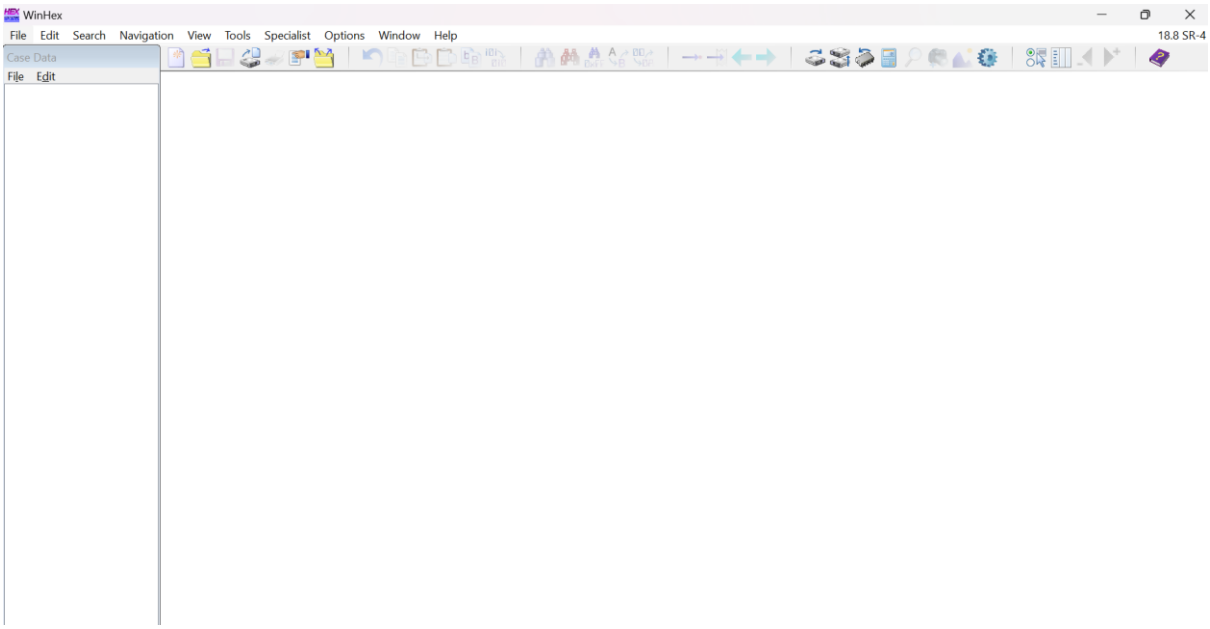
UNDERSTANDING HARD DISK AND FILE SYSTEMS

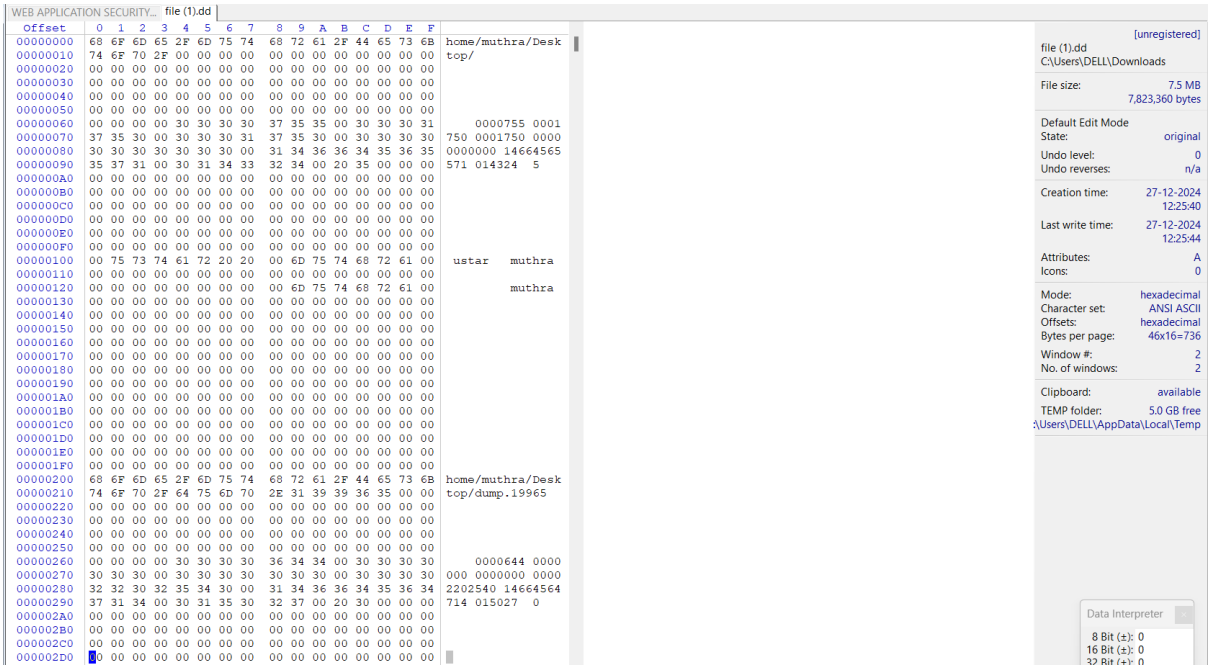
Lab1: Recovering Deleted Files From Hard Disk Using WinHex

