Mag. iur. Dr. techn. Michael Sonntag

Drive investigation

Computer Forensics, Budapest 2008

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

Agenda

- Install the software:
  - → Filedisk
  - → WinHex, Cygwin
- Search for deleted files and reconstruct them
  - → WinHex: Deleted file (FAT)
  - → Reconstruct: If possible
- Discovering hidden files: Wrong extension
  - → Cygwin: "file" command
- Windows ADS
  - → LADS – Find the picture hidden in an ADS
- Timestamps
  - → WinHex: Analyze timestamps and convert them
- Running time of your Windows computer
  - → Analyze the event log

Scenario

❶

❷

❷

❸

Images

- Source of images: http://dftt.sourceforge.net/
  - → ❶ 6-undel-fat.zip
    - » FAT image
  - → ❷ 8-jpeg-search.zip
    - » NTFS image
  - → ❸ 5-fat-daylight.zip
    - » FAT image

- Requirements:
  - → Operating System: Windows (XP; NT, 2K, Vista: ???)
  - → Harddisk space:
    - » Scenarios: 18 MB
    - » Cygwin: 674 MB
    - » Other software: 4 MB

Software installation

- Filedisk: Mounting a disk image as a drive under Windows
  - → Requires Administrator access and a reboot
  - → Procedure:
    - » Copy driver (filedisk.sys) to %SYSTEMROOT%\system32\drivers
    - » Import "filedisk.reg" into the registry (double-click on it)
    - » Reboot the computer
  - → Attention: When mounting an image, you must always give the full path to the file!
    - » E.g. "filedisk /mount 0 C:\temp\image.dd"
- Install "Winhex"
  - → Not really needed; can be run directly from CD!
    - » Copy to harddisk for faster start if desired

Software installation

- Install "Cygwin"
  - → Linux-like environment (and programs) under windows
  - → Procedure:
    - » Execute "setup.exe" and choose to install from local path
      - – Select the Subdirectory with "ftp…" in it as install source
      - – No spaces in the path of destination directory
        E.g. **not** C:\Program Files\...
    - » Change selection to "install" on the "All" selection
  - → Add the binary directory to the path
    - » Control panel – System – Advanced – Environment Variables →
      Add to user variables the complete path, e.g. ";C:\Cygwin\bin"

Search for deleted files: FAT

- Find and recovery the deleted files in image ❶!
- Your task:
  - → Find out, which files did at some time exist in the image
    - » Recovery through WinHex!
    - » Manual recovery not possible due to eval. version limitations
  - → Recover these files
    - » Check their MD5 values
- Document your actions through a log and screen shots!

- Hints:
  - → FAT1 starts at offset 0x1000, FAT2 (=copy) at 0x4000
  - → Root directory is at offset 0x7000

Search for deleted files: FAT

- MD5 table of correctly recovered files
  - → Filename File size MD5 value
  - → \SING.DAT 780 59B20779F69FF9F0AC5FCD2C38835A79
  - → \MULT1.DAT 3801 FFD27BD782BDCE67750B6B9EE069D2EF
  - → \FRAG1.DAT 1584 7A3BC5B763BEF201202108F4BA128149
  - → \FRAG2.DAT 3873 0E80AB84EF0087E60DFC67B88A1CF13E
  - → \DIR1\
  - → MULT2.DAT 1715 59CF0E9CD107BC1E75AFB7374F6E05BB
  - → DIR2\
  - → FRAG3.DAT 2027 21121699487F3FBBDB9A4B3391B6D3E0

Discovering hidden files: Wrong extensions

- Find out, which of all the files in image ❷ are jpg pictures!
- Your task:
  - → Collect all files, except those in archives
    - » How many are these?
  - → Identify their file type
    - » Do this manually (Winhex)
      - – Check first in the internet: How to recognize a JPG file
    - » Use the command "file"
      - – Inspect the "magic" file and find the description for JPG files
    - » Use command "strings" (file1.jpg, file4.jpg, file12.doc, cmd.exe)
  - → Identify the file type of the archives
- Document your actions through a log and screen shots!

Windows ADS

- Find the hidden picture!
- In the image ❷ there is an additional picture hidden
  - → This is located within an alternate data stream
- Your task:
  - → Find the location of the hidden picture
  - → Extract the picture into a separate "normal" file
  - → Add the picture to another file and to a directory
    - » Not "into" the directory, but to the directory entry itself!
    - » Name the ADS "new*picture"
      - – Could you create a normal file with this name?
- Document your actions through a log and screen shots!

Timestamps

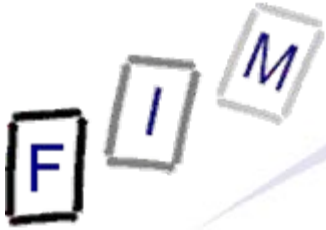
- Find out when the two files in image ❸ were actually created
- Your task:
  - → Check the date through the Windows command line
    - » Would changing the local time zone influence the output?
    - » Compare this to your Windows drive (hint: FAT ⇔ NTFS!)
  - → Find out where the creation time is located on the disk
    - » Don't use the Winhex UI; first think and calculate, then verify!
  - → Manually calculate the creation time from the hex values
    - » Search the internet for the exact format
  - → Use DCode to decode the creation time
  - → When were the files created in UTC?
- Document your actions through a log and screen shots!

Windows Startup/Shutdown time

- Investigate your own computer:
  - → When was it turned on and off during the last week?
    - » Investigate in the Internet which events are logged when!
  - → Draw a timeline to visualize your results!

Conclusions

- Undelete is quite simple on FAT
  - → But complex/impossible on NTFS/EXT3!
  - → "Plain text" search will still work unless actually overwritten
- Hiding files is quite simple: Wrong extensions and ADS
  - → Found only with good knowledge and additional tools
    - » But **VERY** difficult to **REALLY** hide information!
- Even with very simple means a lot of information can be extracted, if it is exactly known where to look for it
  - → But also its limitations must be known!
- Timestamps (or timing issues) are an important aspect for every forensic investigation
  - → The time zone is very important there
    - » Is the data stored in local or UTC (or …) time?
    - » What is the difference to UTC now (and what was it then?)



Questions?

Thank you for your attention!