

IT-forensik och datautvinning



Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp



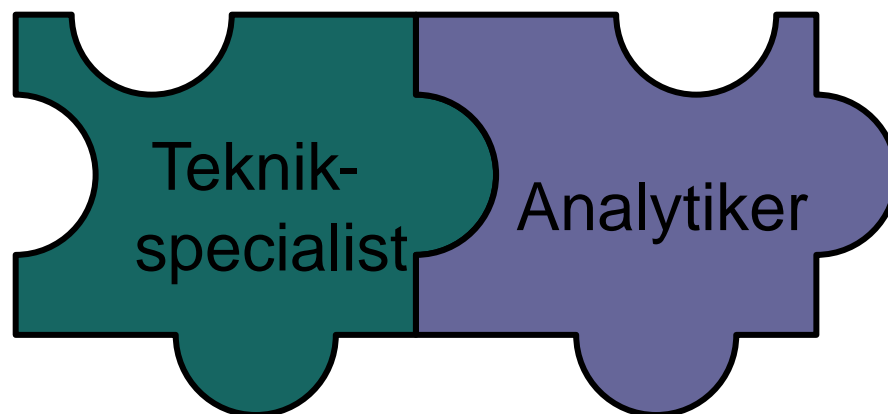
IT-forensikern



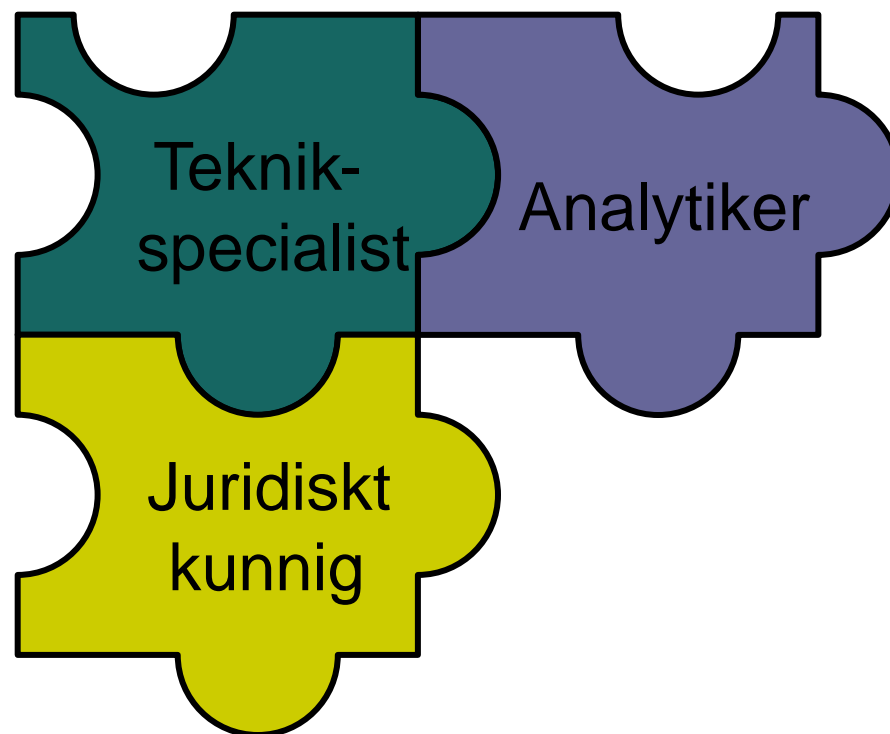
IT-forensikern