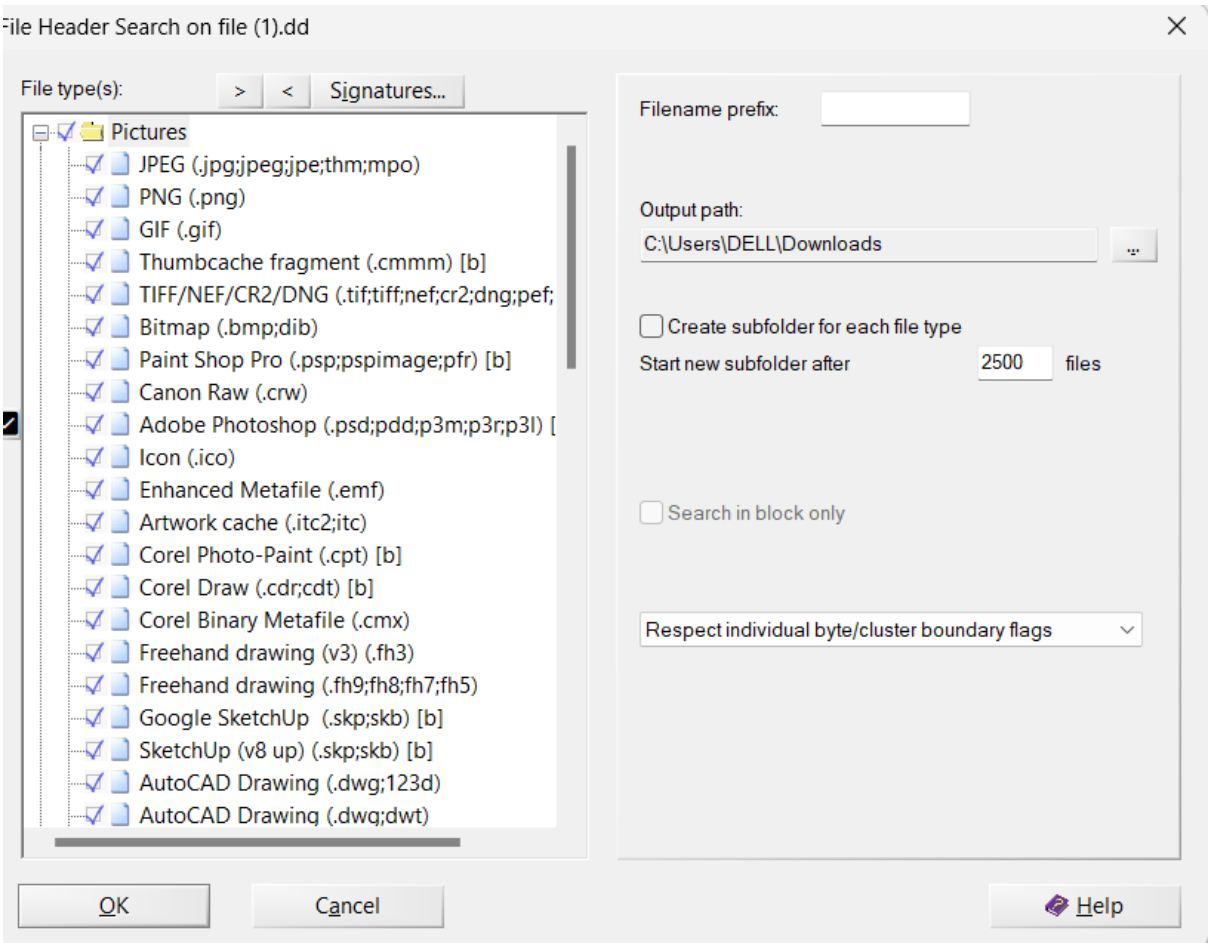
The objective of this lab is to understand how to recover files that have been permanently deleted using the WinHex tool.

