Animesh Parab t2-t21 88

Lab Assignment 5

Aim: To explore Hashdeep tool in kali linux for generating, matching and auditing hash of files.

Lab Outcome Attainment: LO2

Theory:

Hashdeep is a command-line utility for computing and verifying hash values (checksums) of files and directories. It is a versatile and powerful tool primarily used for data integrity verification and digital forensics. Hashdeep can calculate multiple hash values (e.g., MD5, SHA-1, SHA-256, SHA-512) for files and directories and store them in hash databases. You can then use these hash databases to verify the integrity of your files at a later time by comparing the computed hash values with the stored ones. Some key features and use cases of Hashdeep include:

1. **Data Integrity Verification**: Hashdeep is commonly used to ensure that files have not been tampered with or corrupted over time. By periodically recalculating hash values and comparing them to the stored values, you can detect any unauthorized changes.

2. **Forensics and Investigations**: Digital forensics experts use Hashdeep to create hash databases of evidence and verify its integrity during investigations. This helps ensure that the data remains unchanged throughout the legal process.

3. **Comparing Directories**: You can use Hashdeep to compare two directories to find differences between them, even if the file names have changed. This is useful for backup verification and synchronization tasks.

4. **Recursive Hashing**: Hashdeep can recursively calculate hash values for directories and subdirectories, making it efficient for processing large and complex directory structures.

5. **Cross-Platform**: Hashdeep is available for various operating systems, including Linux, macOS, and Windows, making it a versatile tool for cross-platform use.
6. **Support for Multiple Hash Algorithms**: It supports multiple hash algorithms, including MD5, SHA-1, SHA-256, SHA-512, and others, allowing you to choose the level of security and performance you need.

