

Ch. 8

File Signature Analysis and Hash Analysis



Computer Security – an overview
Wecksten, M



Översikt

- File signatures and extensions
- Adding file signatures to EnCase
- Conducting a file signature analysis and evaluating the results
- Understanding the MD5 hash
- Creating hash sets and libraries
- Importing hash sets
- Conducting a hash analysis and evaluating the results

Extensions

- Applikationsanknytning
 - .jpg => bildvisare
 - .html => webläsare
 - ...
- Windows
 - \Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- MAC
 - Filetype/ Creator

Signaturer

- Signatur = unikt mönster för alla filer av en viss typ
- Signaturer hittas i globala fältet under File Signatures
- Exempel

Signaturanalys

- Använd söknappen.
 - För övningens skull – kryssa endast i signaturanalys.
- Match
- *Alias
- Unknown
- !Bad Signature

MD5 / SHA / kryptografiska checksummor

- Sortera bort kända filer (varning!)
- Sortera ut kända skadliga filer.
- Ger oss en möjlighet att i rapporten identifiera tex. olagliga bilder utan att ta med själva bilden i rapporten.

Hash-bibliotek

- Två steg
 - Skapa hash-set
 - Klassificera m.h.a hash-set
- Exempel

Importera hash sets

- Färdiga hash sets
 - NSRL
- Distribuera i organisationen

Hash-analys

- Markera vilka hash-set du vill analysera mot
 - Genomför hashgenerering för de filer du vill kontrollera
 - Analysera resultatet.
 - Conditions