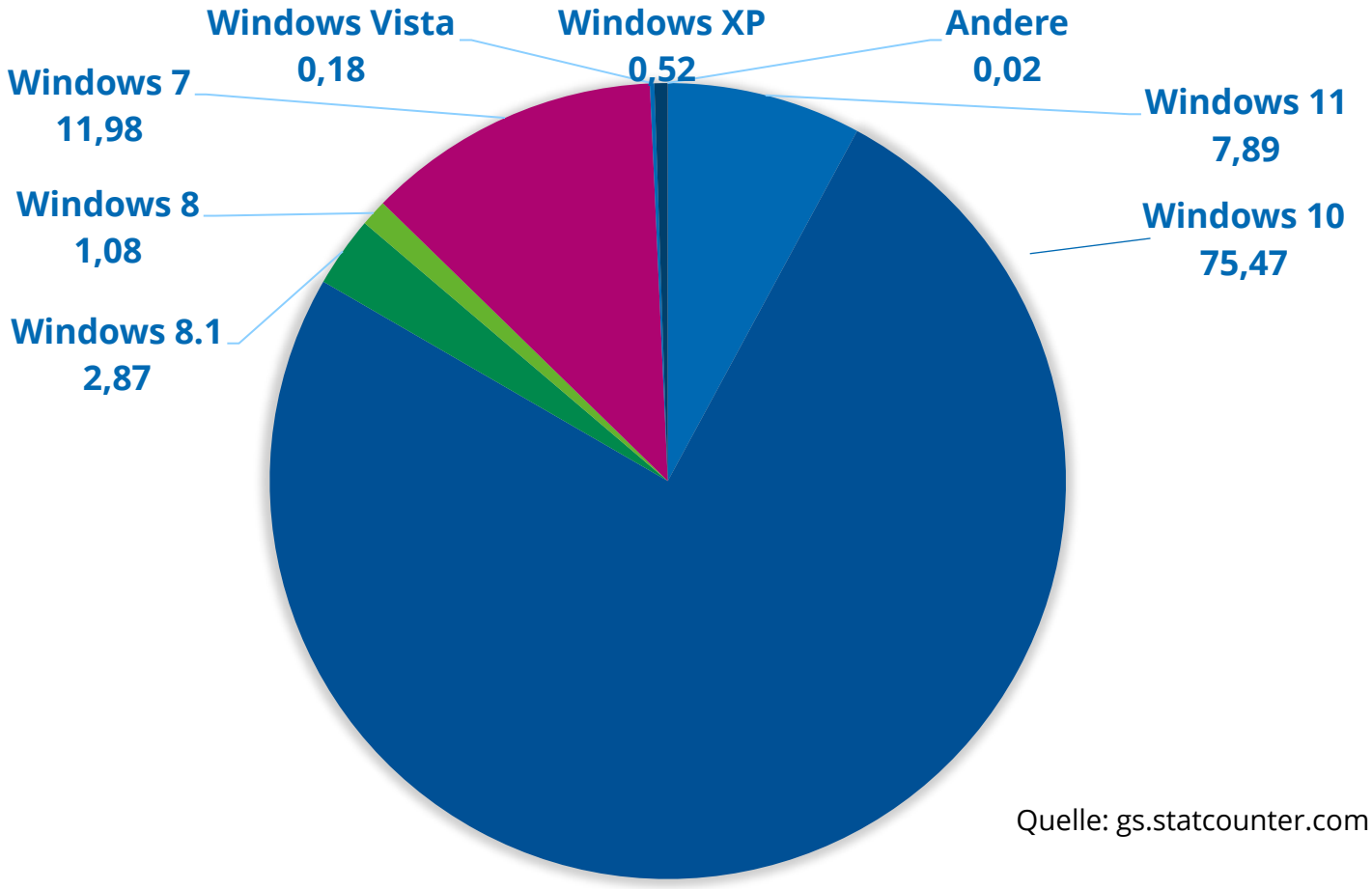
Bundeskriminalamt

Digitale Forensik
Betriebs- und Dateisysteme

Prof. Dr. rer. nat. Dirk Labudde

Windows

Aktueller Anteil der Windows Versionen Februar 2022

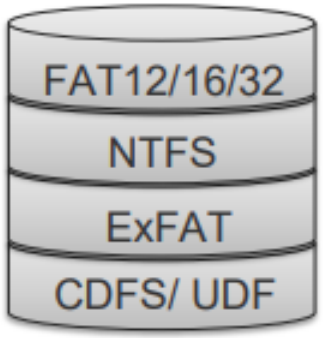


Quelle: gs.statcounter.com

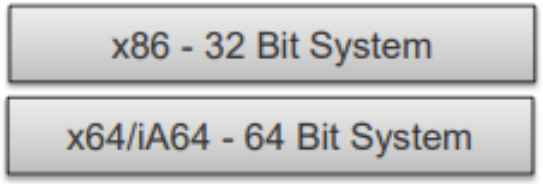
Allgemeine Informationen Windows

Allgemeine Informationen

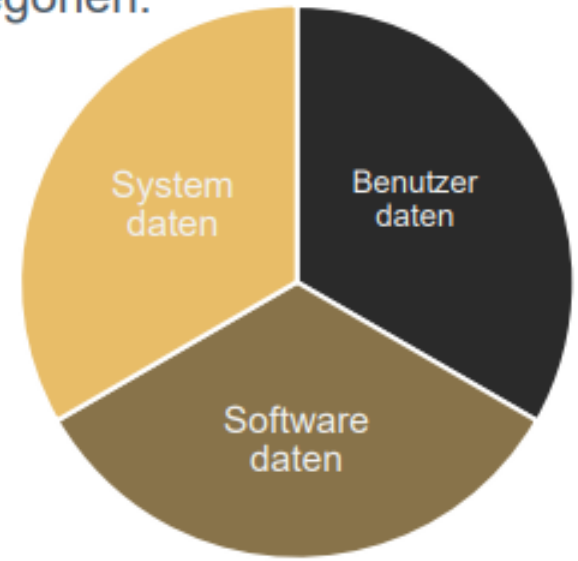
Unterstützte Dateisysteme:



Unterstützte Architekturen:



Die interne Datenaufteilung erfolgt in drei unterschiedlichen Kategorien:



Die logische Trennung dieser Daten findet sich dabei an verschiedenen Stellen im Betriebssystemaufbau wieder.

