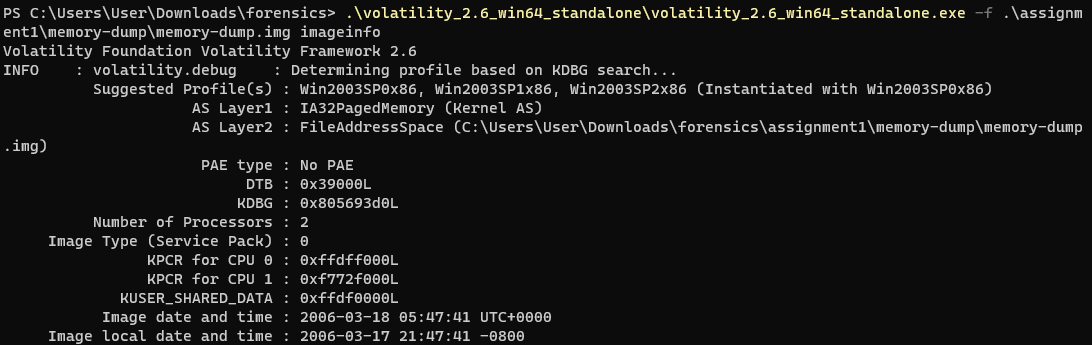
Task 1:

1. Command used : *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img imageinfo*

OS Version: Windows 2003

The 2 most-likely version profiles: Win2003SP0x86, Win2003SP1x86



1. Using the same commands as above,

Address Space Type: IA-32 paging address space

Processor Type: Intel Architecture

32 bits

1. Command used : *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 pslist*

Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit

---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------

0x8619d818 System 4 0 64 209 ------ 0

0x85fa6d88 smss.exe 356 4 3 17 ------ 0 2006-03-18 05:39:03 UTC+0000

0x85f758d8 csrss.exe 412 356 10 338 0 0 2006-03-18 05:39:05 UTC+0000

0x85f665f0 winlogon.exe 436 356 20 463 0 0 2006-03-18 05:39:06 UTC+0000

0x85f47840 services.exe 480 436 17 281 0 0 2006-03-18 05:39:08 UTC+0000

0x85f68b08 lsass.exe 492 436 26 363 0 0 2006-03-18 05:39:08 UTC+0000

0x85f27540 svchost.exe 620 480 11 195 0 0 2006-03-18 05:39:10 UTC+0000

0x85f07c90 svchost.exe 708 480 16 130 0 0 2006-03-18 05:39:11 UTC+0000

0x85ee8408 svchost.exe 852 480 7 105 0 0 2006-03-18 05:39:14 UTC+0000

0x85ee0bf0 svchost.exe 912 480 5 78 0 0 2006-03-18 05:39:15 UTC+0000

0x85ee2d88 svchost.exe 924 480 47 1049 0 0 2006-03-18 05:39:15 UTC+0000

0x85ec2b98 spoolsv.exe 1048 480 11 114 0 0 2006-03-18 05:39:16 UTC+0000

0x85ed3d88 msdtc.exe 1080 480 21 159 0 0 2006-03-18 05:39:16 UTC+0000

0x85eb4d88 svchost.exe 1196 480 2 54 0 0 2006-03-18 05:39:17 UTC+0000

0x85eb16c0 svchost.exe 1228 480 2 35 0 0 2006-03-18 05:39:17 UTC+0000

0x85c18d88 dfssvc.exe 1348 480 9 74 0 0 2006-03-18 05:39:18 UTC+0000

0x85b93608 wmiprvse.exe 1752 620 6 112 0 0 2006-03-18 05:40:57 UTC+0000

0x85b91d88 wmiprvse.exe 1788 620 6 170 0 0 2006-03-18 05:40:58 UTC+0000

0x85ef65f8 explorer.exe 396 380 11 257 0 0 2006-03-18 05:43:31 UTC+0000

0x85b4ad88 msiexec.exe 1480 480 5 72 0 0 2006-03-18 05:43:39 UTC+0000

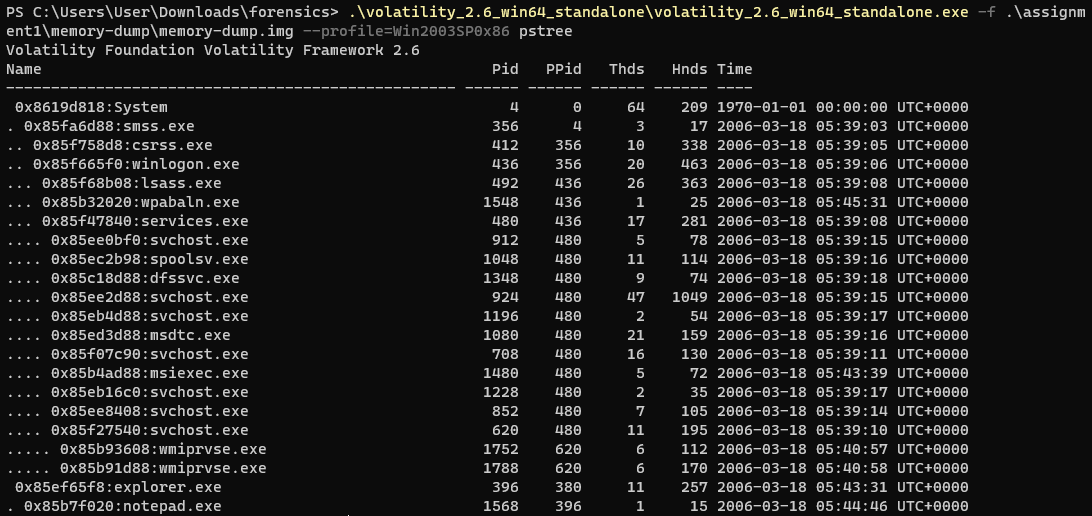
0x85b7f020 notepad.exe 1568 396 1 15 0 0 2006-03-18 05:44:46 UTC+0000

0x85b32020 wpabaln.exe 1548 436 1 25 0 0 2006-03-18 05:45:31 UTC+0000

1. Command used : *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 pstree*

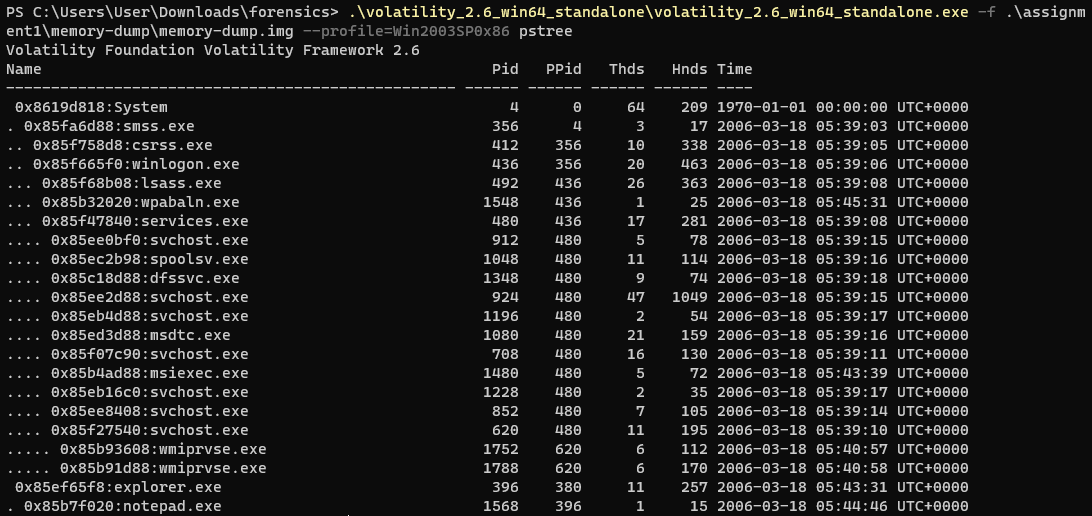
Text-Editor application executable name: notepad.exe

