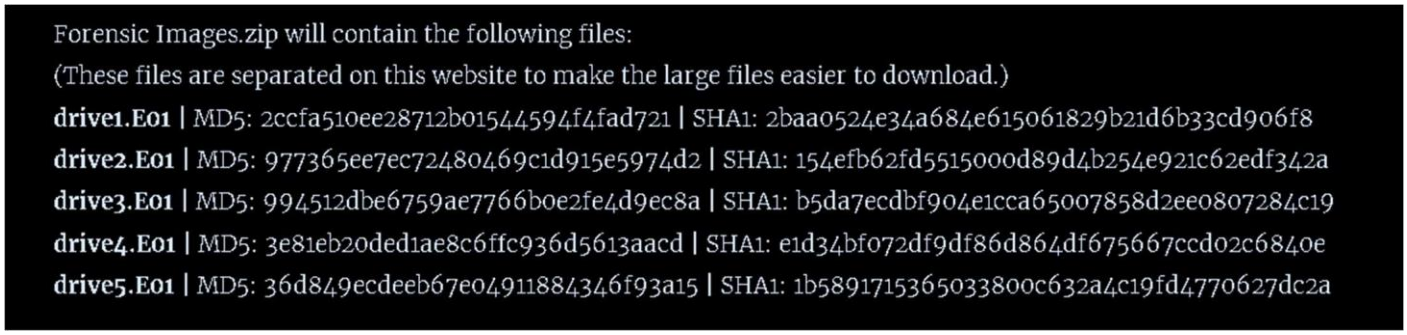
Digital Forensics Lab

Assignment - File System Identification using The Sleuth Kit

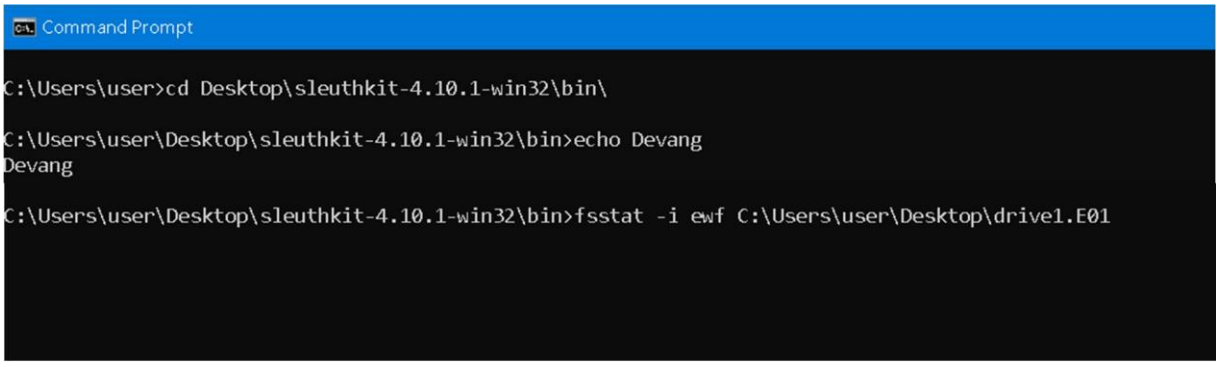
Steps –

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

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



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



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.