Högskolan Dalarna 2009-03-23

Projektarbete

DT2005 – Kriminalteknisk datavetenskap II

Mac OS X forensics – En introduktion

Namn: Kevin Lund

Pers.Nr: 790213-0694

E-post: h06kevlu@du.se

Kursansvarig
Hans Jones

1 Bakgrund och historik

Redan 1984 släppte Apple sin första Macintosh och var det första systemet som innehöll ett grafiskt gränssnitt (GUI) som vanliga personer hade råd med. Ända sedan dess har Macintosh ökat i popularitet och har idag en stor skara anhängare. En del anser till och med att Macintosh anhängare har skapat någon sorts kult.

I takt med ökad popularitet bland Macintosh anhängare ökar också behovet av att utvinna information ur systemen i ett forensiskt syfte. Det finns en del Apple Macintosh datorer i hemmen och på arbetsplatser som använder sig av gamla Mac OS. I detta arbete kommer jag dock att titta närmare på Mac OS X 10.5 (Leopard). Mycket av informationen kan också tillämpas på lite äldre system som 10.3 och 10.4 men detta är inte garanterat.

2 Mac OS X en översikt

Mac OS X bygger i grunden på av Apple uppköpta NeXT och dess operativsystem NeXTSTEP. NeXTSTEP var ett objektorienterat, multitasking Unix OS som byggde på Mach kärnan tillsammans med källkod från BSD Unix. Dessa två delar utgör dagens kärna i OS X med namnet Darwin.

Alla Mac OS X versioner använder sig av det underliggande Unix systemet. Mac OS X är inte bara ett GUI-baserat operativsystem utan det är också kommando drivet genom ett terminalgränssnitt. Det här ger användarna stor flexibilitet och kraft. Större delen av användarskaran håller sig helst till det grafiska gränssnittet medan mera avancerade användare gärna använder sig av terminalen. Mycket av Linux källkod kan kompileras på en Mac utan större ändringar. Det finns ett projekt kallat för **Mac Ports**[1] som underlättar för användaren att kompilera och installera portade program.

2.1 Boot-processen

Apples, Macintosh svar på PC BIOS (Basic Input Output System) är Open Firmware (OF) och Extensible Firmware Interface (EFI). Open Firmware hittar man på Macintosh datorer med PowerPC processorer och EFI på Intelbaserade.

OF eller EFI är tekniskt sätt inte en del av OS X men det utgör en vikig del i Apple-datorernas funktion. Open Firmware är en öppen icke låst, plattformsoberoende boot-firmware som är placerad i BootROM[2]. Open Firmware kan användas för att skräddarsy boot-processen samt användas för att diagnosera, avlusa och kan även användas för programmering. EFI är väldigt likt Open Firmware. (Amit Singh, 2006)

[1] http://www.macports.org/
[2] Är i moderna Apple datorer, ett på moderkortet placerat flash EEPROM.

När man slår på strömmen till en Macintosh dator så aktiveras BootROM. BootROM har två huvudsakliga uppgifter:

1. Initialisering av hårdvara
2. Välja ett operativsystem att köra.

Först så körs en **POST** (Power-On Self Test) process som initialiserar en del hårdvara och kontrollerar att det finns tillräckligt med minne och att minnet är i bra skick. Resten av hårdvaran initialiseras i PowerPC-baserade Macintosh datorer av Open Firmware. OF bygger också ett initialt enhetsträd[3] och väljer sedan vilket OS som skall användas. I Intel-baserade Macintosh datorer så sköter EFI grundläggande initialisering och väljer sedan vilket OS som skall aktiveras.

Om det finns flera operativsystem installerade på datorn så väljer OF eller EFI det operativsystem som valdes senast i Systeminställningar (Startskiva). För att välja OS att boota eller starta ifrån så kan man hålla inne alt-tangenten vid start av datorn.

När sedan BootROM är färdig och en Mac OS X partition på hårddisken har valts så lämnas kontrollen över till BootX (PowerPC) eller boot.efi (Intel). Den huvudsakliga uppgiften som båda dessa s.k. boot-hanterare har är att ladda kärnan och dess miljö.

Man hittar både BootX och booti.efi under:

```
/System/Library/CoreServices
```

Man kan också hitta en kopia av boot.efi under:

```
/usr/standalone/i386/boot.efi
```

Vid tillfällen då man t.ex. bootar från en UFS volym, en RAID volym etc. så kommer en kopia av boot-hanteraren att finnas på en separat HFS+ ”hjälp” volym för att hjälpa systemet att starta. I vissa versioner av Mac OS X så kan man hitta en kopia av kärnan samt mkext[4] cache på hjälpvolymen. I situationer som dessa så kommer inte boot-hanteraren och andra komponenter på root enheten att användas.

Boot-hanteraren försöker först ladda in en för-länkad version av kärnan som innehåller alla enhetsdrivrutiner som är inblandade i själva Boot-processen. Denna för-länkade kärna kan man hitta på följande plats:

```
/System/Library/Caches/com.apple.kernelcaches
```

[3] En hierarkisk representation av enheter som är associerad med datorn.
[4] Är ett komprimerat arkiv som sparar information om en eller flera KEXT (Kernel Extensions) som i sin tur används av boot-hanteraren.

Genom att i förväg länka dessa drivrutiner in i kärnan så minskas boot-tiden. Om det skulle vara så att denna cache skulle saknas, är föråldrad eller korrupt så kommer boot-hanteraren att försöka ladda in samma drivrutiner, alla på en gång i form av ett enkelt, komprimerat arkiv som kallas för mkext cache.

Skulle det visa sig att också denna cache på något sätt vara korrupt, saknas eller föråldrad så kommer boot-hanteraren att leta efter drivrutiner och Kernel Extensions under:

```
/System/Library/Extensions
```

När nu alla drivrutiner som krävs för att boota är inladdade kommer boot-hanteraren att starta initialiseringen av kärnan. Kärnan initialiserar Mach och BSD strukturerna och initialiserar sedan I/O. I/O kitet länkar de inladdade drivrutinerna in i kärnan. När kärnan hittar root-enheten så kommer BSD att ”rootas” utifrån denna enhet. Härefter så tar root systemprocessen **launchd** över och initialiserar loginfönstret.

2.1.1 rEFIt

Apple erbjuder inga verktyg för att få tillgång till EFI. Efter Boot så kommer man inte åt EFI. Det finns dock verktyg för att få tillgång till EFI. Ett av dessa verktyg är rEFIt som kan hittas på Sourceforge.net:

```
http://refit.sourceforge.net/
```

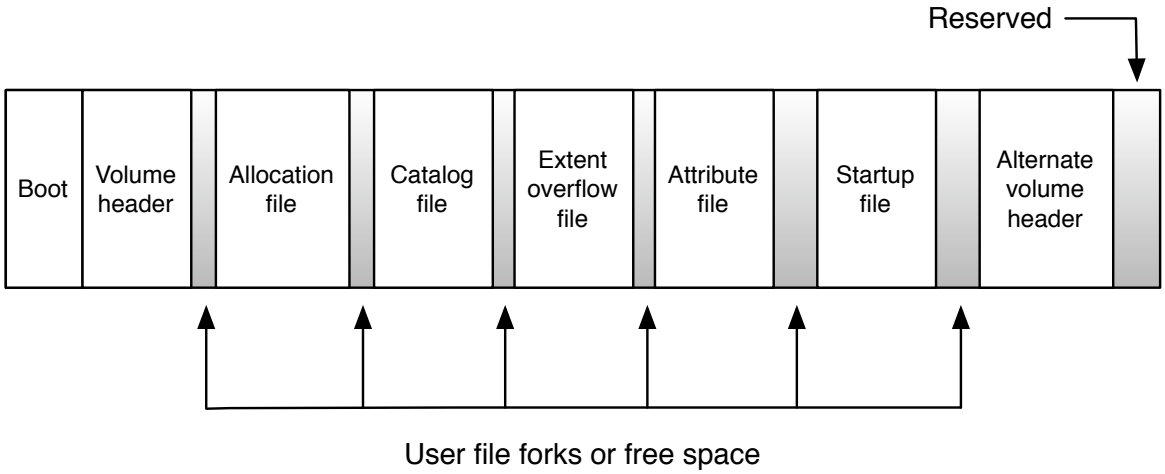
Detta verktyg måste installeras och är inte det lämpligaste verktyget att köra under en Live undersökning. Man kan dock boota med en bootbar disk med detta verktyg installerat och samla in önskad information. Den information man kan få ut rör sig om datum, tid och låg-nivå information. Dokumentation för EFI är inte den bästa så andra medel kanske lämpar sig bättre för att hitta ovanstående information.

Ett användningsområde för detta verktyg är som en boot-meny i de fall man har flera operativsystem installerade på enheten.

2.2 HFS+ och dess datastrukturer

Filsystemet HFS+ (Hierarchical File System Plus) och det äldre HFS är de två dominerande filsystem som man hittar på en Macintosh dator. HFS+ även kallad HFS extended eller Mac OS extended introducerades i samband med att Mac OS 8.1 lanserades i 1998. HFS+ är efterföljaren till det gamla HFS och ger stöd för större filer (blockadresserna är 32-bit istället för 16-bit). HFS+ stöder filnamn upp till 255 tecken UTF-16.

En HFS+ volym är indelad i sektorer som normalt är 512bytes stora. Dessa sektorer är sedan grupperade i allokeringsblock som kan innehålla en eller flera sektorer. Normal storlek på ett allokeringsblock är 4KB. Hur många allokeringsblock som finns på en HFS+ volym bestäms av volymstorleken.



Figur 2.1 Strukturen i en HFS+ volm.