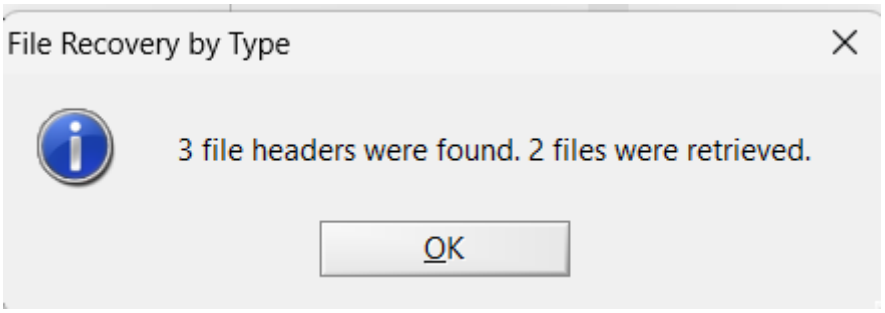
Scenario:

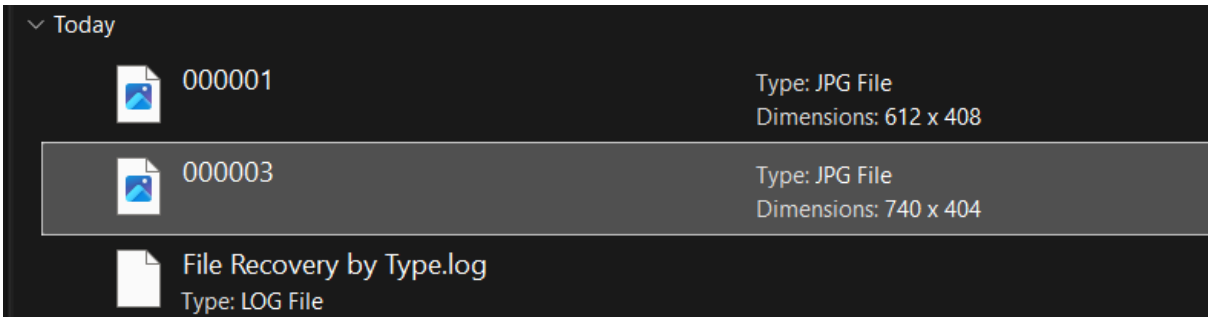
In this lab, you are tasked with recovering critical files that have been accidentally deleted or deliberately removed from a hard disk. The goal is to demonstrate how forensic techniques can be used to retrieve deleted data while maintaining the integrity of the evidence.




WEB APPLICATION SECURITY...
file (1).dd
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 68 6F 6D 65 2F 6D 75 74 68 72 61 2F 44 65 73 6B home/muthra/Desk
00000010 74 6F 70 2F 00 00 00 00 00 00 00 00 00 00 00 00 top/
00000060 00 00 00 00 30 30 30 30 37 35 35 00 30 30 30 31 0000755 0001
00000070 37 35 30 00 30 30 30 31 37 35 30 00 30 30 30 30 750 0001750 0000
00000080 30 30 30 30 30 30 30 00 31 34 36 36 34 35 36 35 0000000 14664565
00000090 35 37 31 00 30 31 34 33 32 34 00 20 35 00 00 00 571 014324 5
00000100 00 75 73 74 61 72 20 20 00 6D 75 74 68 72 61 00 ustar muthra
00000120 00 00 00 00 00 00 00 00 00 6D 75 74 68 72 61 00 muthra
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000200 68 6F 6D 65 2F 6D 75 74 68 72 61 2F 44 65 73 6B home/muthra/Desk
00000210 74 6F 70 2F 64 75 6D 70 2E 31 39 39 36 35 00 00 top/dump.19965
00000260 00 00 00 00 30 30 30 30 36 34 34 00 30 30 30 30 0000644 0000
00000270 30 30 30 00 30 30 30 30 30 30 30 00 30 30 30 30 000 0000000 0000
00000280 32 32 30 32 35 34 30 00 31 34 36 36 34 35 36 34 2202540 14664564
00000290 37 31 34 00 30 31 35 30 32 37 00 20 30 00 00 00 714 015027 0
[unregistered]
file (1).dd
C:\Users\DELL\Downloads
File size: 7.5 MB
7,823,360 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 27-12-2024 12:25:40
Last write time: 27-12-2024 12:25:44
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 46x16=736
Window #: 2
No. of windows: 2
Clipboard: available
TEMP folder: 5.0 GB free
:\Users\DELL\AppData\Local\Temp
Data Interpreter
8 Bit (±): 0
16 Bit (±): 0


