Ch. 10
Advanced EnCase

Computer Security – an overview
Wecksten, M

Översikt

- Locating partitions
- Mounting partitions
- Mounting files
- Windows registry
- EnScript
- Filters
- Email
- Base64
- Encase Decryption Suite
- Virtual File System
- Exporting
- Restoration
- Physical Disk Emulator

Partition restoration

MBR raderad – vad göra

- Försök hitta VBR
- • Varför? Vi kan ju göra fritextsök.
- • Första VBR har sin naturliga plats i slutet av track 1 (=sektor 63)
- • FDISK tömmer MBR men ej VBR
- • Återuppbygga MBR

Add partition

- Demo

Partition finder

- Träffar -> Bookmarks
- • Sortera efter sektor = i ordning på disken
- • Inkapslade partitioner?

Montera filer

- Komplexa filer
  - Zip
  - Tar
  - Cab
- Men även
  - Doc
  - Ppt
  - Pst
  - ...

Registryn

- Vad
- Hur
- ROT13

- Montera i EnCase
- Regmon

- Hur går jag vidare?

EnScript

- C++/Java-liknande
- Change root
- Använda

Filters

- Skrivna i kod
- Hur börja?

Email

- I sökdialogen
- Records
- Varför?

Base64

- Bild -> text

EnCase Decryption Suite

- Underlätta knäckning
- Underlätta om du har lösen

- Knäckning → Rainbow tables
- Återvinning → Memdump-analys

Virtual File System

- Underlättar direktaccess

Physical Disk Emulator

- VFS?
- Alternativ.