ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Amir Alsbih and Christian Schindelhauer

Distributed Storage and

Computer Forensic

2

Tool Review

The Sleuth Kit (TSK)

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

- File System Layer:
  - #fsstat: Display general details of a file system
- Data Layer:
  - #blkstat: Display details of a file system data unit
  - #blkls: List or output file system data units
  - #blkcat: Display the contents of file system data unit
  - #blkcalc: Converts between unallocated disk unit numbers and regular disk unit numbers
- Metadata Layer:
  - #istat: Display details of a meta-data structure
  - #ils: List inode information
  - #icat: Output the contents of a file based on its inode number
  - #ifind: Find the meta-data structure that has allocated a given disk unit or file name
- File Name Layer:
  - #fls: List file and directory names in a disk image
  - #ffind: Finds the name of the file or directory using a given inode
- Journal Layer:
  - #jls: List the contents of a file system journal
  - #jcat: Show the contents of a block in the file system journal
- Media Layer:
  - #mmstat: Display details about the volume system (partition tables)
  - #mmls: Display the partition layout of a volume system (partition tables)
- Disk Layer:
  - #disk_sreset: removes HPA from disk
  - #disk_stat: display size information of a hard disk

4 Windows Forensics

PSEXEC

- psexec: Executes commands on a remote windows machine.
  - Need administrator password
- *psexec –u username –p passsword \\remote_IP command*

6 System Registry

%WINDIR%\System32\Config

- SYSTEM:

  Contains system startup, startup files, machine configurations, …
- SOFTWARE:

  Contains the settings for applications
- NTUSER.DAT:

  Contains the configuration and environement settings
- SAM:

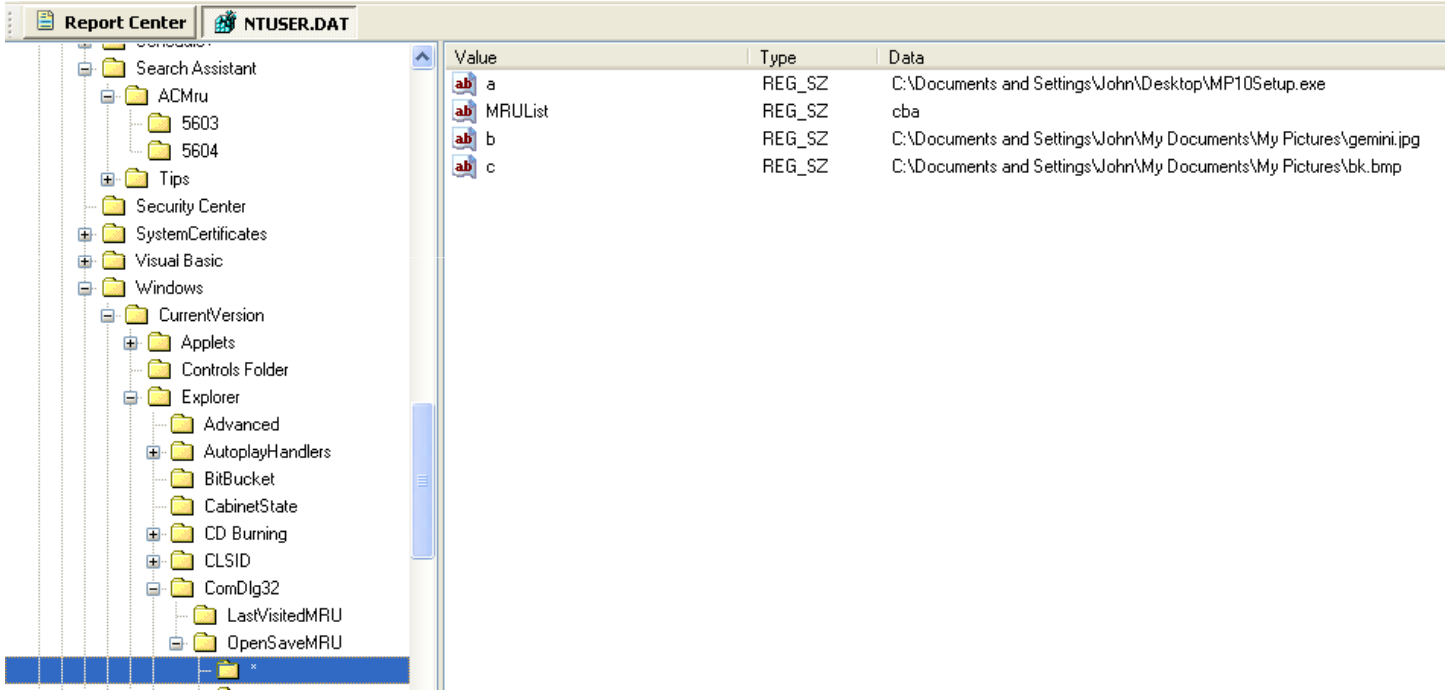
  Contains all the local user accounts and groups
- SECURITY:

  Contains all the security information including password policies, membership of group information,…

NTUSER.DAT - Examples

- Last Files Saved:
  - \Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSave MRU*
- Typed URLS:
  - \Software\Microsoft\Internet Exploter\TypedURLs
- Last Commands Executed:
  - \Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Search History
  - \Software\Microsoft\Search Assistant\ACMru
    - 5603: Part of the Filename
    - 5604: Part of the Filecontent

NTUSER.DAT: Last Files Saved



NTUSER.DAT: Typed URLS

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Report Center | NTUSER.DAT

- GDIPlus
- Internet Connection Wizard
- Internet Explorer
  - Desktop
  - Document Windows
  - Download
  - Explorer Bars
    - {32683183-48a0-441b-a342-7c
  - Extensions
  - Help_Menu_URLs
  - InformationBar
  - IntelliForms
  - International
  - Main
  - Media
  - New Windows
  - PageSetup
  - SearchUrl
  - Security
  - Services
  - Settings
  - Styles
  - Toolbar
  - TypedURLs
  - URLSearchHooks

Value	Type	Data
url1	REG_SZ	http://www.wunderground.com/US/HI/Lihue.html
url2	REG_SZ	http://www.orbitz.com/
url3	REG_SZ	alohaair
url4	REG_SZ	http://www.hawaiianair.com/
url5	REG_SZ	http://www.google.com/
url6	REG_SZ	http://www.noaa.gov/
url7	REG_SZ	http://surfline.com/
url8	REG_SZ	http://orbitz.com/
url9	REG_SZ	http://www.equineonline.com/
url10	REG_SZ	http://www.hotmail.com/
url11	REG_SZ	noaa.com
url12	REG_SZ	http://www.google.com/search?hl=en&q=kauai+weather&btnG=Google+Search
url13	REG_SZ	http://www.ebay.com/
url14	REG_SZ	https://www.expedia.com/pub/agent.dll?qscr=apwd
url15	REG_SZ	http://www.iriver.com/
url16	REG_SZ	http://www.target.com/
url17	REG_SZ	http://www.dillards.com/
url18	REG_SZ	www.urban outfitters.com
url19	REG_SZ	www.ambercrombie and finch.com
url20	REG_SZ	http://www.gap.com/
url21	REG_SZ	www.forever21.com
url22	REG_SZ	http://www.forever21.com/
url23	REG_SZ	www.old navy.com

rip.pl (RegRipper)

- *#rip.pl –r <HIVEFILE> -f <HIVETYPE>*

Hivetype:

- ntuser
- sam
- security
- software
- system

```
TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Fri Apr 29 15:52:21 2005 (UTC)
  url1 -> http://www.wunderground.com/US/HI/Lihue.html
  url2 -> http://www.orbitz.com/
  url3 -> alohaair
  url4 -> http://www.hawaiianair.com/
  url5 -> http://www.google.com/
  url6 -> http://www.noaa.gov/
  url7 -> http://surfline.com/
  url8 -> http://orbitz.com/
  url9 -> http://www.equineonline.com/
  url10 -> http://www.hotmail.com/
  url11 -> noaa.com
  url12 -> http://www.google.com/search?hl=en&q=kauai+weather&btnG=Google+Search
  url13 -> http://www.ebay.com/
  url14 -> https://www.expedia.com/pub/agent.dll?qscr=apwd
  url15 -> http://www.iriver.com/
  url16 -> http://www.target.com/
  url17 -> http://www.dillards.com/
  url18 -> www.urban outfitters.com
  url19 -> www.ambercrombie and finch.com
  url20 -> http://www.gap.com/
  url21 -> www.forever21.com
  url22 -> http://www.forever21.com/
  url23 -> www.old navy.com
```

Timeline for the Registry

- *#regtime.pl –m <HIVETYPE> -r <HIVEFILE> >> bodyfile*
- *HIVETYPE:*
  - HKLM-SYSTEM
  - HKLM-SAM
  - HKLM-SECURITY
  - HKLM-SOFTWARE
  - HKLM-USER-USERNAME

