IT-forensik och datautvinning

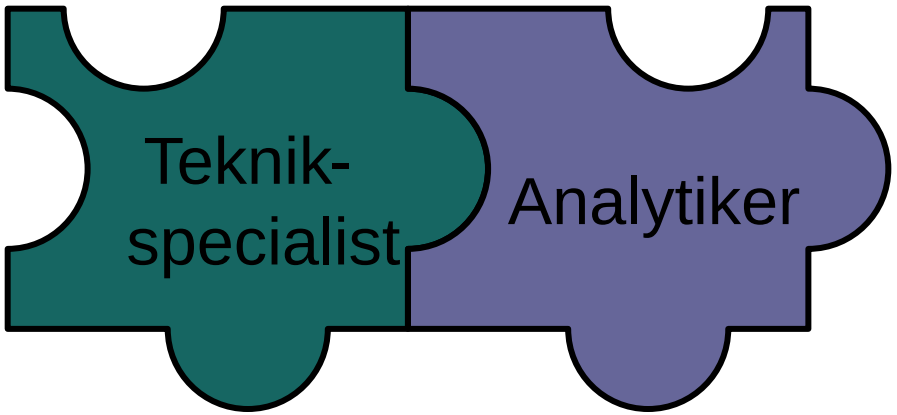
Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

