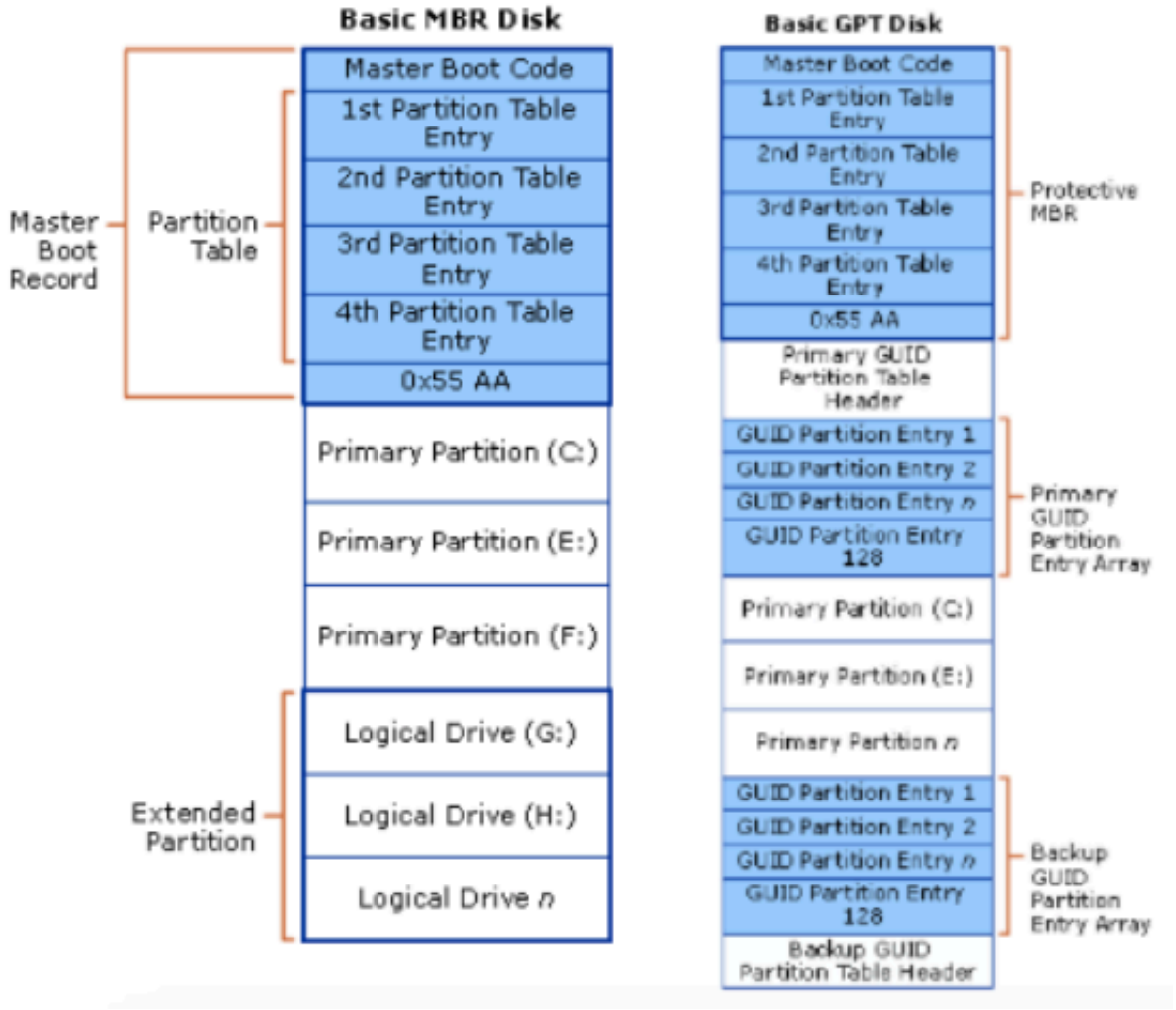
Lösningsförslag / Cheat Sheet

Diskar

Partitionstabeller

Svar från föreläsningar.