Deleted Registry Keys

#Deleted.pl <HIVEFILE>

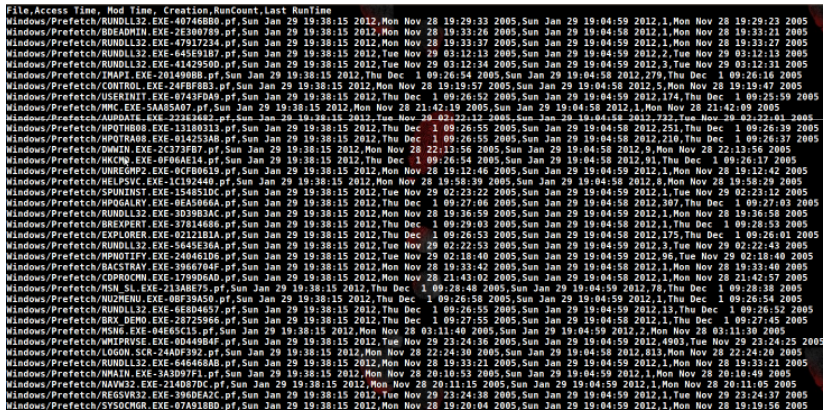
```
"...\SystemRoot\System32\Config\SAM"
[Thu Dec  1 10:03:58 2005]

########## RECOVERED KEYS: ##########

SAM\SAM\Domains\Account\Users\Names\Employee\
[Mon Dec  1 22:23:32 2003]
        -->1007; Default;
SAM\SAM\Domains\Account\Users\000003EF\
[Mon Jul 25 08:00:42 2005]
        -->REG_BINARY; F; 02 00 01 00 00 00 00 00 70 a7 ac 2f 86 55
 01 ef 03 00 00 01 02 00 00 10 02 00 00 00 00 00 00 01 00 d4 0f 00
           ........p<A7><AC>/<86>U<C5>.........µ<AE><C0>Y<B8><C3>..
        -->REG_BINARY; V; 00 00 00 00 bc 00 00 00 02 00 01 00 bc 00
 00 c8 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 00 00 00 00 00 0
00 00 00 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 fc 00 00 00 0
1 00 00 14 00 00 00 00 00 00 00 30 01 00 00 14 00 00 00 00 00 00 00
 00 00 00 14 00 00 00 44 00 00 00 02 00 30 00 02 00 00 00 02 c0 14
07 00 00 00 02 00 58 00 03 00 00 00 00 00 24 00 44 00 02 00 01 05 0
0 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 00 00 14 00 5b 03
 00 00 00 00 05 20 00 00 00 20 02 00 00 54 00 65 00 63 00 68 00 6a
73 00 5c 00 6c 00 6f 00 67 00 69 00 6e 00 2e 00 62 00 61 00 74 00 f
0 01 00 f7 c8 10 5e 1f 79 f1 e4 87 87 62 3c bf a8 d6 d2 02 00 01 00
 cc d8 38
```