PID: 1568



1. Using the same command, looking for the PPID

Command used : *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 pstree*



PID: 396

Name of executable: explorer.exe

Time: 2006-03-18 05:43:31 UTC+0000

1. Command used : *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 dlllist --pid=1568*

*Base Size LoadCount Path*

*---------- ---------- ---------- ----*

*0x01000000 0x14000 0xffff C:\WINDOWS\system32\notepad.exe*

*0x77f40000 0xba000 0xffff C:\WINDOWS\system32\ntdll.dll*

*0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll*

*0x762b0000 0x47000 0xffff C:\WINDOWS\system32\comdlg32.dll*

*0x77290000 0x49000 0xffff C:\WINDOWS\system32\SHLWAPI.dll*

*0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll*

*0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll*

*0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll*

*0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll*

*0x77ba0000 0x54000 0xffff C:\WINDOWS\system32\msvcrt.dll*

*0x70ad0000 0xe6000 0xffff C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.100.0\_x-ww\_8417450B\COMCTL32.dll*

*0x77380000 0x7dd000 0xffff C:\WINDOWS\system32\SHELL32.dll*

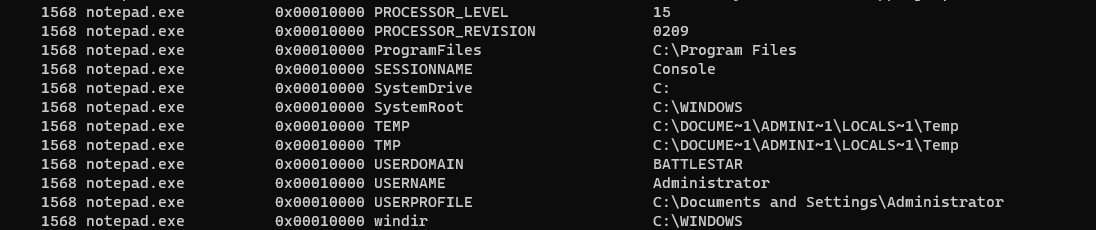
*0x73070000 0x26000 0xffff C:\WINDOWS\system32\WINSPOOL.DRV*

*0x71b70000 0x33000 0x1 C:\WINDOWS\system32\UxTheme.dll*

1. Command Used: *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 --pid=1568 envars*

Username: Administrator

Windows domain: BATTLESTAR

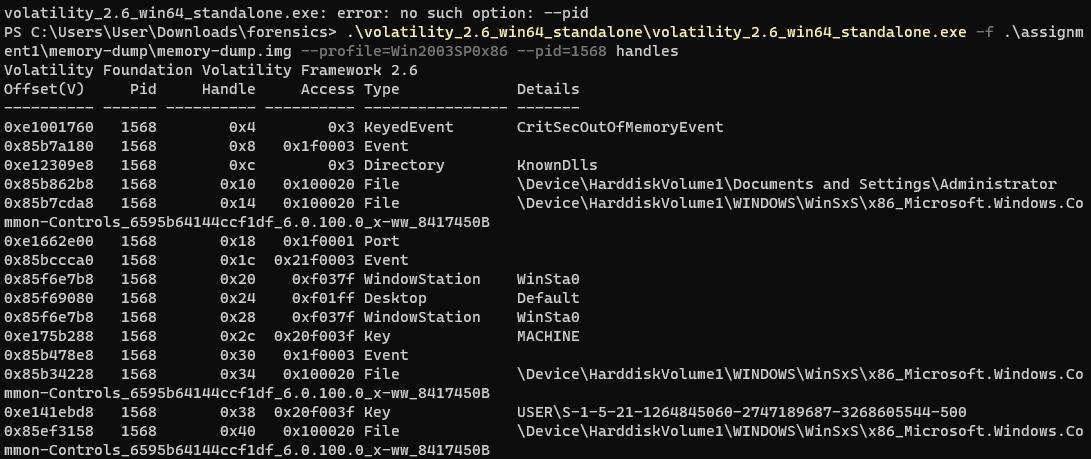


1. Command Used: *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 --pid=1568 handles*

Files:

\Device\HarddiskVolume1\Documents and Settings\Administrator

\Device\HarddiskVolume1\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.100.0\_x-ww\_8417450B