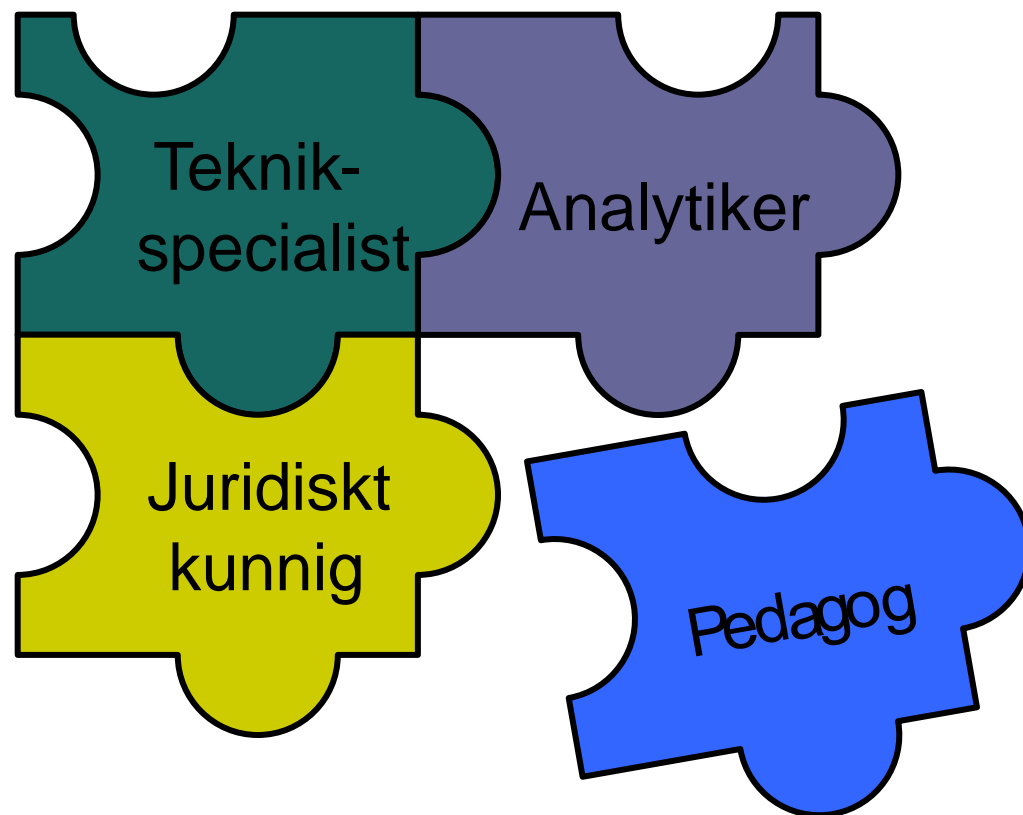
IT-forensikern



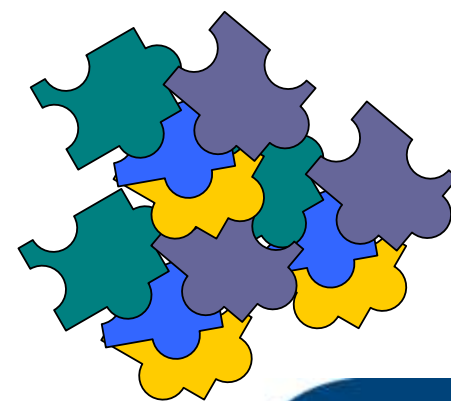
IT-forensikern



IT-forensikern



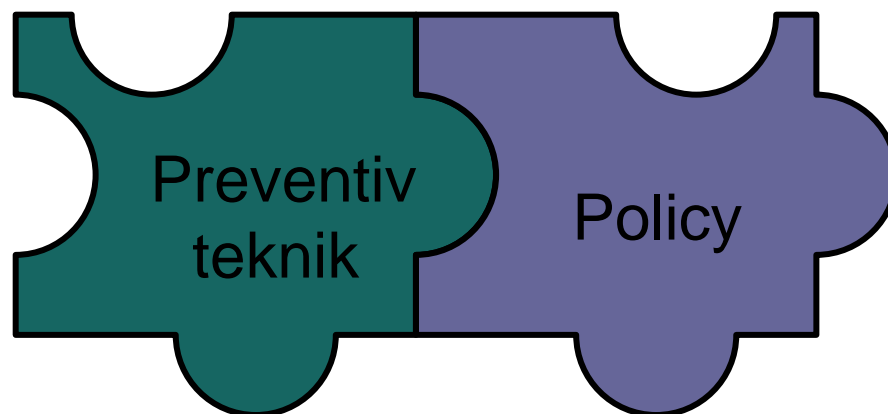
IT-forensiska uppdrag



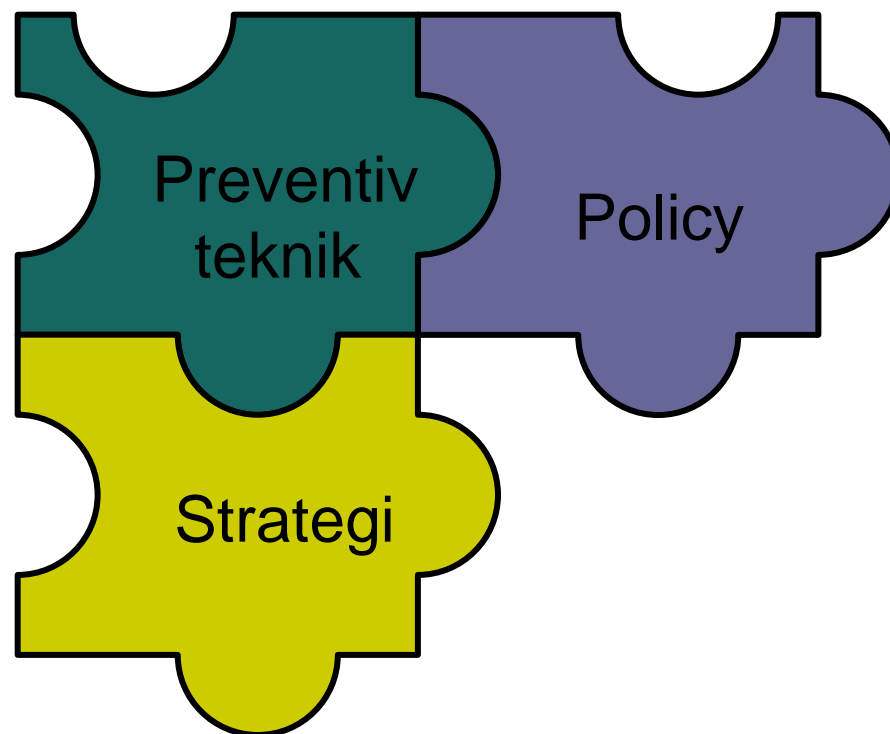
