



175 lines (116 loc) · 4.78 KB

Preview

Code

Blame



Raw



Ex. No 6: Use Sleuth Kit to Analyze Digital Evidence

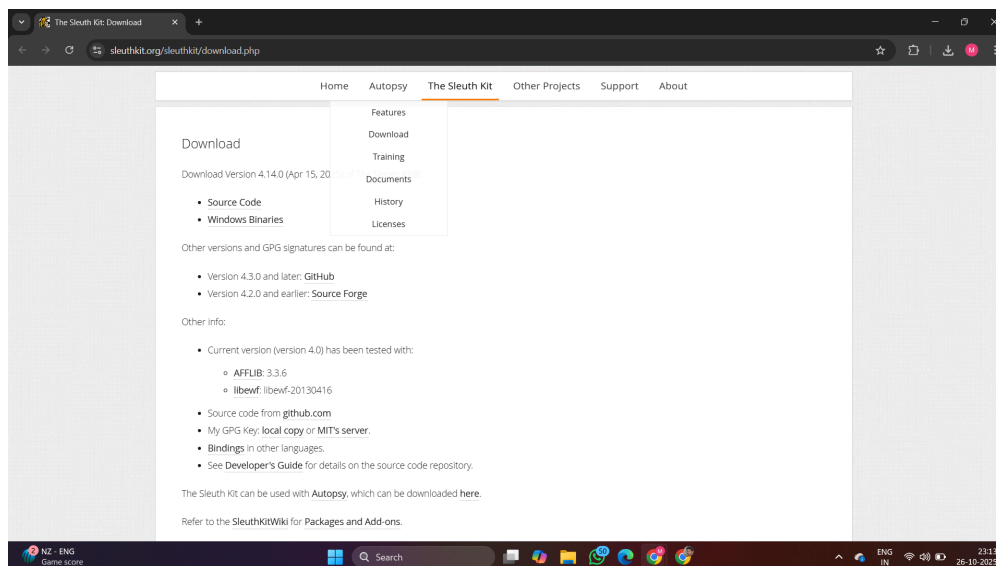
Aim

To analyze a disk image and recover digital evidence using **The Sleuth Kit (TSK)** command-line tools.

Steps

Step 1: Installation

- Download and install **The Sleuth Kit (TSK)** for Windows from its [official website](#).
- Follow on-screen installation instructions.



Step 2: Acquire the Disk Image

- Create or obtain a forensic disk image using tools like **FTK Imager** or **dd**.
- Supported formats: `.dd` , `.raw` , `.img` , `.E01`
- Example evidence files:
 - `4De1l Latitude CPi.E01`
 - `4De1l Latitude CPi.E02`

Step 3: (Optional) Mount the Disk Image

- Use **OSFMount** to mount the `.E01` or `.dd` image as a virtual drive.
- This helps in manually browsing the contents if needed.

Step 4: Analyze the File System

Navigate to Sleuth Kit:

Run:

```
cd C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.26200.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\M J B NAIDU>cd C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin
C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin>
```

Identify File System Type:

Run:

```
fsstat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```

This command gives details about the file system type, layout, and structure.

```
C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin>fsstat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4Dell Latitude CPi.E01"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: B26CB1CE6CB18D9B
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 2097152
First Cluster of MFT Mirror: 4755208
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 12305
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 9510415
Total Sector Range: 0 - 9510415

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
$FILE_NAME (48) Size: 68-578 Flags: Resident,Index
$OBJECT_ID (64) Size: 0-256 Flags: Resident
$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
$VOLUME_NAME (96) Size: 2-256 Flags: Resident
$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
$DATA (128) Size: No Limit Flags:
$INDEX_ROOT (144) Size: No Limit Flags: Resident
$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
```

List Partitions:

Run:

```
mmls.exe "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4Dell Lati
```

This lists all partitions present in the disk image.

