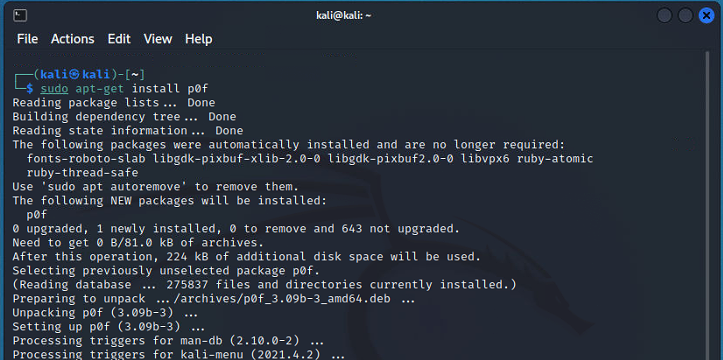
Linux Forensics

Part I Identifying Devices and OSs with p0f

**Step 1 & 2 & 3**

In this step we are going to install p0f, which uses fingerprinting technique based on analyzing the structure of TCP/IP packet to determine the operating system.

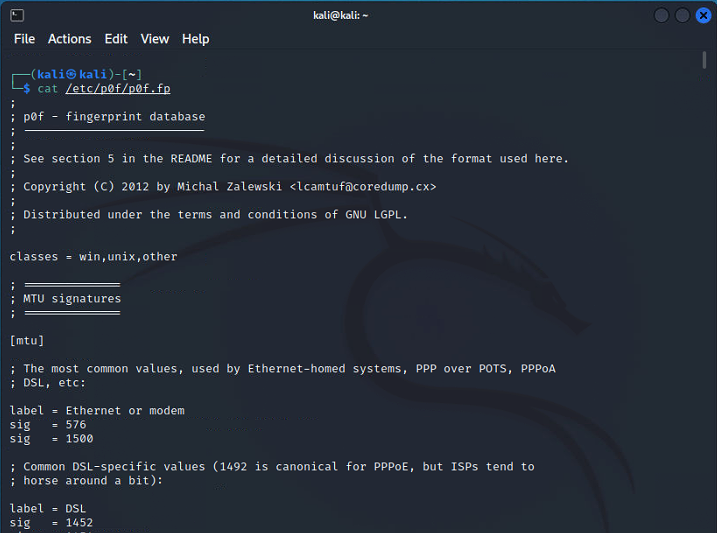


P0f can use filters to include or exclude particular networks, hosts or packets.

**Step 4**

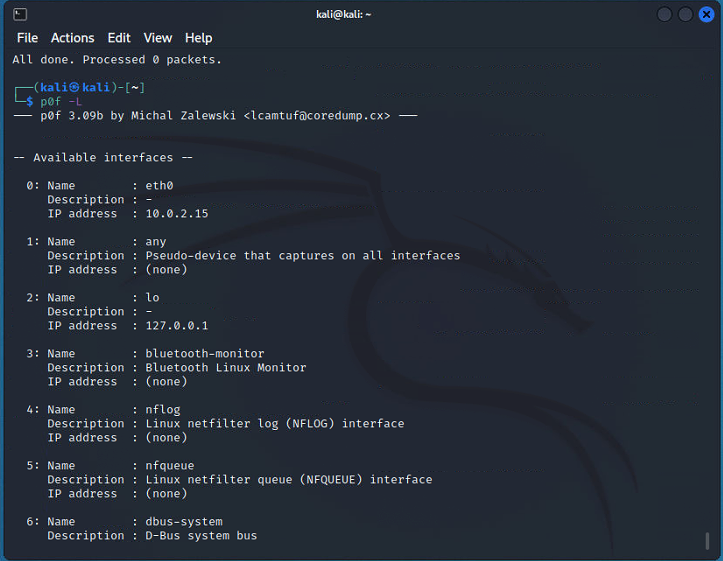
The main database of p0f fingerprinting is stored at the location of **/etc/p0f/p0f.fp**.

To read the stored file we are going to use “**cat**”



**Step 5**

**P0f** **-L** is going to display the following all of the interfaces of the device



**Step 6**

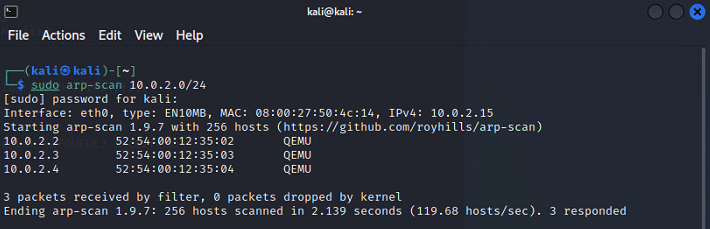
Using just **p0f** command without any flag is going to fingerprint the processes in the whole device.