IT-forensiska uppdrag



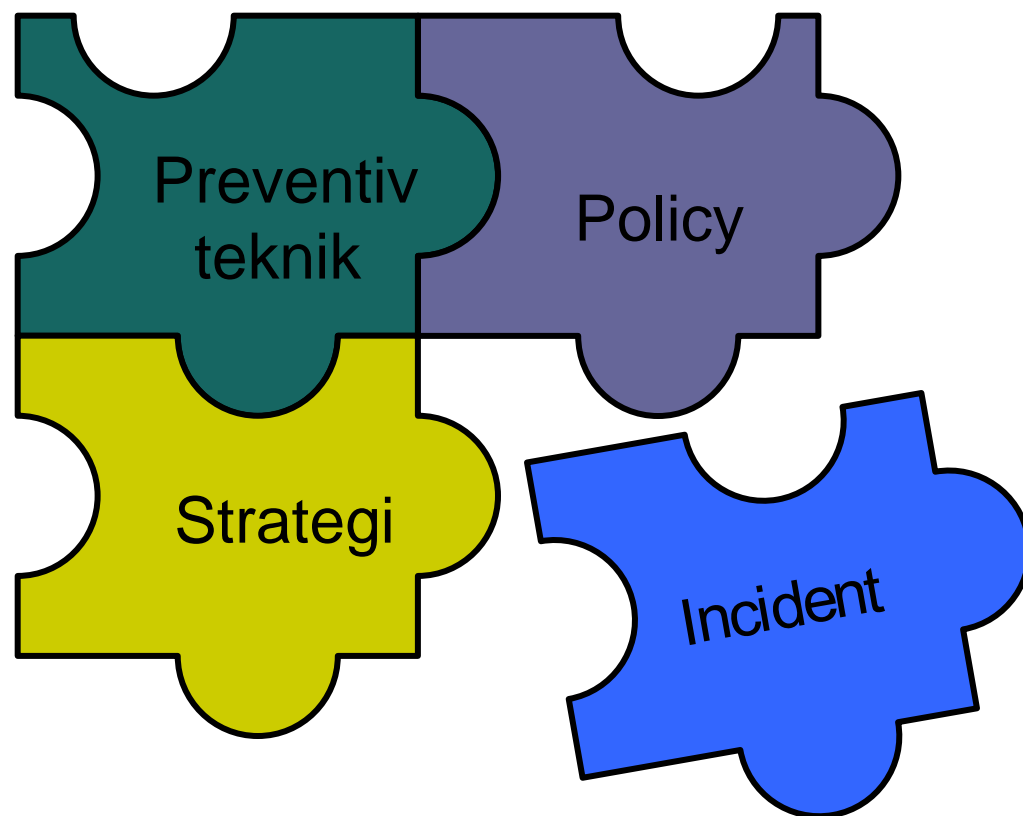
IT-forensiska uppdrag



IT-forensiska uppdrag



IT-forensiska uppdrag



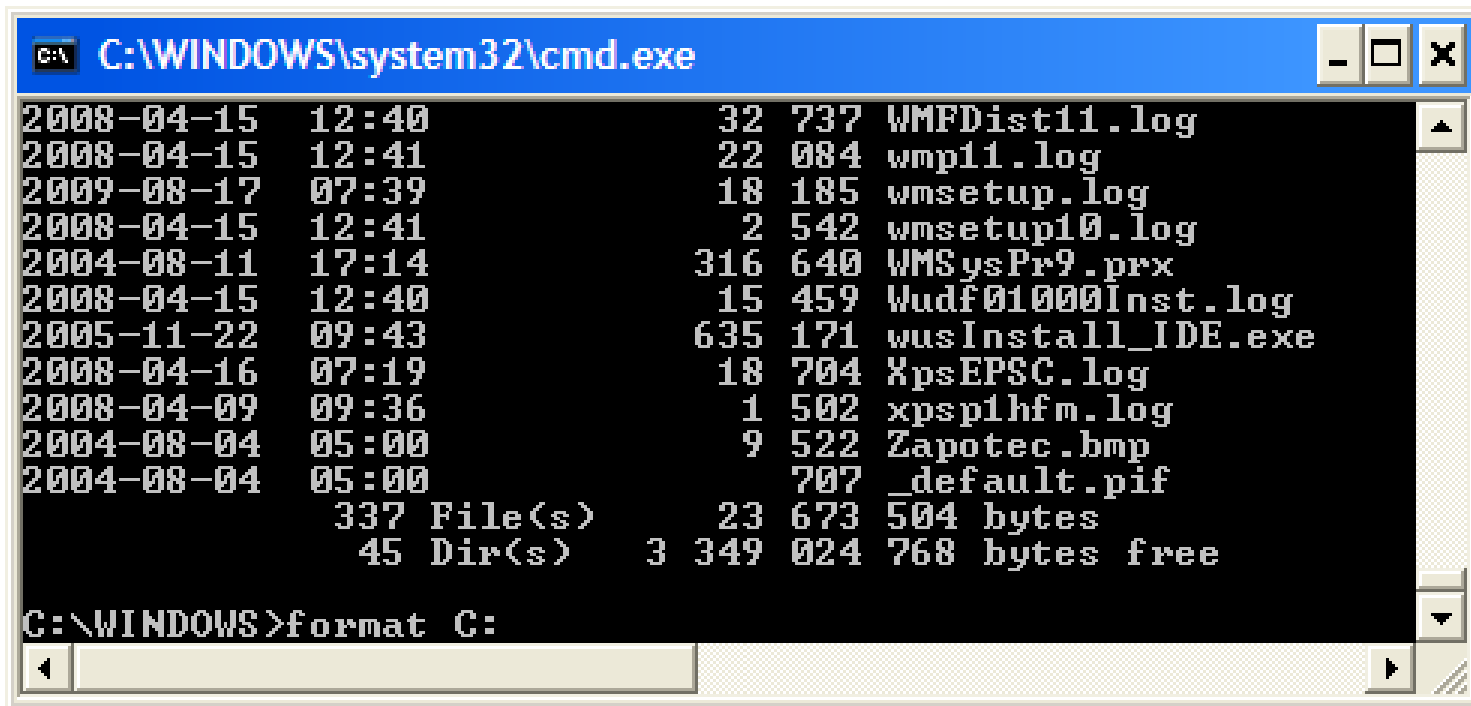
Vilka spår lämnar du efter dig om du...



