Analystekniker

Återställning av forensisk kopia
Raderade filer

Mattias Weckstén
IT-forensik och informationssäkerhet 120/180 hp

Återställning

- Forensisk kopia
- Kvalificerad forensisk kopia
- Borttagna filer
- Oallokerat utrymme
- Slackutrymme
- Skapa fillistningar
- Genomföra datasökningar

- (240)

Återställning av forensisk kopia

- Segementerad kopia
  - cat sammanfogar
- (242-243)

Återställning av kvalificerad kopia

- Beror på hur den kvalificerade kopian skapades
- Antagligen ”inbyggt”

- (244)

Montering av forensisk kopia

- NASAs utökade loopback-enhet
- Kräver kernel-stöd
  - Troligen inte ett problem

- (248-252)

Återställning av raderade filer

- Fatback
- TASK
- Foremost

- (260-264)

AutoPsy

- (264-268)

Grundläggande skrapning

- Foremost
  - Jobbar med signaturer
- (268-270)

Oallokerat, fritt och slackutrymme

- ntfsget
- (275-277)

Lista filer & metadata

- CATALOG
- Spara som kommaseparerad (semikolon) fil och ladda som ett kalkylark

- (278-281)

Whitelist/blacklist

- NIST
- Egna listor
- Skapa databas

- (282)

Förbereda för strängsökning

- Properitära format
- Packade filer
- Krypterade filer

- (282-283)

Strängsökning

- Sökteknik
  - Begränsa träffarna till en mängd som går att granska manuellt
  - Vilka måldata har du? Har man hackat lösenord eller kört program så har det kanske lämnat spår efter sig.
- (284-288)

Förbered

- Valfria fördjupningsuppgifter
  - Forensic Carving, Jim Keyzer
  - A smart carving approach, Metz och Mora
  - Introduktion till reguljära uttryck