3

Wichtige Verzeichnisfade

- Systemdaten findet man im Windows Verzeichnis, je nach Betriebssystemversion als „WINDOWS“, „WIN“ oder „WINNT“ benannt.
- Softwaredateien befinden sich im Programm Verzeichnis je nach Betriebssystemversion als „Programme“ oder „Program Files“ benannt.
- Benutzerdaten befinden sich im Benutzerdaten-Verzeichnis. Für die Windows Versionen Windows 95,98 und ME im Verzeichnis „Eigene Dateien“.
  Unter Windows NT, 2000 und XP im Verzeichnis „Dokumente und Einstellungen“ und unter Windows Vista, Windows 7, 8 und 10 im Verzeichnis „Users“ in einem Benutzerverzeichnis benannt nach dem Benutzerkontonamen.

Einstellungen und Anwenderspezifische Daten zu einzelnen installierten Software-anwendungen werden in Unterverzeichnissen gespeichert.

Unter Windows NT, 2000 und XP in:

- „\Anwendungsdaten“ und „\Lokale Einstellungen\Anwendungsdaten“

Unter Windows Vista, 2003, 2008, 2012, 2013, 7, 8 und 10 in:

- „\AppData\Local“, „\AppData\LocalLow“ und „\AppData\Roaming

Besonderheiten 64 und 32 Bit Systeme

Windows (64 Bit) Besonderheiten

Seit der Einführung von 64- Bit Windows Betriebssystemen wird 32Bit und 64Bit-Software in unterschiedlichen Verzeichnissen installiert.

Dazu werden alle 32Bit-Programme auf 64Bit-Betriebssystemen in ein Programmverzeichnis mit dem Präfix „(x86)“ installiert. Auch auf Systemebene wurde eine solche Trennung vollzogen.

Im Windows Verzeichnis befindet sich auf 64Bit-Betriebssystemen das Verzeichnis

„SysWOW64“

in dem sich die 32 Bit Systemkomponenten des Betriebssystems befinden. Bei der forensischen Untersuchung sind je nach Sachverhalt daher auch diese Verzeichnisse von Bedeutung.

Historie

FAT wurde mit QDOS im Jahre 1980 eingeführt und steht für File Allocation Table.

	FAT12	FAT16	FAT32
DOS 1.x	Keine Festplattenunterstützung		
DOS 2.x	X		
DOS 3.x	X	X	
DOS 4.x-6.x	X	X	X
DOS 7.x-8x	X	X	X
DOS 8	X	X	X
Windows 95	X	X	
Windows 95B und C	X	X	X
Windows NT 3.x	X	X	X
Windows NT 4.0	X	X	X
Windows 98	X	X	X
Windows 2000	X	X	X
Windows ME	X	X	X
Windows XP	X	X	X
Windows Server 2003	X	X	X
Windows Vista	X	X	X
Windows 7/8/10/SERVER	X	X	X

MICROSOFT UNTERSTÜTZUNG für FAT
Windows 1.0x bis 3.x sind nicht aufgezählt, weil sie nur von DOS aus installiert werden können.

Benutzerverwaltung

Windows Benutzerverwaltung mittels SID:

- Die Benutzerverwaltung auf Windows Betriebssystemen wird mit Hilfe eines Security Identifier, kurz SID realisiert.
- Die SID ist geeignet um jedes System, jeden Benutzer und jede Gruppe dauerhaft zu identifizieren.
- An die SID sind die in Access Control Lists festgelegten Zugriffsrechte und Eigentümer gebunden die auf NTFS Dateisystemen die Benutzerzugriffsverwaltung realisieren.
- Werden Benutzernamen geändert oder gelöscht bleiben deren SID unverändert derjenigen Datei oder demjenigen Verzeichnis zugeordnet.

Beispiel SID

- S-1-5-21-7623811015-3361044348-030300820-1013
- Erläuterung zum Aufbau:
  - S – Kurzzeichen für SID
  - 1 – Revisionsnummer,
  - 5 – Identifier Authority
  - 21-76.....0300820 – Domäne oder lokales System,
  - 1013 – Benutzernummer
    (Gruppen von SID's - 500er System, 1000er Benutzer)

0 Null-account Authority
1 World Authority
2 Local Authority
3 Creator Authority
4 Non-unique Authority
5 NT Authority

Lokale Standartbenutzerkonten:
- Administratorkonto SID S-1-5-LokaleDomäne-500
- Gastkonto SID S-1-5-LokaleDomäne-501

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

- Die gespeicherten Daten werden in sogenannte Registrierungshives aufgeteilt und in Schlüsseln (Keys) mit Name Wert Paaren (Values) abgelegt.
- Ein Hive speichert damit einen Teilbaum der Registry. Alle Daten sind in einem Binärformat abgelegt.
- Bei Windows NT4, Windows 2000 und spätere haben die Dateien das **Windows NT Registry File (REGF) Format**. Für Windows 95, 98 und Me sind die Dateien im **Windows 9x Registry File (CREG)** Format organisiert.
- Ein Hive ist dabei nicht zwangsweise mit einem Haupt- oder Wurzelschlüssel identisch. So gibt es Wurzelschlüssel, die aus mehreren einzelnen Hives bestehen.