File Header Search on file (1).dd
File type(s):
>
<
Signatures...
Pictures
JPEG (.jpg;jpeg;jpe;thm;mpo)
PNG (.png)
GIF (.gif)
Thumbcache fragment (.cmmm) [b]
TIFF/NEF/CR2/DNG (.tif;tiff;nef;cr2;dng;pef;
Bitmap (.bmp;dib)
Paint Shop Pro (.psp;pspimage;pfr) [b]
Canon Raw (.crw)
Adobe Photoshop (.psd;pdd;p3m;p3r;p3l) [
Icon (.ico)
Enhanced Metafile (.emf)
Artwork cache (.itc2;itc)
Corel Photo-Paint (.cpt) [b]
Corel Draw (.cdr;cdt) [b]
Corel Binary Metafile (.cmx)
Freehand drawing (v3) (.fh3)
Freehand drawing (.fh9;fh8;fh7;fh5)
Google SketchUp (.skp;skb) [b]
SketchUp (v8 up) (.skp;skb) [b]
AutoCAD Drawing (.dwg;123d)
AutoCAD Drawing (.dwg;dwt)
Filename prefix:
Output path:
C:\Users\DELL\Downloads
Create subfolder for each file type
Start new subfolder after
2500
files
Search in block only
Respect individual byte/cluster boundary flags
OK
Cancel
Help


File Recovery by Type
3 file headers were found. 2 files were retrieved.
OK


Today
000001
Type: JPG File
Dimensions: 612 x 408
000003
Type: JPG File
Dimensions: 740 x 404
File Recovery by Type.log
Type: LOG File

Lab2: Analysing File Systems Types Using The Sleuth Kit(TSK)

Objective: The objective of this lab is to help investigators learn and perform files system analysis. The Sleuth Kit (TSK) is used to obtain:

1. File system type

2.Meta data information

3.Content information

Use fsstat -f ntfs “path” command to see the file system details.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Har
d Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin> .\fsstat -f ntfs "C:\Users\DELL\Downloads\
ntfs-img-kw-1.dd"
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: BA50ED9250ED5623
OEM Name: NTFS
Volume Name: KW-SRCH-1
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 5355
First Cluster of MFT Mirror: 8032
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 39
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 16063
```

```
Total Cluster Range: 0 - 16063
Total Sector Range: 0 - 16063

$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
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin> istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd"
```

Use the istat tool to view the details of metadata structure.

Master File Table has an entry for every file and directory hence it is required to find all other files. The layout of the MFT is determined by processing entry 0 in the MFT.

```
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 0
MFT Entry Header Values:
Entry: 0        Sequence: 1
$LogFile Sequence Number: 1075381
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 16384           Actual Size: 16384
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
```

MFT entry 1 is for MFTMirr file, which has a non-resident attribute that contains a backup copy of the first MFT entries.

```
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 1
MFT Entry Header Values:
Entry: 1        Sequence: 1
$LogFile Sequence Number: 1052784
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFTMirr
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 4096    Actual Size: 4096
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 82
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 4096  init_size: 4096
8032 8033 8034 8035 8036 8037 8038 8039
```

The boot file system metadata file is located in MFT entry 7 and contains the boot sector of the file system.

```
          v: print version
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Har
d Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\n
tfs-img-kw-1.dd" 7
MFT Entry Header Values:
Entry: 7        Sequence: 7
$LogFile Sequence Number: 0
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0  ()
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
```

```
$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0  ()
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Boot
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 8192    Actual Size: 8192
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 76
Type: $SECURITY_DESCRIPTOR (80-3)   Name: N/A   Resident   size: 116
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 8192  init_size: 8192
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
```

The volume file system metadata file is located in MFT entry 3 and contains the volume label and other version information.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 3
MFT Entry Header Values:
Entry: 3        Sequence: 3
$LogFile Sequence Number: 1087457
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0  ()
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Volume
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$OBJECT_ID Attribute Values:
Object Id: 62f00e35-3570-d9b2-4dcd-63d18edb73da

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-1)   Name: N/A   Resident   size: 80
Type: $OBJECT_ID (64-6)   Name: N/A   Resident   size: 16
Type: $SECURITY_DESCRIPTOR (80-2)   Name: N/A   Resident   size: 116
Type: $VOLUME_NAME (96-4)   Name: N/A   Resident   size: 18
Type: $VOLUME_INFORMATION (112-5)   Name: N/A   Resident   size: 12
```

