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. Analyis
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 tillvägagångsätt. 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

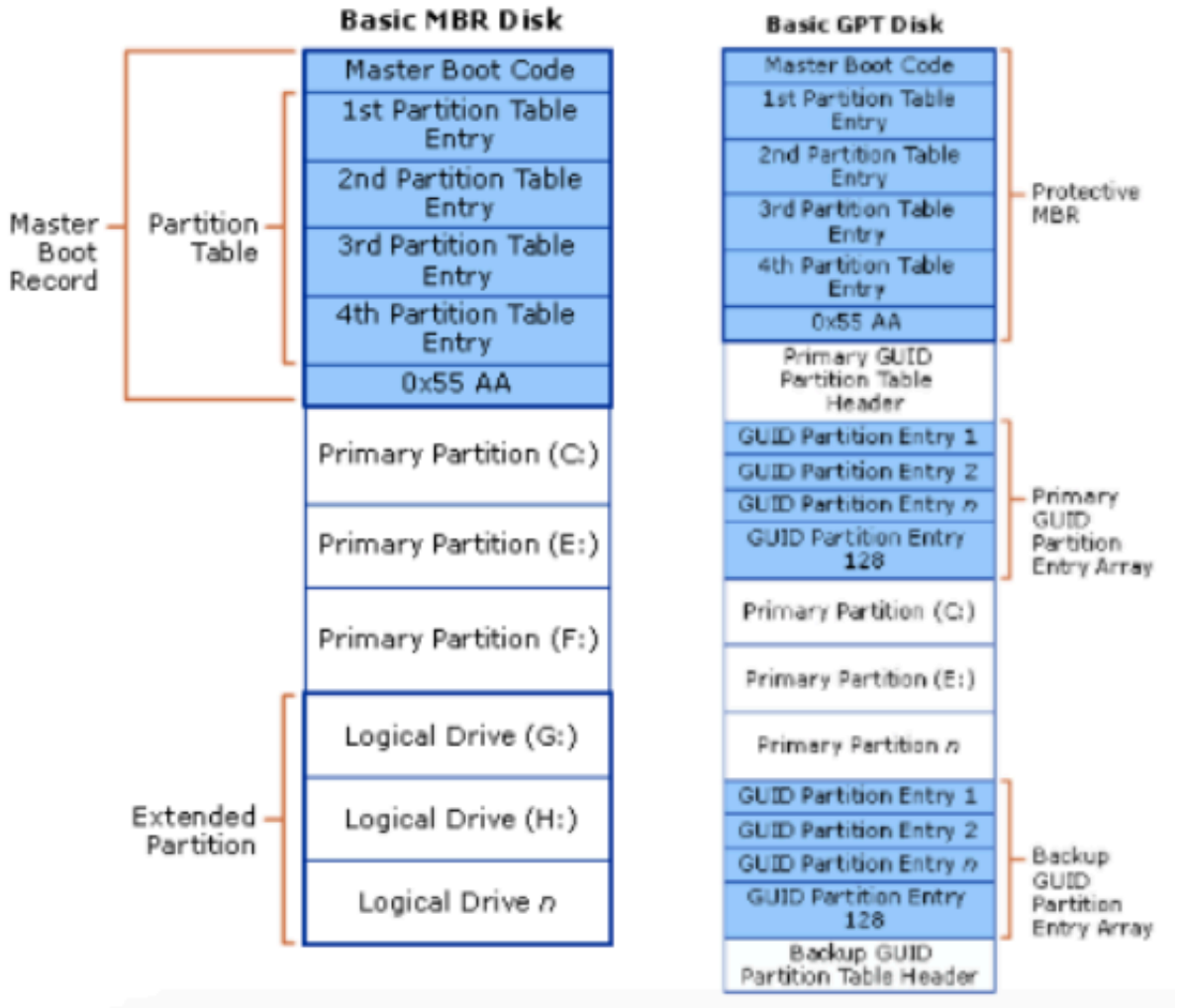
Att översätta "ettor och nollor" till något förståeligt. Det finns idag ingen standard för att samverka mellan länder / enheter. Pusselbitar kan lätt fördärvas vid en oförsiktig hantering.