IT-forensikern

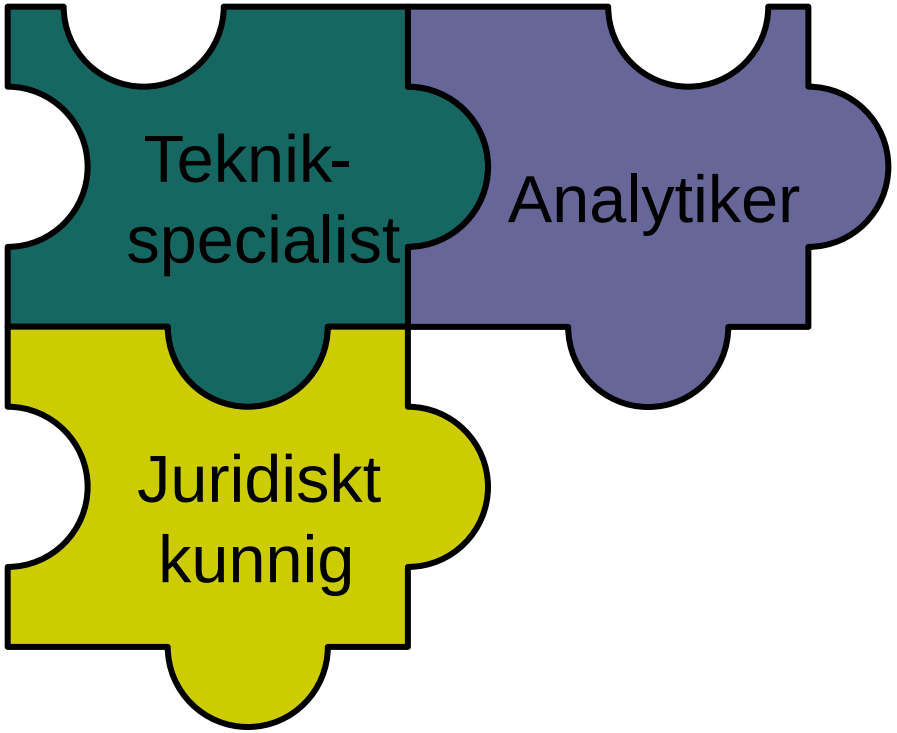
Mattias Weckstén

IT-forensikern

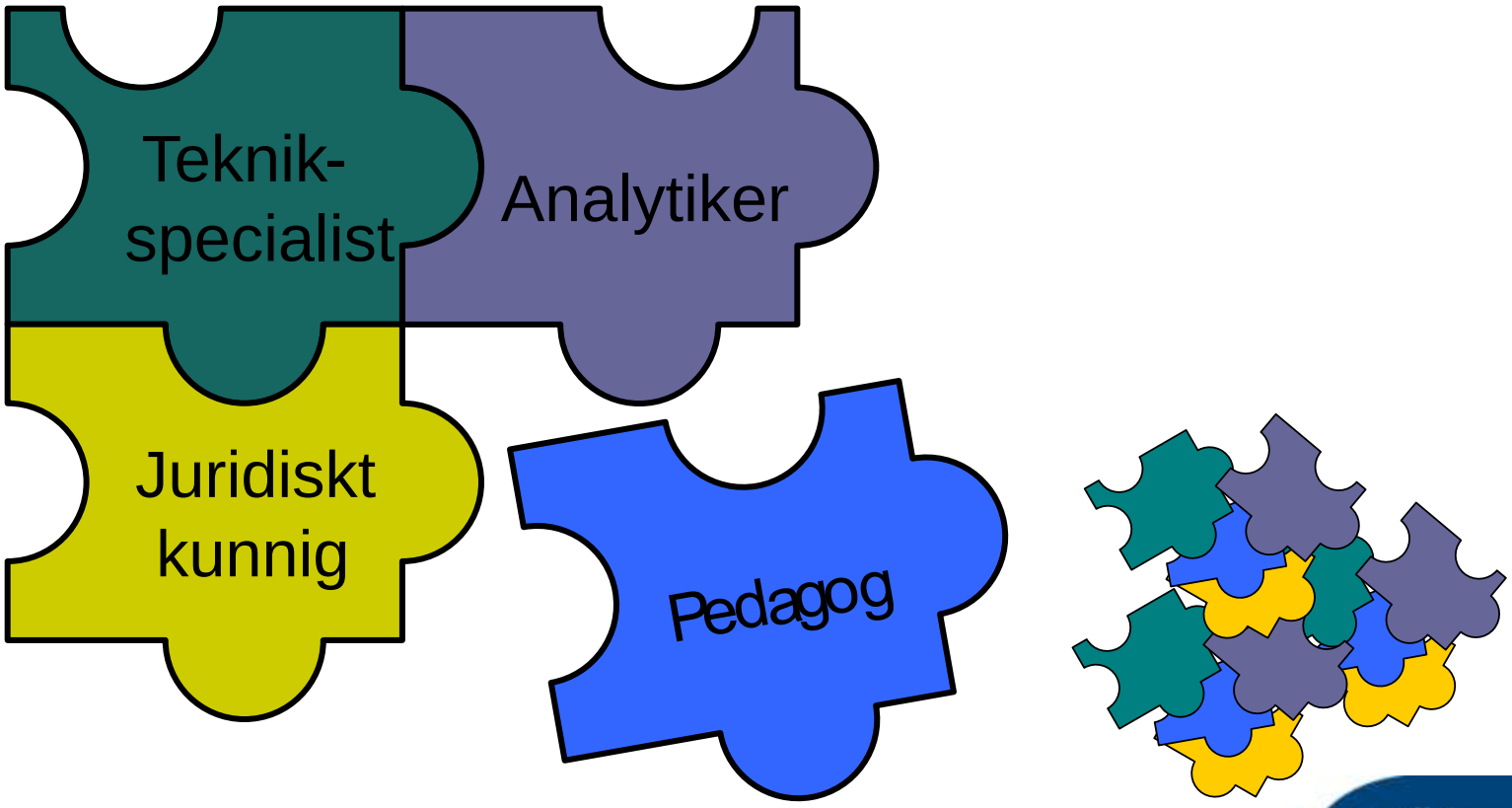
IT-forensikern



IT-forensikern