The MFT entry for AttrDef filesystem metadata file is 4.it defines the name and type identifiers for each type of attribute.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System
 Analysis Tools\The Sleuth Kit (TSK)\bin>                                    > .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 4
MFT Entry Header Values:
Entry: 4        Sequence: 4
$LogFile Sequence Number: 1053965
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0  ()
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $AttrDef
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 36352           Actual Size: 36000
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 82
Type: $SECURITY_DESCRIPTOR (80-3)   Name: N/A   Resident   size: 116
Type: $DATA (128-4)   Name: N/A   Non-Resident   size: 2560  init_size: 2560
5339 5340 5341 5342 5343
```

The MFT entry of the Bitmap file system metadata file that determine status of the cluster is 6.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File Syste
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 6
MFT Entry Header Values:
Entry: 6        Sequence: 6
$LogFile Sequence Number: 1052934
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Bitmap
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 2048    Actual Size: 2008
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 80
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 2008  init_size: 2008
8128 8129 8130 8131
```

NTFS keep track of the damaged clusters by allocating them to a $Data attribute of the Bad Clus file system metadata file. The MFT entry is 8.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 8
MFT Entry Header Values:
Entry: 8        Sequence: 8
$LogFile Sequence Number: 1053084
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (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: 82
Type: $DATA (128-2)   Name: N/A   Resident   size: 0
Type: $DATA (128-1)   Name: $Bad   Non-Resident   size: 8224768  init_size: 0
```

Secure file metadata file system store the security descriptors that define the access control policy for a file or a directory. The MFT entry for that is 9.

```
Analysis Tools\The Sleuth Kit (TSK)\bin> .\istat -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd" 9
MFT Entry Header Values:
Entry: 9        Sequence: 9
$LogFile Sequence Number: 1086357
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 257  (S-1-5-21-1757981266-484763869-1060284298-1003)
Created:        2003-10-23 22:42:59.693550400 (India Standard Time)
File Modified:  2003-10-23 22:42:59.693550400 (India Standard Time)
MFT Modified:   2003-10-23 22:42:59.693550400 (India Standard Time)
Accessed:       2003-10-23 22:42:59.693550400 (India Standard Time)

$FILE_NAME Attribute Values:
Flags:
Name: $Secure
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        2076-11-29 14:24:34.000000000 (India Standard Time)
File Modified:  2076-11-29 14:24:34.000000000 (India Standard Time)
MFT Modified:   2076-11-29 14:24:34.000000000 (India Standard Time)
Accessed:       2076-11-29 14:24:34.000000000 (India Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-7)   Name: N/A   Resident   size: 80
Type: $DATA (128-8)   Name: $SDS   Non-Resident   size: 264040  init_size: 264040
16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31
32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47
48 49 50 51 52 53 54 55
56 57 58 59 60 61 62 63
64 65 66 67 68 69 70 71
72 73 74 75 76 77 78 79
```

```
288 289 290 291 292 293 294 295
296 297 298 299 300 301 302 303
304 305 306 307 308 309 310 311
312 313 314 315 316 317 318 319
320 321 322 323 324 325 326 327
328 329 330 331 332 333 334 335
336 337 338 339 340 341 342 343
344 345 346 347 348 349 350 351
352 353 354 355 356 357 358 359
360 361 362 363 364 365 366 367
368 369 370 371 372 373 374 375
376 377 378 379 380 381 382 383
384 385 386 387 388 389 390 391
392 393 394 395 396 397 398 399
400 401 402 403 404 405 406 407
408 409 410 411 412 413 414 415
416 417 418 419 420 421 422 423
424 425 426 427 428 429 430 431
432 433 434 435 436 437 438 439
440 441 442 443 444 445 446 447
448 449 450 451 452 453 454 455
456 457 458 459 460 461 462 463
464 465 466 467 468 469 470 471
472 473 474 475 476 477 478 479
480 481 482 483 484 485 486 487
488 489 490 491 492 493 494 495
496 497 498 499 500 501 502 503
504 505 506 507 508 509 510 511
512 513 514 515 516 517 518 519
520 521 522 523 524 525 526 527
528 529 530 531
Type: $INDEX_ROOT (144-11)   Name: $SDH   Resident   size: 56
Type: $INDEX_ROOT (144-14)   Name: $SII   Resident   size: 56
Type: $INDEX_ALLOCATION (160-9)   Name: $SDH   Non-Resident   size: 4096  init_size: 4096
5344 5345 5346 5347 5348 5349 5350 5351
Type: $INDEX_ALLOCATION (160-12)   Name: $SII   Non-Resident   size: 4096  init_size: 4096
8040 8041 8042 8043 8044 8045 8046 8047
Type: $BITMAP (176-10)   Name: $SDH   Resident   size: 8
```

To list the file and directory names use the fls command line.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\fls -f ntfs "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd"
r/r 4-128-4:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-1:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-1:    $MFT
r/r 1-128-1:    $MFTMirr
r/r 9-128-8:    $Secure:$SDS
r/r 9-144-11:   $Secure:$SDH
r/r 9-144-14:   $Secure:$SII
r/r 10-128-1:   $UpCase
r/r 3-128-3:    $Volume
d/r 38-128-4:   dir-n-6:there
d/d 38-144-1:   dir-n-6
d/r 30-128-3:   dir-r-4:there
d/d 30-144-1:   dir-r-4
r/r 33-128-3:   file-n-1.dat
r/r 35-128-3:   file-n-3.dat
r/r 36-128-3:   file-n-4.dat
r/r 37-128-3:   file-n-5.dat
r/r 37-128-5:   file-n-5.dat:here
r/r 27-128-1:   file-r-1.dat
r/r 29-128-1:   file-r-3.dat
r/r 29-128-3:   file-r-3.dat:here
d/d 31-144-1:   System Volume Information
-/r * 34-128-1: file-r-2.dat
d/d 39: $OrphanFiles
```