Det finns total nio stycken olika strukturer som bygger upp en HFS+ volym:

1. Sektorerna 0 och 1 är **Bootblocken** som innehåller information och instruktioner som är nödvändiga för att starta upp, boota systemet.
2. Sektor 2 består av **Volume Header** eller **Volymsidhuvudet** och innehåller information om hela volymen. Informationen är t.ex. storleken på allokeringsblocken, datum och tid när volymen skapades och placeringen av andra volymstrukturer som t.ex. Katalogfilen och Extent Overflow File. Volymsidhuvudet finns alltid på samma plats.
3. **Allokeringsfilen** håller reda på vilka allokeringsblock som är lediga respektive upptagna. Varje allokeringsblock består av en bit. En etta indikerar ett upptaget allokeringsblock och en nolla ett ledigt. Platsen på denna struktur kan variera.
4. **Katalogfilen** är ett B*-träd som innehåller register över alla filer och mappar som finns lagrade på volymen. Ett register i Mac OS X har storleken 8 KiB.
5. **Extent Overflow File** är ett annat B*-träd som sparar information om de allokeringsblock som är allokerade till varje fil.
6. **Attributfilen** är ytterligare ett B*-träd. Attributfilen kan spara tre olika typer av 4KiB register: *Inline Data Attribute records*, *Fork Data Attribute records* och *Extension Attribute records*. Inline Data Attribute register sparar små attribut som får plats inuti registret i sig. Fork Data Attribute registren innehåller referenser till maximalt åtta stycken s.k.

extents som kan innehålla större attribut. Extension Attribute registren används för att bygga ut Fork Data Attribute när de åtta olika s.k. extents redan är använda.

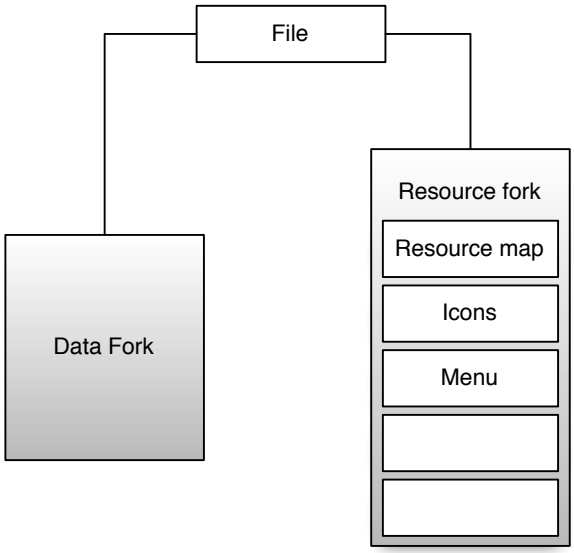
7. **Uppstartsfilen**, är avsedd för icke-Mac OS system som inte har stöd för HFS eller HFS+.
8. Den näst sista strukturen, det **alternativa volymhuvudet** motsvarar Alternate Master Directory Block i en HFS volym.
9. Den sista strukturen är **reserverad för Apple**. Den används under processen då datorn tillverkas.

En fil på ett HFS sysstem har två s.k. gafflar:

1. Data fork
2. Resource fork

En eller båda dessa gafflar kan vara tomma. Data gaffeln innehåller information precis som en vanlig fil innehåller i Linux eller Windows.

Resursgaffeln innehåller däremot Macintosh resurser, data i ett speciellt format som beskriver t.ex. menyer, dialogrutor, ikoner etc. som är associerad med filen. Fördelen med att använda en resursgaffel är att det möjliggör egenskaper som menyer och dialoger på olika språk. Ett exempel på en Mac OS X fil är en vanlig Word-fil där själva texten ligger i datagaffeln och eventuella bilder ligger sparade i resursgaffeln. Resursgaffeln kan bäst jämföras med Alternate Data Streams i NTFS.



Figur 2.2 En OS X fil har två gafflar

Viktigt!

Om en macintoshfil kopieras över till ett filssystem som inte stöder resursgafflar så kommer resursgaffeln att försvinna.

Om man kopierar en macintoshfil till en NTFS volym så kommer resurgaffeln att försvinna.

```
C:\macfiles>dir /a
 Volymen i enhet C har ingen etikett.
 Volymens serienummer är 8C4B-ABD8

 Innehåll i katalogen C:\macfiles

2009-03-18  17:07    <KAT>          .
2009-03-18  17:07    <KAT>          ..
2009-03-18  17:05                31 losen.txt
               1 fil(er)                 31 byte
               2 katalog(er)  38 224 609 280 byte ledigt
```

Ovan har en textfil skriven i Mac OS X med en enkel textredigerare överförts till en NTFS volym. En listning visar bara text filen.

```
E:\macfiles>dir /a
 Volymen i enhet E har etiketten USBMINNE
 Volymens serienummer är 3848-8EC9

 Innehåll i katalogen E:\macfiles

2009-03-18  17:17    <KAT>          .
2009-03-18  17:17    <KAT>          ..
2009-03-18  17:05                31 losen.txt
2009-03-18  17:17             4 096 ._losen.txt
               2 fil(er)              4 127 byte
               2 katalog(er)      65 179 648 byte ledigt
```

Samma fil kopierades över till en FAT32 volym. Här syns en fil med namnet `._losen.txt`. Detta är resursgaffeln. Förs filen över till Mac OS X igen så kommer Mac OS X att hantera resursgaffeln och öppna filen på korrekt sätt.

Apple Macintosh datorer använder sig normalt av två partitionsscheman:

1. **Apple Partition Map** (PowerPC)
2. **GUID Partition Table** (Intel)

Partitionsscheman skall inte förväxlas med filsystemet HFS eller HFS+. Ett partitionsschema är beskrivningen om hur en hårddisk eller annan media är beskrivet, lagt ut på disken för att ett filssystem skall kunna appliceras.

För att undersöka strukturen på disken kan man t.ex. använda det inbyggda verktyget **hdiutil**:

```
Last login: Wed Mar 18 14:00:12 on ttys000
kevin@[~]$ ls /dev/disk*
/dev/disk0     /dev/disk0s1   /dev/disk0s2
kevin@[~]$ sudo hdiutil partition /dev/disk0
Password:
scheme:     GUID
block size: 512
_ ## Type_________________ Name_________________ Start___ Size____
+    MBR                  Protective Master Boo        0        1
+    Primary GPT Header   GPT Header                   1        1
+    Primary GPT Table    GPT Partition Data           2       32
+    Apple_Free                                       34        6
   1 C12A7328-F81F-11D2-BA EFI system partition       40   409600
   2 Apple_HFS             Customer                409640 487725344
+    Apple_Free                                  488134984   262151
+    Backup GPT Table     GPT Partition Data     488397135       32
+    Backup GPT Header    GPT Header             488397167        1

+ synthesized
kevin@[~]$ sudo hdiutil partition /dev/disk0s1
scheme:     none
block size: 512
_ ## Type_________________ Name_________________ Start___ Size____
```

```
+    DOS_FAT_32            hel skiva                   0   409600

+ synthesized
kevin@[~]$ sudo hdiutil partition /dev/disk0s2
scheme:     none
block size: 512
_ ## Type_________________ Name_________________ Start___ Size____
+    Apple_HFS             hel skiva                   0 487725344

+ synthesized
kevin@[~]$
```

Verktyget visar att enheten använder sig av ett GUID partitionsschema med blockstorlek 512 Bytes och innehåller ett flertal partitoner. Sektor 0 är boot sektorn med en storlek på 1 sektor. Sektor 1 är den primära GUID partitionstabellhuvudet och sektor 2 t.o.m. 32 är GUID partition data som beskriver utseendet på disken. Dessa två partitioner finns som kopior i slutet av enheten. Partitioner med Apple free används som utfyllnad och kan vara en plats att gömma information. Den partition som är mest intressant är Apple_HFS customer. En vidare undersökning av denna partition kan göras med verktyget **diskutil**:

```
kevin@[~]$ diskutil info /dev/disk0s2
   Device Identifier:        disk0s2
   Device Node:              /dev/disk0s2
   Part Of Whole:            disk0
   Device / Media Name:      Customer

   Volume Name:              Macintosh HD
   Mount Point:              /
   File System:              Journaled HFS+
                             Journal size 24576 KB at offset 0x10302000
   Owners:                   Enabled

   Partition Type:           Apple_HFS
   Bootable:                 Is bootable
   Media Type:               Generic
   Protocol:                 SATA
   SMART Status:             Verified
   Volume UUID:              DA337BE8-BE0D-30BF-A273-38A1DC9C3226

   Total Size:               232.6 Gi (249715376128 B) (487725344 512-byte blocks)
   Free Space:               137.2 Gi (147269672960 B) (287636080 512-byte blocks)

   Read Only:                No
   Ejectable:                No
   Whole:                    No
   Internal:                 Yes
```

Med journalföring menas ett sätt att genom ett register, logg hålla en journal över ändringar före skrivning på disken. Fördelen med detta är om datorn skulle stoppa p.g.a. strömavbrott eller av annan orsak så kommer journalen att användas för att återställa disken till ett känt fungerande tillstånd.

Viktigt!

Tänk på att om du bryter strömmen till datorn under en forensisk undersökning och senare väljer att boota en forensisk tagen kopia av enheten att journalen kan komma att användas för att återställa information. Detta skulle kunna ge inkorrekt information.

Den enda unika karakteristiken med Apples partitionsschema är att det finns många oanvända områden som kan användas för att gömma information. Data kan också gömmas i sektorer mellan olika strukturer i HFS+ volymen. Givetvis kan information finnas i filers slackutrymme precis som med andra partitionsscheman. Följaktligen så sker en forensisk undersökning av en HFS+ volym på samma sätt som med andra filsystem. Verktyg som följer med t.ex. Sleuth-kit t.ex. **mmls** och vanliga hex-editorer samt andra forensiska verktyg som känner till filsystemet kan användas.