PART II Information gathering and Fingerprinting with arp-scan & nmap

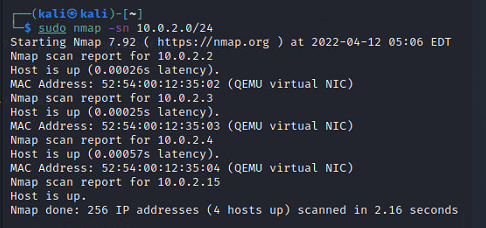
**Step 7**

**arp-scan** is an amazing tool used to list down the contents of ARP table. It shows the number of devices on the network connected to the device.



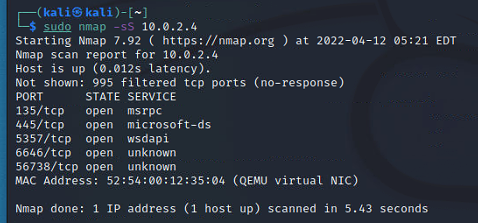
**Step 8**

Another great and famous tool is nmap short for network mapping tool. Here we are using “**-sn**” flag which is going to ping all the devices on the network that are live.



**Step 9**

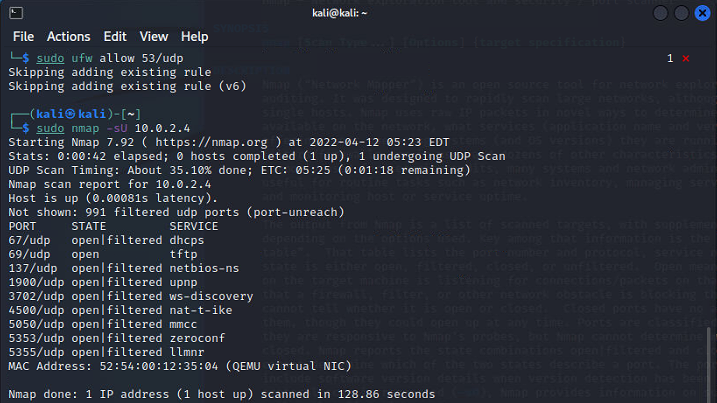
Another flag of **nmap** is “**-sS**” that is used to perform SYN scan on the TCP ports and display the ports that are open



If the ports are been blocked by the firewall, just add rule to the firewall to allow the port’s packet to be send and received.

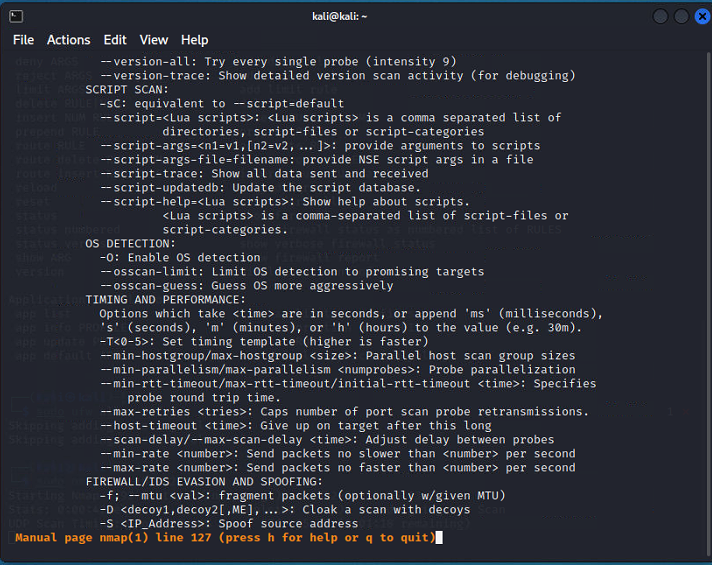
This is done using the command “**ufw allow port/type**”

Using “**-sU**” flag in nmap scans all of the ports having udp transmission



**Step 10**

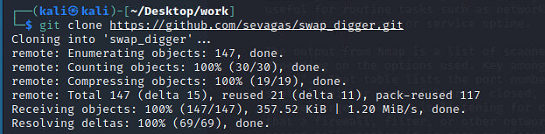
**Nmap** is used to perform a lot of tasks from scanning the network to finding vulnerabilities in it. To learn about nmap we need to use its manual and the command that shows it is “**man nmap**”