IT-forensikern

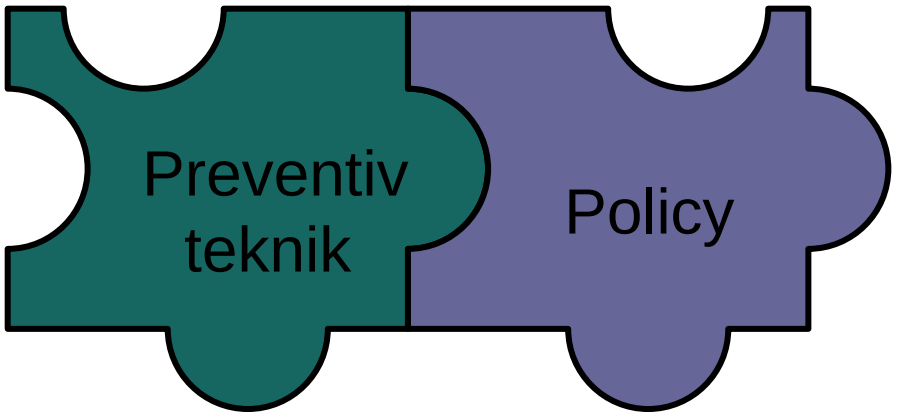


IT-forensiska uppdrag

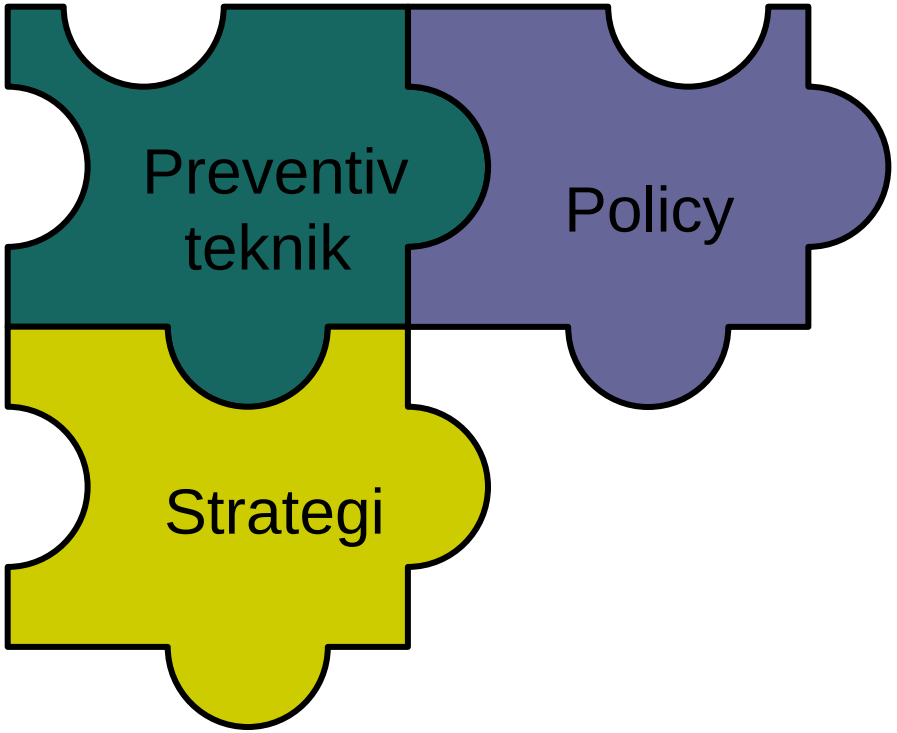
Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