Filsystem

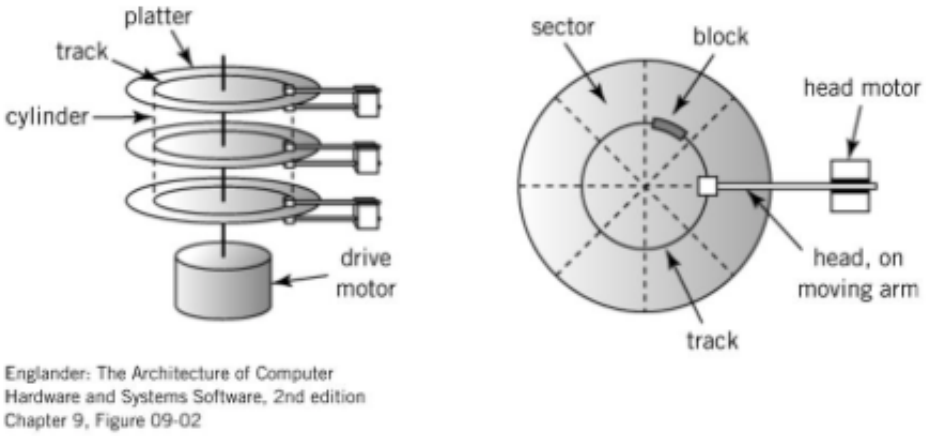
Filsystems uppgift är att lagra data. Olika operativsystem har olika tillvägagångsätt och sparar olika metadata. De flersta filsystem har en hierkisk princip. Andra har grafer eller strömmar. Man brukar ha metoder för att skapa, läsa, modifiera, ta bort och flytta data.

Partitioner

Master Boot Record (MBR), 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.



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 radien av cylinderna. När data läses så läses den i block. Ett blocks storlek varierar.