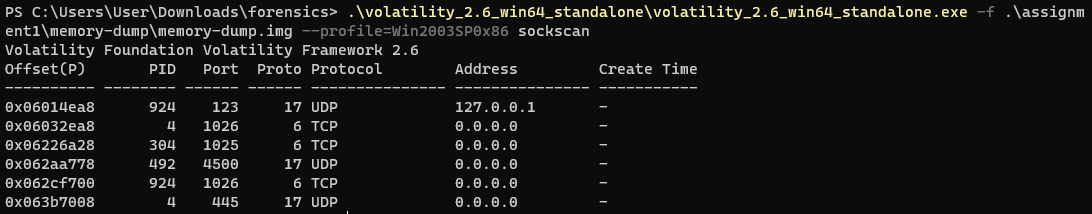
1. Command Used: *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 psscan*

| Executable Name | PID | Exit Time |
| --- | --- | --- |
| dllhost.exe | 1156 | 2006-03-18 05:38:32 UTC+0000 |
| spoolsv.exe | 1644 | 2006-03-18 05:38:31 UTC+0000 |
| setup.exe | 336 | 2006-03-18 05:38:31 UTC+0000 |

1. Command Used: *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 sockscan*

UDP port number: 17

PID: 924



Command Used to find executable name: *volatility\_2.6\_win64\_standalone.exe -f memory-dump.img --profile=Win2003SP0x86 –pid=924 pslist*

Executable Name: svchost.exe

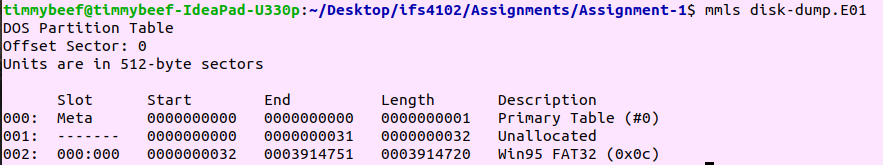
Task 2:

1. Command Used to display layout of disk: *mmls disk-dump.E01*

Sector 0-0 Primary Table

Sector 0-31 Unallocated

Sector 32-3914751 Win95 FAT32



1. Using the information in mmls above to find the file system

Command Used to find file system type of accessible partition: *mmls disk-dump.E01*

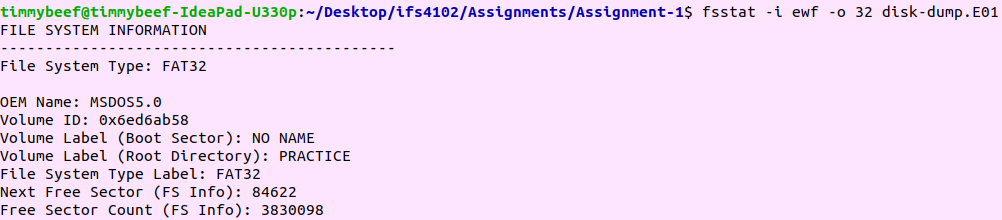
File-System Type: FAT32

1. Use *img\_stat disk-dump.E01* to find out the image type: ewf

Command used to find Volume ID and Label: *fsstat -i ewf -o 32 disk-dump.E01*

Volume ID: 0x6ed6ab58

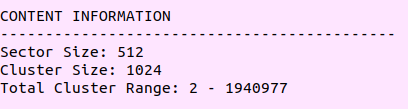
Volume Label: Practice



1. Command used to find Volume ID and Label: *fsstat -i ewf -o 32 disk-dump.E01*

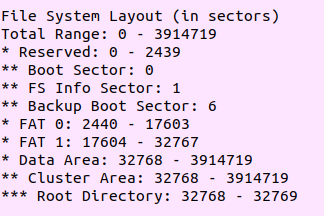
Sector Size: 512 bytes

Cluster Size: 1024 bytes



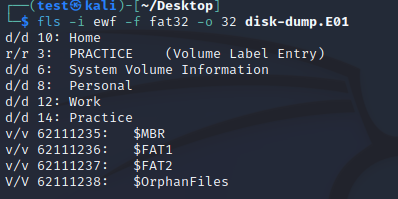
1. Command used to find Volume ID and Label: *fsstat -i ewf -o 32 disk-dump.E01*