Registrierungsdatenbank

Speicherung von Einstellungen in der Registrierungsdatenbank:

- Die Trennung der drei Datenformen ist auch auf Ebene der Registrierung vorhanden.
- Die Datenbanken existieren in Form von Dateien im Verzeichnis:

  „[Root-Laufwerk]/[Windows Verzeichnis]/System32/Config“
- Die Registrierungsdatei für die Benutzereinstellungen befindet sich im jeweiligen Benutzerdaten Verzeichnis unter:

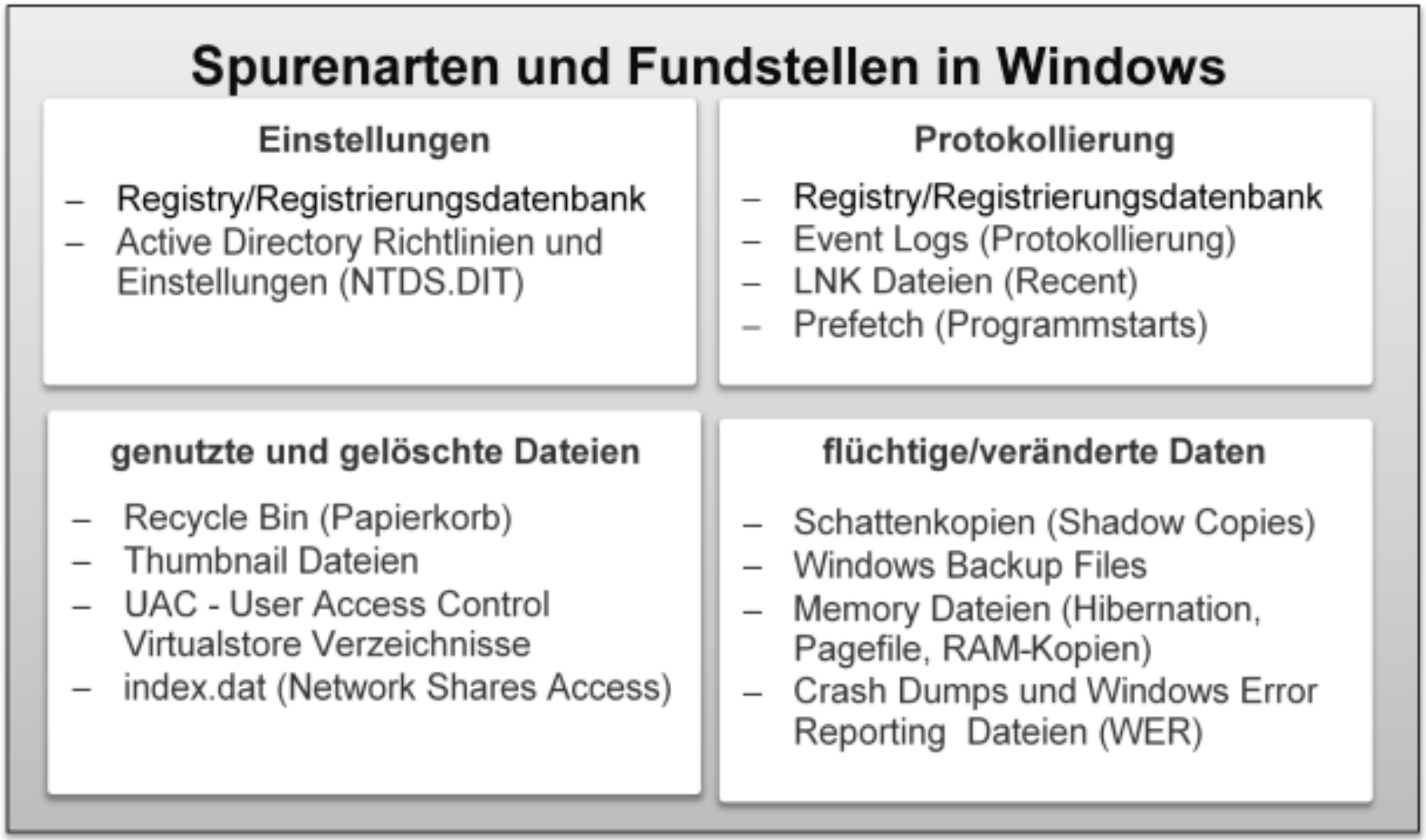
  „[Root-Laufwerk]/[Benutzerdaten Verzeichnis]/[Benutzername]/“
- Die Registrierungsdatei für die Benutzerkontenverwaltung wurde mit Windows NT eingeführt. In ihr werden die Einstellungen zu vorhandenen Benutzern des Betriebssystems gespeichert.
- Seit Windows 7 werden einige der Benutzerinformationen auch in einem weiteren Benutzerspezifischen Schlüssel gespeichert:

  „\AppData\Local\Microsoft\Windows\usrclass.dat“.