How to use **hashdeep :**

1. To check the version of Hashdeep - *Hashdeep -V*

2. To display help about Hashdeep - *Hashdeep -h* or *Hashdeep -hh*

3. To display the manual page of Hashdeep- *man Hashdeep*

4. To display the manual page of any specific hash algorithm supported by Hashdeep- *man md5deep*

5. To hash a file - *Hashdeep filename*

6. To supress any error messages- *Hashdeep -s filename*

7. To apply multiple hash algorithms than default-

   Hashdeep -c md5,sha1,sha256,tiger filename

8. To hash multiple files (say all text files) using md5

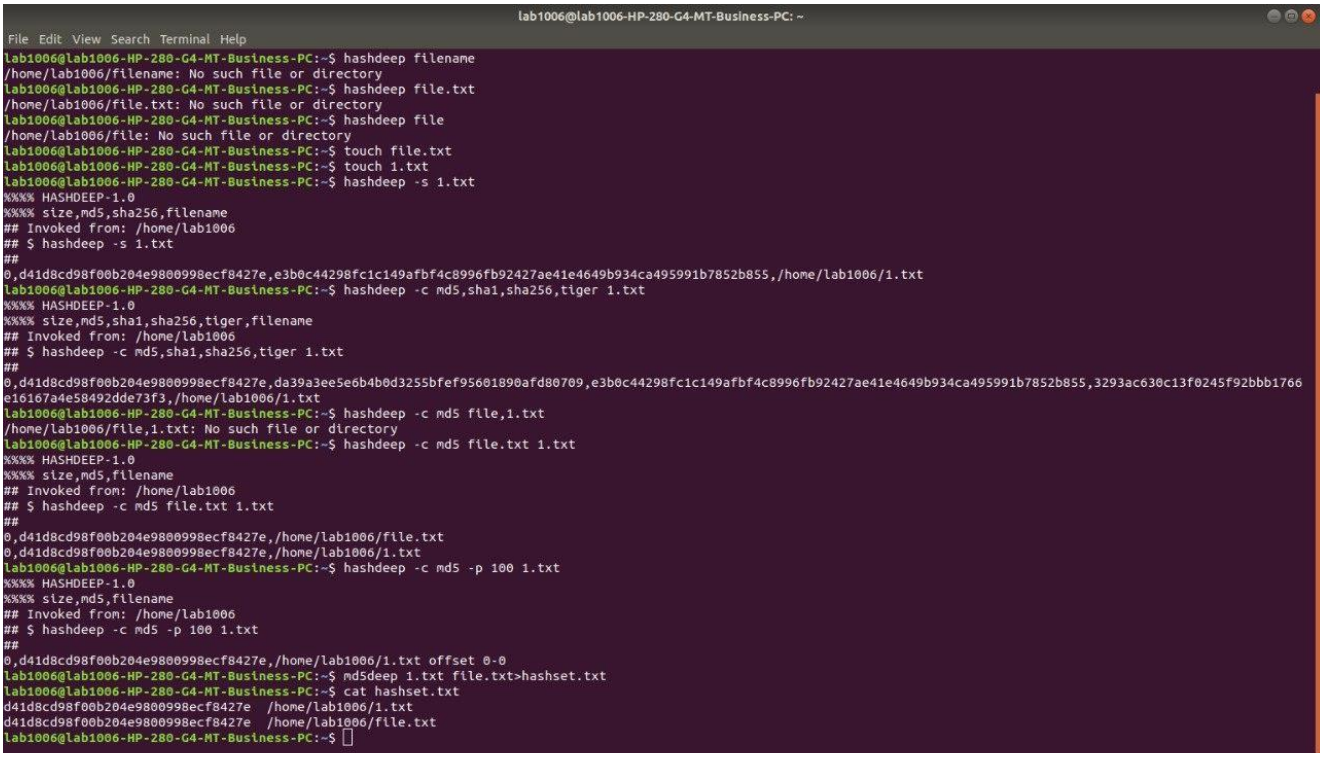
   *Hashdeep -c md5 *.txt*

9. To hash multiple files (say all text files) using md5 and sha1

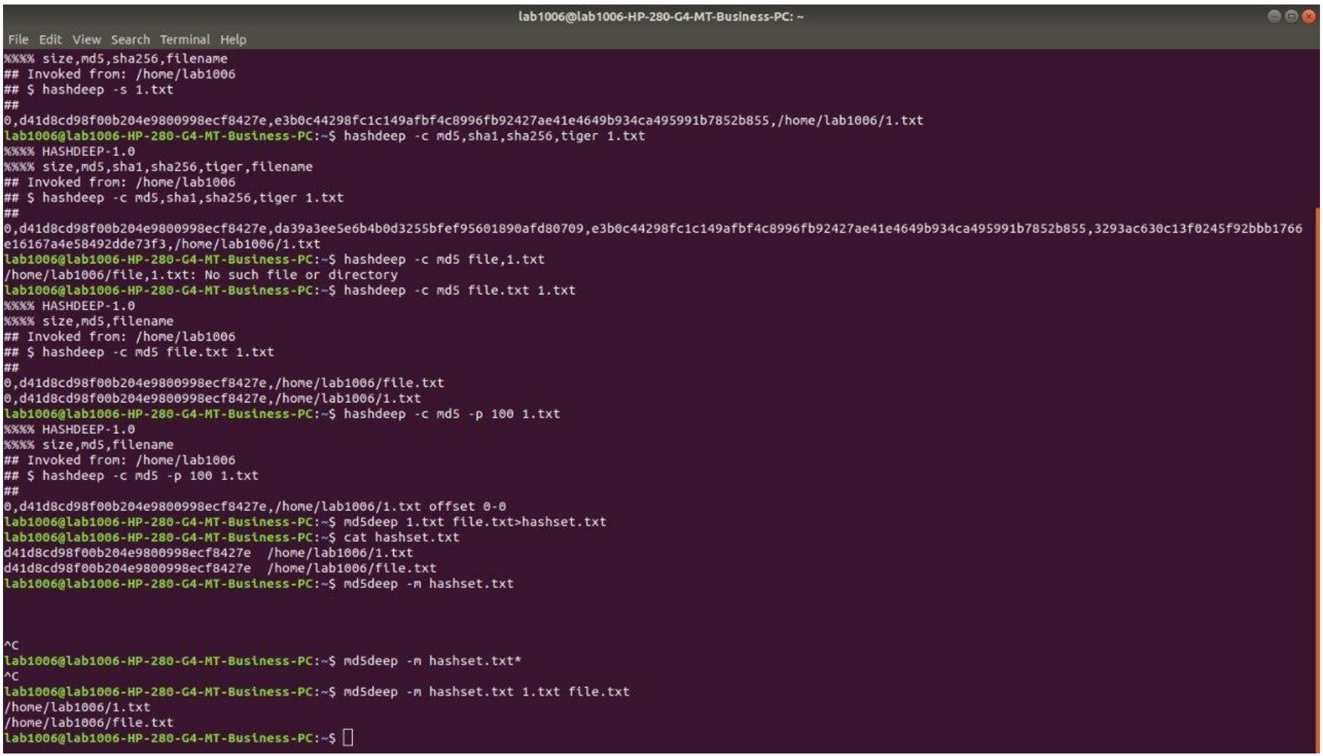
   *Hashdeep -c md5,sha1 *.txt*

10. Hashing block of files-
    Hashdeep -c md5 -p 100 example.txt

Output :