Number of sectors in data area: 3914719-32768+1 = 3881952



1. Command used to find user-created directories: *fls -i ewf -f fat32 -o 32 disk-dump.E01*

Name of user created directories: Personal, Work, Practice



1. Command used to find deleted file and directories: *fls -i ewf -f fat32 -o 32 -rpd disk-dump.E01*

r/r \* 168: Home/New Microsoft Excel Worksheet.xlsx

r/r \* 172: Home/New Microsoft Excel Worksheet.xlsx

r/r \* 177: Home/New Microsoft Excel Worksheet.xlsx~RF108ba82.TMP

r/r \* 182: Home/New Microsoft Excel Worksheet.xlsx~RF108ba82.TMP

r/r \* 184: Home/List.xlsx

r/r \* 186: Home/~$List.xlsx

r/r \* 187: Home/\_F5A0100

r/r \* 188: Home/\_278CD2D.tmp

r/r \* 191: Home/\_XAMPLES.txt

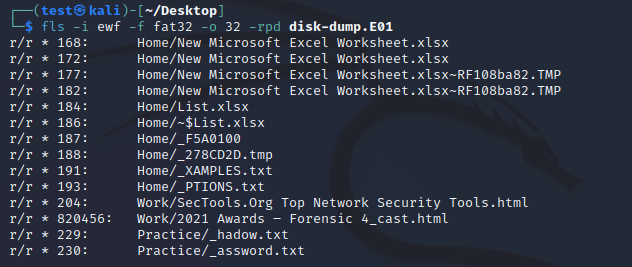
r/r \* 193: Home/\_PTIONS.txt

r/r \* 204: Work/SecTools.Org Top Network Security Tools.html

r/r \* 820456: Work/2021 Awards – Forensic 4\_cast.html

r/r \* 229: Practice/\_hadow.txt

r/r \* 230: Practice/\_assword.txt



1. Command used to find file metadata of Personal directory: *fls -i ewf -f fat32 -o 32 disk-dump.E01 | grep Personal*

File metadata number: 8



1. Command used to find file name of inode 190: *ffind -i ewf -f fat32 -o 32 disk-dump.E01 190*

File name: List.docx



1. What are the recorded MAC times of a folder named Home that resides at the root directory according to the times recorded within its file metadata??????

Command Used: *fls -i ewf -f fat32 -o 32 -l disk-dump.E01 10*

Last Modification Time: 2023-02-05 19:59:40 (+08)

Last Access Time: 2023-02-05 00:00:00 (+08)

Last Changed Time: 0000-00-00 00:00:00 (UTC)

r/r \* 168: New Microsoft Excel Worksheet.xlsx 2023-02-05 19:50:22 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 5760 0 0

r/r \* 172: New Microsoft Excel Worksheet.xlsx 2023-02-05 19:50:26 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 6188 0 0

r/r \* 177: New Microsoft Excel Worksheet.xlsx~RF108ba82.TMP 2023-02-05 19:50:24 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:22 (+08) 0 0 0

r/r \* 182: New Microsoft Excel Worksheet.xlsx~RF108ba82.TMP 2023-02-05 19:50:22 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 5760 0 0

r/r \* 184: List.xlsx 2023-02-05 19:50:26 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 6188 0 0

r/r \* 186: ~$List.xlsx 2023-02-05 19:52:22 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:42 (+08) 165 0 0

r/r \* 187: \_F5A0100 2023-02-05 19:52:12 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 8463 0 0

r/r \* 188: \_278CD2D.tmp 2023-02-05 19:50:26 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 6188 0 0

r/r 190: List.docx 2023-02-05 19:52:12 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:50:20 (+08) 8463 0 0

r/r \* 191: \_XAMPLES.txt 2023-02-05 19:59:14 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:59:12 (+08) 0 0 0

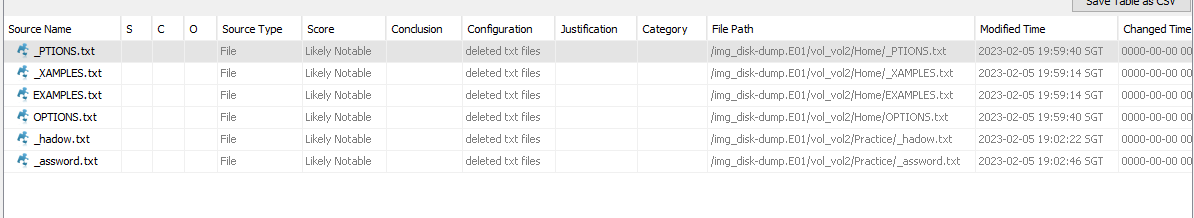
r/r 192: EXAMPLES.txt 2023-02-05 19:59:14 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:59:12 (+08) 15013 0 0

r/r \* 193: \_PTIONS.txt 2023-02-05 19:59:40 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:59:38 (+08) 0 0 0

r/r 194: OPTIONS.txt 2023-02-05 19:59:40 (+08) 2023-02-05 00:00:00 (+08) 0000-00-00 00:00:00 (UTC) 2023-02-05 19:59:38 (+08) 41575 0 0