```
C:\Windows\system32\cmd.e: X + v
Microsoft Windows [Version 10.0.26200.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\M J B NAIDU>cd C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin

C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin>mmls.exe "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4Dell Latitude CPi.E01"
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length  Description
000:  Meta      0000000000 0000000000 0000000001 Primary Table (#0)
001:  -----      0000000000 0000000062 0000000063 Unallocated
002:  000:000    0000000063 0009510479 0009510417 NTFS / exFAT (0x07)
003:  -----      0009510480 0009514259 0000003780 Unallocated

C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin>
```

List Files and Directories

Run:

```
fls.exe -r -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```

This recursively lists all files and directories, including deleted ones.

```
C:\Windows\system32\cmd.e: X + v

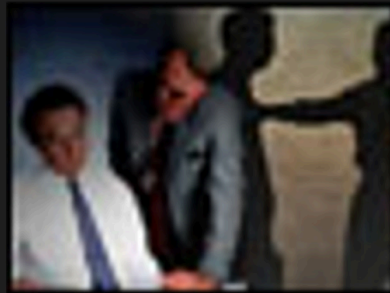
++++ r/r 5745-128-4: UploadM.exe
+++ d/d 6344-144-1: Config
++++ r/r 6345-128-1: config.xml
+ -/r 5714-128-1: desktop.ini
+ -/r 5716-128-4: winnt.bmp
+ -/r 5717-128-4: winnt256.bmp
+ -/r 6073-128-1: control.ini
+ -/r 6323-128-5: WindowsShell.Manifest
+ -/d 6328-144-1: Downloaded Program Files
++ r/r 6329-128-1: desktop.ini
+ -/d 6330-144-1: Offline Web Pages
++ r/r 6331-128-1: desktop.ini
+ -/r 6611-128-1: Windows Update.log
+ -/r 7277-128-4: OEWAblLog.txt
+ -/r 7284-128-4: WMSysPrx.prx
+ -/r 9808-128-6: 0.log
+ -/d 9846-144-6: Installer
++ -/r 9860-128-3: d2a9f.msi
++ -/d 9861-144-1: {350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}
+++ r/r 9862-128-3: places.exe
++ -/r 10179-128-3: ac704.msi
++ -/d 10180-144-6: {6C31E111-96BB-4ADC-9C81-E6D3EEDDD8D3}
+++ -/r 10181-128-3: htmlgen.exe
+++ -/r 10182-128-4: PowerCalc.exe
+++ -/r 10183-128-4: ARPPRODUCTICON.exe
+++ -/r 10184-128-4: Timershot.exe
+++ -/r 10185-128-3: Readme
+++ -/r 10186-128-3: TweakUI.exe
+ -/d 10152-144-1: Downloaded Installations
++ r/r 10153-128-4: Powertoy For Windows XP.msi
+ -/r 11734-128-4: Look@LAN Setup Log.txt
+ -/r 11772-128-3: iun6002.exe
V/V 12305: $OrphanFiles
-/r 228-128-1: pagefile.sys
-/r 343-128-1: hiberfil.sys

C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\sleuthkit-4.14.0-win32\bin>
```

Recover Deleted Files

Run:

```
icat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4De1
```



Step 5: Analyze Metadata

Use the `istat` command to extract metadata of a specific file:

```
istat.exe -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp\Exp_6\4D
```



This provides information such as:

- File creation, modification, and access timestamps
- File size and allocation status

```

MFT Entry Header Values:
Entry: 11366          Sequence: 1
$LogFile Sequence Number: 31327279
Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 295 (S-1-5-21-2000478354-688789844-1708537768-1003)
Created:      2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified: 2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:      2004-08-21 00:35:21.487568000 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: TZ_CAR~1.JPG
Parent MFT Entry: 8375 Sequence: 3
Allocated Size: 0      Actual Size: 0
Created:      2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified: 2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:      2004-08-21 00:35:21.487568000 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Archive
Name: tz_career_boss[1].jpg
Parent MFT Entry: 8375 Sequence: 3
Allocated Size: 0      Actual Size: 0
Created:      2004-08-21 00:35:21.487568000 (India Standard Time)
File Modified: 2004-08-21 00:35:21.487568000 (India Standard Time)
MFT Modified:  2004-08-21 00:35:21.487568000 (India Standard Time)
Accessed:      2004-08-21 00:35:21.487568000 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 90
Type: $FILE_NAME (48-2) Name: N/A Resident size: 108
Type: $DATA (128-4) Name: N/A Non-Resident size: 1644 init_size: 1644
3514379 3514380 3514381 3514382

```

Step 6: Timeline Analysis (Optional)

Generate a chronological timeline of file system activity.