IT-forensiska uppdrag

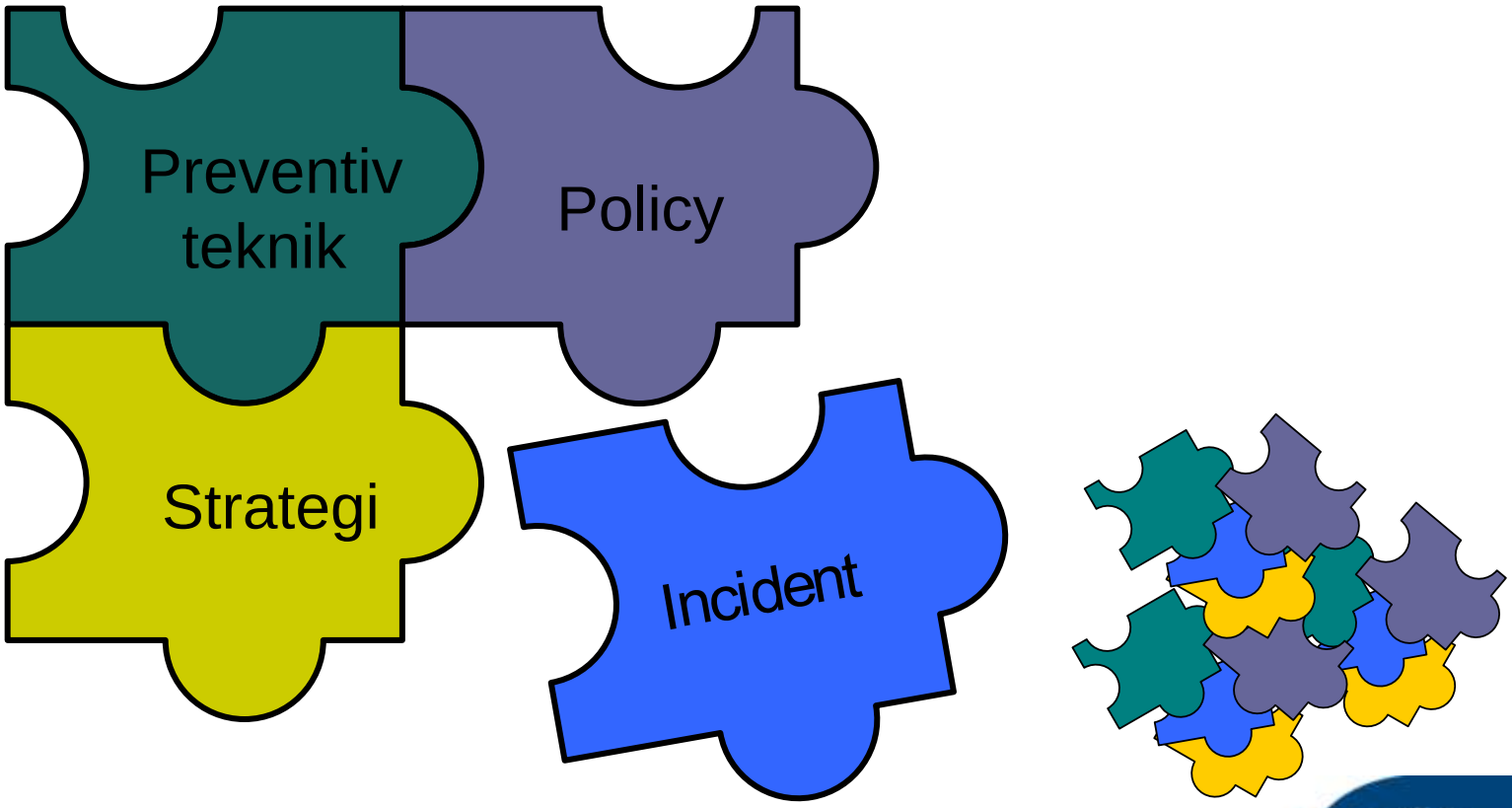
IT-forensiska uppdrag



IT-forensiska uppdrag



IT-forensiska uppdrag

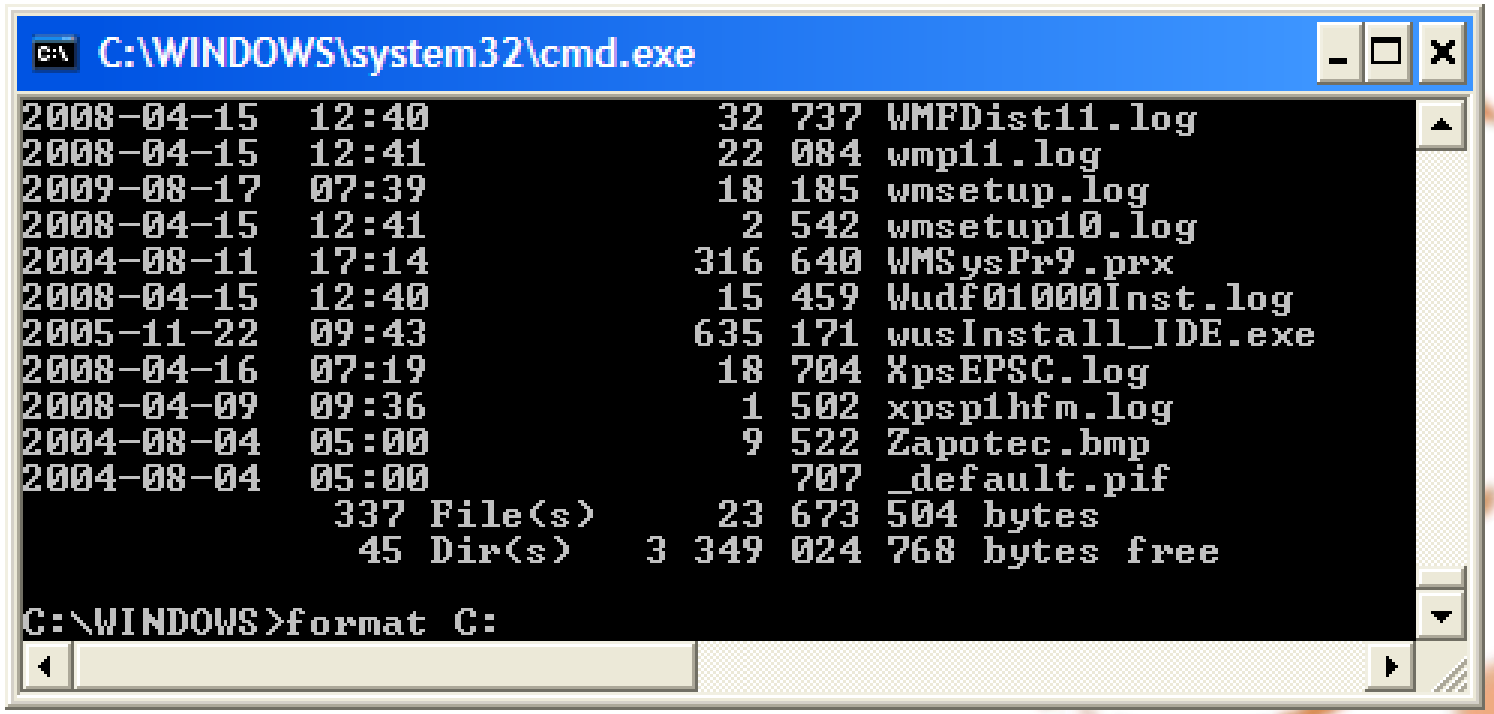


Vilka spår lämnar du efter dig om du…

