Ch. 5
EnCase Concepts

Översikt

- Bevisfilen
- CRC/ MD5
- E01-formatet
- Verifikation
- Hashing
- Case-filen
- Backupper
- Konfigurationsfiler

Avbild eller kvalificerad avbild?

- dd
  - rådata
  - (checksummor)
  - hashsummor
  - olika filer
- EnCase
  - information om fallet (bag&tag)
  - rådata
  - checksummor
  - hashsummor
  - allt i samma fil

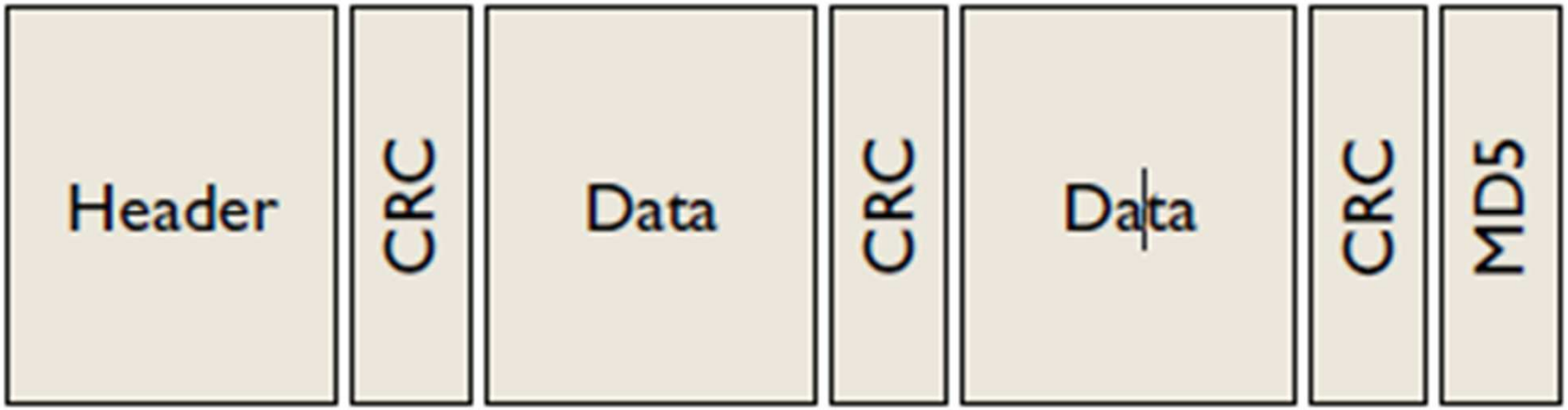
CRC

- CRC-32
- 32 bitars checksumma (4*10^9)
- Snabb och enkel
- Syfte: detektera alla omgångar med bitfel, 1..n bitar i längd
- Varför?

MD5

- Cryptografisk checksumma
- Checksumman är 128 bitar eller 32 hexadecimala tecken
- (~340*10^36)
- Tung att beräkna
- Syfte: att inte kunna forceras på manuell väg, att indikera förändringar

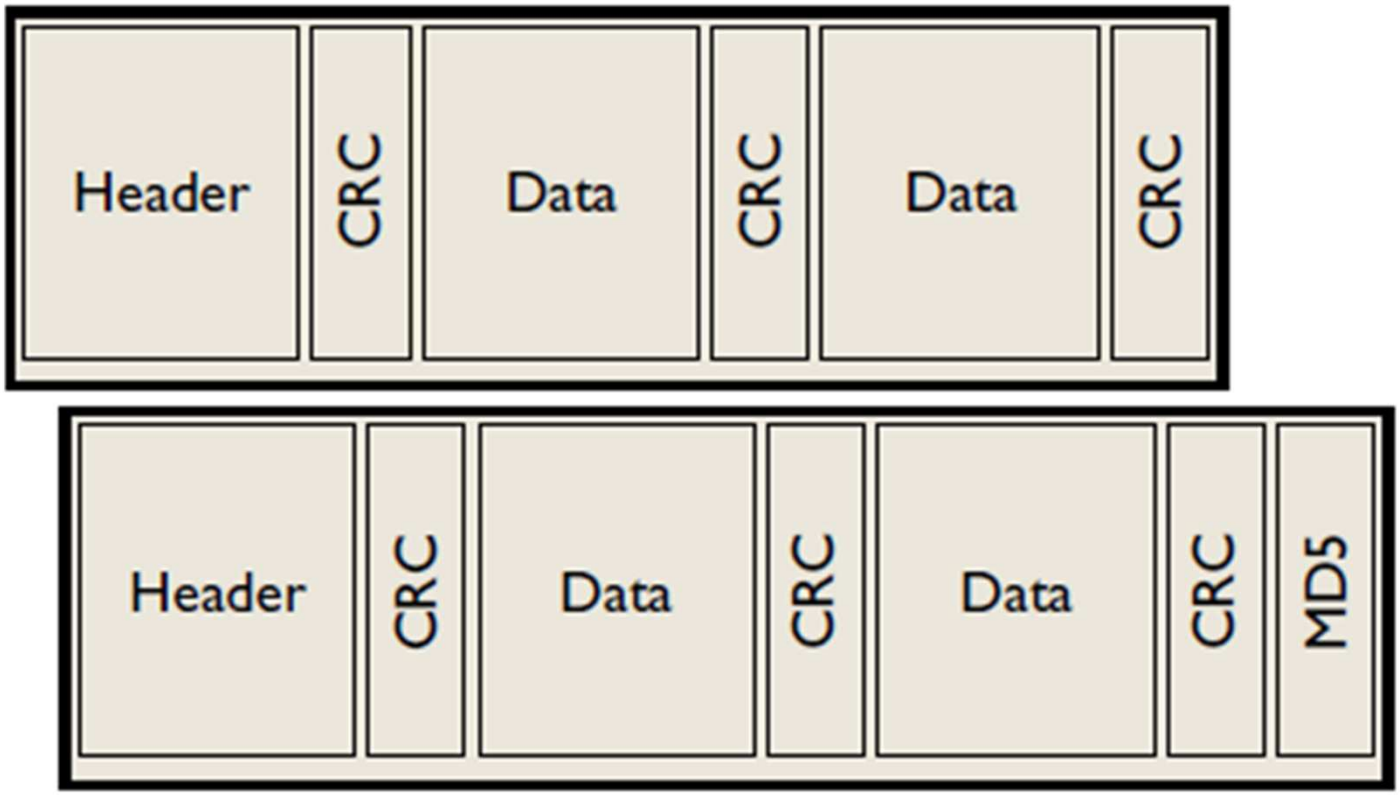
Bevisfilen



Bevisfilen

- Bevisnamn
- Bevisnummer
- Anteckningar
- Datum/tid för inhämtning
- Version av EnCase som användes
- OS som användes
- Komprimeras!

Stora bevisfiler



Verifikation

- Varje datablock kontrolleras mot sin CRC
- Hela datafilen kontrolleras mot MD5
- Krockar?
- Demonstration

Hashning

- Beräknar hashsumma
- Har tidsstämplar
- Kan ge stöd åt rapporten

Case-filen

- Innehåller allt vi gjort
  - Bevisfilen är ju oförändrad
- Pekare till bevisfiler
- Sökresultat
- Backuper!!!
  - Automatisk
  - Manuell

Konfiguration

- Keyword.ini
- TextStyles.ini
- FileSignatures.ini
- FileTypes.ini
- Viewers.ini
- SecurityIDs.ini

- Backup?

Övrigt

- RecordCache
- Återinhämtning
- Bevisfilens storlek