

# Anteckningar Forensik

---

## Akronymer

---

**EBM** = Ekobrottsmyndigheten. Har statsåklagare, forensiker m.m.

**HTA/HTÖ** = Hemlig tele-avlyssning / hemlig tele-övervakning

## Litteratur

---

<https://www.linuxleo.com/Docs/linuxintro-LEFE-4.33.pdf>

## Introduktion

---

### Arbetssätt

1. Preservation
2. Collection
3. Identification
4. Analysis
5. Interpretation
6. Documentation
7. Presentation

*Live forensic* innebär att man undersöker direkt mot ett körande system. *Static forensic* är en "död maskin" - avstängda enheter.

Att föra dagbok är viktigt för att anteckna minnen och tillvägagångssätt. Använd mindmaps.

### Aktörer

Polisen, försvaret, bank, revision, forskning och IT-säkerhets-personal arbetar med Computer Forensics (CF)

Polisen jobbar för:

1. Brottsmål
2. Binda till händelse / kedja av bevis
3. Fria / fälla

### Digitala bevis (CF)

- Vilka spår har vi?
- Hur kan dessa spår hittas?
- Hur kan dessa spår bevaras?
- Hur skall bevis tolkas?

- Vilket bevisvärde har spåren?
- Hur presenteras bevisen för (ofta ej tekniskt kunniga) beslutsfattare?
- Rapportering / dokumentation?

### **Kunskap som inkluderas innefattar**

- Telekommunikation
- Datakommunikation
- Datorsäkerhet
- Informationsäkerhet
- Log-analys
- Network & systems analysis
- Juridik
- Kriminologi
  - Modus operandi (MO)
  - Bedrägeri
  - Våldbrott
- Andra områden som undersökningen leder till

## **Digitala spår**

Data som lagrats och/eller överförts med tillhörande metadata.

### **Lagringsmedia**

- Hårddiskar
- Minneskort
- USB-minnen
- CD/DVD-skivor
- Magnetband

### **Kommunikationssystem**

- Router
- Telefonväxlar
- IoT
- Kameror
- Vitvaror
- Bilar

### **Överflödig data**

- Nycklar till bilar innehåller chip - vem körde senast?
- RFID - vilken lift åkte skidåkaren?
- Automatisk trängselskatt för bilar