2.3 Andra filsystem

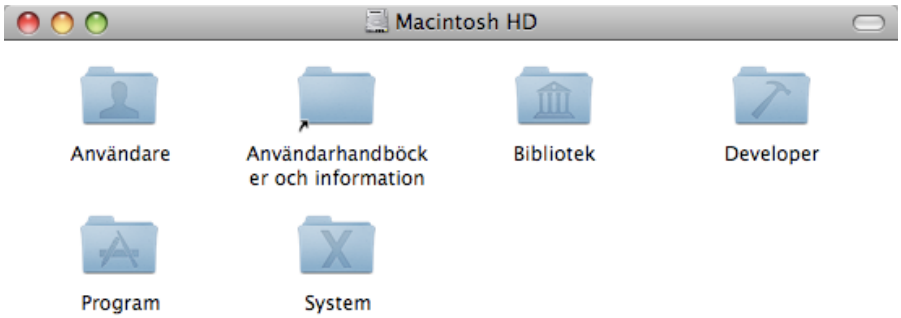
Den 6 juni 2005 meddelade Steve Jobs, VD för Apple att de skulle övergå från att använda PowerPC processorer i sina datorer till att använda processorer från Intel. Användningen av Intel-processorer tillsammans med verktyget BootCamp[5] gör det möjligt att köra andra operativsystem utan virtualisering. Därför är det inte ovanligt i dag att det finns andra partitioner som t.ex. FAT32, NTFS, efs på en modern Mac. Detta är viktigt att tänka på innan man börjar med en forensisk undersökning och förvärv av hårddisk.

2.4 Mac OS X katalogstruktur

För den vanliga användaren så är mycket av den underliggande katalogstrukturen i systemet som standard gömt. Man presenteras för att grafiskt gränssnitt för att kommunicera med underliggande tjänster. Apple har gjort det så för att användare som inte har så mycket kunskap inte skall ställa till med problem. För att se den underliggande katalogstrukturen så kan man använda sig av terminalen.

Tittar man i roten av systemet genom det grafiska gränssnittet så kommer man t.ex. presenteras av följande:

[5] Hjälpmedel, partitioneringsverktyg för att installera andra OS på en Mac. Ingår i Leopard 10.5



Figur 2.3 Synlig katalogstruktur

Listar man root i terminalen ser man följande:

```
kevin@[/]$ ls -1a
.
..
.DS_Store
.Spotlight-V100
.Trashes
.bashrc
.com.apple.timemachine.supported
.fseventsd
.hotfiles.btree
.vol
Användarhandböcker och information
Applications
Desktop DB
Desktop DF
Developer
Library
Network
System
Users
Volumes
bin
cores
dev
etc
home
mach_kernel
mach_kernel.ctfsys
net
private
sbin
tmp
usr
var
```

Som synes så får man tillträde till fler kataloger genom att använda sig av terminalen. Nedan följer en kort beskrivning av vanliga Mac OS X kataloger, dess innehåll och funktion.

Katalog	Beskrivning
/	Root katalogen, förälder till alla andra underliggande kataloger.
/Applications	Är ganska självbeskrivande. Innehåller datorns program.
/Developer	Visar sig när man installerat Apple Developer Tools och innehåller utvecklingsverktyg, dokumentation och filer.
/Library	Delade biblioteksfiler, filer nödvändiga för operativsystemets funtion. Innehåller inställningar för globala program och system.
/Network	Nätverksrelaterade drivrutiner, servrar och bibliotek.
/System	Systemrelaterade filer, bibliotek etc. Kritisk för Mac OS X funktionalitet.
/Users	Alla användarkonton och deras unika filer, inställningar etc. Påminner om /home i Linux.
/Volumes	Monterade enheter och volymer som t.ex. CD, DVD, HDD, DMG, ISO etc.
/bin	Nödvändiga vanliga bibliotek, innehåller program och filer som behövs för att starta systemet och för att systemet skall fungera rätt.
/etc	Maskinens lokala systemkonfiguration, innehåller administrativa konfigurationsinställningar och andra systemfiler.
/dev	Enhetsfiler, alla filer som representerar hårdvara i eller kopplat till datorn.
/usr	Innehåller underkataloger med information, konfigurationsfiler och andra nödvändigheter som används av operativsystemet.
/sbin	Innehåller nödvändiga systembinärer och verktyg för systemadministration.
/tmp	Innehåller temporära filer, cachar etc.
/var	Innehåller föränderlig data. Filer som förändras under tiden systemet körs. Man hittar t.ex. logg filer för systemet under /var/log.

Tabell 1: Mac OS X katalogstruktur och beskrivning

2.5 Användarnas hemmakatalog

En användare hemmakatalog tillsammans med systemloggar och inställningsfiler är troligen det som ger den mest värdefulla information under en utredning.

En användares hemmakatalog innehåller standardkataloger och kataloger specifika till t.ex. ett installerat program. Hemmakatalogen innehåller t.ex. följande kataloger:

- **Desktop**, innehåller alla filer, genvägar etc. som ligger på användarens skrivbord.
- **Documents**, innehåller programspecifika dokument. Dokument från t.ex. Word, Pages, Keynote, Excel spara som standard under denna katalog.
- **Library**, under denna katalog hittar man mycket information. Innehåller loggar, inställningar, webbläsarhistorik, senaste filer etc. En närmare beskrivning följer senare i arbetet.
- **Movies**, innehåller typiskt iDVD filmdata, Quicktime-filmer och andra digitala video material.
- **Music**, innehåller typiskt användarens iTunes musikbibliotek, men även andra musiks relaterade filtyper som t.ex. MP3-filer.
- **Pictures**, innehåller som namnet antyder bilder. iPhoto biblioteket brukar normalt sett sparas i denna katalog.
- **Public**, är en standardkatalog där användare kan lägga till och läsa filer. Användarna kan som standard inte rader filer i denna katalog. Om man inte är ägaren förstås. Används mest i utdelningssyfte i nätverk. Jmf. Mina delade dokument i Windows miljön.
- **Sites**, om man har aktiverat den inbyggda WWW, apache servern så hittar man användares webbsida under denna katalog.

2.5.1 Användarbiblioteket

Användarbiblioteket kommer att innehålla mängder med information som t.ex. användarspecifika drivrutiner, typsnitt, inställningar och systemtillägg. Information som är vikigt för en forensisk utredning som t.ex. webbläsarhistorik, e-post filer, e-postbilagor etc.

Några vanliga kataloger och dess innehåll är:

- **Application Support** – Här hittar man kataloger och filer som härstammar från programinstallationer. Om en användare raderar ett program från sin dator så kommer kataloger och information ligga kvar här om man inte använder speciella s.k. avinstallationsprogram. Ett typiskt gratis sådant program är AppCleaner[6]. Mycket information som kan ha stor vikt i en utredning kan finnas i denna katalog.
- **Automator** – Användarspecifika händelseskript. Dessa skript kan innehålla information om t.ex. automatiserade filkopieringar, serveranslutningar etc.
- **Caches** – Här kan man hitta mycket historisk information. Innehållet i denna katalog är bl.a. information om användning av program, besökta webbplatser, ev. IM kompislistor,

[6] http://www.freemacsoft.net/AppCleaner/

nedladdade filer etc. Den här katalogen bör undersöka noggrant. Program som är borttagna från datorn kan lämna kvar information i denna katalog.

- **Cookies** – Används främst av webbläsare som den inbyggda Safari. Innehåller högst troligtvis en fil med namnet **Cookies.plist**. Mer om s.k. **plist** filer följer senare i arbetet.
- **Favorites** – Innehåller information om favoriter för funktionen ”Anslut till server” i Finder.
- **Logs** - Innehåller loggfiler och information om användning tillhörande ett flertal program.
- **Mail och Mail Downloads** – Innehåller e-postmapper, filer, kontoinformation, regler, signaturer etc. för programmet Mail. Standard e-postklient under Mac OS X.
- **Phones** – Innehåller information om telefoner som har varit anslutna till denne användares konto och dator. Specifik information om telefoner kan hittas under filen Indo.plist (IMEI, Modellnamn etc.)
- **Recent Servers** – Här hittar man information om serveranslutningar som gjorts nyligen. (AFP, FTP, SMB etc.)
- **Safari** – Innehåller information om standardwebbläsaren Safari. Innehåll som t.ex. bokmärken, historik och nedladdningshistorik finns här.

Det finns förutom de ovan nämnda ett flertal andra kataloger med information. Det är viktigt att under en utredning titta igenom användarens och systemets bibliotekskatalog. Väldigt mycket intressant information kan hittas i dessa platser.

2.6 Program och teknologier

Mac OS X har ett flertal robusta tjänster som ligger bakom det grafiska gränssnittet. Automatisering av uppgifter är lätt genom bl.a. shell, Applescript och genom programmet Automator. Automator[7] är ett peka-och-klicka program som gör det enkelt att automatisera uppgifter. Med Mac OS X så medföljer bl.a. perl, pyhton, php, apache http server m.fl. Nedan beskrivs några vanliga program och tjänster i Mac och dess användningsområde.

Viktigt!

Ett program i Mac OS X har filändelsen ”.app”. Programmen är s.k. paket som egentligen bara är en mapp. Flyttas programfilen över till t.e.x. Windows så kommer man se hela mappstrukturen. Detta kan också göras under Mac genom att högerklicka (ctrl-klicka) och sedan välja ”Visa paketets innehåll”. Information kan t.ex. vara gömt i ett programpaket.

2.6.1 Bonjour (Rendezvous)

är en teknologi som utvecklats av Apple och är ett s.k. noll-konfigurations nätverk. Gör det möjligt att automatiskt upptäcka andra datorer och enheter i ett nätverk . Bonjour är installerad som standard i OS X 10.3 och senare.

[7] http://en.wikipedia.org/wiki/Automator_(software)

2.6.2 FileVault

Med FileVault så säkrar användaren sin hemmamapp genom kryptering. Krypteringen består av 128bitars AES och sker automatiskt i bakgrunden. Till skillnad mot Windows Vistas Bitlocker så är det endast användarens hemmamapp som krypteras i Mac OS X. FileVault är inte påslaget som standard men användaren kan aktivera tjänsten genom Systeminställningar → Säkerhet → FileVault.