Registrierungsdatenbank

Typ	Windows 95, 98 und Höher	Windows NT, XP und höher	Korrespondierende Hauptschlüssel
Systemeinstellung	SYSTEM.DAT	SYSTEM	HEK_LOCAL_MACHINE/SYSTEM
Softwareeinstellung	SOFTWARE.DAT	SOFTWARE	HKEY_LOCAL_MACHINE/SOFTWARE
Benutzereinstellungen	USER:DAT	NTUSER.DAT USRCLASS.DAT	HKEY_CURRENT_USER/HKEY_USERS
Benutzerkonten Verwaltung		SAM	HKEY_LOCAL_MACHINE/SAM
Benutzerrechte und Richtlinien		SECURITY	HKEY_LOCAL_MACHINE/SECURITY

Spuren in Windows



McOS

Historie
Grundaufbau
Dateisystem
Wichtige Verzeichnisse
Formate
Benutzerverwaltung
Zeitstempel

Grundaufbau von OSX

OSX ist in vier Schichten aufgebaut:

1. **Benutzerebene** - Aqua, die grafische Benutzerschnittstelle (GUI)
2. **Anwendungsprogrammierebene** - Programmierschnittstellen (APIs) wie Cocoa (und früher Carbon), Java
3. **Bereitstellungsebene** - Grafik-Subsystem (Quartz mit Quartz Compositor, OpenGL), Audio/Video (QuickTime) etc.
4. **Basisebene** - Darwin, das Kern-Betriebssystem

Grundaufbau OSX

OSX ist ein Nachkomme von NeXTSTEP und genau genommen eine (proprietäre) Software-Distribution, wobei Darwin, die Basisebene von BSD abgeleitet ist, und damit ein (freies) Unix, das eigentliche Betriebssystem ist.

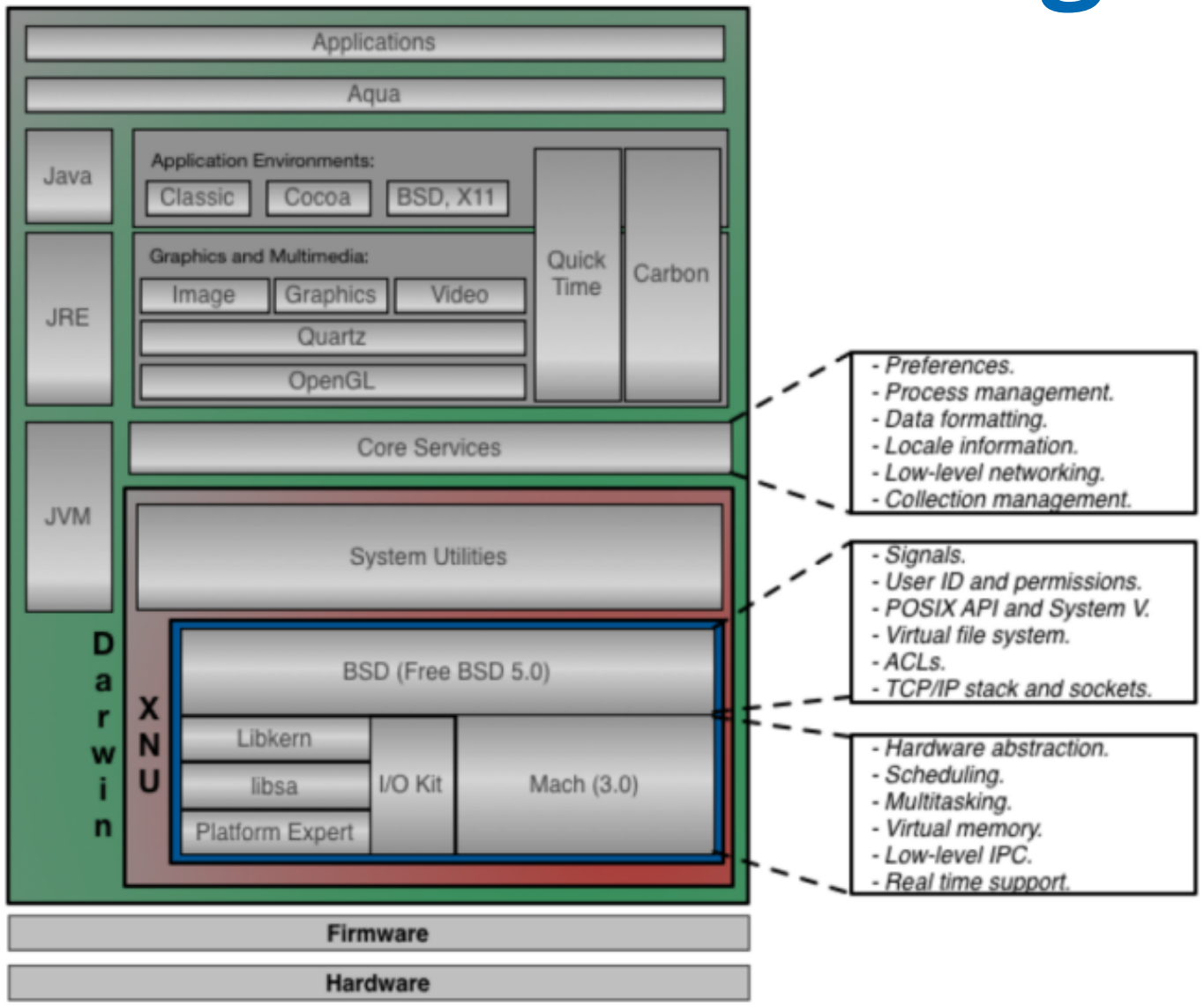
Durch Darwin (vererbt aus BSD) verfügt OS X über Fähigkeiten wie Speicherplatzschutz, präemptives Multitasking, Mehrbenutzerfähigkeit, erweitertes Speichermanagement und symmetrisches Multiprocessing (SMP). Darwin wurde unter die quelloffene Lizenz Apple Public Source License gestellt

Grundaufbau OSX

Der Kernel wurde gegenüber NeXTStep vollkommen überarbeitet - während NeXTStep noch einen reinen Mach-Mikrokernel verwendete, setzt OS X bzw. Darwin auf einen sogenannten Hybridkernel: Dabei werden einige Funktionen in den Kernel integriert, allerdings nicht so viele wie bei einem monolithischen Kernel.