To view only the deleted entries use -d.

```
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\fls -d "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd"
-/r * 34-128-1: file-r-2.dat
```

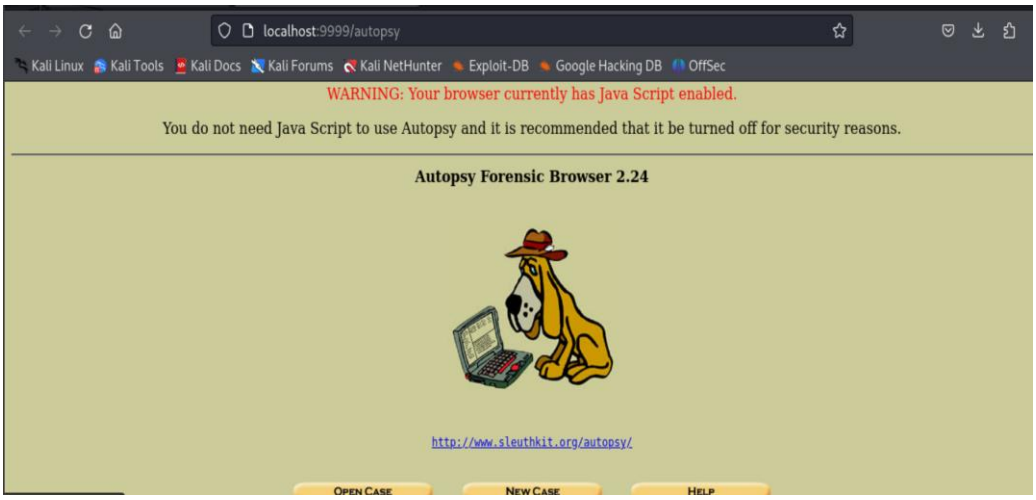
Use img_stat command to see the details of image.

```
PS C:\Users\DELL\Downloads\CHFIv9 Module 03 Understanding Hard Disks and File Systems\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System
 Analysis Tools\The Sleuth Kit (TSK)\bin> .\img_stat "C:\Users\DELL\Downloads\ntfs-img-kw-1.dd"
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 8224768
```

