Forensische Analyse Windows NT

Eduard Blenkers
Senior Consultant

Kopieren von Datenträgern

- Physikalische Kopie des Datenträgers
  - “1:1-Kopie”, “Bit-Stream-Copy”, “Physical-Backup”
- Die Originalplatte nicht beschreibben
  - Jumper am Laufwerk (selten)
  - Mount-Befehl
  - Spezial-Kabel verwenden

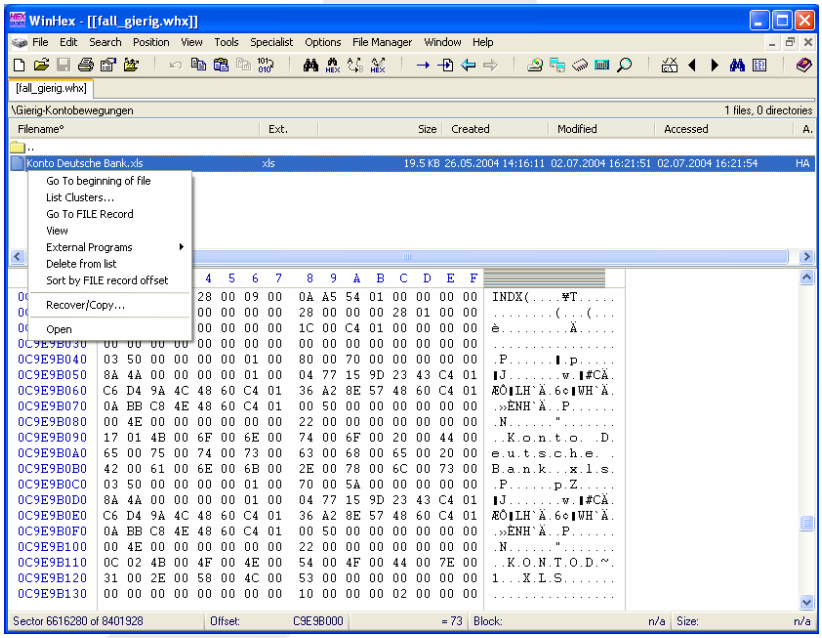
Fallstricke bei Bitstream-Copy

- Defekte Sektoren
  - Im Protokoll beschrieben?
  - Behandlung defekter Sektoren beim Restore?
- Data-Hiding über Bad-Block-Tabelle
  - Bad-Block in FAT manuell gesetzt
  - Bad-Sektor Markierung im Sektor-Header gesetzt
- Host Protected Area?

Festplatten durchsuchen

Was **`find`** oder **`grep`** nicht zeigen

Unerläßlich: WinHex



Alternate Datastreams

- ADS im Einsatz: (nur NTFS-Partition)
  - `echo hello > test.txt:mystream`
  - `dir test.txt` => Filesize 0 Byte
  - `more < test.txt:mystream`
- Suchen mit diversen Tools wie
  - sfind von foundstone.com
  - streams von sysinternals

Slackspace

- Plattenspeicher ist belegt, aber nicht genutzt
  `echo „hallo“ > file.txt`
- Genutzt: 5 Bytes
- Belegt: 1 Cluster (z. B. 2 kByte)
- Unterscheidung
  - RAM-Slack
  - Drive-Slack
- Auslesen z. B. mit WinHex

$LogFile

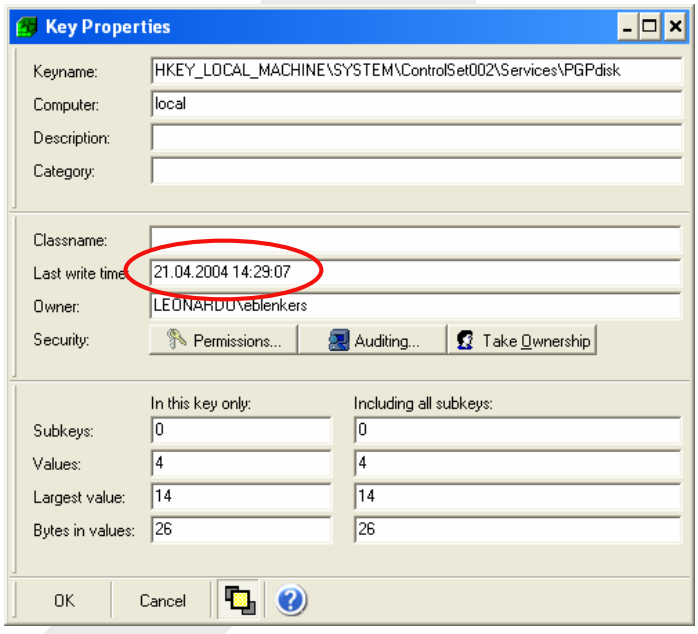
- Enthält Redo bzw. Undo-Logs
- Update Sequence Number (USN)
- Werkzeug: winhex, bintext, gextract, fsutil ...

