

13th lab of Forensics

Rodrigo Castillo

November 9, 2020




1 captures

for the following task, i'll make one script that will execute all the commands listed on the table and then i'll explain every command on the table. The script...

```
netstat -a > netstat.txt
date > date.txt
cat /proc/version > version.txt
cat /proc/uptime > uptime.txt
netstat -l -p > netstat2.txt
history > historial.txt
df -k > df.txt

#ahora comprimo todo
zip -r evidence.zip .

#ahora muestro los procesos
top
```



1 captur

```
total 152
-rw-rw-r-- 1 r r 29 nov 9 16:44 date.txt
-rw-rw-r-- 1 r r 532 nov 9 16:44 df.txt
-rw-rw-r-- 1 r r 15797 nov 9 16:44 evidence.zip
-rw-rw-r-- 1 r r 20939 nov 9 16:44 historial.txt
-rwxrwxr-x 1 r r 220 nov 9 16:44 labforensics.sh
-rw-rw-r-- 1 r r 6752 nov 9 16:44 netstat2.txt
-rw-rw-r-- 1 r r 51384 nov 9 16:44 netstat.txt
-rw-rw-r-- 1 r r 32293 nov 9 16:43 procesos.txt
-rw-rw-r-- 1 r r 0 nov 9 16:44 top.txt
-rw-rw-r-- 1 r r 17 nov 9 16:44 uptime.txt
-rw-rw-r-- 1 r r 158 nov 9 16:44 version.txt
```

Figure 1: script and result

- date:** returns the current date .
- df:** returns the current state of the disks .
- history:** return the history of bash commands .
- netstat:** return the current state of wireless conections.
- top:** return the current processes running.
- uptime** return the cuantity of time that the machine has been on.
- version** return the linux version.