Als Basis Kernel wurde weiterhin Mach verwendet und mit Teilen des monolithischen FreeBSDKernel ergänzt. Der Kernel heißt XNU (X is Not Unix).

MacOSX Grundlegender Aufbau



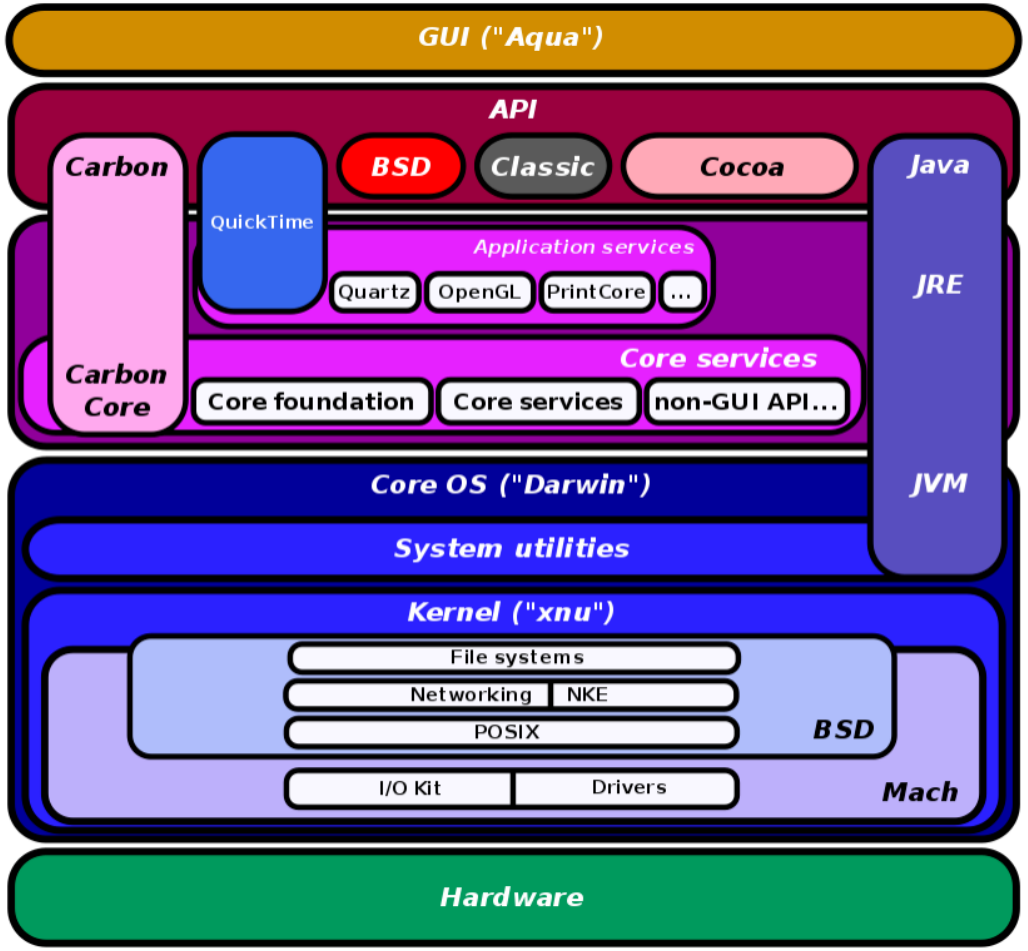


Abbildung: Grundaufbau von OSX (Bild: Joaquín Moreno Garijo)

Dateisysteme

Mac OS X nutzt das Dateisystem HFS und dessen Erweiterung HFS+. Dieses von Apple entwickelte Dateisystem wird auch für externe Datenträger verwendet und kann mit einem Windows basierten System nicht gelesen werden.

Mac OS X kann auch das FAT12/16/32 Dateisystem lesen und schreiben. Damit ist es möglich externe Datenträger, wie Speicherkarten und USB Sticks für den Multibetriebssystembetrieb einzurichten.

Seit der Einführung von macOS X 10.12 wurde das Apple Dateisystem HFS+ durch APFS (Apple File System) ersetzt.