...raderar en fil?



...formaterar en hårddisk?

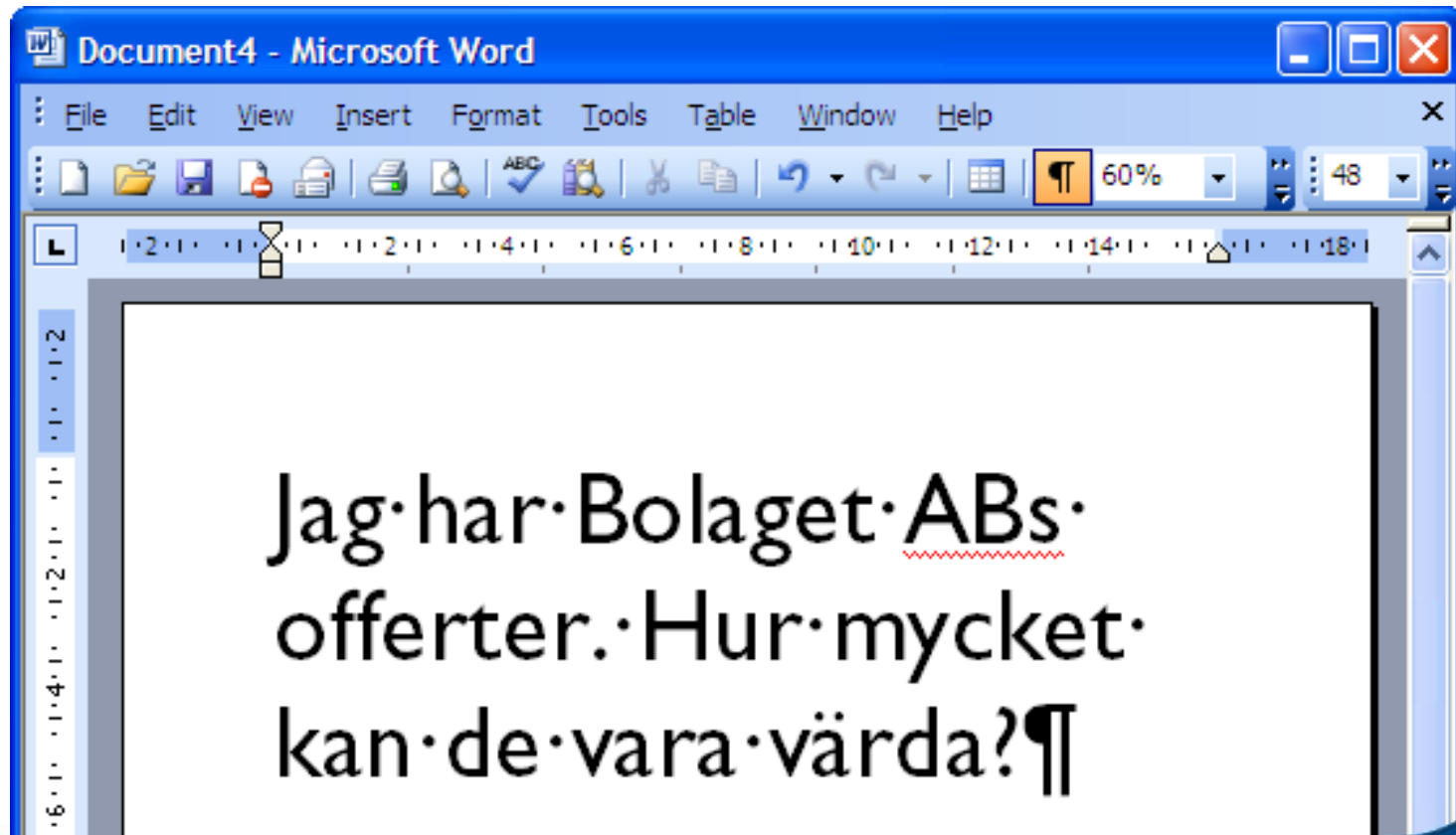


The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The window displays a directory listing of files and folders on the C: drive. The listing includes columns for date, time, size, and filename. At the bottom of the listing, it shows a summary of files and directories, and the amount of free space. Below the listing, the command "format C:" is entered at the prompt.

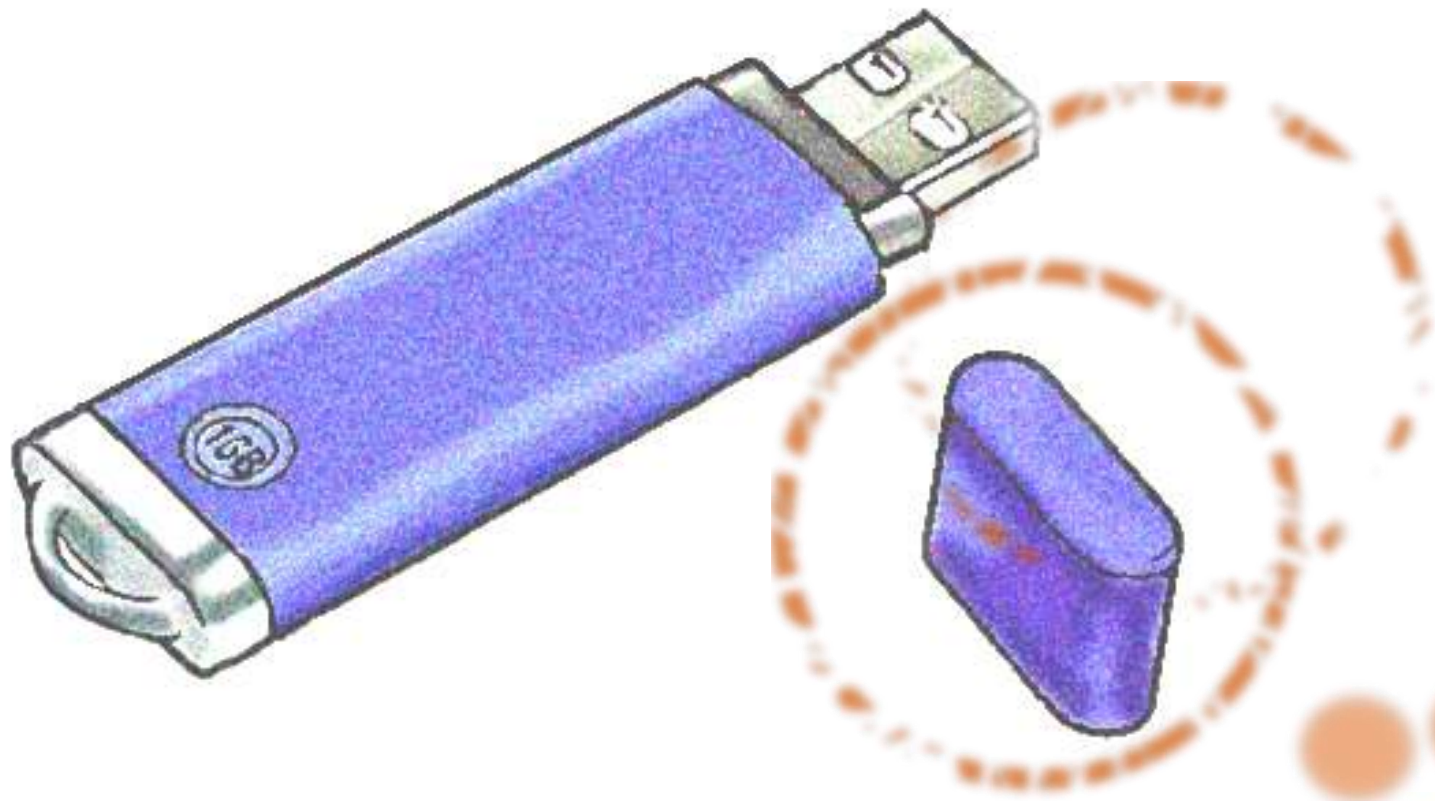
```
C:\WINDOWS\system32\cmd.exe
2008-04-15 12:40      32 737 WMFDist11.log
2008-04-15 12:41      22 084 wmp11.log
2009-08-17 07:39      18 185 wmsetup.log
2008-04-15 12:41         2 542 wmsetup10.log
2004-08-11 17:14     316 640 WMSysPr9.prx
2008-04-15 12:40      15 459 Wudf01000Inst.log
2005-11-22 09:43     635 171 wusInstall_IDE.exe
2008-04-16 07:19      18 704 XpsEPSC.log
2008-04-09 09:36         1 502 xpsp1hfm.log
2004-08-04 05:00         9 522 Zapotec.bmp
2004-08-04 05:00         707 _default.pif
          337 File(s)      23 673 504 bytes
          45 Dir(s)      3 349 024 768 bytes free

C:\WINDOWS>format C:
```

...redigerar text utan att spara?