Master Boot Record (MBR), Guided Partition Table (GPT). MBR har fyra partitioner och 2TB maxstorlek. GPT är det moderna systemet med upp till 128 partitioner. Partitionstyperna kan ha stöd för *basic disk storage* och *dynamic disk storage* där man eventuellt kan expandera partitionen "on-the-fly". Dynamic har även stöd för RAID 5.



Slack space

Svar från sammanställning av andra källor.

På grund av fragmentering av disken kan viss plats slösas.

När en fil sparas på en disk brukar den sparas i ett eller flera *kluster* - en samling kontinuerliga *sektorer* på disken. Vanligtvis så kommer filens storlek inte att vara exakt lika med storleken av klustrena och då kommer viss plats i ett kluster att förbli oanvänt. Denna oanvända yta kallas för *slack space*.

Filsystem

Svar från föreläsningar.

Filsystems uppgift är att lagra data. Olika operativsystem har olika tillvägagångsätt och sparar olika metadata. De flesta filsystem har en hierkisk princip. Andra har grafer eller strömmar. Man brukar ha metoder för att skapa, läsa, modifiera, ta bort och flytta data.

EXT2, EXT3, EXT4

Svar från sammanställning av andra källor.

EXT2 - Second Extended Filesystem, EXT3 - Third Extended Filesystem och EXT4 - Fourth Extended Filesystem är alla filsystem som förekommer i Linux.

EXT2 har en maximal filstorlek på 16GiB till 2TiB beroende på använd blockstorlek (1, 2, 4 eller 8 KiB). Filnamnen får max vara 255 byte. Kan ha 100 miljoner filer. Maximal volymstorlek är 2-32 TiB.

EXT3 är så gott som identiskt med EXT2. Har dock stöd för *journalförande*.

EXT4 har en maximal filstorlek på 16GiB och en maximal volymstorlek på 1EiB (exabyte). Kan ha fyra miljarder filer. Generellt så är EXT4 mer effektivt än de äldra varianterna.

Om en fil exporteras från EXT till ett annat filsystem så som FAT eller NTFS försvinner EXT-specifika värden så som rättigheter.

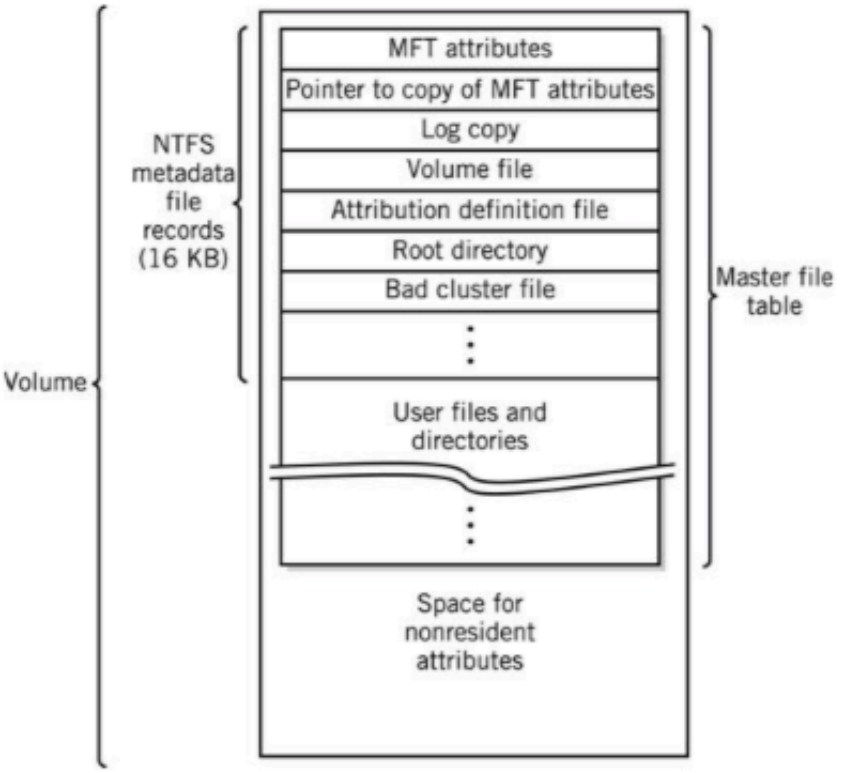
För EXT2 och EXT3 raderas enbart pekare till filer vid borttagning. På så vis blir det lätt att återskapa filer genom att hitta den första delen av filen som sedan pekar vidare till övriga delar av filen.

