

# Anti-forensisk guide



<https://keybase.io/dotchloe>

[@dotchloe](#)

<b>Introduktion</b>	3
Vad är forensik och anti-forensik?	3
Logik och tankesätt	4
<b>Windows</b>	5
Det absolut viktigaste - Kryptering!	5
Stäng av Event-logging i Windows	5
Skanna med CCleaner+CCEnhancer automatiskt varje dag!	6
Stäng av swap!(eller rensa+kryptera), Hibernate och Shadow Copies	7
Ändra MACE på alla filer med Timestomp!	8
Bästa praktik för webbsurfande	9
Bästa praktik för wipe	10
PrivaZer - en extremt grundlig spårrensare	11
USBOblivion - Rensa alla spår av externa medium!	12
<b>Fysisk säkerhet</b>	13
Ha uppsikt över din dator!	13
Skydda BIOS!	14
Limma RAM-minnena med epoxy-lim	14
Var alltid beredd på att kunna bryta strömmen till datorn	16
Omöjliggör användning av DMA-portar	17
<b>Fysisk säkerhet - DMS och liknande skydd</b>	18
<b>Linux</b>	19
Bleachbit	19
secure-erase	19
cryptsetup	20
<b>Övriga operativsystem</b>	21
OS X	21
Android	21

# Introduktion

## Vad är forensik och anti-forensik?

IT-forensik handlar kort och gott om att säkra bevis - data som kan användas mot dig. Den kan visa att du begått ett brott eller en annan handling.

När man tänker på IT-forensik så är nog Polisen det första man får fram i huvudet men det är viktigt att komma ihåg att IT-forensik kan användas av alla - det kan vara en tjuv som snott din dator och vill nu få fram dina raderade nakenbilder eller en konkurrent som tagit din hårddisk för att få fram gamla mail.

Anti-forensik är helt enkelt motsatsen till forensik. Det anti-forensik går ut på är att ta bort, förhindra eller ändra potentiellt bevismaterial som kan användas mot dig. Anti-forensik kan användas både presumtivt och retroaktivt vilket innebär att man kan nyttja dess metoder innan och efter en utförd handling.

Anti-forensik är INTE olagligt i Sverige och är inte ett tecken på att man utför olagliga handlingar.

Det är vanligt att man inom anti-forensiken vill:

- Ta bort data
- Gömma data(kryptering, obfuskering m.m)
- Skapa falsk data

## **Logik och tankesätt**

Det finns en del frågor som man enskilt behöver svara på. Inte bara för att varje system och dator är unik men så är även dess användare. Det är därför viktigt att man själv noggrant kollar igenom de program man vill skydda. Oftast hittar man inställningar som man helst vill ändra, eller filer som skrivs som du vill få bort då de lämnar känsliga spår.

Något som är väldigt viktigt att veta är att du aldrig är skyldig till att tala om ditt lösenord till någon. Vi svenskar har den friheten att kunna kryptera vad vi vill utan några hinder. Så om du någon gång blir frågad att tala om ditt lösenord så säg att du glömt bort det eller liknande. Detta är ett bra tips eftersom det inte kan ge några direkta konsekvenser. Om du totalt nekar till att ge ut ditt lösenord så kan det anses som att du inte samarbetar så bäst är det helt enkelt att säga att du glömt bort lösenorden.

Anti-forensik, integritet och IT-säkerhet går väl hand i hand. Anti-forensik handlar om att ta bort sin data, integritet om att ha kontroll över sin data och IT-säkerhet om att skydda sin data så därför är det väldigt sunt att försöka uppnå ett integritetsvänligt och säkert system samtidigt som man följer denna guide. Ett exempel kan vara att vissa kommersiella program låter inte användaren att kontrollera sin data lika mycket, ett mer konkret exempel är Skype och µTorrent så om du använder dessa två bör du hitta alternativ. För mer integritetsvänliga alternativ vänligen konsultera följande sidor:

<https://www.privacytools.io/>

<https://prism-break.org/en/>

Det är alltså viktigt att du på egen hand kollar upp hur dina program fungerar. Desto mer program du använder ju större är risken att de kommer lämna ifrån sig data om dig. "less i more" helt enkelt. Denna guide kommer inte ge ett fulländat anti-forensisk skydd utan mycket är upp till användaren själv. Ett bra tips är att Googla till sig information om programmen du använder och ser om du kan stänga av loggningsfunktioner eller övriga integritetskränkande inställningar.