Om FileVault är aktiverat så kommer hela hemmamappen att läggas in i en krypterad sparseimage fil med namet: *användarnamn*.spareimage i användarens hemmakatalog. En sparseimage fil är en vanlig DMG-fil där storleken är dynamisk (växer vid behov). En DMG-fil är Mac OS X skivavbildsformat.

För att komma åt en annan användares krypterade hemmamapp så måste man ha administrationsrättigheter och för att komma åt innehållet i hemmamappen så måste man ha användarens lösenord eller huvudlösenordet om ett sådant är aktiverad i Mac OS X säkerhetsinställningar.

För att kopiera en användares krypterade hemmamapp så kan man göra följande:

1. Öppna ett shell i terminalen med root rättigheter: `sudo sh`
2. Kopiera filen till önskad mapp: `cp /Users/kevin/kevin.sparseimage /Bevis-001`
3. Ta ägarskap av filen: `chown användarnamn /Bevis-001/kevin.sparseimage`
4. Lås filen så att inga ändringar kan göras: `chflags uchg /Bevis-001/kevin.sparseimage`

Studerar man den krypterade filen så kommer man inte se annat än rabarbersoppa. Dock kan det vara värt att nämna att en krypterad hemmamapp har följande signatur i filhuvudet: **encrcdsa**

Filen kan sedan monteras i Mac OS X genom att dubbelklicka på filen. Vid lyckad montering så kommer man presenterad för en dialogruta med förfrågan om användarens lösenord till hemmamappen.

Det finns ett program med namnet **vfcrack**[8] som kan vara till hjälp för att knäcka FileVault.

2.6.3 Spotlight

Spotlight är indexeringsmotorn och söktjänsten i Mac OS X som används för att hålla reda på filer och dess metadata. En dold fil med namnet `.spotlight-V100` skapas i roten och innehåller indexeringsdata. Spotlight är som aktiverad som standard och indexerar som standard följande platser:

- Alla hemmakataloger
- Documents, Movies, Music and Pictures katalogerna
- Papperskorgen för alla monterade volymer och användare

[8] http://openciphers.sourceforge.net/oc/vfcrack.php

- ~/Library/Metadata/
- ~/Library/Caches/Metadata/
- ~/Library/Mail/
- ~/Library/Caches/com.apple.AddressBook/Metadata/
- ~/Library/PreferencePanes/
- /Library/PreferencePanes/
- /System/Library/PreferencePanes/
- /Applications

Användarna kan också manuellt lägga till platser som de tycker skall indexeras för snabb sökning, åtkomst. Spotlight kommer också automatisk att indexera extern lagringsmedia (USB, FireWire) när dessa kopplas in i systemet.

Viktigt!

Om datorn innehåller flera användarkonton så kommer alla filer som ligger överst i användarens hemmakatalog (Överst i katalogstrukturen) också att indexeras. Dessa filer kan man söka på men de kan inte ändras. Filer som finns inom Desktop, Documents, Library, Music, Movies och Pictures kommer inte att indexeras eller kunna sökas på från en annan användares konto.

Två användbara terminalverktyg för arbeta med Spotlight index är:

- **mdfind**, ett terminalverktyg för att hitta filer genom spotlightindex.
- **mdls**, visar metadata för en given fil

Som exempel på användning så provar jag i terminalen att söka detta dokument:

```
kevin@[~]$ mdfind DT2005_MacOSX
/Users/kevin/Documents/Microsoft användardata/Office 2008 AutoRecovery/AutoRecovery save of
DT2005_MacOSX_forensics_Kevin_Lund.docx
/Users/kevin/Documents/Utbildning/Högskolan Dalarna/DT2005 - Kriminalteknisk datavetenskap
II/Projekt/DT2005_MacOSX_forensics_Kevin_Lund.docx
```

```
kevin@[~]$ mdls ~/Documents/Utbildning/Högskolan\ Dalarna/DT2005\ -\ Kriminalteknisk\
datavetenskap\ II/Projekt/DT2005_MacOSX_forensics_Kevin_Lund.docx
kMDItemAuthors                = (
    "Kevin Lund"
)
kMDItemComment                = "Rapport för tentamensprojekt i DT1012-Nätverkssäkerhet"
kMDItemContentCreationDate    = 2009-03-17 14:11:22 +0100
kMDItemContentModificationDate = 2009-03-22 17:50:44 +0100
kMDItemContentType            = "org.openxmlformats.wordprocessingml.document"
kMDItemContentTypeTree        = (
    "org.openxmlformats.wordprocessingml.document",
    "org.openxmlformats.openxml",
    "public.zip-archive",
    "com.pkware.zip-archive",
    "public.data",
    "public.item",
    "com.apple.bom-archive",
    "public.archive",
    "public.composite-content",
```

```
    "public.content"
)
kMDItemDisplayName              = "DT2005_MacOSX_forensics_Kevin_Lund.docx"
kMDItemEditors                  = (
    "Kevin Lund"
)
kMDItemFSContentChangeDate      = 2009-03-22 17:50:44 +0100
kMDItemFSCreationDate           = 2009-03-17 14:11:22 +0100
kMDItemFSCreatorCode            = "MSWD"
kMDItemFSFinderFlags            = 0
kMDItemFSHasCustomIcon          = 0
kMDItemFSInvisible              = 0
kMDItemFSIsExtensionHidden      = 0
kMDItemFSIsStationery           = 0
kMDItemFSLabel                  = 0
kMDItemFSName                   = "DT2005_MacOSX_forensics_Kevin_Lund.docx"
kMDItemFSNodeCount              = 0
kMDItemFSOwnerGroupID           = 20
kMDItemFSOwnerUserID            = 501
kMDItemFSSize                   = 166989
kMDItemFSTypeCode               = "WXBN"
kMDItemKind                     = "Microsoft Word-dokument"
kMDItemLastUsedDate             = 2009-03-22 17:50:44 +0100
kMDItemOrganizations            = (
    "Ho\U0308gskolan Dalarna"
)
kMDItemSubject                  = "Nätverkssäkerhet"
kMDItemTitle                    = "Tentamen"
kMDItemUsedDates                = (
    2009-03-17 00:00:00 +0100,
    2009-03-18 00:00:00 +0100,
    2009-03-19 00:00:00 +0100,
    2009-03-20 00:00:00 +0100,
    2009-03-21 00:00:00 +0100,
    2009-03-22 00:00:00 +0100
)
```

Ovan syns metadata för filen, datumen då filen använts, namn etc. I mitt fall så syns det ganska tydligt att jag använt mig av en mall som jag kopierat in text till: Tentamensprojektet i kursen Nätverkssäkerhet. Filen skapades 2009-03-17 14:11:22 +0100.

2.6.4 Finder

Finder är Mac OS X filhanterare. Programmet var en av de första grafiska filhanterarna och har varit en förebild till Windowsanvändarnas ”Utforskaren”.

2.6.5 Disk Arbitration

Disk arbitration är en bakgrundstjänst i Mac OS X som hanterar montering av filsystem. Den här tjänsten kommer automatiskt att montera och visa en inkopplad enhet som t.ex. en extern USB hårddisk. Disk arbitration kommer att montera volymer med läs– och skrivrättigheter vilket inte är önskvärt i forensiskt syfte. När man använder en Mac OS X dator för att undersöka en misstänkts dator så bör denna tjänst vara avstängd. Observera att NTFS volymer endast kommer

att monteras med läsrättigheter om inte *MacFUSE*[9] eller *PARAGAON NTFS for Mac*[10] eller annan liknande tjänst är installerad på systemet.

För att aktivera eller avaktivera Disk Arbitration under Mac OS X gör följande:

1. Ta en säkerhetskopia av filen `/etc/mach_init.d/diskarbitrationd.plist`
   - `sudo cp /etc/mach_init.d/diskarbitrationd.plist /Backup/`
2. Radera /etc/mach_init.d/diskarbitrationd.plist
   - `sudo rm /etc/mach_init.d/diskarbitrationd.plist`
3. Starta om systemet och Disk Arbitration skall vara avstängd.
4. För att aktivera Disk Arbitraion igen så kopiera tillbaka den säkerhetskopierade originalfilen tillbaka till ursprunglig plats.
   - `sudo cp /Backup/diskarbitrationd.plist /etc/mach_init.d/`
5. Starta sedan om systemet!

För mera information om Disk arbitration se mansidan under bilagor.

2.6.6 Address Book

Adressboken är en applikation som följer med Mac OS X som standard. Används av användaren för att lagra namn, adresser, telefonnummer, IM-alias, hemsideinformation etc. Adressboken är också tätt integrerad med andra applikationer som t.e.x. Mail & Safari.

Mera info kan hittas:

- `~/Library/Address Book Plug-Ins`
- `~/Library/Application Support/AddressBook`

2.6.7 iCal

Är det medföljande kalenderprogrammet. iCal är ett enkelt program och användas ganska flitigt av Mac anhängarna. iCal kan också synkroniseras med onlinetjänsten MobileMe. Användarna kan också publicera sina kalendrar online för andra att se.

Information om kalendrar kan hittas här:

- `~/Library/Calendars`

2.6.8 Mail

Är den medföljande och populära e-postklienten. Mail är tätt integrerad med Adressboken och håller också reda på mottagna och skickade e-postadresser som inte finns adressboken. Regler kan skrivas och programmet har en enkel skräpposthanterare. Mail har stöd för flera konton och POP3 & IMAP.

[9] http://code.google.com/p/macfuse/
[10] http://www.paragon-software.com/home/ntfs-mac/

Information kan hittas på följande platser:

- `~/Library/Preferences/com.apple.mail.plist`
- `~/Library/Mail/`
- `~/Library/Mail-attachments/`

2.6.9 .Mac & Mobile Me

.mac eller Mobile Me som det numera heter är en tjänst som köps i tillägg av Apple som ger användarna tillgång till Mail med upp till fem alias adresser. Tjänsten är tätt integrerad med Mac OS X och används för bl.a. säkerhetskopiering online i det medföljande 20GB lagringsutrymmet. MobileMe tillåter synkning av adressbok, Safari bokmärken, iCal kalendrar, nycklar, webblösenord, certifikat etc.