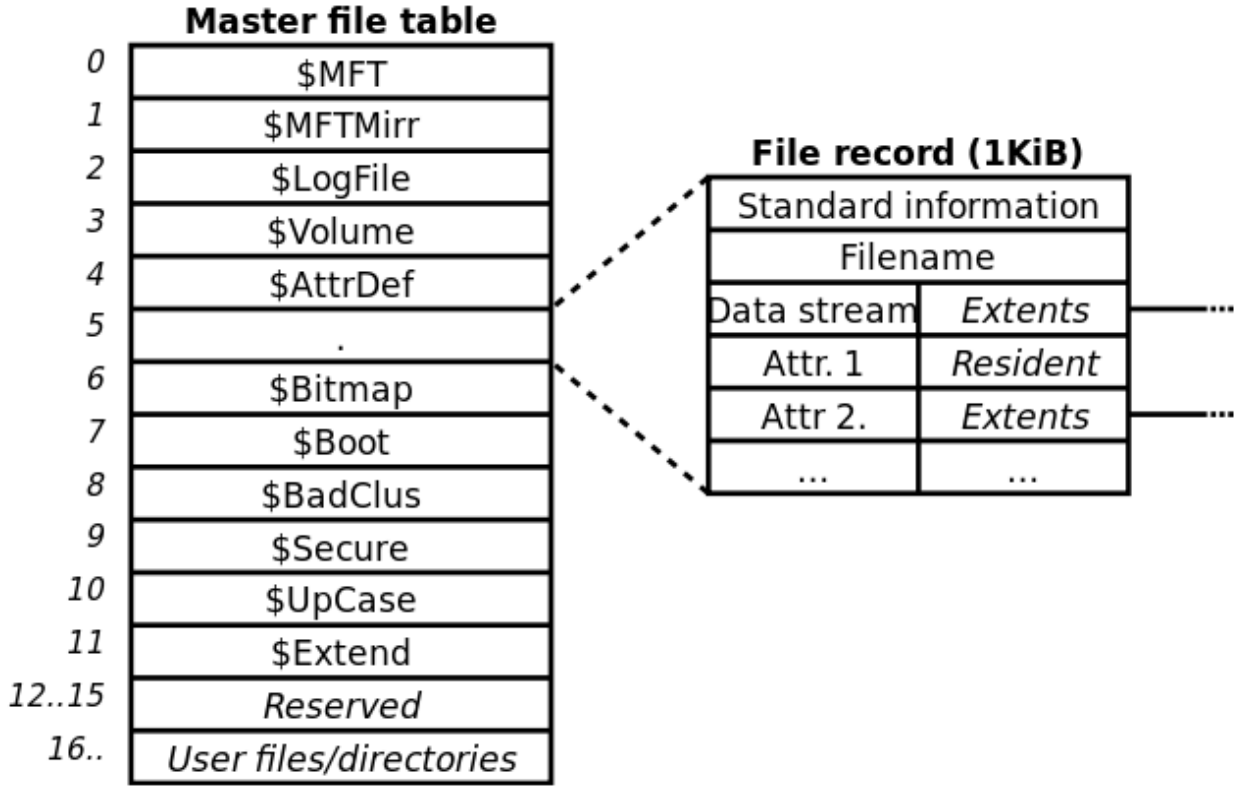
NTFS

Svar från föreläsningar.

New Technology File System.