Task 3:

| Full path names of files | Last Modified Time: |
| --- | --- |
| /img\_disk-dump.E01/vol\_vol2/Home/\_PTIONS.txt | 2023-02-05 19:59:40 SGT |
| /img\_disk-dump.E01/vol\_vol2/Home/\_XAMPLES.txt | 2023-02-05 19:59:14 SGT |
| /img\_disk-dump.E01/vol\_vol2/Practice/\_hadow.txt | 2023-02-05 19:02:22 SGT |
| /img\_disk-dump.E01/vol\_vol2/Practice/\_assword.txt | 2023-02-05 19:02:46 SGT |



1. Ea2ef30c99ececb1eda9aa128631ff31 : /img\_disk-dump.E01/vol\_vol2/Practice/ca\_setup.jpg

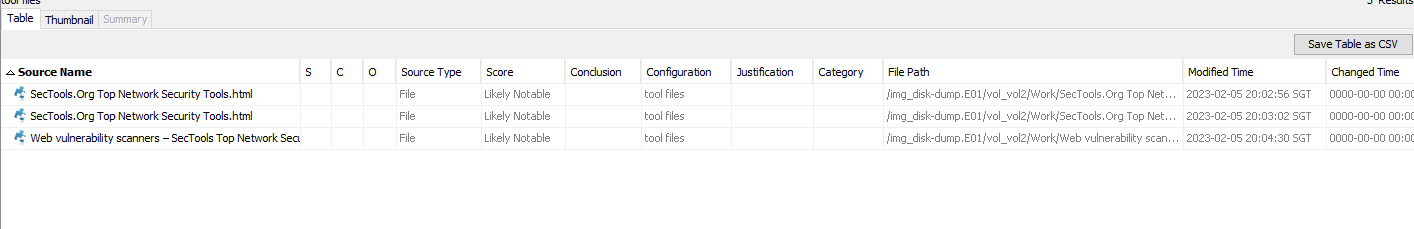
A2a8da835c7341b606f10805fba26687 : /img\_disk-dump.E01/vol\_vol2/Work/Sales-data-1.zip/x64/ophcrack.exe



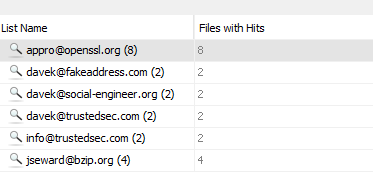
1. /img\_disk-dump.E01/vol\_vol2/Work/SecTools.Org Top Network Security Tools.html d41d8cd98f00b204e9800998ecf8427e (deleted file hash)

/img\_disk-dump.E01/vol\_vol2/Work/SecTools.Org Top Network Security Tools.html

/img\_disk-dump.E01/vol\_vol2/Work/Web vulnerability scanners – SecTools Top Network Security Tools.html



| appro@openssl.org | /img\_disk-dump.E01/vol\_vol2/Work/Sales-data-1.zip/x64/ophcrack\_nogui.exe |
| --- | --- |
| /img\_disk-dump.E01/vol\_vol2/Work/Sales-data-1.zip/x64/ophcrack.exe |
| davek@fakeaddress.com | /img\_disk-dump.E01/vol\_vol2/Personal/SET.pdf |
| davek@social-engineer.org | /img\_disk-dump.E01/vol\_vol2/Personal/SET.pdf |
| davek@trustedsec.com | /img\_disk-dump.E01/vol\_vol2/Personal/SET.pdf |
| info@trustedsec.com | /img\_disk-dump.E01/vol\_vol2/Personal/SET.pdf |
| jseward@bzip.org | /img\_disk-dump.E01/vol\_vol2/Work/Sales-data-1.zip/x64/ophcrack.exe |



| EXAMPLES.txt | password |
| --- | --- |
| passwords |
| password.lst |
| OPTIONS.txt | password |
| passwords |