# Windows

## Det absolut viktigaste - Kryptering!

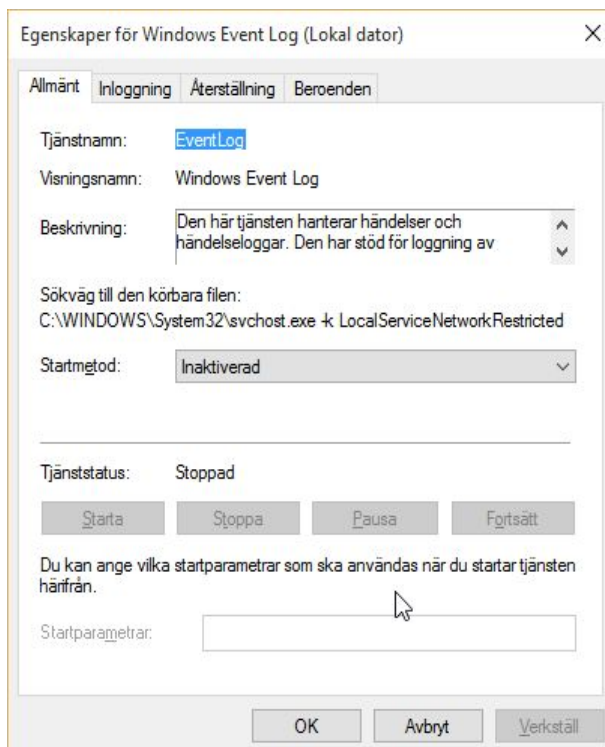
Denna guide kommer inte gå in på kryptering, utan helt enkelt säga att kryptering är ett måste. Bitlocker, Truecrypt, Filevault2 eller DM-crypt spelar ingen roll - kryptering är ett måste!

Försök att kryptera så mycket det går. VPN, HTTPS, 7z med lösenord, fulldiskkryptering, DNScrypt, GPG/PGP osv - Använd det!

Konspirationsteorier att X eller Y innehåller bakdörrar är inte av intresse i detta fall. Tankesättet ska alltid vara att din kryptering inte kommer att hålla och denna guide kommer lära dig hur du tar bort spår och hur du kan skydda din kryptering ytterligare.

## Stäng av Event-logging i Windows

Event-logs sparar massa händelser som hänt i Windows. Dessa har ofta inget värde men för en forensiker så kan de ge ledtrådar om vad som har hänt. Bäst är det att stänga av detta helt.



Tryck WIN+R och skriv **SERVICES.MSC**. Leta sedan upp "Windows Event Log" och dubbelklicka på den. Klicka sedan på knappen "Stoppa". Sedan måste du **välja** "Inaktiverad" från rullistan. Det ska se ut som bilden till vänster.

## **Skanna med CCleaner+CCEnhancer automatiskt varje dag!**

Först ladda ner och installera CCleaner här: <https://www.piriform.com/ccleaner/download/standard>

Efter installation så ska ni även installera CCEnhancer: <https://singularlabs.com/software/ccenhancer/>

Det är alltså viktigt att CCleaner har en STOR lista med saker som ska rensas och du SKA kryssa i precis ALLTINGförutom "wipe free space" för det tar lång tid att rensa. Har ni kommit så här långt så starta upp CMD som adminoch skriv:

```
SchTasks /Create /SC DAILY /TN "clean" /TR "%programfiles%\CCleaner\CCleaner.exe  
/AUTO" /ST 20:00 /RL HIGHEST
```

(Protip: skapa 3 schemalagda aktiviteter med 3 olika tidpunkter för att ha större risk att datorn är igång när schemat körs!)

(Protip2: Kör gärna med /SC onstart för att köra uppgiften i samband med start av operativsystemet!  
)

Vilket kommer spara en schemalagd aktivitet varje dag klockan 20:00. Absolut får ni ändra detta efter behov om ni så vill. Men jag rensar min dator varje dag klockan 20:00 för jag sitter vid den då. Skulle man inte sitta vid datorn så gör det inte så jättemycket då syftet med en schemalagd aktivitet är till så man inte råkat missa att utföra en uppgift.

Vilket kommer automatisk skanna och rensa er dator.

## Stäng av swap!(eller rensa+kryptera), Hibernate och Shadow Copies

Vi vill jättegärna stänga av swap-space eftersom där kan hittas väldigt mycket data som swappas ut ur RAM. page-filen anses ofta att vara en guldgruva för forensiker.