NTFS Volume Layout





Baseras på "lazy writes" - data skrivs när det behövs. Använder logging. Har stöd för backup / redundanta systemdata. Ingen area är reserverad för systemet - hela partitionen finns för data. Använder metadata-filer som börjar med "$". Dessa ska bara kunna läsas av operativsystemet. Tabellen $MFT (Master File table) kan bli upp till 13.5% av diskens storlek. MFTn har en rad för

varje fil på systemet.

Utvecklades under 1990-talet, men är fortfarande det dominerande filsystemet för Microsofts plattformar. Likt Linux-baserade filsystem så är allt en fil.

En kopia av $MFT finns i $MFTMIRR - men den är inte komplett. Den innehåller ungefär så mycket så att man kan starta datorn.

Maximal filstorlek är 16 TiB (16EiB teoretiskt). Filer av 256 bytes eller mindre sparas direkt i MFTn. Tillåter partitioner som är 256 TiB.

Om filer exporteras från en datorn med NTFS till ett USB-minne så finns fortfarande stöd för rättigheter. Om det är ett annat filsystem så som EXT så försvinner denna data.

Vissa små filer sparas direkt i MFTn. Dessa kan ibland återskapas enkelt då enbart pekaren till filen finns kvar. Filer kan även finnas i slack space.

FAT16, FAT32, exFAT

Svar från föreläsningar.

File Allocation Table. Användes i DOS. Så gott som samtliga Windows-versioner har fortfarande stöd för FAT.

Används idag främst i små enheter, routrar, kameror m.m - det är enkelt och kräver inte mycket av systemet.

Tabellen i sig håller koll på vilka block som hör ihop till ett eller flera kluster. När disken börjar bli full kan tabellen behöva de-fragmenteras. På så vis placeras rader nära varandra och tomma block samlas.

Det finns 16 bitar i adressen för FAT16 och 32 för FAT32. Vissa bitar används för olika anledningar.

Först i disken (block noll, cylinder noll, sektor noll) finns *Master Boot Record* (MBR). Efter MBR finns *Boot Record* (BR). Efter BR finns FAT-tabellen (med ev. kopior).

Data som bevis

Svar från föreläsningar.

När man gör en fullständig dumpning av en hårddisk används antingen s.k. *e0* eller *dd*. För dd gör man en checksumma på hela disken. Filer man tar ut ur kopior hashas och kan sparas i databaser för exempelvis BP. Det går även att jämföra filer med vanliga system för att exkludera standardfiler. Man använder alltså checksummor för att slippa se viss känslig data och för att visa att filen inte förändrats från källan. En e0-kopia innehåller hashsummor från filsystemet, men vanligtvis använder man dd utöver detta.

"Chain of custody" är viktigt - man ska kunna verifiera att data inte ändrats från det att den extraherades. Man bör veta vilka som har haft tillgång till materialet, vilka som arbetat med det. Man bör även ha koll på tidpunkter då datan skapades, användes och extraherades.

Metadata

Svar från föreläsningar.

Data om datan. Kan vara saker så som när ett dokument ändrats, skapats, visats etc. Det finns filer så som **.lnk** och **.spl** som innehåller metadata.

En fil finns på många olika sätt. Den kan ligga i disken, vara borttagen, vara skickad som mejl. En bild kan ha ursprung i en RAW-fil, men konverterats till JPEG. Det kan finnas temporära verioner av filen, backup etc. Detta gör att vi kan hitta variationer, versioner och återskapa filer.

Metadata för filer inkluderar *MAC* - modified, accessed, created. Frågor man får ställa sig är om tidstämpeln är inodens ändringsdatum eller filens. Annan metadata inkluderar eventuella program som använts (så som PDF). För bilder finns EXIF som kan innehålla kamera, objektiv, slutartid, färgdjup, GPS-koordinater m.m. Word-filer kan innehålla vem som har skapat filen, ändringar m.m. Gamla versioner hade till och med MAC-adresser lagrade. Filer kan spara dess ursprung så som URL.