En bra idé är att gå igenom information här om tjänsten inhandlats av datorägaren. Brukar spara en plist fil under `~/Library/Preferences` med information synkning, namn etc.

2.6.10 Nyckelhanteraren

Är Apples lösenordshanteringssystem. Innehåller bl.a. lösenord till webbplatser, FTP servrar, SSH konton, nätverksutdelningar, krypterade enheter, privata nycklar, certifikat etc.

I Mac OS X sparas normalt keychain-filer på följande platser:

- `~/Library/Keychains/`
- `/Library/Keychains/`
- `/Network/Library/Keychains/`

Nyckelhanteringsfilen som används som standard är **login.keychain** och finns under hemmakatalogen. Denna fil är den som laddas in automatisk när en användare loggar in i systemet med sitt lösenord.

2.6.11 Safari

Är webbläsaren som följer med som standard i Mac OS X. Den används ganska flitigt av Mac användarna men även andra webbläsare som t.ex. FireFox & Opera är populära.

Safari från och med version 3 använder precis som senare versioner av FireFox, SQLite filer för att spara ner Cache och historik. Safari sparar ner webbformulärlösenord i keychain.

Mer information kan hittas:

- `~/Library/Preferences/com.apple.Safari.plist`
- `~/Library/Caches`
- `~/Library/Safari`

Från om med version 3.1.1 sparas webbcache på följande plats:

- `/private/var/folders`

2.6.12 Program för snabbmeddelanden

Det finns många program för snabbmeddelanden på Mac. Det program som medföljer Mac OS X heter iChat och har stöd för följande protokoll:

- AOL,
- ICQ,
- Jabber och Google Talk
- Bonjour,
- .Mac (Mobile Me)

Andra IM-program är bl.a. AOL Instant Messenger, Adium, Microsoft Messenger, Skype m.fl.

MSN protokollet är det protokoll för snabbmeddelande som är populärast i Sverige. Program som stöder dessa är givetvis de mest populära. De som faller in i den kategorin är Microsoft Messenger och Adium.

Microsoft Messenger sparar ner information om bl.a. historik och data för klienten under `~/Documents/Microsoft userdata/`

Adium sparar istället ner information under: `~/Library/Application Support/Adium 2.0/`

2.7 Mac OS X loggfiler

Mac OS X skapar precis som Linux och andra Unix system många loggfiler. Vissa loggfiler är väldigt detaljerade medan andra är av lite intresse i en forensisk undersökning. Nedan följer några loggfiler som kan vara av intresse för att etablera tidslinje, handlingar och konfigurationer.

Loggfil	Beskrivning / Innehåll
/var/log/crashreporter.log	Innehåller användningshistorik, information skrivs till denna fil när ett program kraschar.
/var/log/cups/access_log	Information om skrivaranslutning.
/var/log/cups/error_log	Information om skrivaranslutning.
/var/log/daily.out	Historik över nätverksinterface och diskstorlek.
/var/log/samba/log.nmbd	Information om anslutningar till Samba enheter (Windowsbaserade enheter).
/var/log/appfirewall.log	Information om brandväggstrafik.
~/Library/Logs	På denna plats finns programspecifika loggar.
~/Library/Logs/DiscRecording.log	Innehåller en logg över CD/DVD media som är utbränt med Finder.
~/Library/Logs/DiscUtility.log	Innehåller en logg över monterade, avmonterade ISO och DMG filer, partitionsinformation om HD, reparationer av behörigheter etc.
~/Library/Logs/iChatConnectionErrors	Innehåller information över förflutna iChat anslutningsförsök. Man hittar data som t.ex. användarnamn, IP-adresser och datum samt tid för försöket.
~/Library/Logs/Sync	Innehåller information över ev. Mobile Me synkning, mobila enheter som t.ex. iPods och mobiltelefoner, tid och datum för händelsen.

Tabell 2: Vanliga loggfiler i Mac OS X och dess innehåll (Kubasiak, 2007)

2.8 Property List Format File (.plist)

Mac OS X och alla andra Mac OS versioner använder sig inte av ett register som Microsoft Windows använder sig av. Istället används s.k. plist-filer för att spara ner innehåll. Plist är en förkortning för ”Property List Format File”. Innehållet i en plist-fil är binärt XML format och kan inte läsas med en vanlig texteditor.

Det finns ett flertal speciella verktyg för att behandla plist-filer på en Mac. Dessa kan laddas ner från t.ex. Macupdate eller versiontracker. Tillsammans med XCode som är Apples motsvarighet till Microsofts Visual Studio så följer det med också med en plist-editor. Ett inbyggt användbart terminalverktyg för att behandla plist-filer är **plutil**.

```
kevin@[~]$ sudo plutil -convert xml1 -o ~/Desktop/SystemVersion.xml
/System/Library/CoreServices/SystemVersion.plist
```