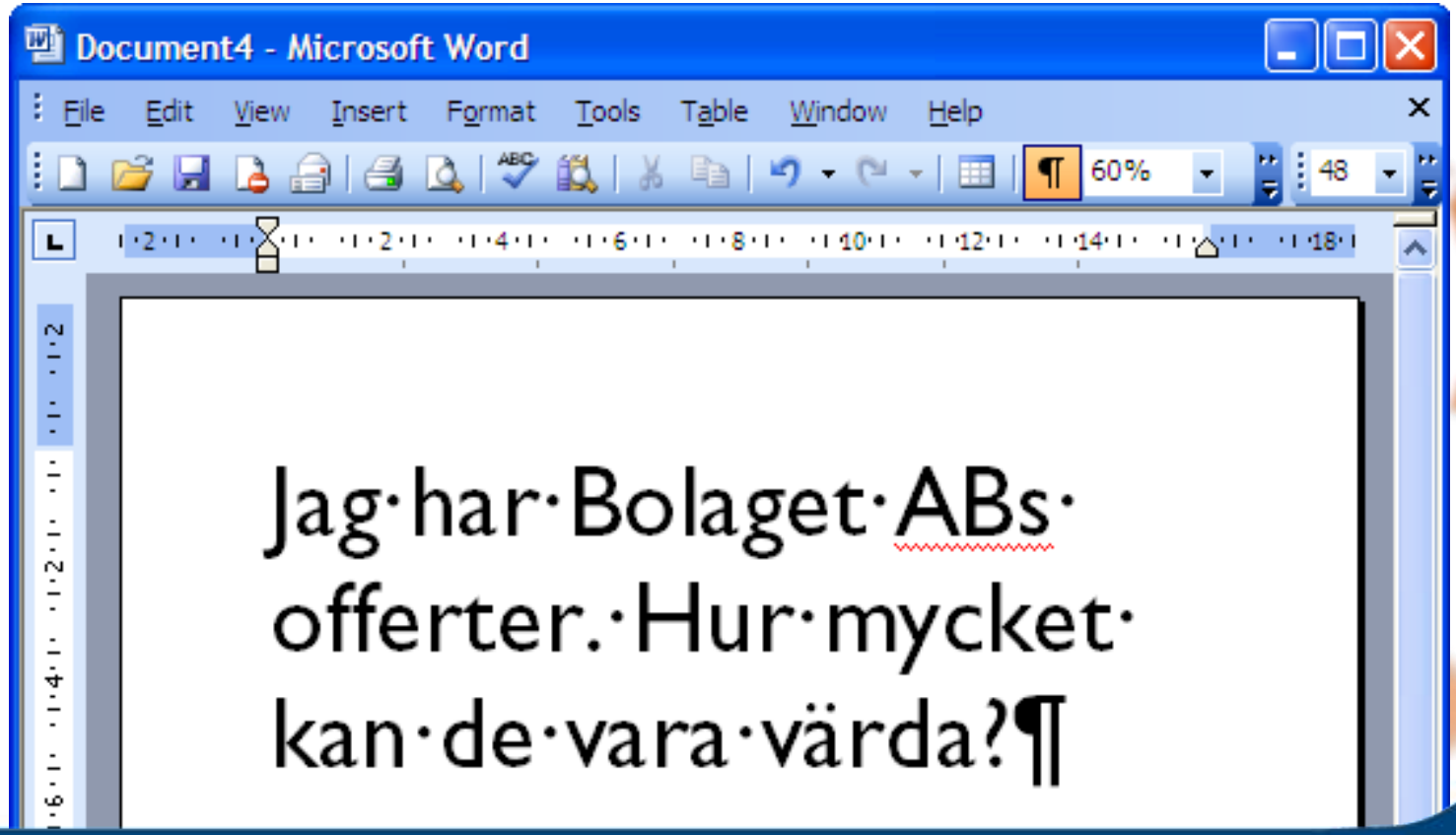
Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

…raderar en fil?

…formaterar en hårddisk?

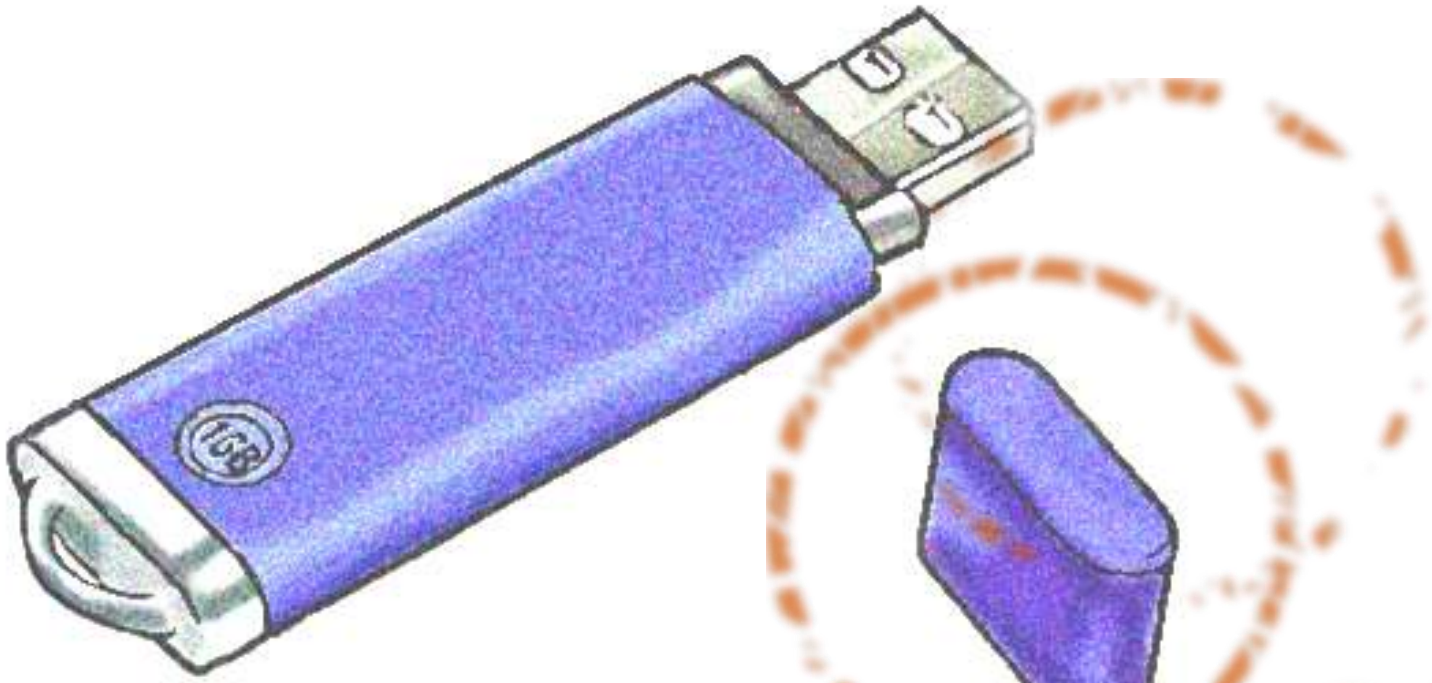


…redigerar text utan att spara?



Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

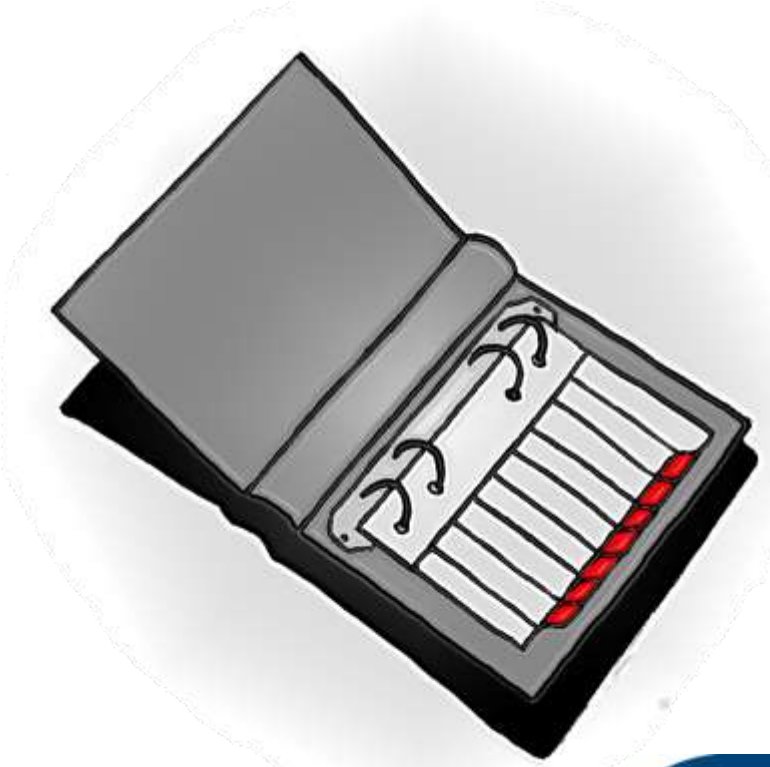
…använder ett USB-minne?



Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

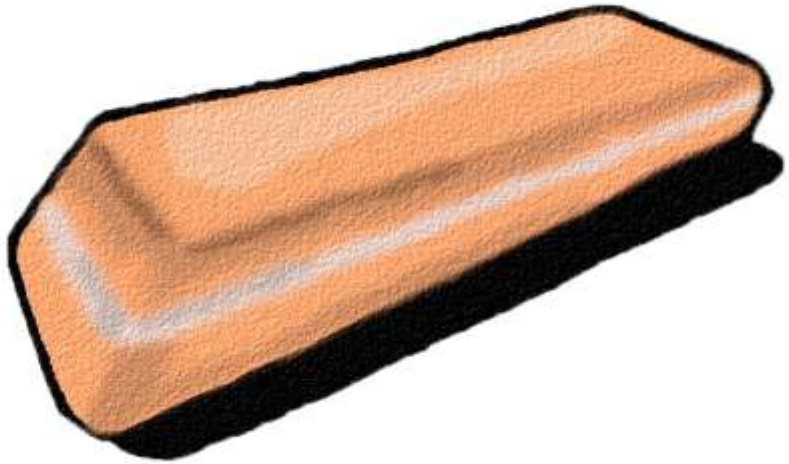
Filer på hårddisken

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



Datautvinning: raderad fil

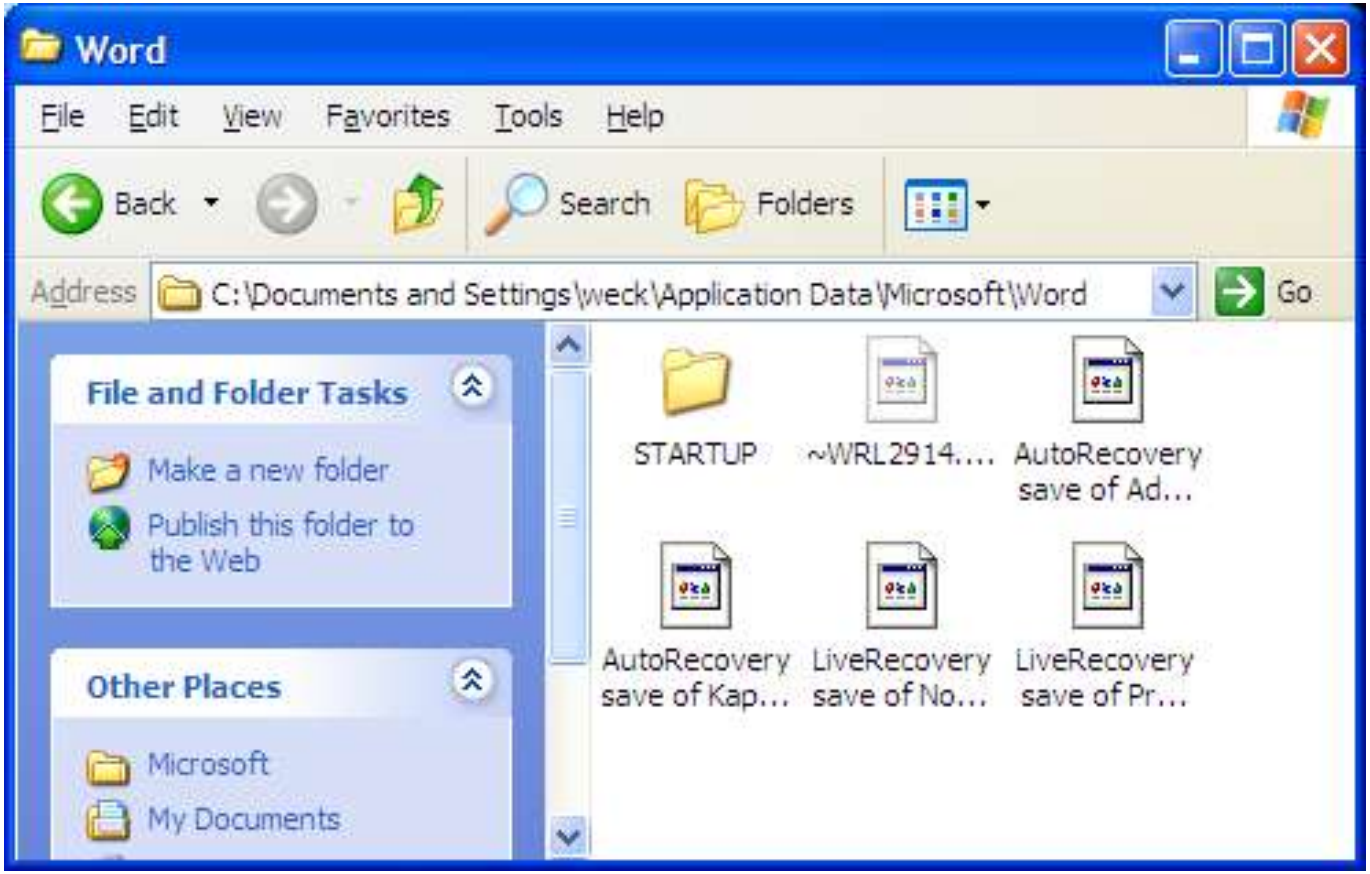
- Återskapa registret
- Leta för hand
- Återskapa data



