

Digital Forensics Lab

Assignment - File System Identification using The Sleuth Kit

Steps –

1. Download and unzip 'The Sleuth Kit' window's binary from its official website (<https://www.sleuthkit.org/sleuthkit/download.php>).

Download

Download Version 4.10.1 (Nov 9, 2020) of The Sleuth Kit®:

- Source Code
- [Windows Binaries](#)

2. Download forensic image of drive from digital forensics workbook's website (<http://www.digitalforensicsworkbook.com/data-sets>)

Forensic Images.zip will contain the following files:

(These files are separated on this website to make the large files easier to download.)

drive1.E01 | MD5: 2ccfa510ee28712b01544594f4fad721 | SHA1: 2baa0524e34a684e615061829b21d6b33cd906f8

drive2.E01 | MD5: 977365ee7ec72480469c1d915e5974d2 | SHA1: 154efb62fd5515000d89d4b254e921c62edf342a

drive3.E01 | MD5: 994512dbe6759ae7766boe2fe4d9ec8a | SHA1: b5da7ecdbf904e1cca65007858d2ee0807284c19

drive4.E01 | MD5: 3e81eb20ded1ae8c6ffc936d5613aacd | SHA1: e1d34bf072df9df86d864df675667ccd02c6840e

drive5.E01 | MD5: 36d849ecdeeb67e04911884346f93a15 | SHA1: 1b5891715365033800c632a4c19fd4770627dc2a

3. Open command prompt and change current directory to C:\Users\user\Desktop\sleuthkit-4.10.1-win32\bin\

```
Command Prompt
C:\Users\user>cd Desktop\sleuthkit-4.10.1-win32\bin\
C:\Users\user\Desktop\sleuthkit-4.10.1-win32\bin>echo Devang
Devang
C:\Users\user\Desktop\sleuthkit-4.10.1-win32\bin>fsstat -i ewf C:\Users\user\Desktop\drive1.E01
```

4. Use command `fsstat -i ewf C:\Users\user\Desktop\drive1.E01`{location of forensic drive in this case}
5. We can see lot of things in the report generated by command like type of file system, sector size and cluster size.

```
Command Prompt
C:\Users\user>cd Desktop\sleuthkit-4.10.1-win32\bin\

C:\Users\user\Desktop\sleuthkit-4.10.1-win32\bin>echo Devang
Devang

C:\Users\user\Desktop\sleuthkit-4.10.1-win32\bin>fsstat -i ewf C:\Users\user\Desktop\drive1.E01
FILE SYSTEM INFORMATION
-----
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x1881387d
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 10440
Free Sector Count (FS Info): 2058552

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 2068991
* Reserved: 0 - 4165
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 4166 - 6178
* FAT 1: 6179 - 8191
* Data Area: 8192 - 2068991
** Cluster Area: 8192 - 2068991
*** Root Directory: 8192 - 8199

METADATA INFORMATION
-----
Range: 2 - 32972806
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 257601

FAT CONTENTS (in sectors)
```