## **Digitala fragment**

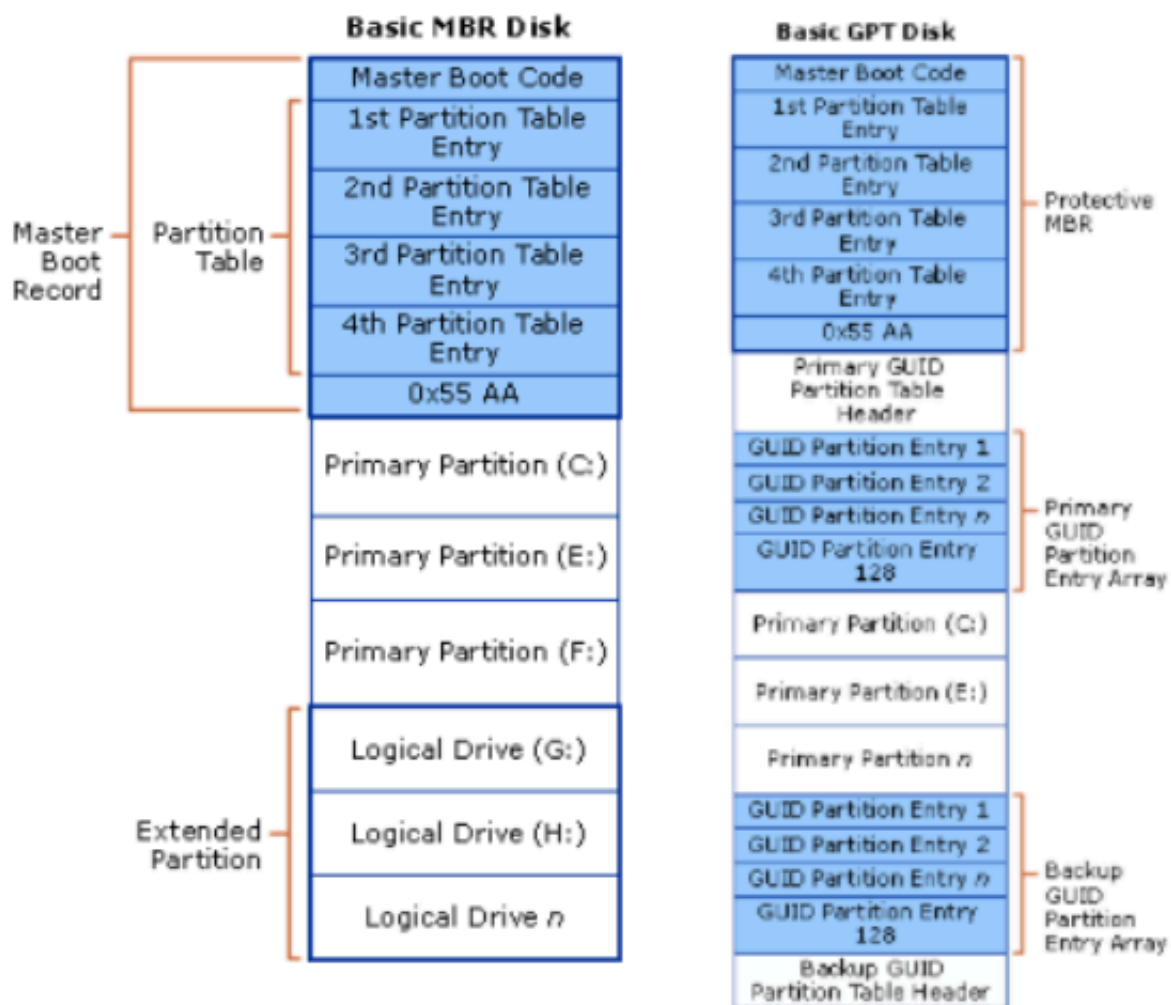
Att översätta "ettor och nollor" till något förståeligt. Det finns idag ingen standard för att samverka mellan länder / enheter. Pusselbitar kan lätt fördärras vid en oförsiktig hantering.

## Filsystem

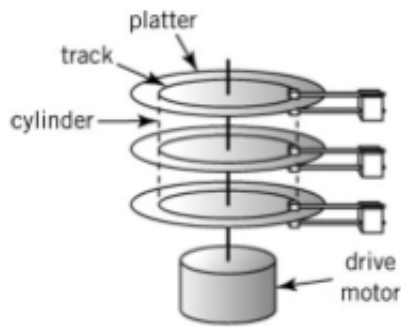
Filsystems uppgift är att lagra data. Olika operativsystem har olika tillvägagångssätt och sparar olika metadata. De flesta filsystem har en hierkisk princip. Andra har grafer eller strömmar. Man brukar ha metoder för att skapa, läsa, modifiera, ta bort och flytta data.

## Partitioner

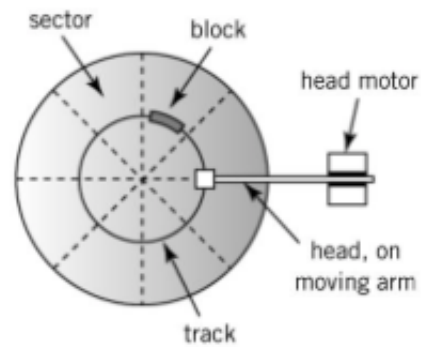
Master Boot Record (MBR), GUID Partition Table (GPT). MBR har fyra partitioner och 2TB maxstorlek. GPT är det moderna systemet med upp till 128 partitioner. Partitionstyperna kan ha stöd för *basic disk storage* och *dynamic disk storage* där man eventuellt kan expandera partitionen "on-the-fly". Dynamic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



## Hårddisk



Englander: The Architecture of Computer Hardware and Systems Software, 2nd edition  
Chapter 9, Figure 09-02



En hårddisk består av cylindrar. Varje cylinder har ett läs-/skrivhuvud. Dessa cylindrar roterar runt och huvudena rör sig fram och tillbaka längs med raden av cylinderna. När data läses så läses den i block. Ett blocks storlek varierar.