Dateien kopieren

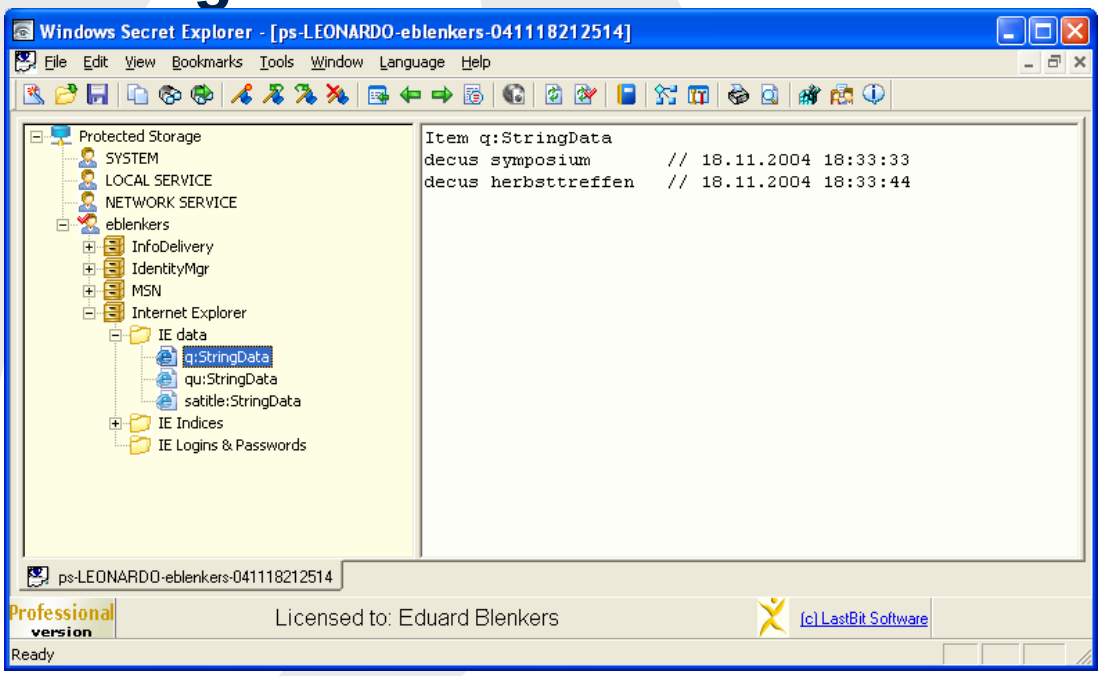
```
copy /B file1.gif+file2.gif file3.gif
```

- Ergebnis: File2.gif ist vor einigen Bildbetrachtern versteckt
- Rekonstruktion z. B. über gextract.exe von NTi

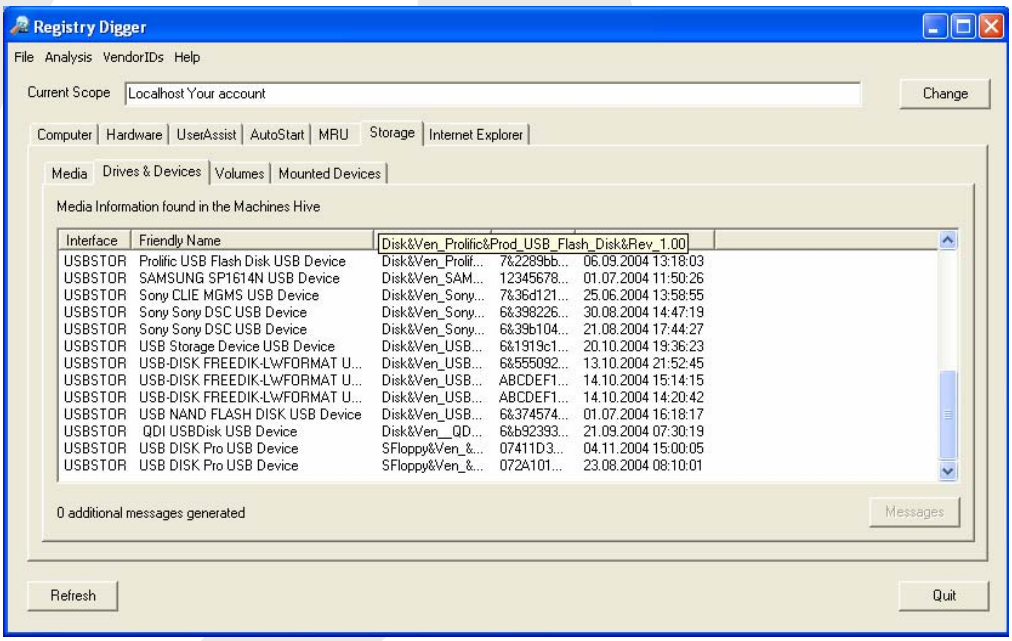
Resplendent Registrar



Secret Explorer: Protected Storage



RegistryDigger: Schneller Überblick



Fragen?

Omicron Deutschland
Herderstr. 26
40721 Hilden
02103 / 28 79-00
www.omicron.ch