Dock kan det uppstå problem om man stänger av swap i Windows. Program och hela operativsystem kan stängas av helt utan förvarning i vissa kritiska fall. Har du dock mycket RAM (mer än 12) så är det ingen större fara. Jag rekommenderar dock starkt till att faktiskt stänga av swap i Windows.

Det är enkelt att stänga av swap, följ denna guide: [http://windows7themes.net/en-us/how-to- ...imization/](http://windows7themes.net/en-us/how-to-...imization/)

Men för er som verkligen har lite RAM så kommer här ett trick.

Man kan skriva över page-filen varje gång man stänger av datorn. Detta är inbyggt i Windows och ändras genom Regedit(Spara nedanstående innehåll i **file.reg** och dubbelklicka på den:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]
```

```
"ClearPageFileAtShutdown"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]
```

```
"NtfsEncryptPagingFile"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies]
```

```
"NtfsEncryptPagingFile"=dword:00000001
```

```
[HKEY_CURRENT_USER\System\CurrentControlSet\Policies]
```

```
"NtfsEncryptPagingFile"=-
```

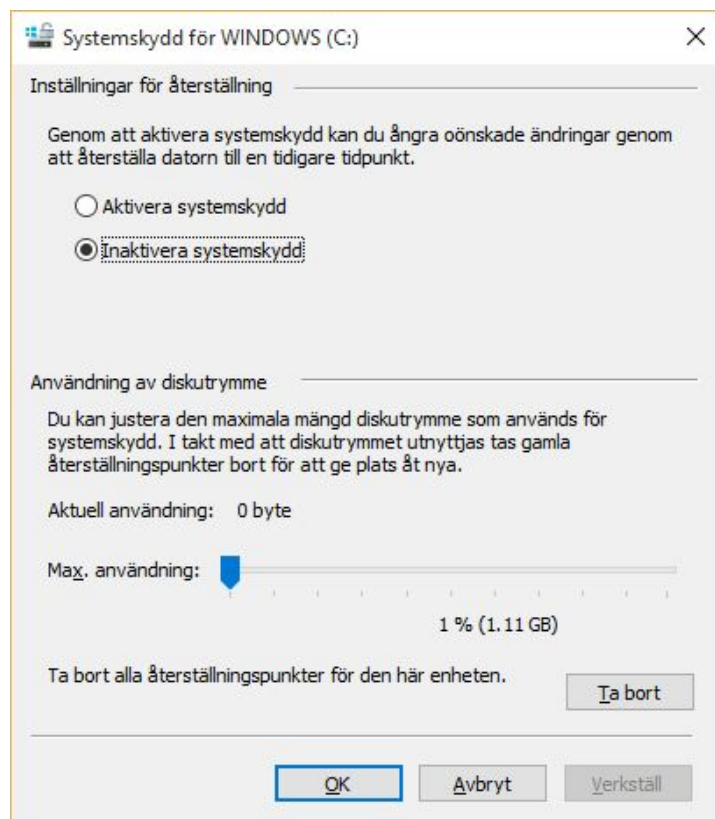
Detta kommer ändra så att Windows rensar page-filen varje gång du stänger av datorn. Så nedstängningen kan ta lite längre tid men är väldigt mycket värt det. Sedan kommer page-filen dessutom att krypteras.

Hibernate är en fil som sparas på hårddisken och den innehåller känslig data då samma data har funnits i RAM. Även fast vårt hårddisk kommer vara krypterad så kan de ge värdefull data om man kommer förbi krypteringen, och det är exakt detta tankesättet vi ska ha.

För att stänga av hibernate så starta CMD som admin och skriv:

```
powercfg -h off
```

Shadow copies är ett sätt att spara kopior på filer och detta är oftast en guldgruva för forensiker så detta vill vi så klart stänga av. För att göra det så tryck på WIN+R och skriv SystemPropertiesProtection.exe, välj sedan din(a) disk(ar) och tryck på "Konfigurera". Sedan bör det se ut så här:





## **Ändra MACE på alla filer med Timestomp!**

Timestomp är ett program som låter dig ändra MACE-attribut(last written, last accessed, created, mft entry modified) på filer och folder i Windows.

Först, ladda ner Timestomp här(direktlänk): <http://www.jonrajewski.com/data/for270/timestomp.exe> -  
Lägg sedan timestop.exe i C:\Windows\System32 så att vi kan nå den när vi vill.

Jag har kodat ett enkelt bat-skript som ändrar alla filers MACE-tider till något slumpmässigt i C:\Users\<användarnamn>. Detta är bra och kan förvirra för en forensiker som ska kolla när filer lades till eller ändrades senast. Du får gärna ändra mappen till vad du vill.

Nu ska vi skapa ännu en schemalagd aktivitet som ändrar alla filer i en specifikt mapp. Spara detta i time.bat