## SSD

Emulerar en HDD.

Transistorer som har olika nivåer av ström. Nivåerna delas in i ett antal värden som tolkas som bitar.

## FAT

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-fracteras. På så vis placeras rader nära varandra och tomma block samlas.

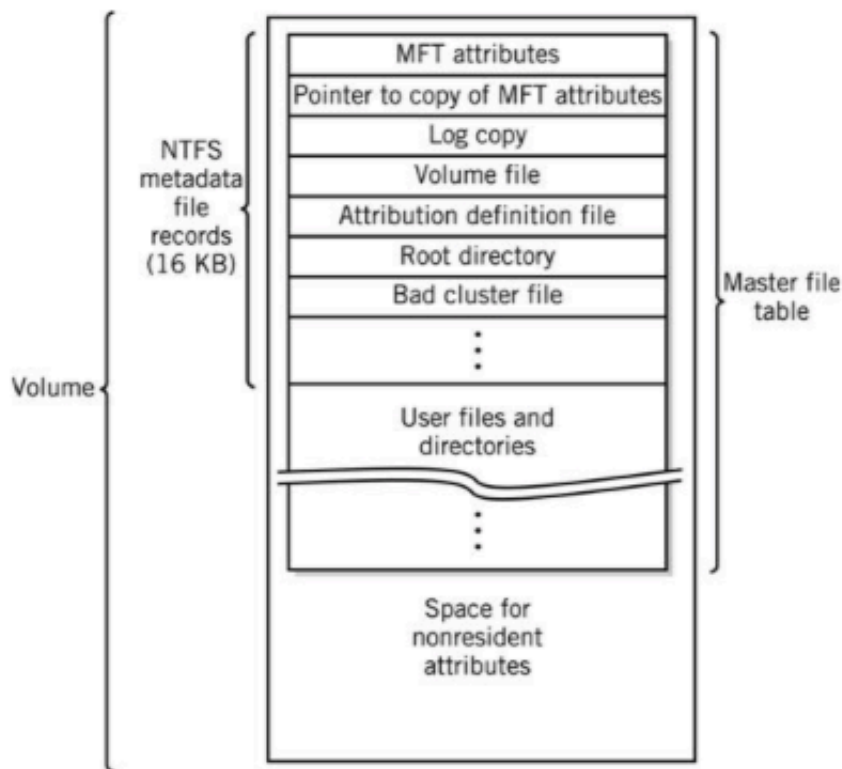
### FAT 16

Det finns 16 bitar i adressen. Vissa bitar används för olika anledningar.

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

## NTFS

# NTFS Volume Layout



Master file table	
0	\$MFT
1	\$MFTMirr
2	\$LogFile
3	\$Volume
4	\$AttrDef
5	.
6	\$Bitmap
7	\$Boot
8	\$BadClus
9	\$Secure
10	\$UpCase
11	\$Extend
12..15	Reserved
16..	User files/directories

File record (1KiB)	
Standard information	
Filename	
Data stream	Extents
Attr. 1	Resident
Attr 2.	Extents
...	...

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.

## Data som bevis

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 hashsummer från filsystemet, men vanligtvis använder man *dd* utöver detta.

## RAID

Redundant Array of Inexpensive Disks / Redundant Array of Independent Disks.

Koppla ihop flera diskar för att förbättra prestanda eller driftsäkerhet.

### RAID 0

Striped. Sätt ihop diskar logiskt för att få en större disk. Data skrivs till diskarna i tur och ordning. Block A hamnar på disk 1, B på disk 2, C på disk 3 o.s.v.