Ovanstående exempel visar en typisk användning av verktyget. I detta fall så konverterade jag filen SystemVersion.plist till XML-fil (SystemVersion.xml) till skrivbordet. XML-filen kan sedan öppnas med en vanlig texteditor eller annat verktyg för att behandla XML-filer. Innehållet i filen är:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>ProductBuildVersion</key>
        <string>9G55</string>
        <key>ProductCopyright</key>
        <string>1983-2008 Apple Inc.</string>
        <key>ProductName</key>
        <string>Mac OS X</string>
        <key>ProductUserVisibleVersion</key>
        <string>10.5.6</string>
        <key>ProductVersion</key>
        <string>10.5.6</string>
</dict>
</plist>
```

Det är enkelt att skriva ett shellskript, Appleskript eller använda sig av Automator för att automatisera denna process. Vanliga program och systemet spara generellt sina inställningar i plist-filer. Det finns många plist-filer och dessa får undersökas från fall till fall men några intressanta är:

Fil	Beskrivning / Innehåll
/System/Library/CoreServices/SystemVersion.plist	Innehåller versionsinformation om installerat OS.
/private/var/log/OSInstall.custom	Ingen plist-fil men innehåller information om datum och tid då OS var installerat (avslutad installation).
/private/etc/hosts	Ingen plist-fil men innehåller information om definerade IP-adresser och dess associerade namn.

Tabell 3: Plist-filer och andra viktiga informationsresurser

Fil (~/Library/Preferences/)	Beskrivning / Innehåll
AdressBookMe.plist	Innehåller data som användaren själv skrivit in om sig själv i Adressboken.
com.apple.Bluetooth.plist	Information om enheter som har varit anslutna via Bluethooth. Visar också senaste datum och tid för anslutningen.
com.apple.dashboard.plist	Information om installerade s.k. Widgets.
com.apple.dock.plist	Information om program tillgängliga i dockan.
com.apple.finder.plist	Information om senaste öppnade mappar, senaste serveranslutningar från Finder och senaste ”Gå till mapp” valet.
com.apple.Grab.plist	Information om senaste mapp som lästs in.
com.apple.mail.plist	Information om Mail.app och dess inställningar som t.ex. kontonamn och vart e-posten ligger lagrad på disken.
com.apple.NetworkUtility.plist	Information om nätverksuppslagningar som t.ex. Whois, Ping och port scans.
com.apple.Prewiew.bookmarks.plist	Senaste dokumenten som öppnats med programmet ”Förhandsgranskning”.
com.apple.print.PrintCenter.plist	Information om senaste anslutna skrivare.
com.apple.quicktimeplayer.plist	Information om senaste uppspelade filmer i Quicktime.
com.apple.Safari.plist	Information om Safari historik som t.ex. senaste söktermer, senaste öppnade lokala filer etc.
com.apple.sidebarlists.plist	Innehåller historisk information om nuvarande och förgående objekt som har visats i Finder Sidebar.
com.apple.systemuiserver.plist	Information om ”egna” menyer som installerats av användaren. Kan vara användbart om man vill se det som körs när användaren loggar in.
com.apple.scheduler.plist	Information om schemalagda automatiska händelser som t.ex. Systemuppdatering eller MobileMe synkning.
com.apple.recentitems.plist	Information om senaste använda program, filer och serveranslutningar.

Tabell 4: Några plist-filer med intressant information.

3 Informationsförvärv

Nedan kommer jag att beskriva tre olika metoder för att på ett forensiskt sätt få tillgång till data på en misstänkts dator. Två av teknikerna kommer att innebära att använda måldatorn direkt och ett tredje sätt genom användning av ytterligare en dator. De tre olika teknikern är **Single-user mode**, **LiveCD** och **Target Disk Mode (Firewire Disk Mode).** Ytterligare ett sätt att få tillgång till information ur en måldator är att fysiskt plocka ut hårddisken ur datorn.

3.1 Mac OS Boot kommandon

Det finns många olika tangentbordskommandon under som orsakar olika handlingar vid boot på Mac. Alla kombinationer fungerar inte med alla Mac datorer. Nedan är några kommandon och dess funktion:

Funktion	Tangentbordskombination
Förbigå startskivan och boota från en extern enhet (HD, CD, DVD)	CMD-ALT-SHIFT-DELETE
Boota från en CD/DVD	C
Boota från en specifik SCSI ID	CMD-ALT-SHIFT-DELETE-#
Mata ut diskett (Floppy Disk)	Håll nere musknappen
Välj en enhet att boota från	ALT
Starta i Targeted Disk Mode	T
OS X Verbose Mode	ALT-V
OS X SIngle-User Mode	ALT-S
Open Firmware	CMD-ALT-O-F

Tabell 5: Mac OS tangentbordskombinationer vid boot.

3.2 Single-user mode

Single-user mode är en av de bästa verktygen inom Macintosh Forensiska utredningar. Det här läget i operativsystemet är ursprungligen tänkt för administratörer att på ett lätt sätt underhålla datorn. I Single-user mode krävs det kunskap om Unix då man kommunicera med OS enbart genom en terminal. I Single-user mode så kommer man att vara root på systemet.

Viktigt!

En avancerad användare kan ha avaktiverat Single-user mode. Om ett försök att boota om i Single-user mode inte lyckas. Anteckna detta i utredningsrapporten.

Efter boot i Single-User mode (se ovan) så presenteras man får ett terminalfönster där man är inloggad som root-användare. Man kan orsaka mycket skada om man inte vet vad man gör i detta läge. Filsystemet är monterat med endast läs-rättigheter. För att montera filsystemet med skriv rättigheter så kan man använda sig av kommandot: `/sbin/mount -uw /`

Följande kommandon är icke destruktiva och kan användas för att samla in information under en utredning:

- **date** – Datum med nuvarande tidszon.
- **date –u** – Datum i UTC
- **hdiutil partition /dev/disk0** – Visar partitionstabellen över boot-enheten
- **hdiutil pmap2 /dev/disk0** – Visar ytterligare information om partitionstabellen för boot-enheten.
- **ls /dev/disk?** – Listar aktiva enhetsfiler för de installerade enheterna.
- **system_profiler SPHardwareDataType** – Visar info om Macintosh hårdvara
- **system_profiler SPSoftwareDataType** – Visar systeminformation om OS
- **system_profiler SPParallelATADataType** – Visar info om ATA enheter
- **system_profiler SPHardwareRAIDDataType** – Visar info om hårdvaru RAID
- **system_profiler SPMemoryDataType** – Visar info om installerat minne
- **system_profiler ParallelSCSIDataType** – Visar info om SCSI enheter
- **system_profiler SPSASDataType** – Visar info om SAS (Serial Attached SCS) enheter
- **system_profiler SPSerialATADataType** – Visar info om SATA enheter

3.3 Live CD

Fördelen med att använda en Boot CD är att systemet och mjukvara är den samma för varje gång man startar. Det är dock viktigt att påpeka att alla boot cd inte fungerar med alla Mac datorer. Man kan, om man har kunskapen att skapa en egen Boot CD.

Att boota från en Live CD är en ganska enkel process. Starta om med skivan i och håll inne ”alt” tangenten eller ”C”. Det finns otroligt många Linux distributioner och att ingående beskriva användningen av dessa ligger utanför ramen i detta arbete. En enkel sökning i en sökmotor för Mac Live Boot CD, Knoppix, Ubuntu etc. är ett sätt att ta fram nödvändig information. Dock skall man vara mycket observant med vilken Live CD, Linux dist. man väljer. Det är av yttersta vikt att man vet vad som händer när man startar från skivan så att potentiell viktig information inte förändras. Linux disten skall ha stöd för EFI, OF, HFS/HFS+ och bör inte automatiskt montera filsystemet.

Några exempel på Linux distributioner som fungerar med Mac är:

- Intel Mac – Ubuntu LiveCD
- Intel Mac – Helix LiveCD
- Intel Mac - Backtrack LiveCD
- PowerPC och Intel Mac – BBT Macquistion CD

Flera distributioner finns med all säkerhet. Använd valfri sökmotor för att hitta mera info. BBT (Blackbag Technologies) erbjuder en prenumeration på en forensisk godkänd Mac Boot CD. Mera info om BBT och Macquisition kan hittas här:
http://www.blackbagtech.com/products/macquisition.htm

3.4 Target Disk Mode

Den tredje metoden är Target Disk Mode eller Firewire Disk Mode som det också kallas. Denna metod är den metod som erbjuder mest flexibilitet. Du kan t.ex. använda en laptop eller stationär dator med valfritt OS för att undersöka måldatorn. Man skall dock se till så att auto-mount på undersökningsdatorn är avslaget. Observera att det inte är säkert att TDM fungerar på måldatorn.

Target Disk Mode är en teknologi som tillåter en Macintosh dator att agera som en extern, firewire enhet. Datorn kommer inte att modifiera data eller filsystem om inte användaren uttryckligen vill det.

Viktigt!

Target Disk Mode fungerar endast på interna ATA enheter. TDM kommer endast att ansluta till den ATA enhet som är angiven som Master på Ultra ATA bussen. TDM kommer inte att ansluta till ATA-slavar, ATAPI eller SCSI enheter. Man kan med andra ord inte få tillgång till alla interna enheter om det finns fler än en installerade. Använd ex. LiveCD om det misstänks att datorn innehåller flera interna enheter.

För att använda sig av TDM och ta en forensisk skivabild av enheten så använd följande steg:

1. Se till så att det OS som används på undersökningsdatorn inte har auto-mount påslaget. Om en Mac används så avaktivera Disk Arbitration. (se ovan)
2. Se till att måldatorn är avstängd. Om en laptop är måldatorn se till så att AC-adaptern är inkopplad.
3. Koppla ihop måldatorn med undersökningsdatorn med en FireWire kabel. Undersökningsdatorn behöver inte vara avslagen.
4. Starta måldatorn och omedelbart håll inne ”T”-knappen tills en FireWire symbol visas.
5. På undersökningsdatorn öppna ett terminalfönster och leta upp den anslutna TDM datorn t.ex. `ls /dev/disk?`
6. Ta en MD5 summa på enheten: `md5 /dev/disk1 > /Bevis/targetMac_start.md5`
7. Använd det inbyggda verktyget dd för att ta en skivavbild: `dd if=/dev/disk1 conv=noerror,sync of=/Bevis/targetMac.dd` **Se till så att utrymme finns!**
8. Ta en ny MD5 summa: `md5 /dev/disk1 > /Bevis/targetMac_end.md5`
9. Stäng av måldatorn genom att hålla inne strömknappen.
10. Koppla bort kabeln.

3.5 Fysisk urplockning av intern HD

Att plocka bort den interna hårddisken kan på en Macintosh vara en komplicerad uppgift. Vissa Mac datorer kan upplevas som om de mer eller mindre är svetsade ihop. Sidan iFixit[11] visar med detaljerade bilder på hur man plockar isär olika Mac modeller. Andra källor för att hitta information om hur man plockar isär en Mac utan att förstöra den är bl.a. YouTube.

Viktigt!

Kom ihåg att använda en fysisk skrivspärr på HD innan den undersöks.

3.6 Live undersökning

En liveundersökning av en dator innebär att spara ner all flyktig information av vikt. Eftersom Mac har inbyggt stöd för både Perl och Python är det mycket troligt att de skript skrivna för Linux/Unix i detta ändamål kommer att fungera rakt av i Mac. Detta bör dock i förhand undersökas och bekräftas på en annan Mac. Jag skulle dock vilja tipsa om ett program med namn **MacLockPick II** från Subrosasoft som underlättar detta arbete. Programmet finns för både Windows och Mac och samlar in information från ett flertal olika källor utan konfiguration. Programmet kan också byggas ut med hjälp av s.k. Plugins.

Mer info om programmet kan hittas på följande platser:

- http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=product_info&cPath=1&products_id=2&zenid=778622c0b02fa36a10156fdc2b2fcf30
- http://www.macosxforensics.com/Resources/maclockpickii/maclockpickii.html

3.7 Minnesdump på en Mac

Virtuellt minne på en Mac sparas under `/var/vm` och hittar en enhetsfil på minnet under `/dev/mem*` på vissa Mac OS. Finns en enhetsfil så kan en minnesdump göras med hjälp av **dd** på följande sätt: `dd if=/dev/mem of=memdump.img conv=noerror,sync`

På alla Mac OS system så finns det ingen enhetsfil för minnet. Men på alla nyare Mac (efter 2005) så finns det en funktion som kallas för Safe Sleep. Denna funktion är tänkt att användas för att återställa datorn om det skulle bli strömavbrott under datorns viloläge eller om batteriet på en bärbar dator är på väg att ta slut. När datorn går ned i viloläge så kommer hela datorns minne att kopieras ned till disk, okrypterat. Innehållet i denna fil kommer att kopieras över till minnet igen när datorn väcks ur sitt viloläge.

Denna fil kan man hitta under `/var/vm/sleepimage`. Kopiering av denna fil sker på samma sätt som ovan med dd eller helt enkelt kopiera filen. Givetvis så bör MD5 eller SHA1 summar tas innan och efter processen.

[11] http://www.ifixit.com/Guide

4 Bilagor

4.1 MAN sidor

4.1.1 Diskarbitrationd

```
DISKARBITRATIOND(8)       BSD System Manager's Manual      DISKARBITRATIOND(8)

NAME
     diskarbitrationd -- disk arbitration daemon

SYNOPSIS
     diskarbitrationd [-d]

DESCRIPTION
     diskarbitrationd listens for connections from clients, notifies clients
     of the appearance of disks and filesystems, and governs the mounting of
     filesystems and the claiming of disks amongst clients.

     diskarbitrationd is accessed via the Disk Arbitration framework.

     Options:

     -d       Report detailed information in /var/log/diskarbitrationd.log.
              This option forces diskarbitrationd to run in the foreground.

     The file /etc/fstab is consulted for user-defined mount points, indexed
     by filesystem, in the mount point determination for a filesystem.  Each
     filesystem can be identified by its UUID or by its label, using the con-
     structs ``UUID'' or ``LABEL'', respectively.  For example:

        UUID=DF000C7E-AE0C-3B15-B730-DFD2EF15CB91 /export ufs   ro
        UUID=FAB060E9-79F7-33FF-BE85-E1D3ABD3EDEA none    hfs   rw,noauto
        LABEL=The\040Volume\040Name\040Is\040This none    msdos ro

FILES
     /etc/fstab
     /var/log/diskarbitrationd.log
     /var/run/diskarbitrationd.pid
     /System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist

SEE ALSO
     fstab(5)

Darwin                          July 18, 2004                          Darwin
```

4.1.2 Plutil

```
PLUTIL(1)                 BSD General Commands Manual                PLUTIL(1)

NAME
     plutil -- property list utility

SYNOPSIS
     plutil [command_option] [other_options] file
             ...

DESCRIPTION
     plutil can be used to check the syntax of property list files, or convert
     a plist file from one format to another.

     The first argument indicates the operation to perform, one of:

     -help          Show the usage information for the command and exit.