```
cd %USERPROFILE%
setlocal enabledelayedexpansion
SET /A d=%RANDOM% %% 26 +2
SET /A m=%RANDOM% %% 10 +2

for /r %%a in (*) do (
timestomp.exe "%%a" -z "Monday %m%/%d%/2015 2:55:55 AM"
)
```

Spara time.bat i %USERPROFILE% sedan kör detta i CMD(behöver inte vara som admin):

```
SchTasks /Create /SC DAILY /TN "time" /TR "%USERPROFILE%\time.bat" /ST 20:15
```

## **Bästa praktik för webbsurfande**

Det är väldigt mycket rekommenderat att alltid surfa i inkognito/private browsing eftersom detta inte lämnar några direkta spår. Dock kan det bli lite jobbigt att behöva logga in på hemsidor varje gång men det är en bra vana faktiskt. Använd gärna en lösenordshanterare så slipper ni skriva i lösenord varje gång.

**Firefox:** sätt *browser.privatebrowsing.autostart* i *about:config* till *true*

**Chrome:** Ändra genvägen så att den slutar på `—incognito`. Läs mer utförligt [här](#)

När det kommer till nerladdade filer så se till att dessa läggs på ett separat krypterat medium. Skapa gärna en Truecrypt-container på några Gb och montera den vid varje start. Om du nu är väldigt lat så kan du skapa en .bat-fil som automatiskt monterar containern efter lösenord. (spara detta i mount.bat):

```
"C:\Program Files\TrueCrypt\TrueCrypt.exe" /v C:\container.tc /lx /a /e /q
```

(OBS. ni kan lägga till /p "lösenord" med "" runt lösenordet för att fullt automatiskt montera filen. Detta är dock inte rekommenderat då du har lösenordet i klartext.)

Ovanstående kod kommer montera en TC-container som finns i C:\ med namnet container.tc och den kommer monteras med enhetsbokstaven X(/lx - letter). Lösenordet ska ha "" runt om sig!

Ställ nu in i Chrome och/eller Firefox att alla nerladdningar ska sparas i X:

## **Bästa praktik för wipe**

wipe är det näst viktigaste att syssla med om du håller på med anti-forensik. Till detta är det Eraser som är det att rekommendera. Detta eftersom Eraser är open source och fungerar med alla sorts diskar. Eftersom PrivaZer redan rensar på bra så behöver vi egentligen inte rensa hela disken med detta är helt upp till dig. Personligen använder jag enbart Eraser till att rensa papperskorgen och för att snabbt radera filer(högerklicka > Eraser > Erase)


Kolla på denna video jag gjorde: [https://www.youtube.com/watch?v=L\\_XTeFKngyw](https://www.youtube.com/watch?v=L_XTeFKngyw)



## **PrivaZer - en extremt grundlig spårrensare**

Ladda ner och installera PrivaZer här: <http://privazer.com/download.php> -- Efter installation så följ gärna denna video för att schemalägga PrivaZer: <https://www.youtube.com/watch?v=-qvTI8kEg4M>

Ni får så klart skanna manuellt med PrivaZer också om ni så vill men personligen föredrar jag ett automatiskt schema då jag lätt glömmer bort att rensa. Ett kombination av både schema och manuellt startande är väl bäst.

## **Schemalagda rensningsuppgifter : 2**



	Senaste rensning
<input checked="" type="checkbox"/>  WINDOWS (C:)	2015-09-23 20:13:54
<input checked="" type="checkbox"/>  Lokal disk (D:)	2015-09-23 20:05:10

## **USBOblivion - Rensa alla spår av externa medium!**

Tyvärr behövs ett annat program än PrivaZer och CCleaner då de inte rensar alla spår av externa medium i Windows. kanske det kommer implementeras senare, vem vet men för närvarande behövs ett annat program! Och det finns! USBOblivion är ett sådant program som skannar och sedan rensar alla spår!

Ladda ner: <http://www.cherubicsoft.com/en/projects/usboblivion>

Eller varför inte lägga till det i ett option i vårt redan skrivna bat-skript? Så slipper vi tänka på det!(Lägg USBOblivion64.exe i C:\Windows\System32). Då ser time.bat ut så här:

```
cd %USERPROFILE%
setlocal enabledelayedexpansion
SET /A d=%RANDOM% %% 26 +2
SET /A m=%RANDOM% %% 10 +2

for /r %%a in (*) do (
timestomp.exe "%%a" -z "Monday %m%/%d%/2015 2:55:55 AM"
)
USBOblivion64.exe -enable -auto -nosave -silent
```

Starta sedan CMD som admin och skriv:

```
SchTasks /Create /SC DAILY /TN "time" /TR "%USERPROFILE%\time.bat" /ST 20:15
```

Och svara "y" på om du vill ersätta den redan skapade aktiviteten.

Du får ju så klart starta USBOblivion när du vill om du nu inte vill ha det i skriptet, eller starta skriptet när du vill.

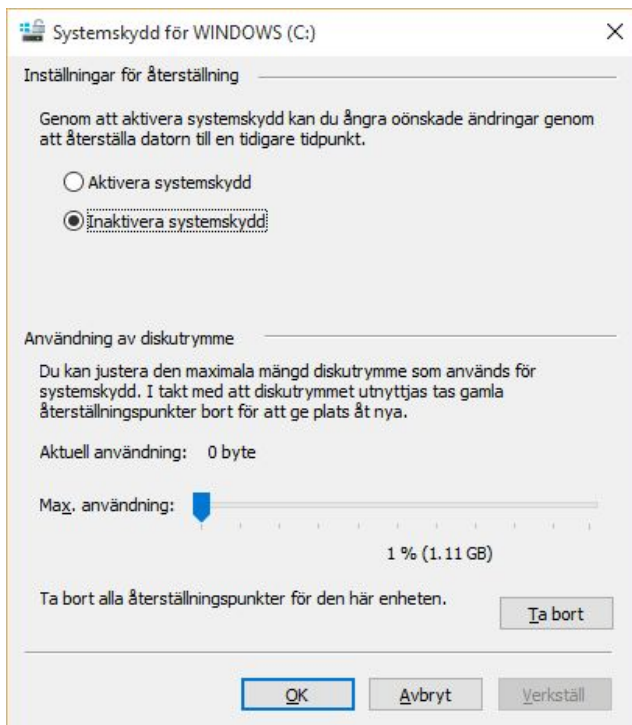
# Fysisk säkerhet

Fysisk säkerhet är oberoende för vilket operativsystem du kör. Tyvärr är det relativt svårt med fysisk säkerhet då man generellt sett inte kan skydda sig på ett komplett sätt, dock finns det ett par saker man kan göra för att försvåra om din maskin blir attackerad fysiskt.

## Ha uppsikt över din dator!

Det är mycket viktigt att du använder ditt operativsystems inbyggda utloggningssystem eftersom om användaren är utloggad så kommer man inte komma in utan ett lösenord och inga program kan köras utan korrekt lösenord. Bäst är det så klart att stänga av datorn helt men ibland behöver man gå ifrån datorn. Viloläge ska du dessutom också hålla dig borta från.

I Windows är det mycket enkelt då du trycker på WIN+L så låser skärmen sig. Dock vill du också att detta ska hända automatiskt efter en viss tid av inaktivitet. Det är bäst att du googlar dig till hur du gör i just ditt operativsystem för det kan skilja sig åt. I Windows 10 ska det se ut så här:

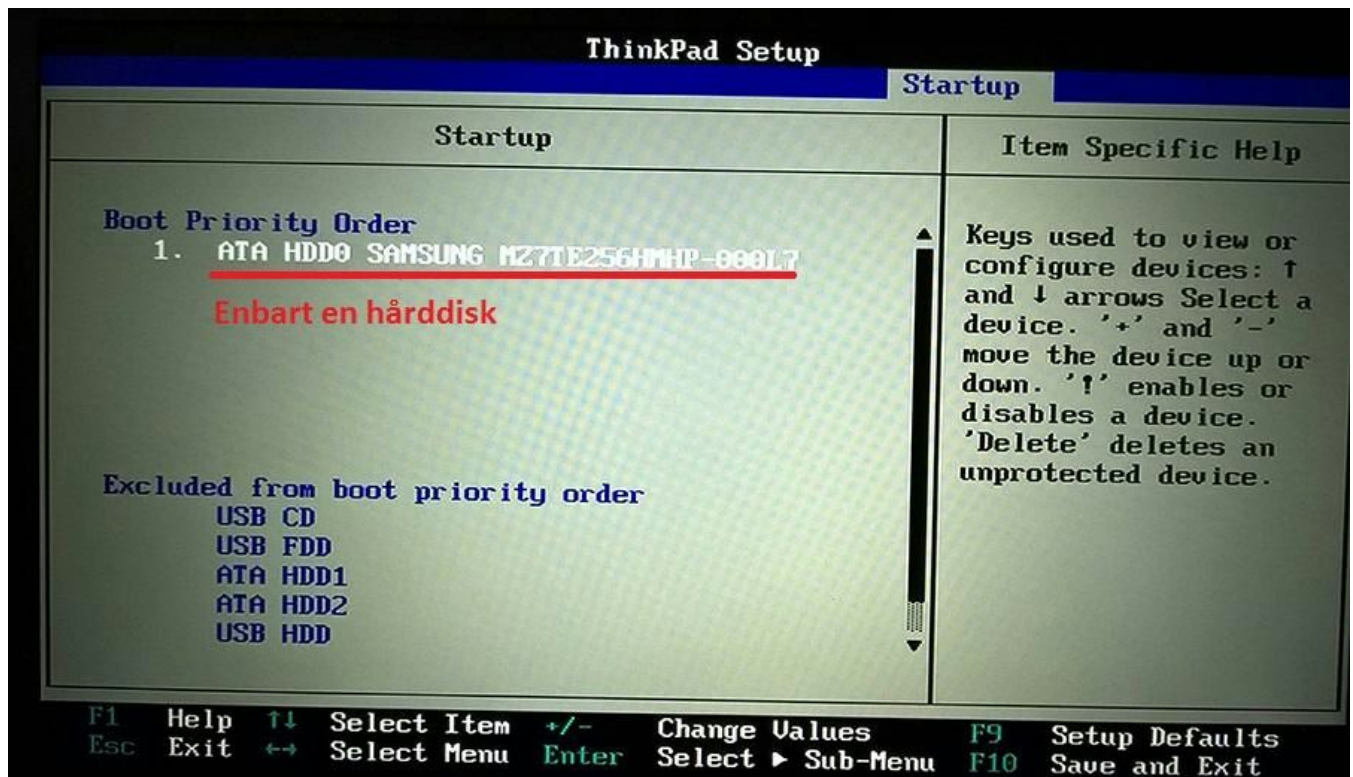


## Skydda BIOS!

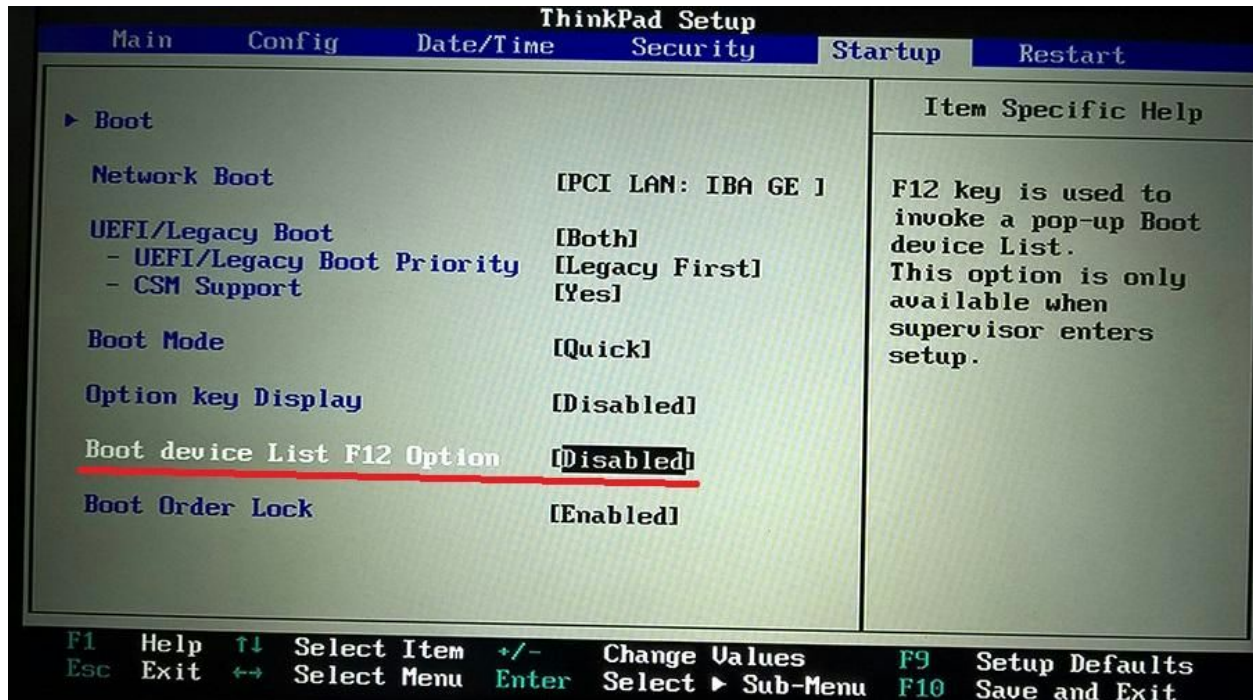
Det är viktigt att man skyddar BIOS genom att sätta ett lösenord så att man inte kan gå direkt in i inställningarna och ändra inställningar.

Väl inne i BIOS vill du ändra inställningarna så att man inte får boota med ett USB-minne eller andra externa medium, t.ex CD-rom. Detta vill du ändra för att annars kan man boota upp datorn med kod som skrapar RAM efter data eller annan kod som kan injektera elaka bootloaders som snor dina kryptonycklar(s.k Evil Maid-attack).

Här är två exempelbilder på hur det bör och kan se ut. Men kom ihåg att det kommer se olika ut beroende på vilken typ av BIOS-version du har.







