Computer Forensics

Göran Fornbrandt

Computer Forensics

Insamlandet av digitala spår som kan

presenteras och användas i rättsliga sammanhang

Var finner vi elektroniska bevis?

- Hårddiskar

- Mobiltelefoner

- Handdatorer

- Flashminnen

- USB-pinnar

- CD-skivor, disketter m.m.

Digitala spår i kriminalutredningar

- Ett mord som utfördes för 10 år sedan skulle hypotetiskt kunna finna sin lösning i en dator som tidigare ägts av misstänkt trots att den har varit omformaterad och ominstallerad samt använts flera år efter händelsen.

- En forensisk undersökning av hårddisken visar att mördarens detaljerade planer går att återskapa.

Digitala spår i företagssammanhang

- Kopiering av företagssensitiv information till tredje part
  - Kunddatabaser
  - Produktutveckling
  - Patent m.m.
- Brytande av policy regler (Omfattande surfande, nedladdning av musik, pornografi m.m.)
- Ekonomiska oegentligheter som bedrägerier, förskingring m.m

Digitala spår i datorn

- Filer
- Cookies
- Cache-minne
- Internethistorik
- E-mail kommunikation

Vad sparas på hårddisken?

- Aktivt sparade filer
- Anslutning av nya enheter
- Sökningar på Internet
- Data automatsparas utan användarens vetskap

Raderad information

Finns den?

- Visuellt raderad för användaren
- Innehållsförteckningen borta informationen finns kvar
- Hur länge?

Computer Forensics Metodologi

Bevissäkra

data

Metodologi

- Starta aldrig originaldisken i traditionell miljö
- Dator i drift! Olika lösningar beroende på programvara, system.
- Gör aldrig en analys på originaldisken

Metodologi - bevissäkring

- Dokumentation/märkning av chassi och tillhörande hårddisk

Metodologi - bevissäkring

En spegelkopia görs av hårddisken från

”Original” till   ”arbets-kopia”

- Checksummor skapas som visar överensstämmelse mellan original - kopia

Computer Forensics Metodologi

Bevissäkra data

Analys

Metodologi - analys

- Text, bilder m.m.
- Borttaget/ledigt utrymme
- E-mail i sin helhet/fragment, loggar m.m.
- Tecken på kopiering
- Var på hårddisken informationen finns och när den skapades

Metodologi - analys

Ytterligare funktioner

- Sökningar kan göras på kopian utan att tidstämplar och innehåll förändras
- Visuellt raderade dokument kan återskapas

Computer Forensics Metodologi

Bevissäkra Data → Analys → Resultat rapport

Chain of Custody

Metodologi - rapport

- Resultat av vad som framkommit vid analysen presenteras i en rapport
- Rapporten skall vara skriven så att även icke tekniskt insatta förstår sammanhanget

Vikten av rätt metodologi

- Rätt utförda förstahandsåtgärder ger god grund för fortsatt utredningsarbete

- Rättssäkerhet – skall gå att använda i domstol
- Svensk rätt

  - Fri bevisprövning

- Kan fria/fälla eller bli en pusselbit i utredningen