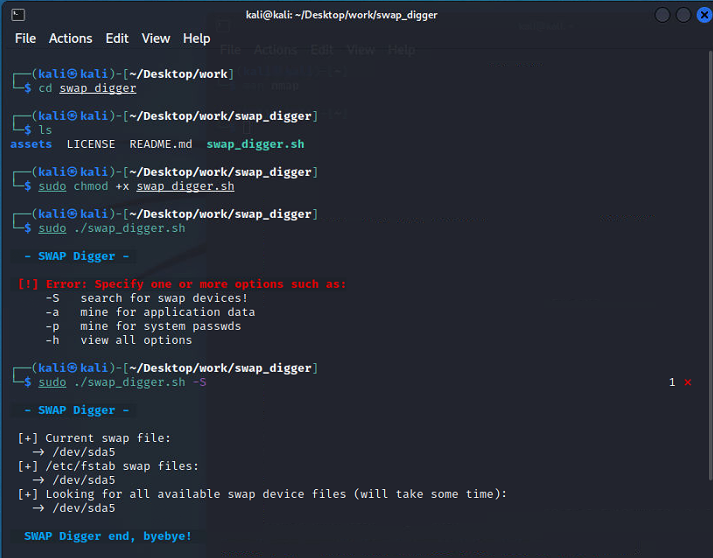
Part III: Information Gathering with swap\_digger

**Step 11**

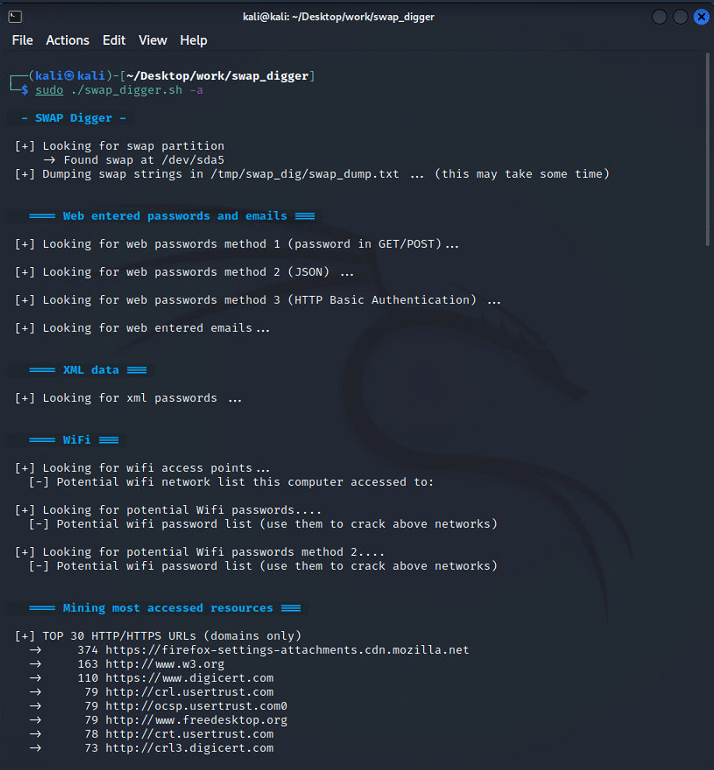
**Swap\_digger** is an information gathering tool that is used to analyze Linux swap files to retrieve passwords, usernames, credentials and much more. It is not built-in tool in linux so we have to git clone its repository