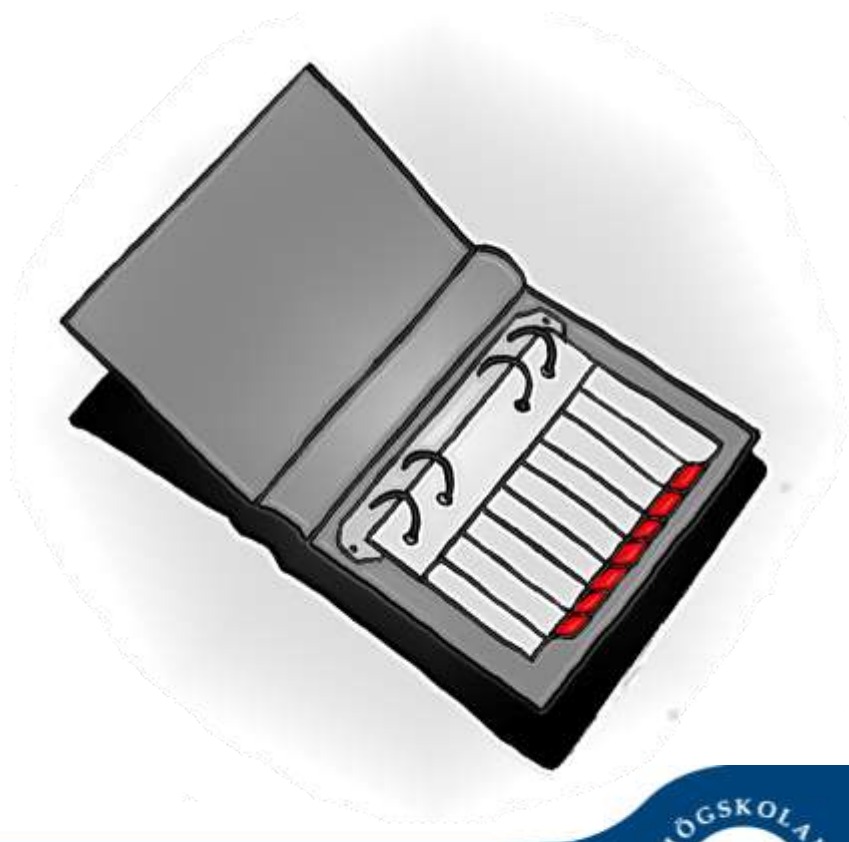


...använder ett USB-minne?



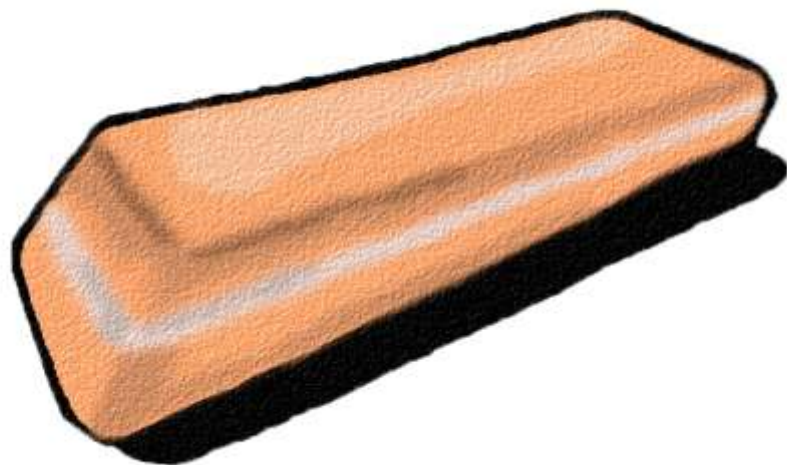
Filer på hårddisken

- Hårddisk = Pärm med register
- Skriva fil = Sätta in dokument
- Radera fil = Sudda i registret
- Formatera = Nytt register