Ljudfiler kan ha album, spårlängd, spårnummer m.m.

Thumbs.db

Används generellt i Windows. Finns många olika versioner av filen. Filen underlättar för användaren. Sparar förhandsgranskning (thumbnails) för filer i varje mapp. Bilder i Thumbs.db försvinner kanske inte när bilden i sig tas bort. I nyare versioner finns filer i %Application data%/Explorer/.

Windows Registry

Svar från föreläsningar

Ansvarar för användarinformation för nyligen inloggade användare, samt systeminformation. Sparas i registry-filer - applikationsinformation, speciella användarpreferenser och hårdvarukonfigurationer. Alltid i minnet. Allt som sker på datorn sparas.

Vissa delar tillhör "running config" och ser inte likadan ut för ett körande system och ett system i vila.

Filerna är SYSTEM.DAT, USER.DAT (NTUSER.DAT), SAM, SECURITY.DAT.

Varje användare har en USER.DAT. Finns i C:\%windows%\Profiles\%user%.

Hives

- HKEY_LOCAL_MACHINE
- HKEY_CLASSES_ROOT
    - Innehåller information som behövs för att starta en applikation
    - Associationer mellan filer och applikationer
    - Namn på diskar
    - Ikoner och filtyper
- HKEY_CURRENT_CONFIG
- HKEY_DYN_DATA

    - Nuvarande state - enbart i minnet
- HKEY_USERS
    - Default user settings
    - Vem som är inloggad
    - Bakgrund och andra preferenser
- HKEY_CURRENT_USER
    - Som HKEY_USERS fast med vissa förändringar

Varje hive delas upp i nycklar och undernycklar. Hive -> key -> sub-key -> value. Det finns olika värden så som DWORD.

Processer

Svar från föreläsningar.

Den första processen som startas i Linux är `systemd` eller `initd`. Den låser upp kerneln och kör den.

Metadata för processer inkluderar namn på process, startadress i minnet, PID, UID (user id), SID (security id - ibland), PPID (parent PID).

I Windows finns processen `svchost.exe`. Processen har med massvis att göra - nätverk, minneshantering etc.

Processer är volatila. Spår finns enbart i minnet.

Processverktyg

```
TaskManager
tasklist /v
# PStools
PSlist
# PSTools (visar mer information)
pslist -x
# PSTools (visar trädvy)
pslist -t
# sysinternals
Listdlls
# sysinternals
handle
```

Metoder

Live Forensic

Svar från föreläsningar.

Med Live Forensic menas analys av ett körande system. Väldigt viktigt för att säkra volatila bevis som körande processer, nätverksanslutningar, systemtid, inloggade användare, kommandohistorik etc.

Static Forensic

Svar från föreläsningar.

Med Static Forensic menas analys av ett system eller en komponent i vila - så som en hårddisk. Här kan man extrahera icke-volatil data så som filer, delar av registret, email, swap-filer, använda USB-enheter etc.

Network Forensic

Svar från föreläsningar.

Med Network Forensic menas analys av nätverk. Vanligtvis består detta av övervakad data i ett nätverk där man kan hitta vilka enheter som kommunicerar med varandra och vilken data dessa skickar. Det går att hitta vilka enheter som tillhör en IP-adress, vilka sidor som besöks m.m.

Cloud Forensic

Svar från föreläsningar.

Det finns flera dimensioner av problemet. Dels juridiska problem - man kan få tillgång till en VM genom domslut, men hur ska man gå till väga vid analys av hosten? Dumpar man minne får man ju tillgång till alla gäster på systemet, vilket inte är önskvärt.

Ett annat problem kan vara stora nätverk där det är många VMs som används i en tjänst. De ser likadana ut och fungerar på samma sätt. Om en blir hackad, hur utför man en analys? Vilken fysisk maskin kör den virtuella maskinen? Svårt att veta vart saker körs.

När man arbetar med VM kan man ta en snapshot och klona VM:en. Man kan sidan göra om disken och arbeta med den genom att använda traditionella verktyg.