### RAID 1

Mirroring. Används för redundans. Två diskar innehåller samma sak.

### RAID 0+1

Använder fyra diskar. Två par av redundanta diskar.

### RAID 5

Använder fem diskar, minst tre måste användas. För ett block används fyra diskar för raid 0, en disk för paritet. Med den datan kan man återskapa en disk om den går förlorad.

## Verktyg

---

1. Sysinternals
2. Top view
3. Proc view
4. dd (viktig - behöver hashas vid sidan om)
5. f0 (viktig - som dd fast allt är hashat automatiskt)
6. Autopsy
7. The Coroner's Toolkit (TCT)
8. Penguin Sleuth kit

9. Helix tools
10. Nessus
11. nasl
12. nmap
13. nikto
14. hping
15. aircrack
16. aircrack-ng
17. airtraf
18. network miner
19. ncase
20. fdk
21. mobile edit
22. samedump2
23. hashcat
24. jack the ripper
25. Cain & Abel (password recovery)
26. DEFT (DFIR toolkit)
27. CAINE
28. <https://futureboy.us/stegano/decinput.html>

## Redovisning av en IT-undersökning

---

Skriv som om du skriver för barn. Använd inte avancerade tekniska ord. De som läser rapporten är inte specialister. Det blir inte trovärdigt om ingen förstår texten.

- Brottrubricera inte
- Skriv endast om ändamål eller uppdrag som givits
- Innehåll ska inte gå att misstolka
- Om information av övrigt intresse hittas, sparas den i "slasken"
- Sammanfattningen ska vara kort och lättläst (ej IP-adresser, referenser etc.)
- Var objektiv - hitta både saker som talar för och mot
- Vad grundar du synpunkterna på?
- Hur vet du det?
- Om du hittar ett "spår" - kör hela spåret fullt ut (så som vid en tidpunkt). Blanda inte analyser

## Metadata

---

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.

## 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/.

## Steganografi - Data Hiding

---

"Steganos" - dold, "graphia" - "writing" - Covered Writing. Men vi använder flera olika media.

Exempel kan vara text i text - göm ett meddelande i första tecknet på varje ord.

**A**lla **n**io **d**uvor **e**rtappades **r**ökandes **s**oyaplantor

Andra exempel är att gömma data i alpha-kanalen för bilder, använda modifierade färpaletter för bilder etc. Kända exempel är covert channels, color palette modification, formatting modification, data appending, word substitution, encoding algorithm modification etc.

Exempel på verktyg är OutGuess, Steganography Tools, Invisible Secrets, Information Hiding Homepage, Steg Detect, StegoArchive, <https://futureboy.us/stegano/decinput.html>.

## Windows Registry

---

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.

## Windows Forensics

---

Det finns volatil och ej volatil data. Registret består av båda typer. Det är mycket viktigt att man säkrar de volatila filerna.

### SID

Ett unikt värde för varje användare.

Ett värde som slutar på...

- 500 tillhör admin
- 501 tillhör guest
- 1001 tillhör första användarkontot
- 1002 tillhör andra användarkontot
- ...

### DLL sökväg (DLL hijacking)

1. Samma mapp som EXE
2. PATH-variabeln
3. System

### Volatilt

- Systemtid
- Inloggade användare
- Nätverksinformation
- Nätversstatus
- Kommandhistorik
- etc.

Så fort man kommer åt en enhet så sparar man nuvarande tidszon etc. Alla bevis och tidsramar bygger på lokal tid. Använd inte GUI - alltid CMD i bakgrunden. En dator kan vara hackad och logga tangentbordet. Använd pålitliga verktyg.