Dateisysteme OSX

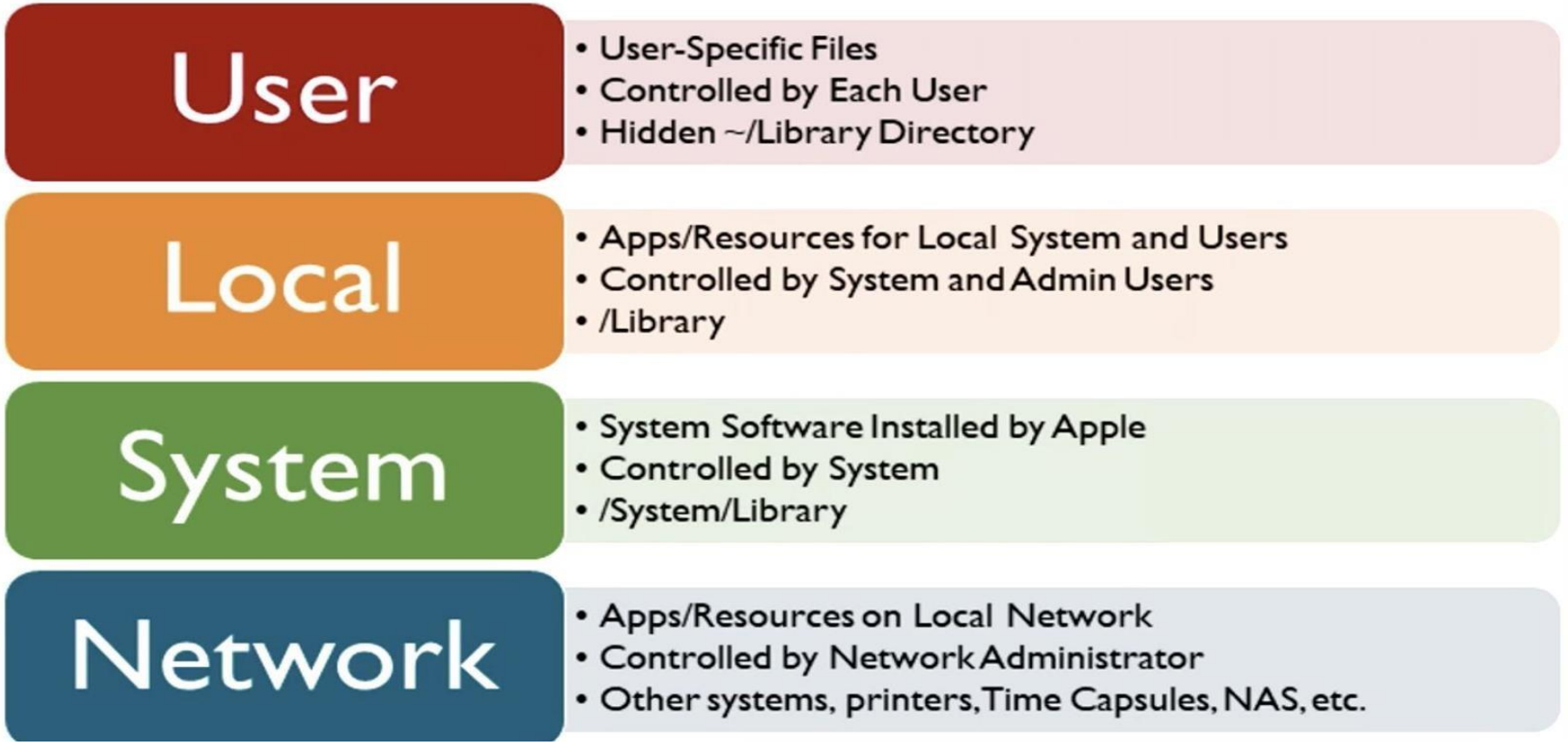
OSX unterstützt verschiedene weitere lokale Dateisysteme wie NTFS, exFAT, UFS, UDF, sowie ZFS (die beiden letztgenannten nur lesend). Der Schreibzugriff auf NTFS wurde in Mac OS X 10.6 hinzugefügt, ist standardmäßig jedoch abgeschaltet und muss durch einen Eintrag in fstab aktiviert werden.

Unterstützte Netzwerkdateisysteme sind AFP, FTP, NFS, SMB/CIFS und Web-DAV.

Mit der Zusatzsoftware ***MacFUSE*** und entsprechenden Plugins wie NTFS-3G (für Schreib/Lesezugriff auf NTFS-Datenträger bis OS X 10.6) sind weitere Dateisystemtypen unter OS X verfügbar.

Hierbei werden zusätzlich eine Menge für die Forensik relevante Dateisysteme nutzbar, wie durch das Mounten von EWF-Images und BDE- Volumes, etc.

Wichtige Verzeichnisse

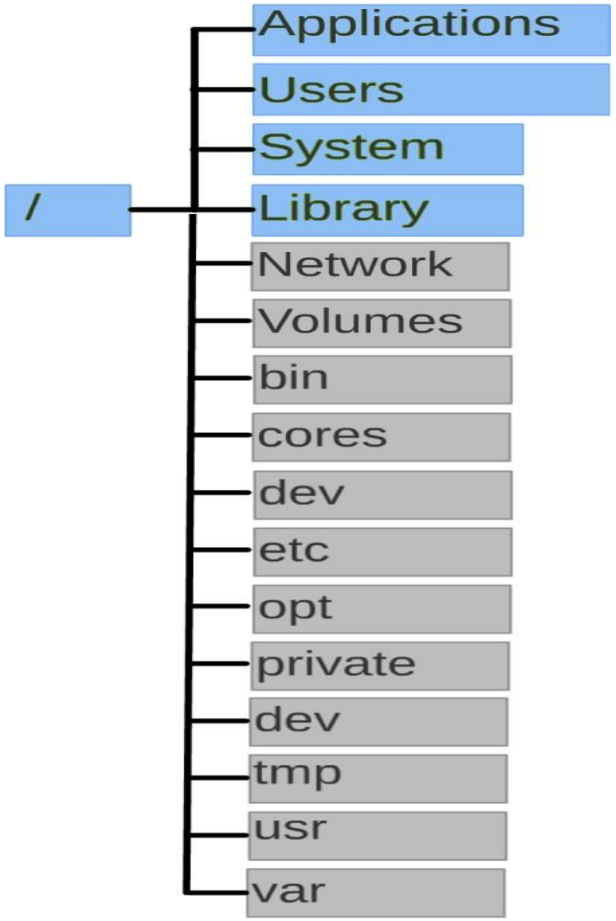


Wichtige Verzeichnisstrukturen

Die Verzeichnisstrukturen eines Mac OS X lässt den UNIX- Ursprung erkennen. Unterschiede gibt es jedoch bei den on Apple entwickelten Bestandteilen.