LAB3: Analyzing Raw Image using Autopsy

Autopsy is a digital forensics platform used to analyze disk images, including raw disk images (like .dd files). It's a graphical interface built on The Sleuth Kit (TSK) and makes it easier to examine raw disk images for forensic purposes.

```
$ sudo autopsy
[sudo] password for kali:

                Autopsy Forensic Browser
              http://www.sleuthkit.org/autopsy/
                      ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Fri Dec 27 21:28:47 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```



Create new case

letters, numbers, and symbols.

100

2. **Description:** An optional, one line description of this case.

test

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

Creating Case: `100`

Case directory (`/var/lib/autopsy/100/`) created
Configuration file (`/var/lib/autopsy/100/case.aut`) created

We must now create a host for this case.

host1

2. **Description:** An optional one-line description or note about this computer.

newcase

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

GMT

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

Adding host: host1 to case 100

Host Directory (/var/lib/autopsy/100/host1/) created

Configuration file (/var/lib/autopsy/100/host1/host.aut) created

We must now import an image file for this host

ADD IMAGE

Case: 100
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

ADD IMAGE FILE | CLOSE HOST | HELP

FILE ACTIVITY TIME LINES | IMAGE INTEGRITY | HASH DATABASES | VIEW NOTES | EVENT SEQUENCER

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/kali1/Desktop/ntfs-img-kw-1.dd

2. **Type**
Please select if this image file is for a disk or a single partition.

○ Disk ◉ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

◉ Symlink ○ Copy ○ Move

NEXT

CANCEL | HELP

Image File Details

Local Name: images/ntfs-img-kw-1.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- (•) Ignore the hash value for this image.
- ( ) Calculate the hash value for this image.
- ( ) Add the following MD5 hash value for this image:

[ ]

[ ] Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

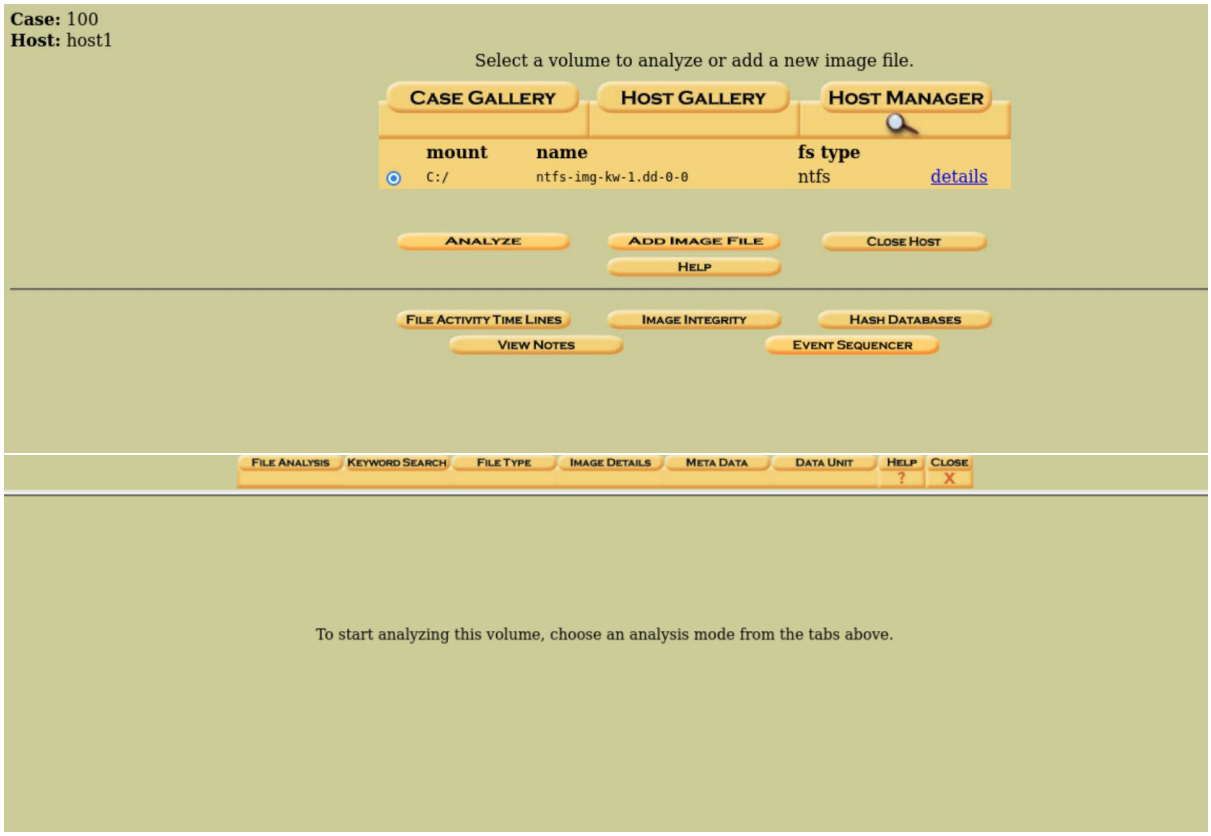
Partition 1 (Type: ntfs)

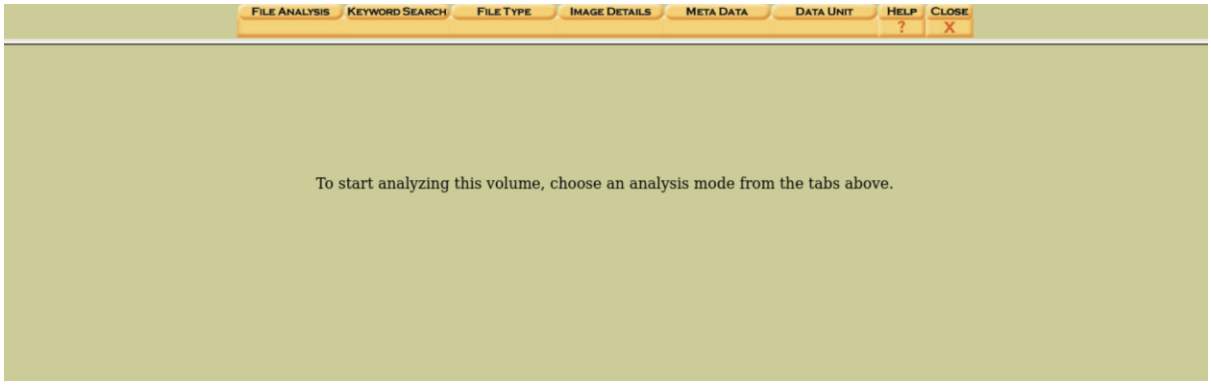
Mount Point: C: File System Type: ntfs

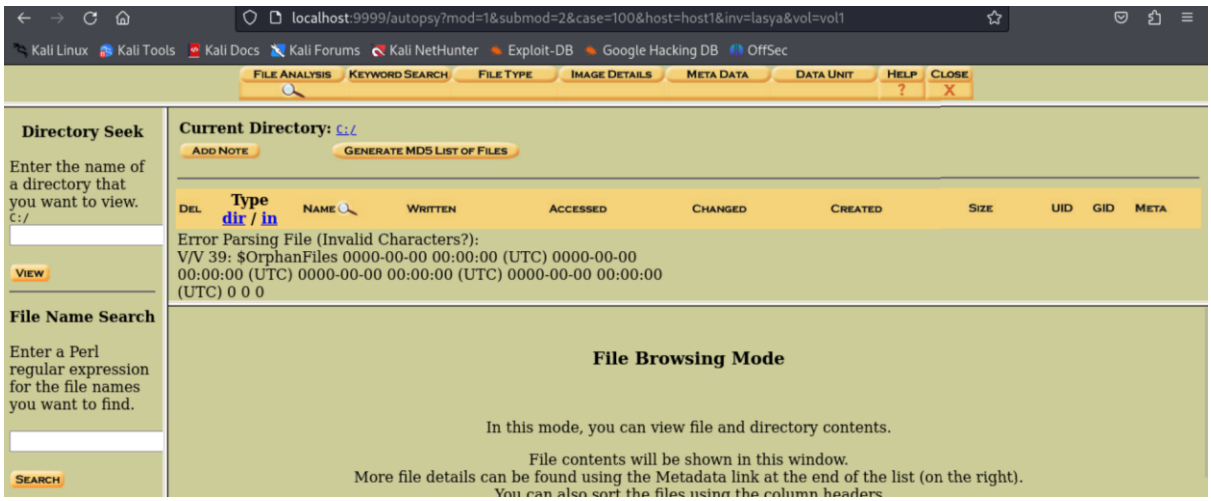
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Volume image (0 to 0 - ntfs - C:) added with ID vol1

OK ADD IMAGE


Case: 100
Host: host1
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
C:/
ntfs-img-kw-1.dd-0-0
ntfs
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
To start analyzing this volume, choose an analysis mode from the tabs above.


FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
To start analyzing this volume, choose an analysis mode from the tabs above.


localhost:9999/autopsy?mod=1&submod=2&case=100&host=host1&inv=lasya&vol=vol1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH
Current Directory: C:/
ADD NOTE
GENERATE MD5 LIST OF FILES
DEL
Type
dir / in
NAME
WRITTEN
ACCESSED
CHANGED
CREATED
SIZE
UID
GID
META
Error Parsing File (Invalid Characters?):
V/V 39: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0
File Browsing Mode
In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