     -lint          Check the named property list files for syntax errors.
                    This is the default command option if none is specified.

     -convert fmt   Convert the named file to the indicated format and write
                    back to the file system.  If the file can't be loaded due
                    to invalid syntax, the operation fails.

                    fmt is one of:  xml1, for version 1 of the XML plist format
                                    binary1, for version 1 of the binary plist
                                    format

     There are a few additional options:

     --             Specifies that all further arguments are file names

     -s             Don't print anything on success.

     -o path        Specify an alternate path name for the result of the -con-
                    vert operation; this option is only useful with a single
                    file to be converted.  Specifying - as the path outputs to
                    stdout (only allowed with XML output).

     -e extension   Specify an alternate extension for converted files, and the
                    output file names are otherwise the same.
```

4.2 Initial Data Gathering

Denna information är hämtad från:
http://www.macosxforensics.com/Analysis/InitialDataGathering/InitialDataGathering.html

Operating System Installation Date

- `/var/log/OSInstall.custom`

Operating System Version

- `/System/Library/CoreServices/SystemVersion.plist (OS X Client)`
- `/System/Library/CoreServices/ServerVersion.plist (OS X Server)`

Last Software Update

- `/Library/Preferences/com.apple.SoftwareUpdate.plist`

Registation Information during Operating System Installation

- `/var/db/.AppleSetupDone`

Current Time Zone

- `/etc/localtime (link file pointing to current time zone) OR`
- `/Library/Preferences/.GlobalPreferences.plist`

Auto-Login User and Last Login User

- `/Library/Preferences/com.apple.loginwindow.plist`

Home Folders

- `/Users/username`

User Auto-Launch Items

- `/Users/username/Library/Preferences/loginwindow.plist`

Deleted Users

- `/Library/Preferences/com.apple.preferences.accounts.plist`

Network Settings

- `/Library/Preferences/com.apple.alf.plist - Firewall Settings`
- `/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist - Airport (Wireless) Settings`
- `/Library/Preferences/SystemConfiguration/com.apple.nat.plist - Internet Sharing Settings`
- `/Library/Preferences/SystemConfiguration/com.apple.network.identification.plist - Historical Network TCP/IP Assignments with Timestamps`
- `/Library/Preferences/SystemConfiguration/com.apple.NetworkInterfaces.plist - Onboard Interfaces`

- /Library/Preferences/SystemConfiguration/com.apple.preferences.plist - Network Configuration for each interface

Bluetooth History

- /Library/Preferences/com.apple.Bluetooth.plist

Instant Messaging

- /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

Peer to Peer

- /Users/Library/Preferences/Limewire/*

Safari

- /Users/username/Library/Safari/Bookmarks.plist - User's Bookmarks
- /Users/username/Library/Safari/Downloads.plist - Contents of the user's Downloads window in Safari
- /Users/username/Library/Safari/History.plist - Safari browser history
- /Users/username/Library/Safari/LastSession.plist - defines the last browsing session (window and tabs that were open)

Log Files

- /var/log/*
- /Users/username/Library/Logs/*

Sleep File and Virtual Memory

- /var/vm/sleepimage
- /var/vm/swapfile0

4.3 MacOS X 10.4 Command Line Utilities and Daemons

```
apropos              - search the whatis database for strings
arp                  - address resolution display and control
asr                  - Apple Software Restore; copy volumes (e.g. from disk images)
atlookup             - looks up network-visible entities (NVEs) registered on the AppleTalk
network system
autodiskmount        - disk support tool
automount            - automatic server mount / unmount daemon
awk                  - pattern-directed scanning and processing language
basename, dirname    - return filename or directory portion of pathname
bash                 - GNU Bourne-Again Shell
bless                - set volume bootability and startup disk options
blued                - The Mac OS X bluetooth daemon
bootparamd           - boot parameter server
bzcmp, bzdiff        - compare bzip2 compressed files
bzgrep, bzfgrep, bzegrep - search possibly bzip2 compressed files for a regular expression
bzip2, bunzip2       - a block-sorting file compressor, v1.0.2 bzcat - decompresses
files to stdout bzip2recover - recovers data from damaged bzip2 files
cal                  - displays a calendar
calendar             - reminder service
cat                  - concatenate and print files
chflags              - change file flags
chgrp                - change group
chmod                - change file modes or Access Control Lists
chown                - change file owner and group
chpass, chfn, chsh   - add or change user database information
chroot               - change root directory
cksum, sum           - display file checksums and block counts
cksum(n)             - calculate a cksum(1) compatible checksum
clear                - clear the terminal screen
cmp                  - compare two files byte by byte
compress, uncompress - compress and expand data
configd              - System Configuration Daemon
cp                   - copy files
cron                 - daemon to execute scheduled commands (Vixie Cron)
crontab              - maintain crontab files for individual users (V3)
cupsd                - common unix printing system daemon
cvs                  - Concurrent Versions System
date                 - display or set date and time
dd                   - convert and copy a file
defaults             - access the Mac OS X user defaults system
df                   - display free disk space
diff                 - compare files line by line
diff3                - compare three files line by line
diffpp               - pretty-print diff outputs with GNU enscript
diffstat             - make histogram from diff-output
dig                  - DNS lookup utility
disable, enable      - stop/start printers and classes
diskarbitrationd     - disk arbitration daemon
disklabel            - manipulate and query an Apple Label disk label
disktool             - disk support tool
diskutil             - Modify, verify and repair local disks
ditto                - copy files and directories to a destination directory
dmesg                - display the system message buffer
domainname           - set or print the name of the current NIS domain
drutil               - interact with CD/DVD burners
dscl                 - Directory Service command line utility
du                   - display disk usage statistics
dump                 - filesystem backup
dumpfs               - dump file system information
dynamic_pager        - dynamic pager external storage manager
echo                 - write arguments to the standard output
ed                   - text editor
emacs                - GNU project Emacs
enscript             - convert text files to PostScript
env                  - set and print environment
expand, unexpand     - expand tabs to spaces, and vice versa
expr                 - evaluate expression
fdisk                - DOS partition maintenance program
fibreconfig          - Tool for configuring settings for Fibre Channel controllers
and targets
file                 - determine file type
find                 - walk a file hierarchy
```

```
fsck                - filesystem consistency check and interactive repair
fsck_hfs            - HFS file system consistency check
fsck_msdos          - DOS/Windows (FAT) file system consistency check
ftp                 - Internet file transfer program
getconf             - retrieve standard configuration variables
gpt                 - GUID partition table maintenance utility
grep, egrep, fgrep  - print lines matching a pattern
groups              - show group memberships
gzexe               - compress executable files in place
gzip, gunzip, zcat  - compress or expand files
hdik                - lightweight in-kernel disk image mounting tool
hdiutil             - manipulate disk images (attach, verify, burn, etc)
head                - display first lines of a file
heap                - List all the malloc-allocated buffers in the process's heap
hexdump, hd         - ASCII, decimal, hexadecimal, octal dump
host                - DNS lookup utility
hostname            - set or print name of current host system
ifconfig            - configure network interface parameters
info                - read Info documents
installer           - system software and package installer tool
ioreg               - show I/O Kit registry
iostat              - report I/O statistics
ip6                 - Enable or disable IPv6 on active interfaces
ip6config           - Configure IPv6 and 6to4 IPv6 tunnelling
ip6fw               - controlling utility for IPv6 firewall
ipconfig            - view and control IP configuration state
ipfw                - IP firewall and traffic shaper control program
jar                 - Java archive tool
java                - Java interpreter
kadmin              - Kerberos V5 database administration program
kadmind             - KADM5 administration server
kdb5_util           - Kerberos database maintainance utility
kextload            - loads, validates, and generates symbols for a kernel extension (kext)
kextstat            - display status of dynamically loaded kernel extensions
kextunload          - terminates and unloads kernel extensions
kill                - terminate or signal a process
killall             - kill processes by name
ktrace              - enable kernel process tracing
last                - indicate last logins of users and ttys
lastcomm            - show last commands executed in reverse order
launchctl           - Interfaces with launchd
launchd             - System wide and per-user daemon/agent manager
ldapsearch          - LDAP search tool
ldapwhoami          - LDAP who am i? tool
less                - opposite of more
lessecho            - expand metacharacters, such as * and ?, in filenames on Unix
systems
ln, link            - make links
locale              - display locale settings
locate              - find files
login               - log into the computer
logname             - display user's login name
logresolve          - resolve hostnames for IP-adresses in Apache logfiles
look                - display lines beginning with a given string
lookupd             - directory information and cache daemon
ls                  - list directory contents
lsbom               - list contents of a bom file
lsof                - list open files
lsvfs               - list known virtual file systems
machine             - print machine type
man                 - format and display the on-line manual pages
md5                 - calculate a message-digest fingerprint (checksum) for a file
mdfind              - finds files matching a given query
megaraid            - Command Line Utility for MegaRAID management
merge               - three-way file merge
mesg                - display (do not display) messages from other users
mkdir               - make directories
mnthome             - mount an AFP (AppleShare) home directory with the correct
privileges
mount               - mount file systems
mount.cifs          - mount using the Common Internet File System (CIFS)
mount_afp           - mount an afp (AppleShare) filesystem
mount_cd9660        - mount an ISO-9660 filesystem
mount_cddafs        - mount an Audio CD
mount_fdesc         - mount the file-descriptor file system
```