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

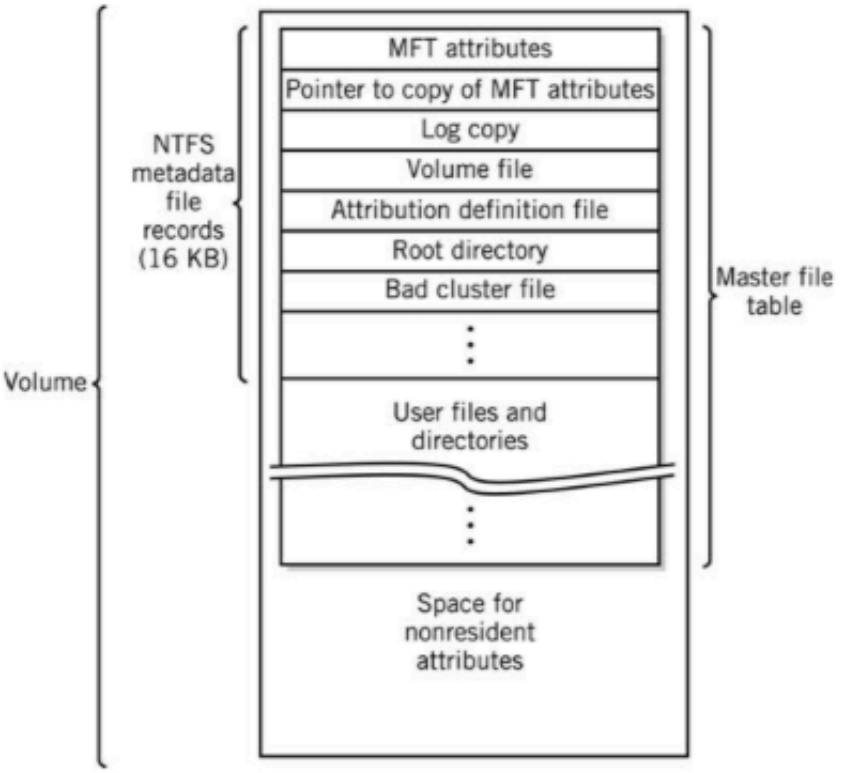
FAT 16

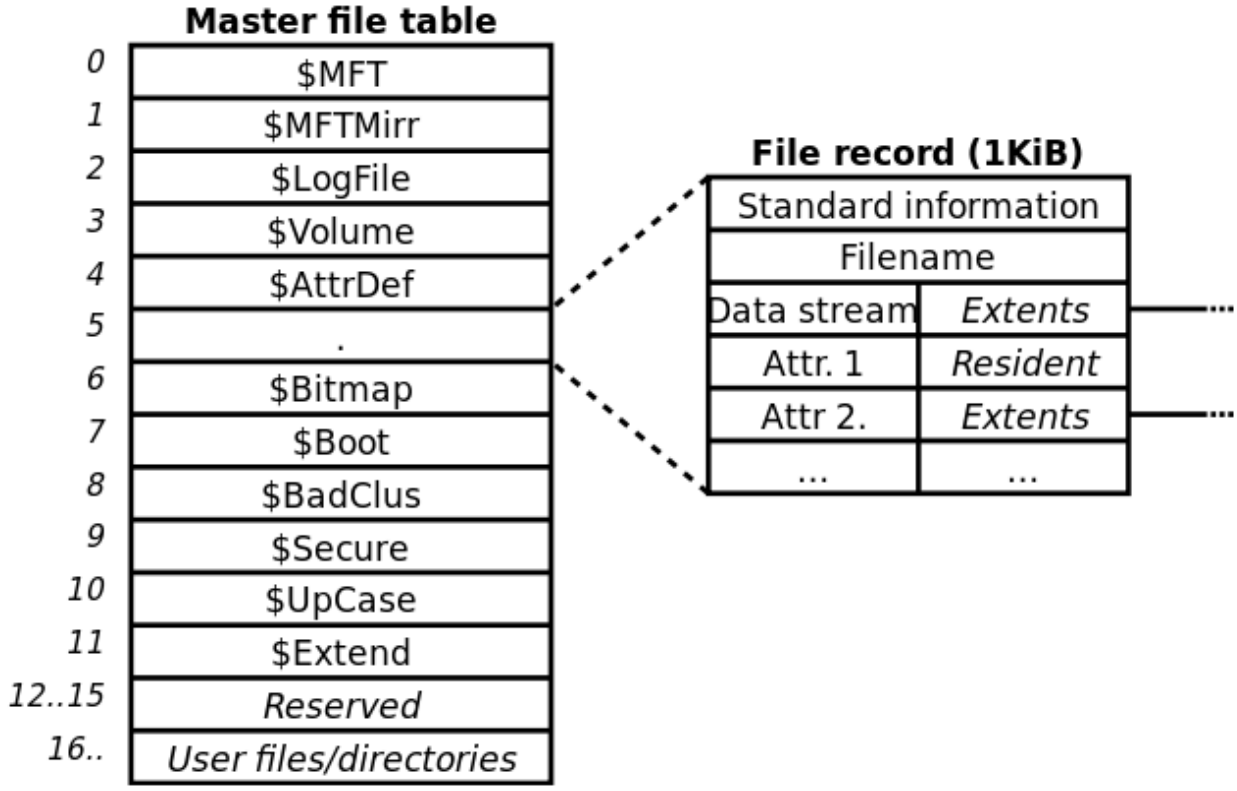
Det finns 16 bitar i adressen. Vissa bitar används för olika anledningar.

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





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 hashsummor från filsystemet, men vanligtvis använder man dd utöver detta.

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. airsnort
17. airtraf
18. network miner
19. ncase
20. fdk
21. mobile edit
22. samdump2
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

```
# Systemtid
date /t & time /t
# Innehåller starttid och sessioner till datorn
net statistics server
net statistics workstation
```

Användare

```
#Från pstools
PsLoggedOn
net sessions
# Från sysinternals
LogonSessions
```

Öppna filer

```
# Från pstools
openfiles
# Från pstools
psfile
net file
```

Nätverksverktyg

```
ipconfig /all
arp -a
# Network connections
netstat -r
netstat -ano
```

Processverktyg

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

```
wmic service list
wmic service list brief
wmic useraccount list
wmic volume list
wmic sysaccount list
```

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

```
reg export
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.

```
mimikatz# sekurlsa::minidump lsass.dmp
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.

Volatility

```
# Hitta typ av minne (profile). Anges i ordning av sannolikhet
volatility -f Win7.raw imageinfo

# Hitta processträdet
volaitlity -f Win7.raw --profile [profile] pstree

# Leta efter processer som söker genom
volatility -f Win7.raw --profile [profile] psscan winlogon.exe

# Leta efter processer som har med nätverk att göra
volatility -f Win7.raw --profile [profile] netscan
```

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 modiferar 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.