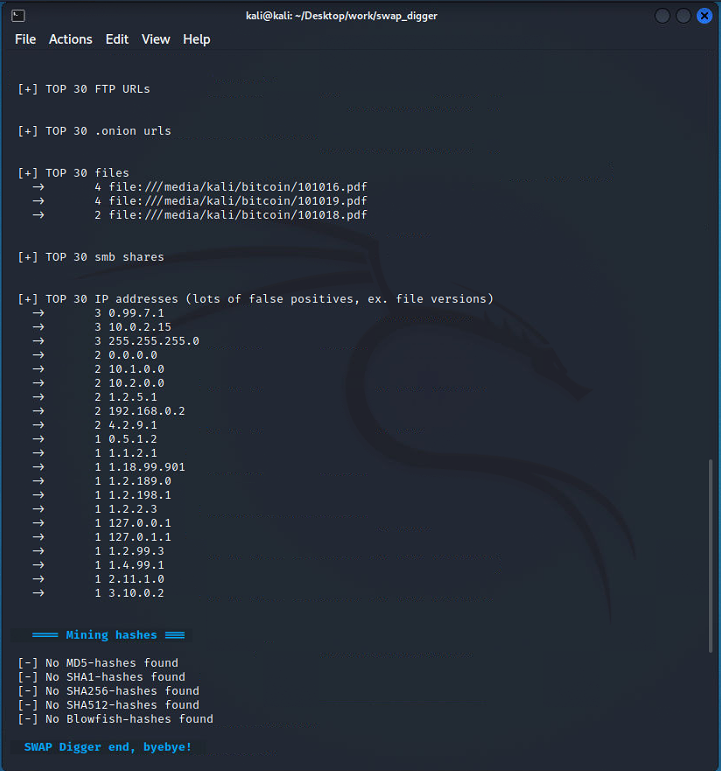


**-S** flag in swap\_digger looks for all available swap device files.



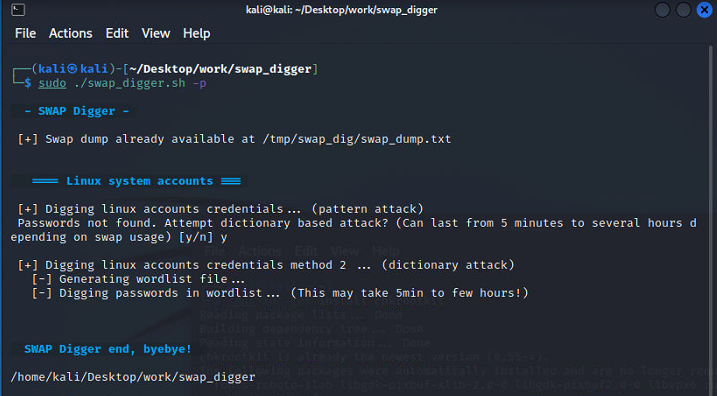
**-a** flag in swap\_digger is used to search all data related to applications that are there





**Step 12**

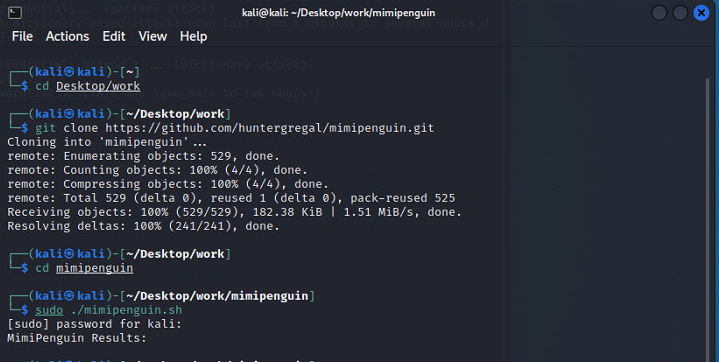
**-p** flag in swap\_digger is used to dig passwords in the linux device



Part IV: Password Dumping with mimipenguin

**Step 13**

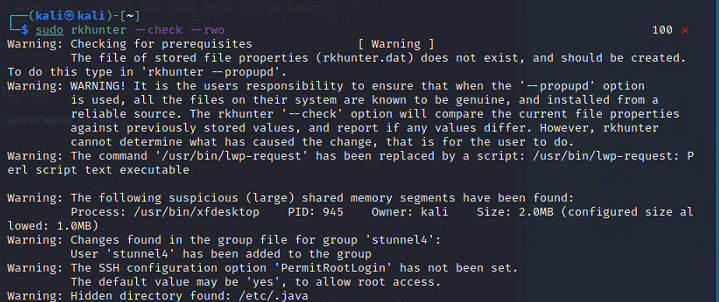
**Mimipenguin** is an opensource tool that is used to dump passwords