Windos Prefetch

- Help increase the efficency of the system by pre loading of content
- *#pref.pl –d PREFETCH_DIRECTORY –c*
- *List:*
  - *Last access*
  - *Last modification*
  - *Number of times the programm was executed*
  - *File creation of the prefetch file*



```
File,Access Time, Mod Time, Creation,RunCount,Last RunTime
Windows/Prefetch/RUNDLL32.EXE-40746BB0.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:29:33 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:29:23 2005
Windows/Prefetch/BDEADMIN.EXE-2E300789.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:33:26 2005,Sun Jan 29 19:04:58 2012,1,Mon Nov 28 19:33:21 2005
Windows/Prefetch/RUNDLL32.EXE-47917234.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:33:37 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:33:27 2005
Windows/Prefetch/RUNDLL32.EXE-645E9187.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 03:12:13 2005,Sun Jan 29 19:04:59 2012,2,Tue Nov 29 03:12:13 2005
Windows/Prefetch/RUNDLL32.EXE-41429500.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 03:12:34 2005,Sun Jan 29 19:04:59 2012,3,Tue Nov 29 03:12:31 2005
Windows/Prefetch/IMAPI.EXE-201490BB.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:54 2005,Sun Jan 29 19:04:58 2012,279,Thu Dec  1 09:26:16 2005
Windows/Prefetch/CONTROL.EXE-24FBF8B3.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:19:57 2005,Sun Jan 29 19:04:58 2012,5,Mon Nov 28 19:19:47 2005
Windows/Prefetch/USERINIT.EXE-0743FDA9.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:52 2005,Sun Jan 29 19:04:59 2012,174,Thu Dec  1 09:25:59 2005
Windows/Prefetch/MMC.EXE-5AA85A07.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 21:42:19 2005,Sun Jan 29 19:04:58 2012,1,Mon Nov 28 21:42:09 2005
Windows/Prefetch/AUPDATE.EXE-222E2682.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 02:22:12 2005,Sun Jan 29 19:04:58 2012,732,Tue Nov 29 02:22:01 2005
Windows/Prefetch/HPQTHB08.EXE-13180313.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:55 2005,Sun Jan 29 19:04:58 2012,251,Thu Dec  1 09:26:39 2005
Windows/Prefetch/HPQTRA08.EXE-014253AB.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:55 2005,Sun Jan 29 19:04:58 2012,210,Thu Dec  1 09:26:37 2005
Windows/Prefetch/DWWIN.EXE-2C372FB7.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 22:13:56 2005,Sun Jan 29 19:04:58 2012,9,Mon Nov 28 22:13:56 2005
Windows/Prefetch/HKCMD.EXE-0F06AE14.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:54 2005,Sun Jan 29 19:04:58 2012,91,Thu Dec  1 09:26:17 2005
Windows/Prefetch/UNREGMP2.EXE-0CFB0619.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:12:46 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:12:42 2005
Windows/Prefetch/HELPSVC.EXE-1C192440.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:58:39 2005,Sun Jan 29 19:04:58 2012,8,Mon Nov 28 19:58:29 2005
Windows/Prefetch/SPUNINST.EXE-154851DC.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 02:23:22 2005,Sun Jan 29 19:04:59 2012,1,Tue Nov 29 02:23:12 2005
Windows/Prefetch/HPQGALRY.EXE-0EA5066A.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:27:06 2005,Sun Jan 29 19:04:58 2012,307,Thu Dec  1 09:27:03 2005
Windows/Prefetch/RUNDLL32.EXE-3D39B3AC.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:36:59 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:36:58 2005
Windows/Prefetch/BREXPERT.EXE-37814686.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:29:03 2005,Sun Jan 29 19:04:58 2012,1,Thu Dec  1 09:28:53 2005
Windows/Prefetch/EXPLORER.EXE-02121101A.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:53 2005,Sun Jan 29 19:04:58 2012,175,Thu Dec  1 09:26:01 2005
Windows/Prefetch/RUNDLL32.EXE-5645E36A.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 02:22:53 2005,Sun Jan 29 19:04:59 2012,3,Tue Nov 29 02:22:43 2005
Windows/Prefetch/MPNOTIFY.EXE-240461D6.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 02:18:40 2005,Sun Jan 29 19:04:59 2012,96,Tue Nov 29 02:18:40 2005
Windows/Prefetch/BACSTRAY.EXE-3966704F.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:33:42 2005,Sun Jan 29 19:04:58 2012,1,Mon Nov 28 19:33:40 2005
Windows/Prefetch/CDPROCMN.EXE-179906AD.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 21:43:02 2005,Sun Jan 29 19:04:58 2012,1,Mon Nov 28 21:42:57 2005
Windows/Prefetch/MSN_SL.EXE-213ABE75.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:28:48 2005,Sun Jan 29 19:04:59 2012,76,Thu Dec  1 09:28:38 2005
Windows/Prefetch/NU2MENU.EXE-0BF39A50.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:58 2005,Sun Jan 29 19:04:59 2012,1,Thu Dec  1 09:26:54 2005
Windows/Prefetch/RUNDLL32.EXE-6E8D4657.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:26:55 2005,Sun Jan 29 19:04:59 2012,13,Thu Dec  1 09:26:52 2005
Windows/Prefetch/BRX_DEMO.EXE-28725966.pf,Sun Jan 29 19:38:15 2012,Thu Dec  1 09:27:55 2005,Sun Jan 29 19:04:58 2012,1,Thu Dec  1 09:27:45 2005
Windows/Prefetch/MSNG.EXE-04E65C15.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 03:11:40 2005,Sun Jan 29 19:04:59 2012,2,Mon Nov 28 03:11:30 2005
Windows/Prefetch/WMIPRVSE.EXE-0D449B4F.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 23:24:36 2005,Sun Jan 29 19:04:59 2012,4903,Tue Nov 29 23:24:25 2005
Windows/Prefetch/LOGON.SCR-24ADF392.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 22:24:30 2005,Sun Jan 29 19:04:58 2012,813,Mon Nov 28 22:24:20 2005
Windows/Prefetch/RUNDLL32.EXE-646468AB.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:33:21 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:33:21 2005
Windows/Prefetch/NMAIN.EXE-3A3D07F1.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 20:10:53 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 20:10:49 2005
Windows/Prefetch/NAVW32.EXE-214D87DC.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 20:11:15 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 20:11:05 2005
Windows/Prefetch/REGSVR32.EXE-396DEA2C.pf,Sun Jan 29 19:38:15 2012,Tue Nov 29 23:24:38 2005,Sun Jan 29 19:04:59 2012,1,Tue Nov 29 23:24:37 2005
Windows/Prefetch/SYSOCMGR.EXE-07A918BD.pf,Sun Jan 29 19:38:15 2012,Mon Nov 28 19:20:04 2005,Sun Jan 29 19:04:59 2012,1,Mon Nov 28 19:19:56 2005
```

Thumbnail-
Internet Explorer intel

- *#vinetto –s –o Output Thumbs.db*
- *#pasco –d, index.dat*