### Datum och tid

```
1 # Systemtid
2 date /t & time /t
3 # Innehåller starttid och sessioner till datorn
4 net statistics server
5 net statistics workstation
```

### Användare

```
1 #Från pstools
2 PsLoggedOn
3 net sessions
4 # Från sysinternals
5 LogonSessions
```

## Öppna filer

```
1 # Från pstools
2 openfiles
3 # Från pstools
4 psfile
5 net file
```

## Nätverksverktyg

```
1 ipconfig /all
2 arp -a
3 # Network connections
4 netstat -r
5 netstat -ano
```

## Processverktyg

```
1 TaskManager
2 tasklist /v
3 # PStools
4 PSlist
5 # PSTools (visar mer information)
6 pslist -x
7 # PSTools (visar trädvy)
8 pslist -t
9 # sysinternals
10 Listdlls
11 # sysinternals
12 handle
```

Vidare verktyg för att dumpa minne för en process inkluderar Process Explorer, FTK Imager och Belkasoft RAM Capturer. Winpmem (Rekall forensic suite, full dump, aff4), PMDump, ProcDump, Process Dumper.

## Services, User accounts, volumes etc

```
1 wmic service list
2 wmic service list brief
3 wmic useraccount list
4 wmic volume list
5 wmic sysaccount list
```

```
1 # Hämta hem körda kommandon
2 doskey /history
```

```
1 reg export
2 regedit
```

För pstools kan man använda `--accepteula` för att godkänna EULA som annars öppnas i popup.

## Icke-volatilt

- Filer
- Registret
- Email
- Swap-filer
- USB-enheter
- etc.

Last access time. Kan stängas av med

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate` och `fsutil`.

Swap (Page) file: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`.

Wireless network password: `netsh wlan show profile` `netsh wlan show profile name=SSID key=clear`.

USB devices `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR`  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses`.

Nyligen körda filer sparas i `C:\Windows\Prefetch` som `.pf`-filer. Kan öppnas med NirSoft prefetch viewer. Innehåller saker så som använda DLLer, när det användes etc.

## Lösenordshantering

Windows lagrar lösenord som två olika hash. Lösenordet skickas till processen lsass. Processen jämför hashet med ett lagrat i SAM-filen. Processen lagrar även lösenordet krypterat i minnet för att kunna använda lösenordet igen utan att skriva in det varje gång.

Processen sparar lösenordet i minnet även om en användare loggar ut. Ibland används hashet som lösenord. Om man extraherar detta från minnet kan man använda det för att skicka vidare i en så kallad "pass the hash"-attack.

Använd process-viewer (sysinternals) för att dumpa minnet för lsass. Använd mimikatz för att extrahera lösenord.

```
1 mimikatz# sekurlsa::minidump lsass.dmp
2 mimikatz# sekurlsa::logonpasswords
```

## Övrigt

<https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf>

## Windows-processer

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).

Processen `svchost.exe` har med massvis att göra - nätverk, minneshantering etc.

För processer jämför man en användares SIDs med processens. Om en användare inte har SIDn som används i processen som startats av användaren är det en anomali. Antagligen har processen fått ett högre privilegium än användaren.

## Volatility

```
1 # Hitta typ av minne (profile). Anges i ordning av sannolikhet
2 volatility -f Win7.raw imageinfo
3
4 # Hitta processträdet
5 volaitlity -f Win7.raw --profile [profile] pstree
6
7 # Leta efter processer som söker genom
8 volatility -f Win7.raw --profile [profile] psscan winlogon.exe
9
10 # Leta efter processer som har med nätverk att göra
11 volatility -f Win7.raw --profile [profile] netscan
12
13 # Leta efter SIDs och deras koppling till processer
14 volatility -f Win7.raw --profile [profile] getsids
15
16 # Leta efter processer som körde kommandon (möjlig inväg vid attack)
17 volatility -f Win7.raw --profile [profile] cmdscan
18
19 # Third Party-modul. Hitta kommandon som kördes
20 volatility -f Win7.raw --profile [profile] cmdline -p [PID]
21
22 # List DLLs and paths
23 volatility -f Win7.raw --profile [profile] dlllist
24
```

```
25 # Dump a process
26 volatility -f Win7.raw --profile [profile] procdump -p [PID] -D [output-
    folder]
27
28 # Dump a process's memory
29 volatility -f Win7.raw --profile [profile] memdump -p [PID] -D [output-
    folder]
```

Om volatiltiy inte hittar någon starting point (No PAE), så misslyckades sannolikt analysen. Antagligen skapades minnesfilen på ett felaktigt sätt.

