Ch. 9
Windows OS Artifacts

Översikt

- Windows date&time
- Recycle bin & INFO
- Windows Vista Recycle bin
- Links
- Folders
- Recent folder
- Desktop folder
- My Documents
- Send To
- Temp
- Favorites
- Windows Vista Low
- Cookies
- History
- Temporary Internet files
- Swap
- Hibernation
- Printing
- Shadow copy
- Event logs

Tidszon

- Viktigt, speciellt om datorn stått i annan tidszon.
- Windows = 64-bit tidsstämpel, upplösning 100ns
- Trick: för att jämföra två tidsstämplar räcker det att beräkna differensen och räkna om denna till en offset i timmar eller minuter.
- Problem: Olika filsystem lagrar tid på olika vis.
- Tidsinställningarn hittas i registryn.
- BIOS tidsuppfattning krävs också.
- Trixigt = Case-processorn

Unix/ Windows time

- 32 bit, upplösning 1 sekund
- Start 1970
- Slut 2038 – varför?

Papperskorgen

- Kasta i papperskorgen
- Radera fil från MFT
- Skapa ny referens i papperskorgen enligt DX#.EXT
- XP -> # = {1..}

INFO2

- Filnamn och sökväg -> INFO2
  - Både i ASCII och Unicode
  - Tidsstämpel för borttagning
  - Index
- Records = 800 byte
- Tom = 20 bytes
  - INFO2-filens slack!
  - Radering: X -> 0x00

Vems var filen?

- Namnet på papperskorg-foldern = SID
- SID kan slås upp i SAM och mappas mot en användare
- Endast för lokala användare!

Papperskorgen avstängd?

- Recycle bin properties
- HKEY/LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/BitBucket
- NukeOnDelete

Recycling in Vista

- Hela filen/foldern blir en indexfil

Link files

- Varför är länkar viktiga?

Länkar

- Påvisar aktivitet från användaren
- • Länken kanske finns kvar trots att filen är borta
- • Volymens serienummer
- • Filens storlek
- • Tidsstämplar
- • (Recent-foldern)
- • Trixigt -> Case-processorn

Special folders

- Systemfolder
- • Användarfolder
- • Recent
- • Desktop
- • Documents
- • Send To
- Temp
- • Favorite
- • Cookies
- • History
- • Vista Low

Interesting files

- Temporärfiler (Internet)
- • Swap
- • ClearPageFileAtShutdown ?
- • Hibernation
- • Hur hantera?
- • Printspol

Vista shadow copy

Events

Vista Shadow Files

- ”Autobackup”
- • Ej öppet.
- • Vanlig sökning.

Event Logging

- • Audit level
- • Parsing

Event Log Analysis

Advanced EnCase

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?