Datautvinning: formaterad hårddisk

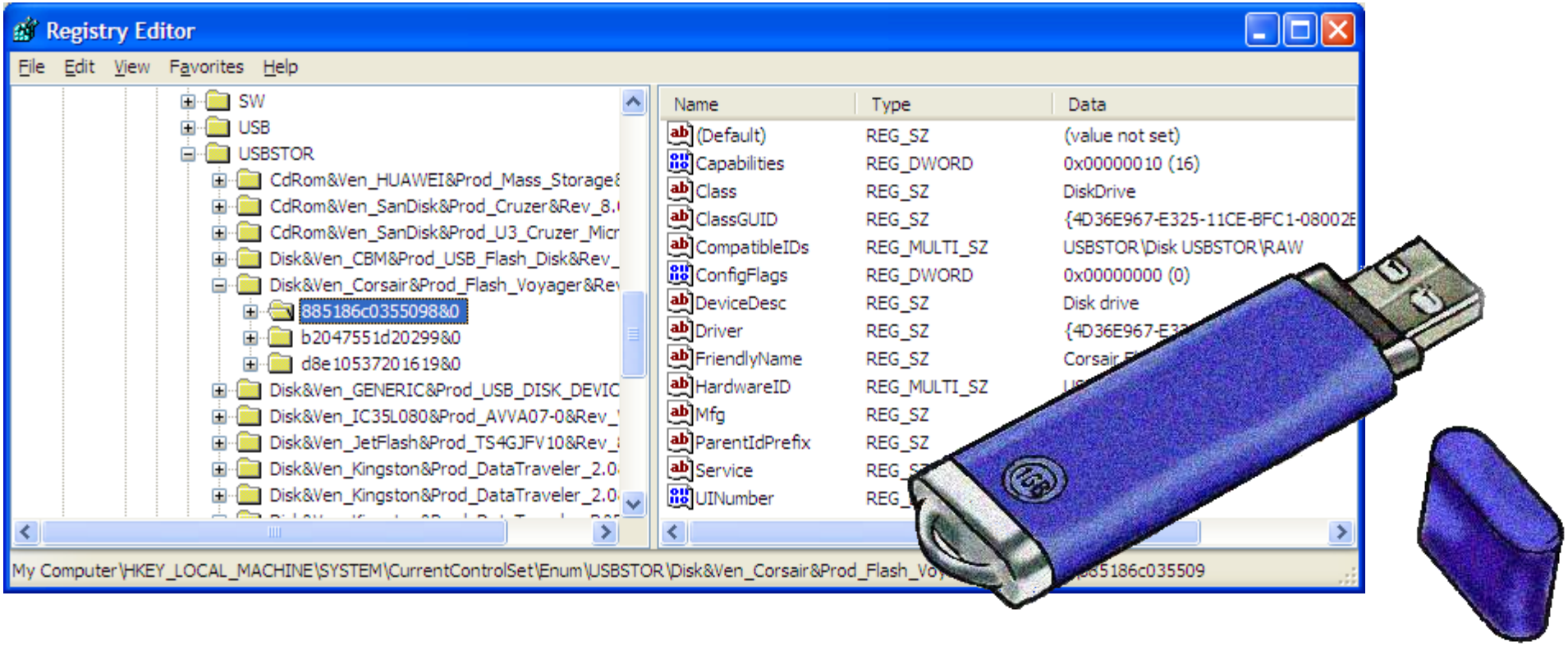
- Återskapa register
- Analysera data

Datautvinning: MS Word-tempfil



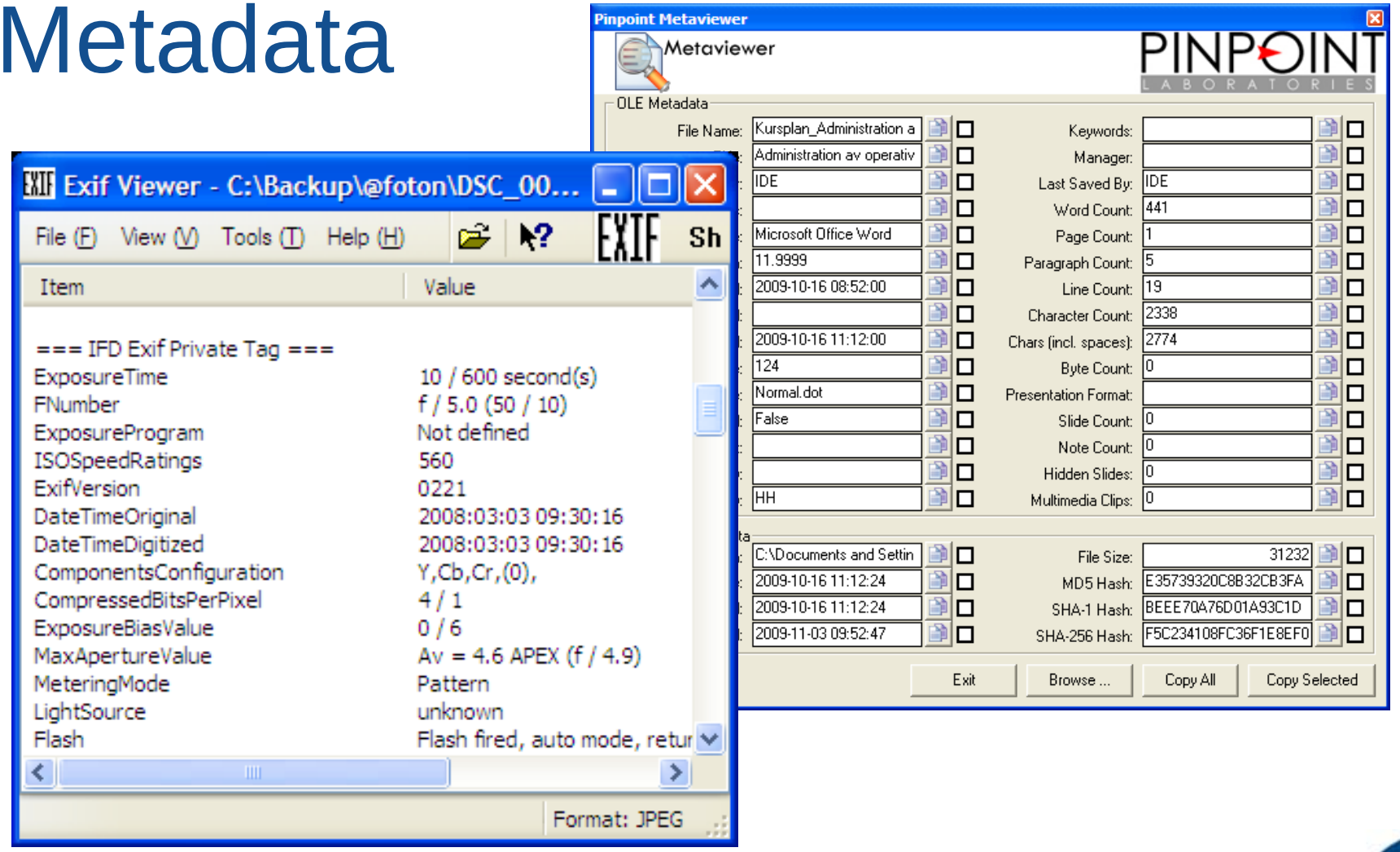
Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

Windows konfigurationsdatabas



Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

Metadata



Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

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-foren-siska verktyg I	Utredning av IT-brott eller Examensarbete
	Datornätverk I	Datornätverk II	Nätverkssäkerhet	Riskanalys och IT-säkerhetssystem

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