Datautvinning: raderad fil

- Återskapa registret
- Leta för hand
- Återskapa data

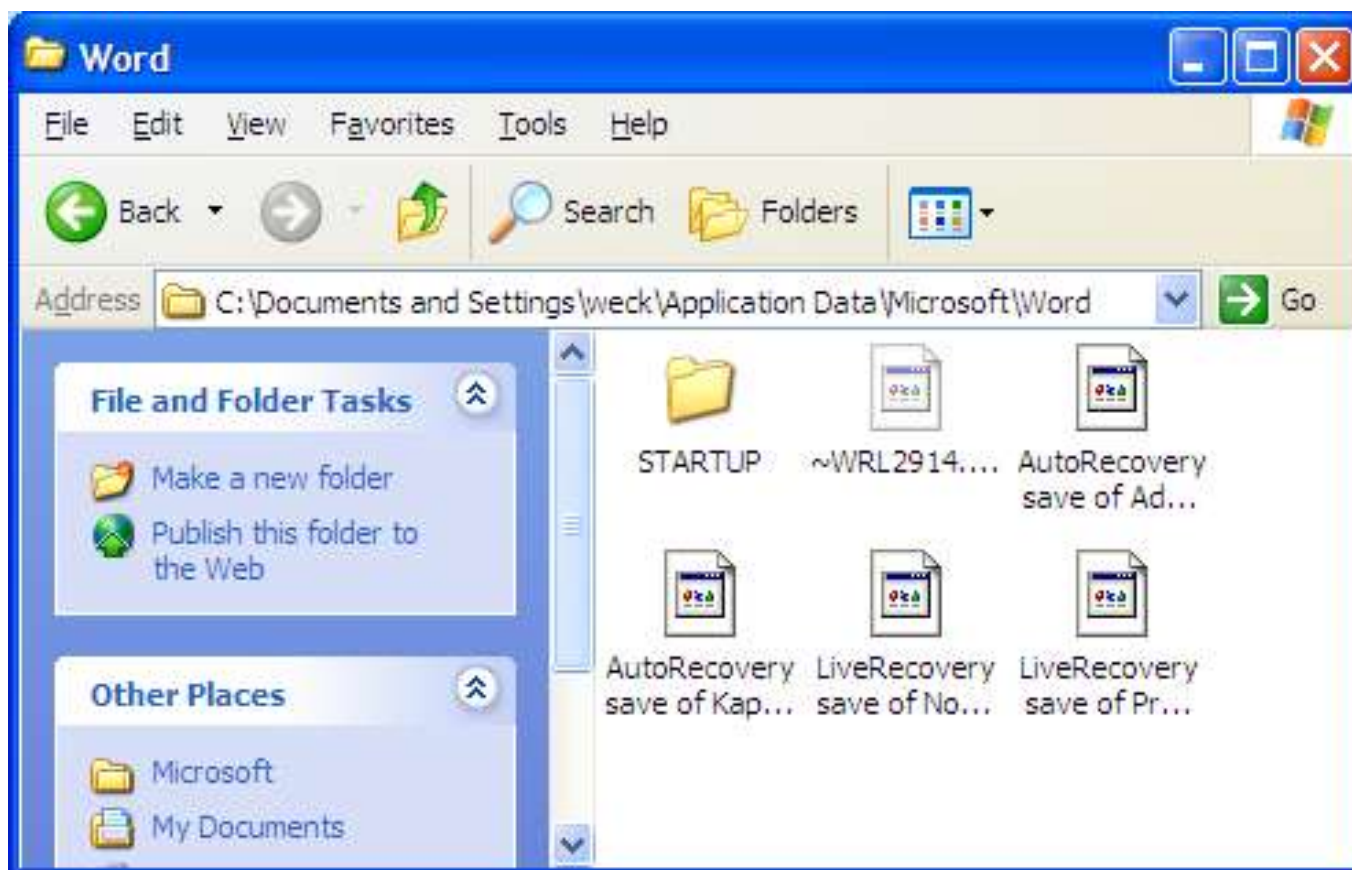


Datautvinning: formaterad hårddisk

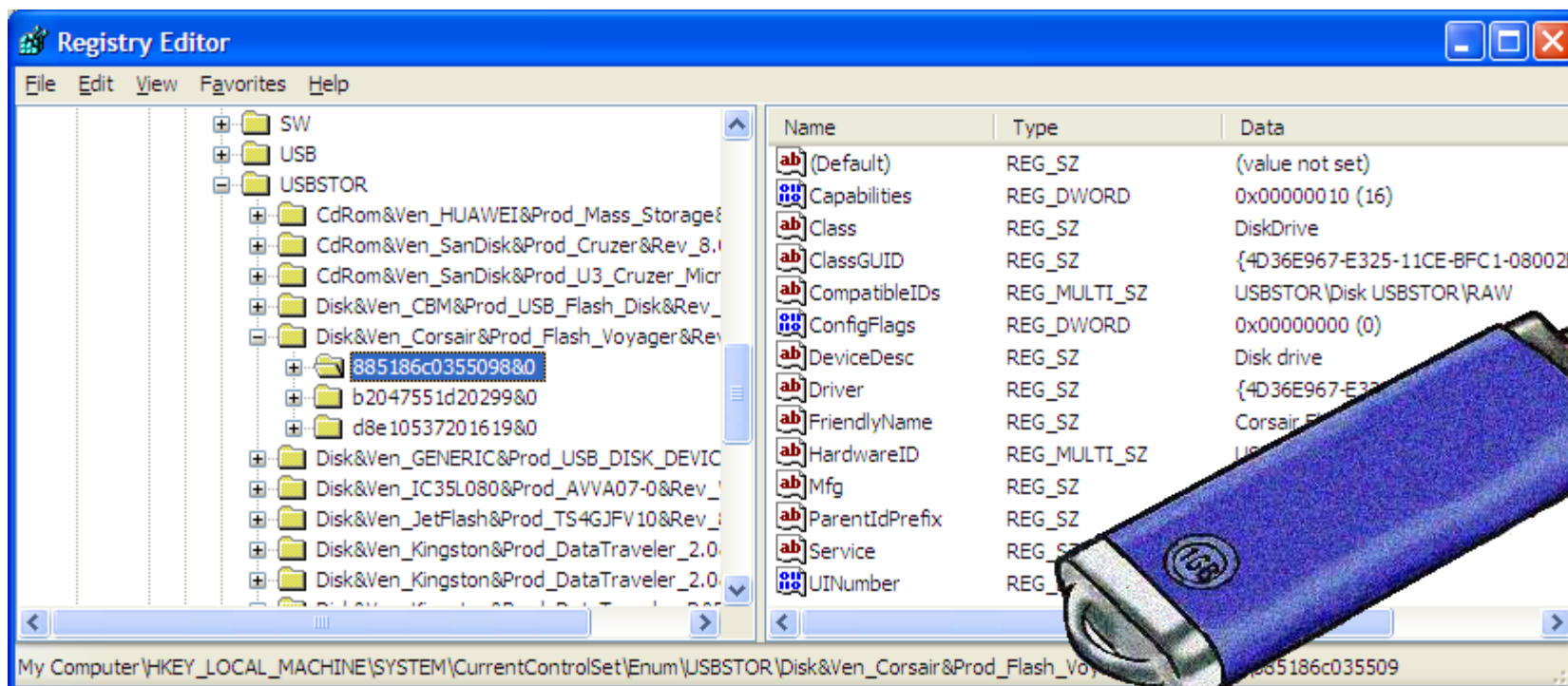
- Återskapa register
- Analysera data



Datautvinning: MS Word-tempfil



Windows konfigurationsdatabas



Metadata

EXIF Exif Viewer - C:\Backup\@foton\DSC_00...

File (F) View (V) Tools (T) Help (H) EXIF Sh

Item	Value
=== IFD Exif Private Tag ===	
ExposureTime	10 / 600 second(s)
FNumber	f / 5.0 (50 / 10)
ExposureProgram	Not defined
ISOSpeedRatings	560
ExifVersion	0221
DateTimeOriginal	2008:03:03 09:30:16
DateTimeDigitized	2008:03:03 09:30:16
ComponentsConfiguration	Y,Cb,Cr,(0),
CompressedBitsPerPixel	4 / 1
ExposureBiasValue	0 / 6
MaxApertureValue	Av = 4.6 APEX (f / 4.9)
MeteringMode	Pattern
LightSource	unknown
Flash	Flash fired, auto mode, retur

Format: JPEG

Pinpoint Metaviewer

Metaviewer

PINPOINT LABORATORIES

OLE Metadata

File Name: Kursplan_Administration a

Kursplan_Administration a		Keywords:	
Administration av operativ		Manager:	
IDE		Last Saved By:	IDE
		Word Count:	441
Microsoft Office Word		Page Count:	1
11.9999		Paragraph Count:	5
2009-10-16 08:52:00		Line Count:	19
		Character Count:	2338