Om en process inte har en PPID är det sannolikt rot-processen eller en abnormalitet.

Vissa virus modifierar datan i processträdet genom att plocka bort fält så som processnamn. Vissa parent-processer tar bort namnet för child-processer. Man kan använda `psscan` för att försöka återuppbygga datan. Avsaknad av namn ersätts med namnet för parent processes.

För att se om en process är legitim (exempelvis om namnet är "chrome.exe") bör man se till PPID.

## Incident response

---

1. Preperation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow up - lessons learned

## Android Forensics

---

- Collection - samla in data från mobiler, SIM-kort etc.
- Harvesting - leta efter saker som är lätt att hitta
- Reduction - ta bort kända filer / rensa upp
- Identification - identifiera insamlad data
- Acquisition - extrahera data från enheter
- Preservation - se till att bevisen är säkrade (säkra integritet)
- Examination and Analysis - sök, filtrera, examinera
- Reporting - dokumentera bevisen

## Intressepunkter

- Bilder
- Kontakter
- SMS / MMS
- Filmer
- GPS-koordinater för bilder / filmer
- Applikationer (Skype etc.)
- Samtalshistorik

# Anti-forensics

---

Man kan förstöra data, gömma data eller gör andra förebyggande åtgärder för att hindra forensiska undersökningar.

- Data hiding
- Artifact wiping
- Trail obfuscation
- Attack against CF tools / processes

## Browser forensics

---

Webbläsare sparar olika saker. De använder inte samma tidsstämplar. De brukar alla använda UTC. Internet Explorer använder 1601-01-01, Firefox 1970-01-01, Chrome 1601-01-01, Safari 2001-01-01 och Opera 1970-01-01 som start för epoken.

De brukar spara data i Windows registry - typed URLs, historik m.m.

## Recycler.bin

---

Papperskorgen skiljer sig mellan olika filsystem. UNIX har ett användarsystem, Windows har NTFS och FAT. I FAT finns inga ägare - de delar papperskorg. De har olika namn på "mappen". I NTFS finns en fil, INFO2 som innehåller användarens SID. På så vis kan bara ägaren återställa en fil i papperskorgen. Endast användaren Backup kan ändra rättigheter. Recycler.bin finns normalt i roten på filsystemet för NTFS. För FAT heter den RECYCLER.

## Web

---

Att "tröska" genom mängder av webbdata är mycket svårt. Det finns verktyg så som "website archive", "website watcher" och "archive.org" som kan arkivera eller visa arkiv av webbsidor. Website watcher automatiserar / "spindlar" en webbsida för att extrahera data över tid. Kan användas för att leta stulet gods etc.

## Cloud Forensics

---

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 kлона VM:en. Man kan sedan 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.

## Inför tentamen

---

**Notera:** se "Example Exam.pdf" på GitHub.

Frågor är kunskapsfrågor - kan du den här termen? En annan typ är utredande - förklara / diskutera vad static forensic är.

Uppgifter med höga poäng även besvaras med mycket text.

## Filer

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 versioner 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 tidsstämpeln 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.

## Metoder

---

- Live forensic
- Static forensic
- Network forensic
- Cloud forensic

Kunna diskutera och placera följande metodik i ordning.

1. Time analysis
2. Harvesting
3. Reconstruction
4. Reduction
5. Carving
6. Preservation
7. Recovery
8. Report
9. Analysis

## Rapport

Tre nyckelpunkter

- Objektivitet / ingen brottsrubricering
- Lättförståelig / anpassad till läsaren

- Utförlig analys, men ändå relevant

## **Modus Operandi**

Tillvägagångssätt / beteende - hur en gärningsman handlar.

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