Apple hält sich bei seiner Verzeichnisstruktur nicht streng an den Filesystem Hierarchy Standard (FHS). Der Standard ist aber noch erkennbar.

Zudem sind viele Sytsemordner bei OSX versteckt (graue Verzeichnisse)



Wichtige Verzeichnisstrukturen

Das MAC OS X Betriebssystem teilt Daten ebenfalls in die Kategorien Systemdaten, Benutzerdaten und Softwaredaten auf.

Anwendungen befinden sich im Verzeichnis ***„Application“*** im Root Verzeichnis.

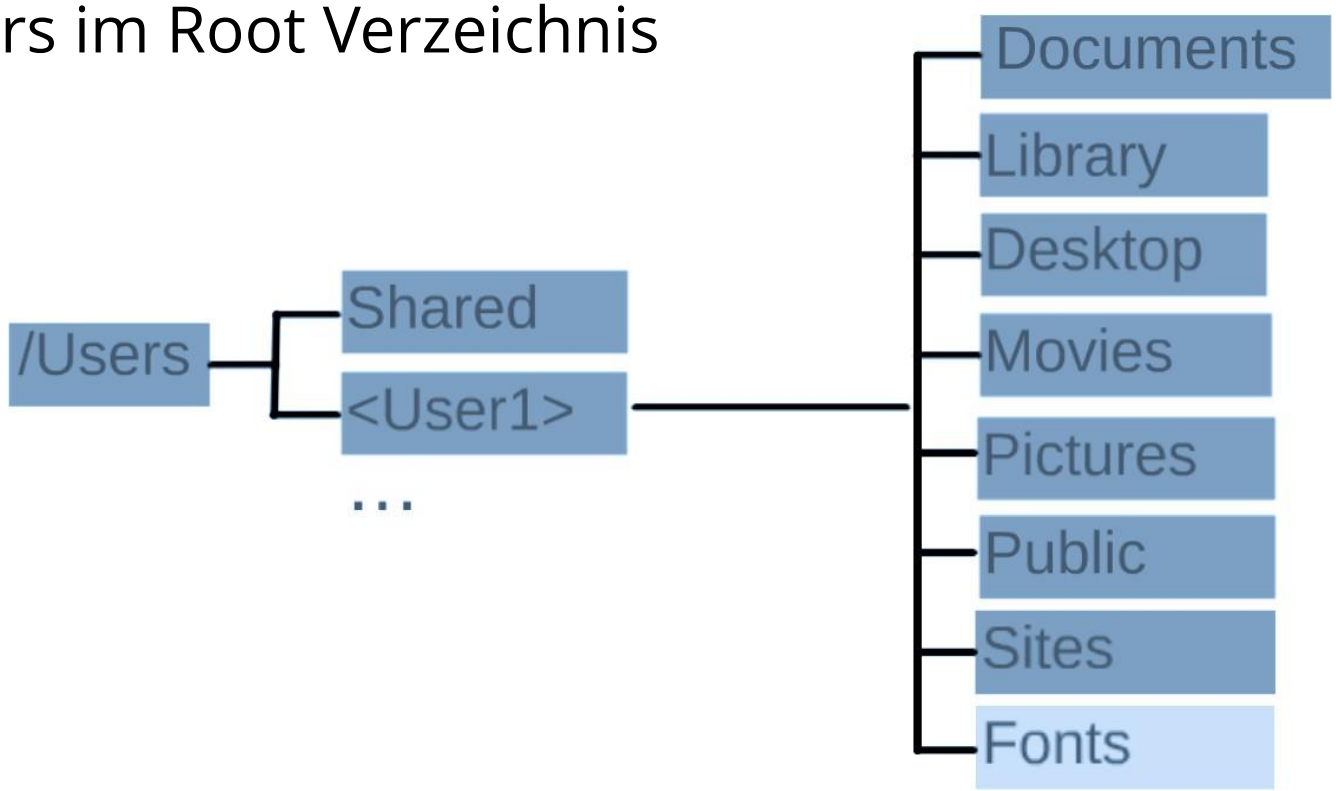
Systemdaten finden sich zum einen im Verzeichnis: ***„…/System/Library/“***

und zum Anderen im: ***„…/Library“*** Verzeichnis im Root Verzeichnis selbst.

Die für jeden Benutzer gültigen Systemeinstellungen werden im Benutzerverzeichnis ebenfalls im Unterverzeichnis ***„…/Users/[Name]/Library“*** abgelegt.

Wichtige Verzeichnisstrukturen

Benutzerdaten befinden sich im jeweiligen Unterverzeichnis des Benutzers, im Verzeichnis Users im Root Verzeichnis



Formate

OS X speichert jede Menge Informationen die für den IT-Forensiker von Interesse sein können. Diese Informationen sind in einer ganzen Reihe verschiedener Formate abgelegt.

Einige sind leicht zu interpretieren, wie Plain Text, XML oder Datenbanken. Andere haben aber proprietäre Binärformate. Einige Dateiformate sind gut dokumentiert, andere leider gar nicht und mussten Reverse Engineered werden.

Für die meisten Binärformate bringt OSX aber eigene Viewer mit. Das ist ein Grund, dass sich Apple Rechner am besten auf einem Apple auswerten lassen.