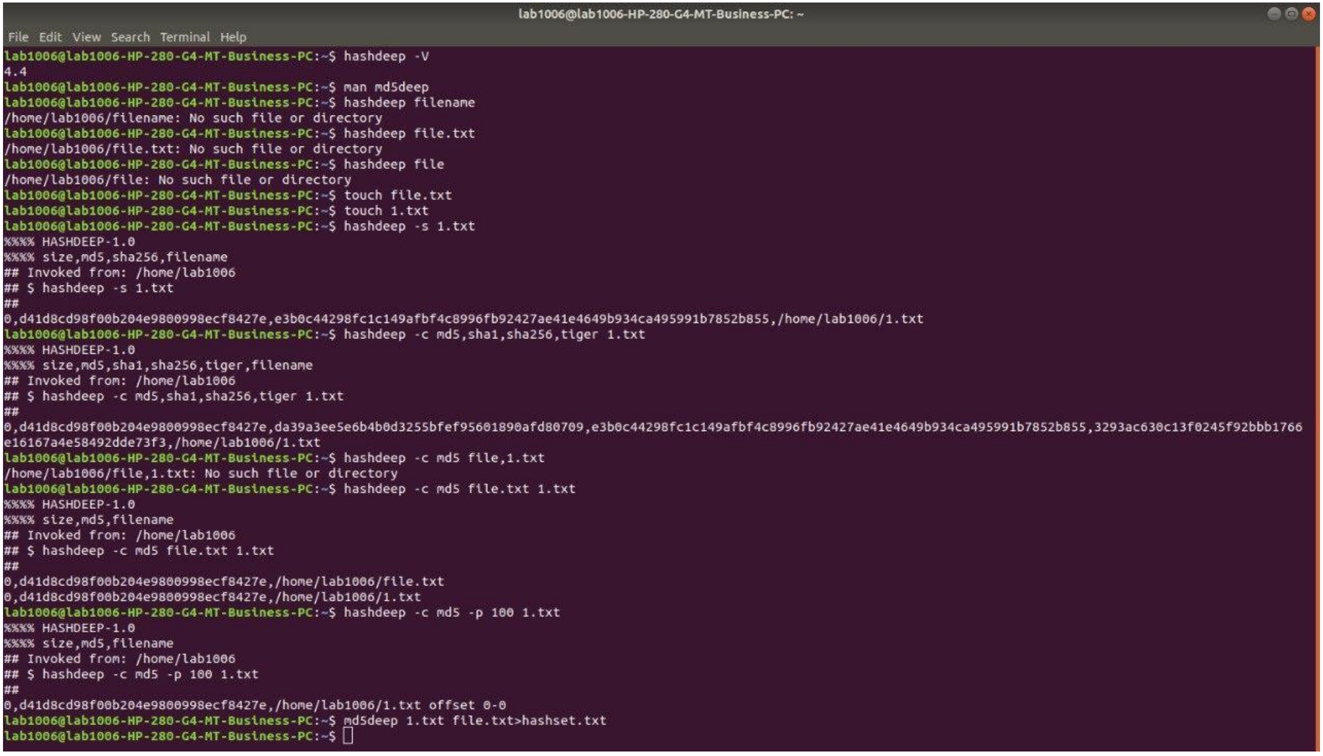

lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep filename
/home/lab1006/filename: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep file.txt
/home/lab1006/file.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep file
/home/lab1006/file: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ touch file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ touch 1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256,tiger 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,da39a3ee5e6b4b0d3255bfef95601890afd80709,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,3293ac630c13f0245f92bbb1766
e16167a4e58492dde73f3,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file,1.txt
/home/lab1006/file,1.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file.txt 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 file.txt 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/file.txt
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 100 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt offset 0-0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep 1.txt file.txt>hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/1.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```



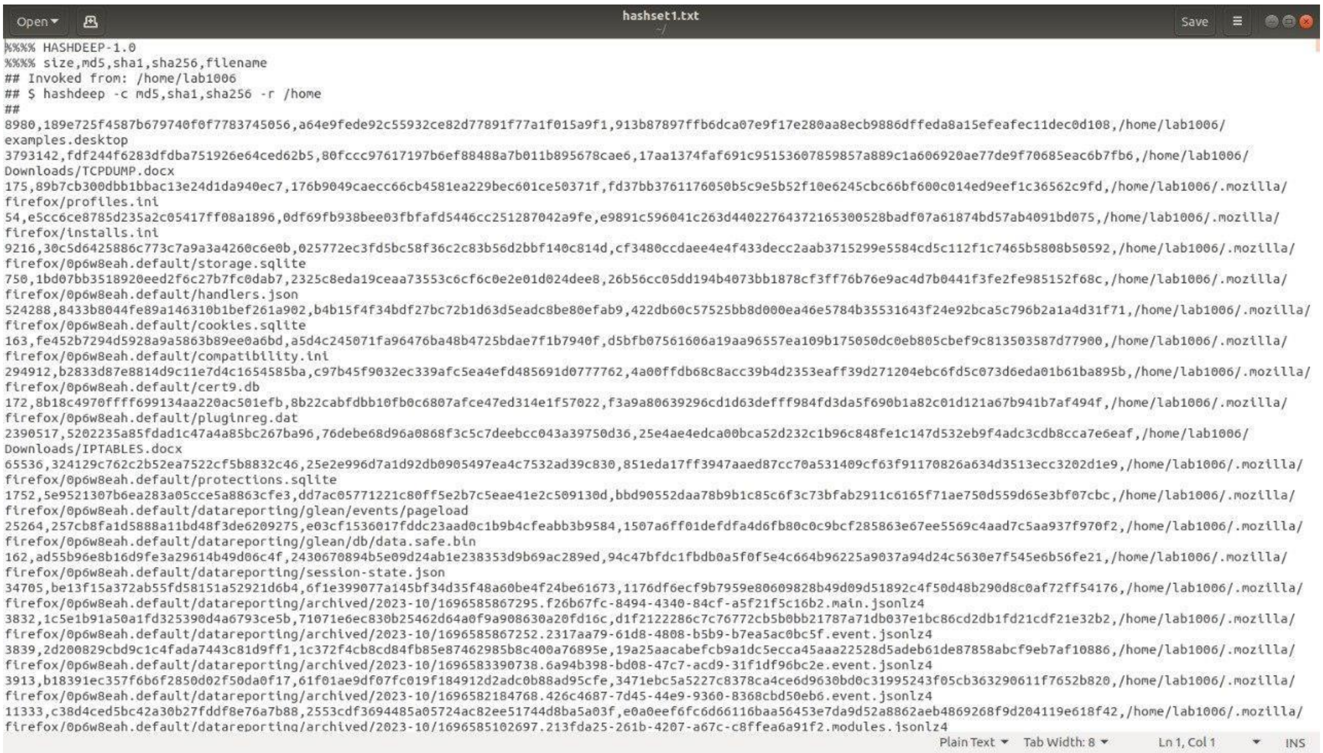
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256,tiger 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,da39a3ee5e6b4b0d3255bfef95601890afd80709,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,3293ac630c13f0245f92bbb1766
e16167a4e58492dde73f3,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file,1.txt
/home/lab1006/file,1.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file.txt 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 file.txt 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/file.txt
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 100 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt offset 0-0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep 1.txt file.txt>hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/1.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt



^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt*
^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt 1.txt file.txt
/home/lab1006/1.txt
/home/lab1006/file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```

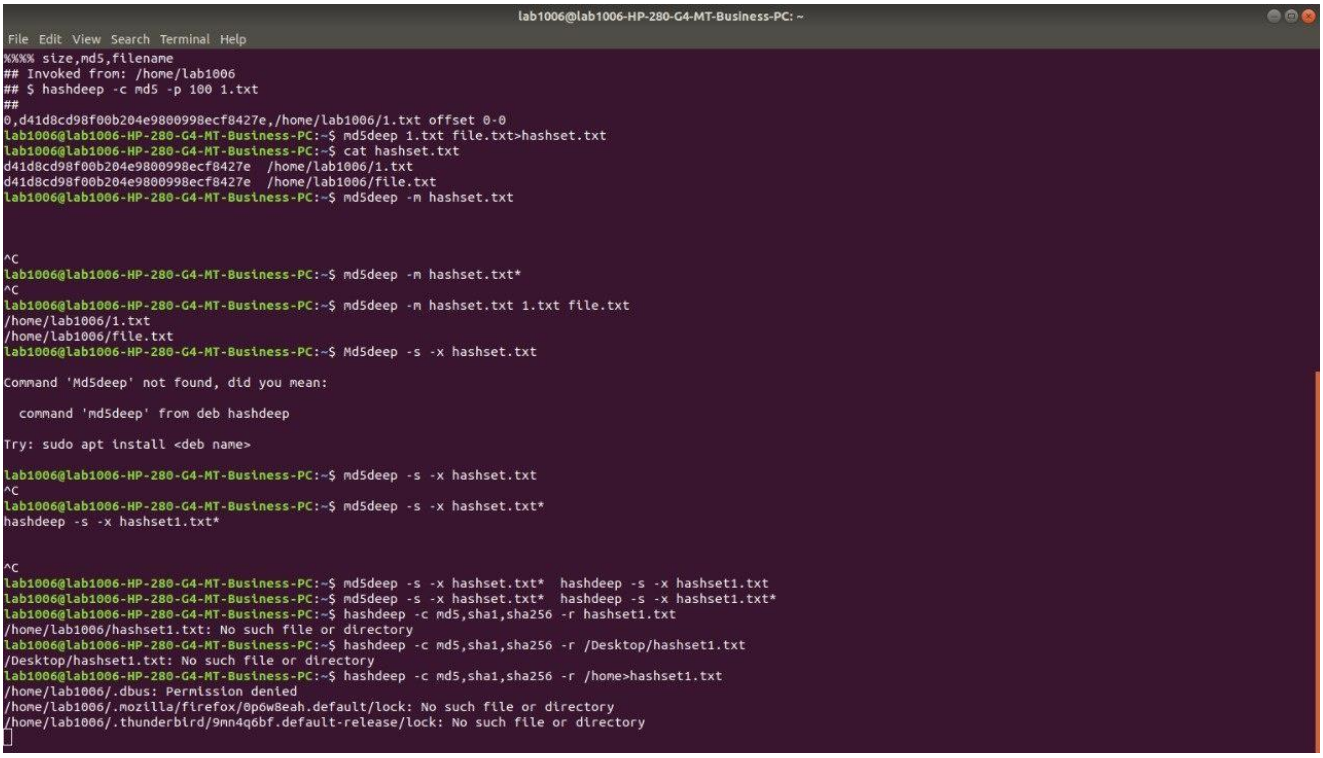


lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -V
4.4
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man md5deep
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep filename
/home/lab1006/filename: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep file.txt
/home/lab1006/file.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep file
/home/lab1006/file: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ touch file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ touch 1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256,tiger 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,da39a3ee5e6b4b0d3255bfef95601890afd80709,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,3293ac630c13f0245f92bbb1766
e16167a4e58492dde73f3,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file,1.txt
/home/lab1006/file,1.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 file.txt 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 file.txt 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/file.txt
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 100 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt offset 0-0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep 1.txt file.txt>hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```



```
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256 -r /home
##
8980,189e725f4587b679740f0f7783745056,a64e9fede92c55932ce82d77891f77a1f015a9f1,913b87897ffb6dca07e9f17e280aa8ecb9886dffeda8a15efeafec11dec0d108,/home/lab1006/
examples.desktop
3793142,fdf244f6283dfdba751926e64ced62b5,80fccc97617197b6ef88488a7b011b895678cae6,17aa1374faf691c95153607859857a889c1a606920ae77de9f70685eac6b7fb6,/home/lab1006/
Downloads/TCPDUMP.docx
175,89b7cb300dbb1bbac13e24d1da940ec7,176b9049caecc66cb4581ea229bec601ce50371f,fd37bb3761176050b5c9e5b52f10e6245cbc66bf600c014ed9eef1c36562c9fd,/home/lab1006/.mozilla/
firefox/profiles.ini
54,e5cc6ce8785d235a2c05417ff08a1896,0df69fb938bee03fbfafd5446cc251287042a9fe,e9891c596041c263d4402276437216530052 8badf07a61874bd57ab4091bd075,/home/lab1006/.mozilla/
firefox/installs.ini
9216,30c5d6425886c773c7a9a3a4260c6e0b,025772ec3fd5bc58f36c2c83b56d2bbf140c814d,cf3480ccdaee4e4f433decc2aab3715299e5584cd5c112f1c7465b5808b50592,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/storage.sqlite
750,1bd07bb3518920eed2f6c27b7fc0dab7,2325c8eda19ceaa73553c6cf6c0e2e01d024dee8,26b56cc05dd194b4073bb1878cf3ff76b76e9ac4d7b0441f3fe2fe985152f68c,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/handlers.json
524288,8433b8044fe89a146310b1bef261a902,b4b15f4f34bdf27bc72b1d63d5eadc8be80efab9,422db60c57525bb8d000ea46e5784b35531643f24e92bca5c796b2a1a4d31f71,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/cookies.sqlite