2009-10-16 11:12:00		Chars (incl. spaces):	2774
124		Byte Count:	0
Normal.dot		Presentation Format:	
False		Slide Count:	0
		Note Count:	0
		Hidden Slides:	0
HH		Multimedia Clips:	0

File Size: 31232

MD5 Hash: E35739320C8B32CB3FA

SHA-1 Hash: BEEE70A76D01A93C1D

SHA-256 Hash: F5C234108FC36F1E8EF0

Exit Browse ... Copy All Copy Selected

Frågeställning:

- Vem ansvarar för raderad information?
- Vilken information sipprar ut?
- Vilka etiska aspekter måste beaktas?
- Är du beredd när incidenten väl inträffar?

IT-forensik och informationssäkerhet, 120/180 hp

	Termin 1		Termin 2	
År 1	Introduktion till IT-forensik	Kriminologi och IT-relaterad brottslighet	Programmering	Datautvinning från digitala lagringsmedia
	Administration av datorsystem	Administration av operativsystem	Juridik med IT-rätt	Grundläggande websystem

	Termin 3		Termin 4	
År 2	Biometrisk identifiering	Trådlösa nätverk	Avancerade IT-forensiska verktyg I	Utredning av IT-brott eller Examensarbete
	Datornätverk I	Datornätverk II	Nätverkssäkerhet	Risikanalys och IT-säkerhetssystem

	Termin 5		Termin 6	
År 3	Avancerade IT-forensiska verktyg II	Underrättelseverksamhet och spårning på internet	Examensarbete	
	Tillämpad matematik och statistik		Krypteringsmetoder och säkring av datasystem	Valbar kurs