Efter GDPR har vissa implementerat "One Button Take Out" som innebär att ett företag enkelt kan lämna en molntjänst så som IBM.

Vidare körs vissa tjänster som containrar.

Tillvägagångssätt

Svar från föreläsningar.

Observera att ordningen är något tvetydig.

1. Collection - samla in data från mobiler, SIM-kort etc.
2. Carving - hitta borttagna filer etc.
3. Harvesting - leta efter saker som är lätt att hitta
4. Reduction - ta bort kända filer / rensa upp
5. Identification - identifiera insamlad data
6. Acquisition - extrahera data från enheter
7. Reconstruction - återskapa data från borttagna filer, slack space etc.

8. Preservation - se till att bevisen är säkrade (säkra integritet)
9. Examination and Analysis - sök, filtrera, examinera
10. Time Analysis - bygg upp en tidslinje över bevis
11. Recover - Säkerställ att enheten fungerar som tidigare om den infekterats
12. Reporting - dokumentera bevisen

Rapportskrivning

Svar från föreläsningar / gästföreläsning.

Se seperat dokument angående detta.

Tre nyckelpunkter

- Objektivitet / ingen brottsrubricering
- Lättförståelig / anpassad till läsaren
- Utförlig analys, men ändå relevant

Struktur

Fetstilt är viktigt, kursivt mindre viktigt.

Det är ingen "C-uppsats" - det är kort och sammanfattande.

- **Inledande uppgifter**
  - Kan vara i punktform
  - Undersökning behärd av
  - Anledning till undersökningen
  - Handläggare / medundersökare
  - Plats och tider för undersökningen
  - Övrig information
- **Sammanfattning**
  - En tredjedel av en A4 att sammanfatta en hel undersökning, men kan vara så kort som "vid undersökningstillfället har ingen lagrad information påträffats som anses vara av intresse för aktuell utredning" eller liknande
- *Innehållsförteckning*
- *Bakgrundsuppgifter*
- **Beskrivning av material**
  - Vad är det som undersöks, en stationär dator, vilken (serienummer etc.)?
  - Vissa bevis förstörs då de saknar koppling till fallet
  - Kan vara bilder på datorn (med serienummer)
- **Iakttagelser och undersökningar**
  - Enda stället man kan vara teknisk. Förklara IT-termer (kan göras med fotnot)
  - "hash" har olika betydelser beroende på åhörare - MD5 eller gräs - ett digitalt fingeravtryck
  - EXIF-data säger inte mycket - en karta kan hjälpa visualisera
  - "Rå information"
  - Kan innehålla skärmdumpar. Markera viktiga delar

    - Historik etc. kan komma i appendix
    - "**Användaren** av datorn gjorde A" - inte misstänkt
- **Analys och slutsats**
    - Innehåller inte särskilt mycket. Forensiker kan komma att bli tillfrågade att presentera allt som hittats och då kommer ytterligare presentationer ändå
    - Sy ihop undersökningen, använd specialistkompetens, använd värdeord (se nedan)
    - Fanns inget av intresse - ta inte med denna punkt - finns istället i sammfattningen
- Materialförteckning
    - Vad har undersökts?
    - Materialmärkning (internt nummer), beslagsnummer, benämning (mobiltelefon, dator), datum och tid för beslag, vem som tog objektet i beslag
    - I Sverige attackeras inte Chain of Custody, men i andra länder förekommer det. Men det är viktigt att tänka på ändå
    - Måste vara noggrant
- *"Undersökningsmetoder"*
    - Metoden ska förklaras, men allt måste inte förklaras. Ibland vill man "inte utbilda kriminella" för hur man gör saker
    - Bevissäkring av hårddisk och hashning ska vara med
    - Kan beskriva hur materialet handskats

Modus Operandi

Svar från föreläsningar.

Tillvägagångssätt / beteende - hur en gärningsman handlar.

Kan bestå av hur personen uttrycker sig, vilka metoder de använder och hur de avser tjäna pengar.