```
mount_ftp            - mount a FTP filesystem
mount_hfs            - mount an HFS/HFS+ file system
mount_msdos          - mount an MS-DOS file system
mount_nfs            - mount NFS file systems
mount_ntfs           - mount an NTFS file system
mount_smbfs          - mount a shared resource from an SMB file server
mount_udf            - mount a UDF filesystem
mount_webdav         - mount a WebDAV filesystem
mountd               - service remote NFS mount requests
msgs                 - system messages and junk mail program
mtree                - map a directory hierarchy
mv                   - move files
named                - Internet domain name server
nano                 - Nano's ANOther editor, an enhanced free Pico clone
natd                 - Network Address Translation daemon
net                  - Tool for administration of Samba and remote CIFS servers
netinfod             - NetInfo daemon
netstat              - show network status
newfs                - construct a new file system
newfs_hfs            - construct a new HFS Plus file system
newfs_msdos          - construct a new MS-DOS (FAT) file system
nfsd                 - remote NFS server
nice                 - execute a utility with an altered scheduling priority
nologin              - politely refuse a login
notifyd              - notification server
ntpd                 - Network Time Protocol (NTP) daemon
ntpdate              - set the date and time via NTP
ntptrace             - trace a chain of NTP servers back to the primary source
nvram                - manipulate Open Firmware NVRAM variables
open                 - open files and directories
open-x11             - run X11 programs
pagesize             - print system page size
passwd               - modify a user's password
paste                - merge corresponding or subsequent lines of files
patch                - apply a diff file to an original
pbcopy, pbpaste      - provide copying and pasting to the pasteboard (the Clip-
board) from command line
pcscd                - PC/SC Smartcard Daemon
pdisk                - Apple partition table editor
ping                 - send ICMP ECHO_REQUEST packets to network hosts
ping6                - send ICMPv6 ECHO_REQUEST packets to network hosts
pl                   - converts between ASCII and binary plist formats
plutil               - property list utility
pmset                - modify power management settings
portmap              - RPC program,version to DARPA port mapper
pr                   - print files
printenv             - print out the environment
printf               - formatted output
ps                   - process status
pwd                  - return working directory name
quot                 - display total block usage per user for a file system
quota                - display disk usage and limits
quotacheck           - filesystem quota consistency checker
quotaon, quotaoff    - turn filesystem quotas on and off
rarpd                - Reverse ARP Daemon
rcp                  - remote file copy
reboot, halt         - stopping and restarting the system
renice               - alter priority of running processes
repquota             - summarize quotas for a file system
restore              - restore files or file systems from backups made with dump
rev                  - reverse lines of a file
rlogin               - remote login
rm, unlink           - remove directory entries
rmdir                - remove directories
routed               - network RIP and router discovery routing daemon
rsh                  - remote shell
rwho                 - who is logged in on local machines
rwhod                - system status server
say                  - Convert text to audible speech
scp                  - secure copy (remote file copy program)
screencapture        - capture and manipulate clipboard contents
screenreaderd        - VoiceOver daemon
sftp                 - secure file transfer program
sftp-server          - SFTP server subsystem
showmount            - show remote nfs mounts on host
```

```
shutdown             - close down the system at a given time
sleep                - suspend execution for an interval of time
smbclient            - ftp-like client to access SMB/CIFS resources on servers
smbd                 - server to provide SMB/CIFS services to clients
smbstatus            - report on current Samba connections
snmpd                - daemon to respond to SNMP request packets
snmptable            - retrieve an SNMP table and display it in tabular form
snmptrapd            - Receive and log SNMP trap messages
sort                 - sort lines of text files
split                - split a file into pieces
spray                - send many packets to host
srm                  - securely remove files or directories
ssh                  - OpenSSH SSH client (remote login program)
sshd                 - OpenSSH SSH daemon
stat, readlink       - display file status
strings              - find the printable strings in a object, or other binary, file
strip                - remove symbols
su                   - substitute user identity
sudo, sudoedit       - execute a command as another user
sum(n)               - calculate a sum(1) compatible checksum
sw_vers              - print Mac OS X operating system version information
sync                 - force completion of pending disk writes (flush cache)
syslog               - Apple System Log utility
syslog.conf(5)       - syslogd(8) configuration file
syslogd              - Apple System Log server
system_profiler      - reports system hardware and software configuration
tail                 - display the last part of a file
talk                 - talk to another user
tar                  - tape archiver; manipulate "tar" archive files
tcpdump              - dump traffic on a network
tcsh                 - C shell with file name completion and command line editing
telnet               - user interface to the TELNET protocol
tftp                 - trivial file transfer program
tim                  - authetication server
time                 - time command execution
timed                - time server daemon
timutil              - authetication server utility
top                  - display and update sorted information about processes
touch                - change file access and modification times
traceroute           - print the route packets take to network host
traceroute6          - print the route IPv6 packets will take to the destination
tty                  - return user's terminal name
umount               - unmount filesystems
uname                - Print operating system name
uniq                 - report or filter out repeated lines in a file
unzip                - list, test and extract compressed files in a ZIP archive
update               - flush internal filesystem caches to disk frequently
update_prebinding    - Update prebinding information when new system libraries or
frameworks are installed
uptime               - show how long system has been running
users                - list current users
uuencode, uudecode   - encode/decode a binary file
vers_string          - produce version identification string
vim                  - Vi IMproved, a programmers text editor
vipw                 - edit the password file
visudo               - edit the sudoers file
vpnd                 - Mac OS X VPN service daemon
w                    - display who is logged in and what they are doing
wc                   - word, line, character, and byte count
whatis               - search the whatis database for complete words
whereis              - locate programs
which                - locate a program file in the user's path
who                  - display who is on the system
whoami               - display effective user id
whois                - Internet domain name and network number directory service
winbindd             - Name Service Switch daemon for resolving names from NT servers
write                - send a message to another user
xgrid                - submit and monitor xgrid jobs
xinetd               - the extended Internet services daemon
zcmp, zdiff          - compare compressed files
zgrep                - search possibly compressed files for a regular expression
zip, zipcloak, zipnote, zipsplit - package and compress (archive) files
zipgrep              - search files in a ZIP archive for lines matching a pattern
zipinfo              - list detailed information about a ZIP archive
zsh                  - the Z shell
```

4.4 Mac OS X Admin Hack

Hämtat från: http://www.hackmac.org/?q=node/4

Here's how to create an admin account without knowing the current administrator password.

This is nothing new to people familiar with unix, and can't really be classified as a "hack", but it's an easy way to make an admin account without a password. This particular method is used if you, for some reason, can't get into your account at all, for example: you lost your password and you account is protected with FileVault. This process basically forces your computer to re-run setup, which is what you see when you setup a new Mac.

This process will take about 5-10 minutes. If you have a password, or WEP code for your network or internet, be sure to have that at hand.

If the computer doesn't have an Open Firmware Password, that this should work fine. If it does, than you're out of luck

Step 1: Boot in single user mode (Single user mode bypasses the GUI, which is all the visual stuff, and gives you something called "root access") by pressing Command + S (Apple+S) when the first shade of blue appears on the screen, and holding it down until the screen turns black with white text.

Step 2: Wait for all the code stuff to load. Now, the first thing we need to do in single user mode is mount the hard drive so we can edit it. You enter this command in : /sbin/mount -uw /

It should say something about removing orphaned unlinked files.

Step 3: We are going to delete a little file that tells your computer every time you start up that you've completed the setup by entering this command: rm /var/db/.applesetupdone

It should just bump down, waiting for the next command if it worked.

Step 4: Now type, reboot

Step 5: It should shut down and reboot. Than, a setup window will appear, asking you what language you want your computer to be in, just like you see when you setup a newly purchased Mac.

A welcome video will play after you select the language. It has some pretty cool music, but if your in a room with other people, I'd mute it right after the video starts, or have headphones handy.

Step 6: Setup the computer. Select "DO NOT TRANSFER MY DATA". Don't worry, all your old stuff will still be there. Choose your internet connection and network, here is where you need your WEP or security password if you have one.

Step 7: Create a new local account to administer that computer. You usually want to enter the name of the computer as the longname, and the shortname what you'll log in as. Say your computer's old name was "Frank's Computer", than just put Frank as the longname, because it

will automatically as " 's Computer" at the end. MAKE SURE THAT BOTH USERNAMES ARE DIFFERENT FROM THE EXSISTING ONES, OTHERWISE IT WILL OVERWRITE.

Step 8: Finish the setup, and you should automatically be logged into your new administrator account.

5 Litteraturförteckning

Amit Singh. (2006). *Mac OS X Internals: A Systems Approach.* Westford: Addison Wesley Professional.

Apple. (den 11 07 2008). *Introduction to the File System Overview*. Hämtat från Apple Developer Connection: http://developer.apple.com/documentation/MacOSX/Conceptual/BPFileSystem/BPFileSystem.html

Apple. (den 19 11 2008). *The Boot Process*. Hämtat från Apple Developer Connection: http://developer.apple.com/documentation/MacOSX/Conceptual/BPSystemStartup/Articles/BootProcess.html

Davis, W. S., & Rajkumar, T. M. (2004). *Operating Systems - A systematic view, sixth edition.* Miami, Oxford: Pearson Education Inc.

Kubasiak, R. R. (den 29 05 2007). Macintosh Forensics - A Guide for the Forensically Sound Examination of a Macintosh Computer.

Lester, A. (den 01 04 2006). *The Power of mdfind*. Hämtat från Macdevcenter: http://www.macdevcenter.com/pub/a/mac/2006/01/04/mdfind.html?page=1

Mac OS X Forensics. (u.d.). *Mac OS X Forensics*. Hämtat från macosxforensics.com: http://www.macosxforensics.com

Wikipedia. (u.d.). *Apple Inc.* Hämtat från Wikpedia: http://en.wikipedia.org/wiki/Apple_Inc.

Wikipedia. (u.d.). *Boot Camp (Software)*. Hämtat från Wikipedia: http://en.wikipedia.org/wiki/Boot_Camp_(software)

Wikipedia. (u.d.). *Finder (software)*. Hämtat från Wikipedia: http://en.wikipedia.org/wiki/Finder_(software)

Wikipedia. (u.d.). *HFS Plus*. Hämtat från Wikipedia: http://en.wikipedia.org/wiki/HFS_Plus

Wikipedia. (u.d.). *Keychain (Mac OS)*. Hämtat från Wikipedia: http://en.wikipedia.org/wiki/Keychain_(Mac_OS)

Wikipedia. (u.d.). *NeXTSTEP*. Hämtat från Wikipedia: http://en.wikipedia.org/wiki/NeXTSTEP