Formate

- **Basic Security Modules (BSM):** Binärdateien, die die Kernel Logs speichern. Es gibt mehrere BSM-Dateien, die jeweils mehrere Token fester oder variabler Länge enthalten. Ähnlich zu den EVT, EVTX Dateien bei Windows.
- **Binary Apple Syste Log (ASL):** Standardformat für die Daemon Logs, Binärdaten in doppelt verlinkten Listen.
- **Keychain**: Ein binäres Datenbank-Format in dem Passwörter und Zertifikate von Applikationen, Webseiten, Netzwerken und Ähnlichem abgelegt werden.
- **Plist:** OS X und die Applikationen legen ihre Konfiguration in Plist Dateien ab. Es gibt zwei Unterformate: Plists die XML enthalten Binäre Plists (BPlist)
- **SQLite:** Userapplikationen wie Chrome, Skype, Firefox, etc. aber auch einige Caches von OSX selbst werden im SQLite Datenbankformat abgelegt.

Benutzerverwaltung

Dem Ursprung von ac OSX angelehnt ist das Betriebsystem Multiuserfähig uns bietet eine entsprechende Benutzerverwaltung mit Benutzer und Gruppen an.

OSX unterscheidet zwischen:

- normalen Benutzern (user)
- Systemverwalter (admin) und dem
- Superuser (root).

Normale Benutzer können keine Änderungen am System vornehmen oder Software außerhalb ihrer Benutzerordner installieren. Alle von Usern gestartete Programme werden mit den entsprechenden Nutzerrechten des Users ausgeführt.

Benutzerverwaltung

Die Benutzer der Gruppe **Admin** verfügen über weitergehende Rechte, sie dürfen systemweite Einstellungen vornehmen, Software installieren und verfügen über Schreibzugriff auf diverse Systemverzeichnisse.

Nur nach gesonderten Authentifizierungen können tiefergreifende Änderungen am System vorgenommen werden. Ein nutzbares Root-Benutzerkonto, das dauerhaft über Berechtigungen des Superusers verfügt, gibt es nach Systeminstallation nicht. Zwar gibt es einen Benutzer „root“, dieser ist jedoch standartmäßig deaktiviert. Kann jedoch explizit aktiviert werden.

Zeitstempel

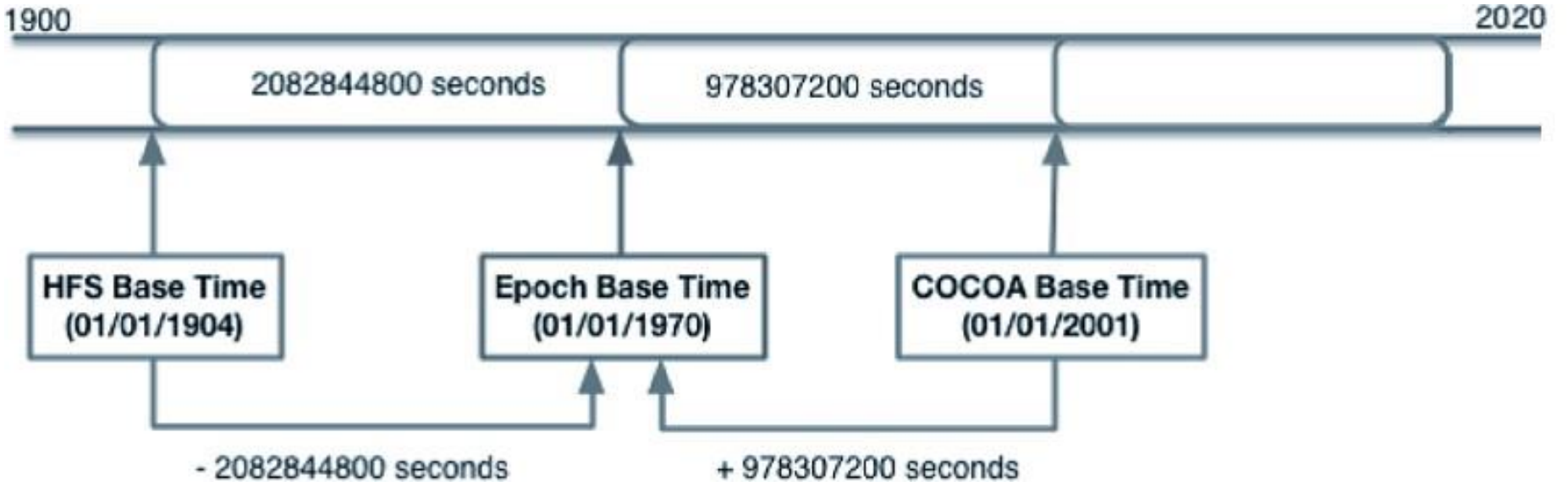
OSX verwendet drei unterschiedliche Zeitstempel:

- **HFS Time**: 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1904 zählt
- **Epoch:** 4 Byte HexWert, der die Sekunden seit dem 01. Januar 1970 zählt
- **Cocoa:** 64 Bit - Integer der die Sekunden seit dem 01. Januar 2001 zählt

Aus Dokumentation passenden Zeitstempel ermitteln.

Zeitstempel

OSX verwendet drei unterschiedliche Zeitstempel:



3 Schutzebenen

- Schutz von Inhalten und Dateisystemberechtigungen von Systemdateien und –verzeichnissen
- Schutz von Prozessen gegen Code-Injection, Laufzeitanbindung (wie Debugging) und Dtrace
- Schutz vor unsignierten Kernel-Erweiterungen ("kexts").

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

Dirk.labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de