1. Create a **body** file:

```
fls.exe -m / -r -o 63 "C:\Users\M J B NAIDU\OneDrive\Desktop\DF Lab Exp
```

```
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/car.bmp|5675-128-4|r/r/nx/nx/nx|0|0|6968|1092954577|998589600|1092954577|1092954577|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/cat.bmp ($FILE_NAME)|5669-48-5|r/r/nx/nx/nx|0|0|80|1092954576|998589600|1092954576|
1092954576
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/cat.bmp|5669-128-4|r/r/nx/nx/nx|0|0|6968|1092954576|998589600|1092954576|1092954576|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/chess.bmp ($FILE_NAME)|5676-48-5|r/r/nx/nx/nx|0|0|84|1092954577|998589600|1092954577|
1092954577
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/chess.bmp|5676-128-4|r/r/nx/nx/nx|0|0|6968|1092956701|998589600|1092954577|1092954577|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/dirt bike.bmp ($FILE_NAME)|5677-48-5|r/r/nx/nx/nx|0|0|92|1092954578|998589600|
1092954578|1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/dirt bike.bmp|5677-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/dog.bmp ($FILE_NAME)|5678-48-5|r/r/nx/nx/nx|0|0|80|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/dog.bmp|5678-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/drip.bmp ($FILE_NAME)|5679-48-5|r/r/nx/nx/nx|0|0|82|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/drip.bmp|5679-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/duck.bmp ($FILE_NAME)|5680-48-5|r/r/nx/nx/nx|0|0|82|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/duck.bmp|5680-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/fish.bmp ($FILE_NAME)|5670-48-5|r/r/nx/nx/nx|0|0|82|1092954576|998589600|1092954576|
1092954576
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/fish.bmp|5670-128-4|r/r/nx/nx/nx|0|0|6968|1092954576|998589600|1092954576|1092954576|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/frog.bmp ($FILE_NAME)|5681-48-5|r/r/nx/nx/nx|0|0|82|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/frog.bmp|5681-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/guitar.bmp ($FILE_NAME)|5672-48-5|r/r/nx/nx/nx|0|0|86|1092954577|998589600|1092954577|
1092954577
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/guitar.bmp|5672-128-4|r/r/nx/nx/nx|0|0|6968|1092954577|998589600|1092954577|1092954577|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/horses.bmp ($FILE_NAME)|5682-48-5|r/r/nx/nx/nx|0|0|86|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/horses.bmp|5682-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/kick.bmp ($FILE_NAME)|5683-48-5|r/r/nx/nx/nx|0|0|82|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/kick.bmp|5683-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|1092954578|
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/lift-off.bmp ($FILE_NAME)|5684-48-5|r/r/nx/nx/nx|0|0|90|1092954578|998589600|
1092954578|1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/lift-off.bmp|5684-128-4|r/r/nx/nx/nx|0|0|6968|1092954578|998589600|1092954578|
1092954578
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/palm tree.bmp ($FILE_NAME)|5685-48-5|r/r/nx/nx/nx|0|0|92|1092954579|998589600|
1092954579|1092954579
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/palm tree.bmp|5685-128-4|r/r/nx/nx/nx|0|0|6968|1092954579|998589600|1092954579|
1092954579
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/pink flower.bmp ($FILE_NAME)|5671-48-5|r/r/nx/nx/nx|0|0|96|1092954576|998589600|
1092954576|1092954576
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/pink flower.bmp|5671-128-4|r/r/nx/nx/nx|0|0|6968|1092954576|998589600|1092954576|
1092954576
0|/Documents and Settings/All Users/Application Data/Microsoft/User Account Pictures/Default Pictures/red flower.bmp ($FILE_NAME)|5686-48-5|r/r/nx/nx/nx|0|0|94|1092954579|998589600|
1092954579|1092954579
```

2. Generate the timeline:

```
mactime -b body.txt > timeline.txt
```



This file lists the **MAC (Modified, Accessed, Changed)** timestamps of all files.

Step 7: Reporting

1. Collect all analysis outputs:

- filesystem_info.txt
- partitions.txt
- file_list.txt
- metadata_info.txt
- timeline.txt (if created)

2. Review and summarize findings such as:

- File system type and structure
- Deleted or recovered files
- File metadata insights
- Activity timeline (if available)

Step 8: Finalize and Store Evidence

- Archive all reports and analysis files securely.
- Maintain the **chain of custody** to ensure evidence integrity.
- Store archives in a **secure and access-controlled** environment.

Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully analyzed the given disk image using **The Sleuth Kit (TSK)**.
Extracted file system information, recovered deleted files, analyzed metadata, and generated a forensic timeline report.