### Limma RAM-minnena med epoxy-lim

Att limma fast RAM-stickorna kommer förhindra att någon kan ta av dem för att sedan stoppa in dem i ett annat moderkort för att utläsa data i dem. Om man limmar fast stickorna så kommer du aldrig att kunna byta RAM igen så detta är en vågad aktion men det ger mycket säkerhet. Du bör tänka efter noggrant om du verkligen vill göra detta.

Du köper Epoxy-lim, t.ex <http://www.kjell.com/sortiment/hus-hals...lim-p53365> och sedan limmar du vid sidan av RAM-pinnarna så att de sitter fast. Kolla på bilden där det röda strecket är; där ska limmet vara



### **Var alltid beredd på att kunna bryta strömmen till datorn**

Du bör köpa en grenkontakt med huvudström-brytare, de ser ut så här:



Så att du alltid kan nära till hands bryta all ström som går till datorn. Tyvärr kan det bli problem om du använder en laptop då de går på batteri. Dock kan du ha som vana att när du är hemma så tar du av din laptops batteri och kopplar sladden direkt in i väggen.

Om du dock har en laptop och vill använda dess batteri så får du tänka på att snabbt kunna ta av batteriet ur datorn. Sedan är det alltid, oavsett typ av datorn viktigt att låsa skärmen så fort du inte sitter vid den.



## Omöjliggör användning av DMA-portar

DMA(direct memory access) gör direkt tillgång till en dators minne för snabbare användning. Om du aldrig använder dessa så kan du lika bra omöjliggöra dem genom att antagligen fylla ingången med epoxy-lim eller plocka ut den ur datorn(om det är möjligt). Exempel på DMA-anlutningar är:

- IEEE 1394 (Firewire)
- Thunderbolt
- PCI och PCI express
- ExpressCard

Det finns dokumenterade fall där dessa ingångar har använts för att utläsa data ur RAM så som kryptonycklar. Dock skulle jag påstå att risken är relativt liten att detta kan exploateras beroende på situation. Om du är osäker på att du kanske kommer ha användning av någon av ovanstående portar någon gång så förstör dem inte.



IEEE1394 (Firewire) - ingång



Thunderbolt-port på en Macbook

Thunderbolt port



Express-card ingång.

# Fysisk säkerhet - DMS och liknande skydd

DMS står för *Dead Mans Switch* och kan inom anti-forensiken beskrivas som ett program som låter en snabbt skydda din data om det blir kritiskt läge. En DMS ska vara enkel att trigga och handlingen ska "fail-proof" och vara snabb(helst stänga av datorn eller avmontera diskar).