```
MD5 Values for files in C:/ (ntfs-img-kw-1.dd-0-0)

ad617ac3906958de35eacc3d90d31043  -     $AttrDef
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus:$Bad
7810ad2a077259a0c749b35c5d2b68e2  -     $Bitmap
085c7e7f76ecce7093e7009e64a12805  -     $Boot
982d5b0b8273638af199ef42f2ad2618  -     $LogFile
697a7d36f41249be73121e6a74ae8b20  -     $MFT
5fe3f6772286df48378a08b15556bfdd  -     $MFTMirr
153746ff480b662c5a95193082ed404c  -     $Secure:$SDS
ea040d3151178184bb523d6bf3c3eab8  -     $Secure:$SDH
17f25ce4ac91855edf1e7f3108ee8adc  -     $Secure:$SII
6fa3db2468275286210751e869d36373  -     $UpCase
d41d8cd98f00b204e9800998ecf8427e  -     $Volume
049109e97e7dfe3213cf21a95d713cdc  -     file-n-1.dat
03f92745c1c3dfc078cc0a192bb9d2cf  -     file-n-3.dat
ecf3d88d78f6b05ef57fd93b591902f5  -     file-n-4.dat
2b21e56e1eee66419cdb36b3abf72029  -     file-n-5.dat
759681c75ae452d8abfb57760f665a36  -     file-n-5.dat:here
544fdd2d47f570b912807d1c871f81e0  -     file-r-1.dat
d201f17f7447fa75362bd61ac3aa7706  -     file-r-3.dat
0d9332a3532a8adaf34bcb79e1442c0b  -     file-r-3.dat:here
```