163,fe452b7294d5928a9a5863b89ee0a6bd,a5d4c245071fa96476ba48b4725bdae7f1b7940f,d5bfb07561606a19aa96557ea109b175050dc0eb805cbef9c813503587d77900,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/compatibility.ini
294912,b2833d87e8814d9c11e7d4c1654585ba,c97b45f9032ec339afc5ea4efd485691d0777762,4a00ffdb68c8acc39b4d2353eaff39d271204ebc6fd5c073d6eda01b61ba895b,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/cert9.db
172,8b18c4970ffff699134aa220ac501efb,8b22cabfdbb10fb0c6807afce47ed314e1f57022,f3a9a80639296cd1d63defff984fd3da5f690b1a82c01d121a67b941b7af494f,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/pluginreg.dat
2390517,5202235a85fdad1c47a4a85bc267ba96,76debe68d96a0868f3c5c7deebcc043a39750d36,25e4ae4edca00bca52d232c1b96c848fe1c147d532eb9f4adc3cdb8cca7e6eaf,/home/lab1006/
Downloads/IPTABLES.docx
65536,324129c762c2b52ea7522cf5b8832c46,25e2e996d7a1d92db0905497ea4c7532ad39c830,851eda17ff3947aaed87cc70a531409cf63f91170826a634d3513ecc3202d1e9,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/protections.sqlite
1752,5e9521307b6ea283a05cce5a8863cfe3,dd7ac05771221c80ff5e2b7c5eae41e2c509130d,bbd90552daa78b9b1c85c6f3c73bfab2911c6165f71ae750d559d65e3bf07cbc,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/glean/events/pageload
25264,257cb8fa1d5888a11bd48f3de6209275,e03cf1536017fddc23aad0c1b9b4cfeabb3b9584,1507a6ff01defdfa4d6fb80c0c9bcf285863e67ee5569c4aad7c5aa937f970f2,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/glean/db/data.safe.bin
162,ad55b96e8b16d9fe3a29614b49d06c4f,2430670894b5e09d24ab1e238353d9b69ac289ed,94c47bfdc1fbdb0a5f0f5e4c664b96225a9037a94d24c5630e7f545e6b56fe21,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/session-state.json
34705,be13f15a372ab55fd58151a52921d6b4,6f1e399077a145bf34d35f48a60be4f24be61673,1176df6ecf9b7959e80609828b49d09d51892c4f50d48b290d8c0af72ff54176,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/archived/2023-10/1696585867295.f26b67fc-8494-4340-84cf-a5f21f5c16b2.main.jsonlz4
3832,1c5e1b91a50a1fd325390d4a6793ce5b,71071e6ec830b25462d64a0f9a908630a20fd16c,d1f2122286c7c76772cb5b0bb21787a71db037e1bc86cd2db1fd21cdf21e32b2,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/archived/2023-10/1696585867252.2317aa79-61d8-4808-b5b9-b7ea5ac0bc5f.event.jsonlz4
3839,2d200829cbd9c1c4fada7443c81d9ff1,1c372f4cb8cd84fb85e87462985b8c400a76895e,19a25aacabefcb9a1dc5ecca45aaa22528d5adeb61de87858abcf9eb7af10886,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/archived/2023-10/1696583390738.6a94b398-bd08-47c7-acd9-31f1df96bc2e.event.jsonlz4
3913,b18391ec357f6b6f2850d02f50da0f17,61f01ae9df07fc019f184912d2adc0b88ad95cfe,3471ebc5a5227c8378ca4ce6d9630bd0c31995243f05cb363290611f7652b820,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/archived/2023-10/1696582184768.426c4687-7d45-44e9-9360-8368cbd50eb6.event.jsonlz4
11333,c38d4ced5bc42a30b27fddf8e76a7b88,2553cdf3694485a05724ac82ee51744d8ba5a03f,e0a0eef6fc6d66116baa56453e7da9d52a8862aeb4869268f9d204119e618f42,/home/lab1006/.mozilla/
firefox/0p6w8eah.default/datareporting/archived/2023-10/1696585102697.213fda25-261b-4207-a67c-c8ffea6a91f2.modules.jsonlz4
```



lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 100 1.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/lab1006/1.txt offset 0-0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep 1.txt file.txt>hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/1.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt



^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt*
^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset.txt 1.txt file.txt
/home/lab1006/1.txt
/home/lab1006/file.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ Md5deep -s -x hashset.txt

Command 'Md5deep' not found, did you mean:

  command 'md5deep' from deb hashdeep

Try: sudo apt install <deb name>

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -x hashset.txt
^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -x hashset.txt*
hashdeep -s -x hashset1.txt*


^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -x hashset.txt*  hashdeep -s -x hashset1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -x hashset.txt*  hashdeep -s -x hashset1.txt*
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256 -r hashset1.txt
/home/lab1006/hashset1.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256 -r /Desktop/hashset1.txt
/Desktop/hashset1.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256 -r /home>hashset1.txt
/home/lab1006/.dbus: Permission denied
/home/lab1006/.mozilla/firefox/0p6w8eah.default/lock: No such file or directory
/home/lab1006/.thunderbird/9mn4q6bf.default-release/lock: No such file or directory
```

Conclusion :

We understood hashdeep and its versatile command-line utility that computes and verifies checksums (hash values) for files and directories, offering data integrity assurance and digital forensics capabilities. It supports multiple hash algorithms, making it a reliable tool for detecting file tampering and ensuring the integrity of data across different platforms.