Ett manuellt DMS-skydd är när man själv behöver trigga DMS'en och ett automatiskt DMS-skydd triggas när en specificerad handling sker, t.ex sätter in ett USB-minne eller drar ut Ethernet-sladden.

Jag tänker inte skriva någon guide för någon av dessa DMS'er eftersom jag anser att de kan passa olika användare olika bra. Du får helt enkelt kolla in om det är något som skulle passa dig.

Dock rekommenderar jag YONTMA som jag kört ett år och det fungerar helt automatiskt. YONTMA sätter datorn i hibernate om Ethernet-sladden eller strömsladden dras ut när datorn är utloggad(WIN+L i Windows). Läs gärna denna guide som jag skrev för YONTMA:  
<https://www.flashback.org/sp49077816> - Kom dock ihåg att YONTMA är designad till laptops men fungerar ändå bra på stationära datorer.

## **Manuella DMS-skydd**

<https://github.com/0xPoly/Centry> - Linux och OS X

[https://github.com/qnrq/panic\\_bcast](https://github.com/qnrq/panic_bcast) - Linux

<https://github.com/ensconce/AFT> - Windows (har inte fått den att fungera)

<https://github.com/defuse/swatd> - Linux

## **Automatiskt DMS-skydd**

<https://github.com/iSECPartners/yontma> - Windows och OS X

<https://github.com/redpois0n/usbwatcher> - Windows, Linux och OS X

<https://github.com/hephaest0s/usbskill> - Linux och OS X

<https://github.com/ncatlin/lockwatcher> - Linux och Windows

# Linux

Linux sparar inte lika mycket info eller spår som andra operativsystem. Windows är väldigt känt för att spara onödig information men det är inte Linux. Dock finns det fortfarande saker kvar som man behöver göra. Linux har inte alls lika många program som Windows men jag ska ta upp det absolut viktigaste.

## **Bleachbit**

Ladda ner eller kolla med din pakethanterare(*apt-get install bleachbit* i debian-baserade distar).

Bleachbit är Linux motsvarighet till CCleaner och är väldigt grundlig. Bleachbit är enklast att använda i GUI men fungerar fint i CLI. Dock är det lite krångligt att för första gången förstå hur det fungerar. Läs mer här:[http://bleachbit.sourceforge.net/docume ... mmand-line](http://bleachbit.sourceforge.net/docume...mmand-line)

Exempel: om du vill rensa allt system-relaterat så kan du skriva:

```
# bleachbit --preview system.*
```

Vilket kommer skanna igenom allting(precis som med CCleaner). Sedan kan du skriva över den hittade informationen med

```
# bleachbit --overwrite --clean system.*
```

## **secure-erase**

(*apt-get install secure-delete*) är ett gäng program som kan säkert skriva över mappar och filer. Dessutom kommer ett program med som rensar RAM. RAM i Linux fungerar olikt än hos Windows då Linux inte på samma sätt frigör minne.

Man bör egentligen inte ersätta ett redan skapat program med ett alias så därför är det bättre att ni vänjer er vid att använda srm istället. Dock bör ni lägga detta i er .profile:

```
alias srm='srm -f -l -z'
```

sdmem är enkelt att använda. Detta program skriver data i RAM tills RAM tar slut, skriv detta som root:

```
sdmem -ll
```

Lägg gärna detta kommando som ett cron varje halvtimme eller så. Då slänger du detta i din crontab:

```
*/30 * * * * sdmem -ll >/dev/null 2>&1
```

### **cryptsetup**

Ni vet att man inte bör ha swap och detta gäller oavsett operativsystem. Men det är väl värt att nämna att man kan kryptera swap med hjälp utan cryptsetup i Linux. Nedan är ett exempel hur man kan skapa en krypterad swap-fil:

```
# dd if=/dev/zero of=swapfile bs=1M count=100
# loop=$(losetup -f)
# losetup ${loop} swapfile
# cryptsetup open --type plain --key-file /dev/urandom ${loop} swapfile
# mkswap /dev/mapper/swapfile
# swapon /dev/mapper/swapfile
```

Programmet sswap som kom med i secure-delete rensar swap-partitioner. För att göra detta behöver du först avaktivera swap för att rensa partitionen, därefter kör:

```
sswap -ll /dev/<vart swap nu finns>
```

Använder du en swap-fil så kan du enkelt överskriva den med srm.

## Övriga operativsystem

De operativsystem som listas nedanför har jag inte stor koll på. Dock länkar jag de program jag använder till de olika operativsystemen och tycker de fungerar bra.

### **OS X**

CCleaner finns till OS X: <https://www.piriform.com/ccleaner-mac>

Följ denna guide för att ha ett separat Filevault-lösenord:

<https://swehack.org/viewtopic.php?f=8&t=732> eller

<http://www.engadget.com/2011/12/12/prevent-certain-accounts-from-unlocking-filevault-2/>

### **Android**

Android har också CCleaner: <https://www.piriform.com/ccleaner-android>

Det finns även SD Maid som rensar rätt bra:

<https://play.google.com/store/apps/details?id=eu.thedarken.sdm>

Efter du rensar så skriv över ledigt utrymme med Secure Wipe:

<https://play.google.com/store/apps/details?id=com.pinellascodeworks.securewipe>