Part V: Further Linux Digital Forensic Tools

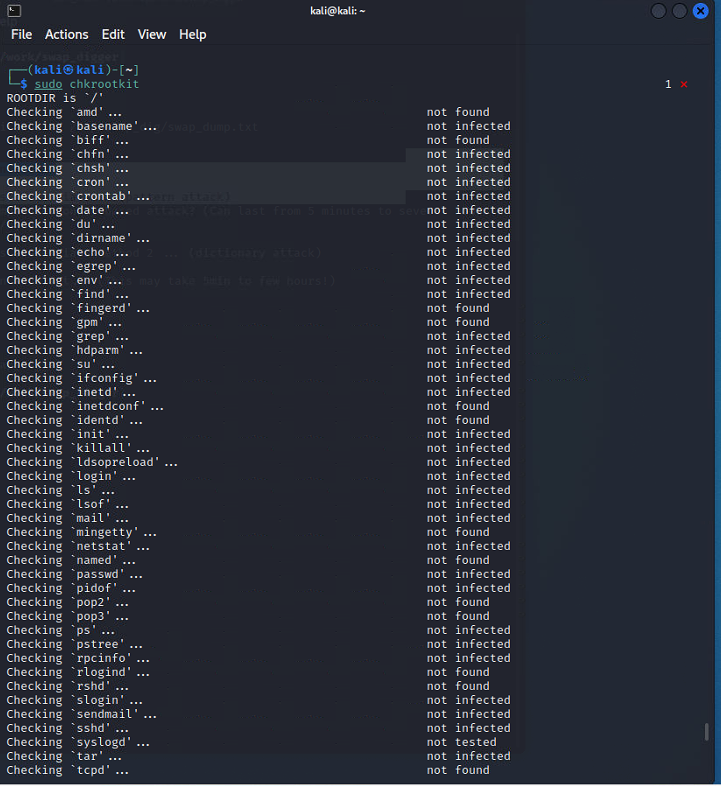
**Step 14**

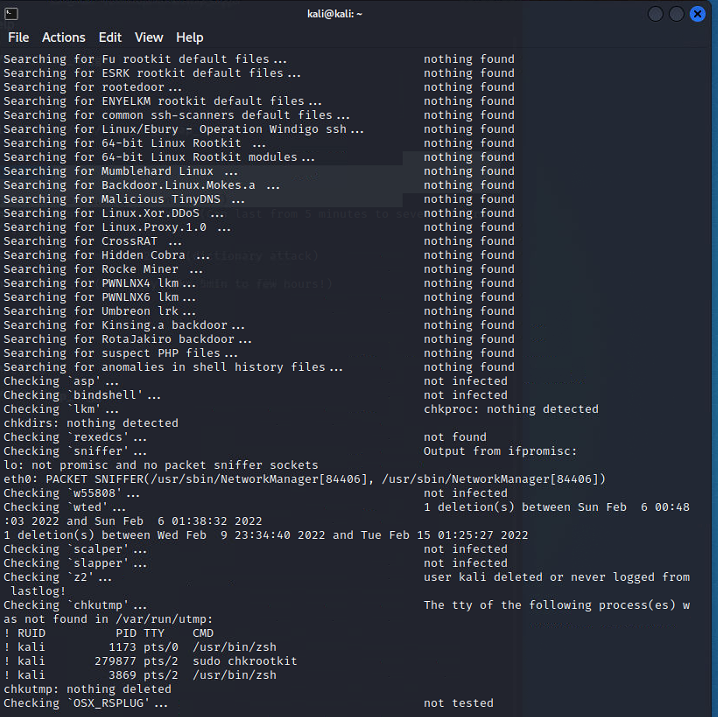
Check for the presence of rootkits, suspicious files, or hidden directories using **rkhunter**



**Step 15**

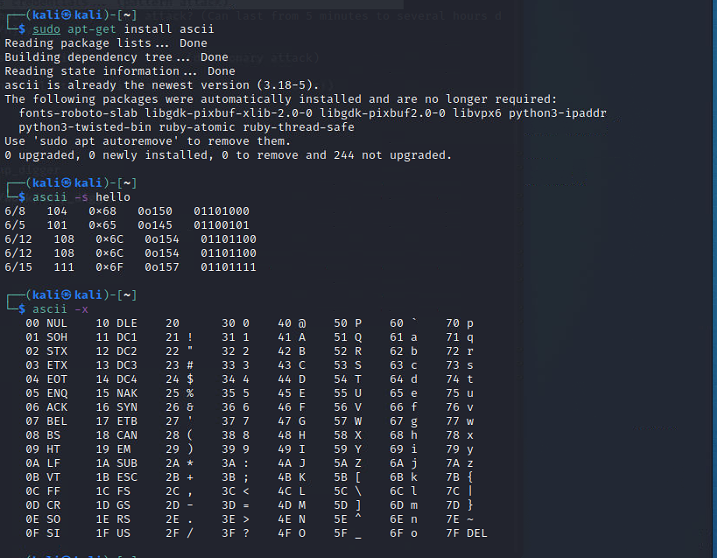
Check for the presence of rootkits using **chkrootkit**.





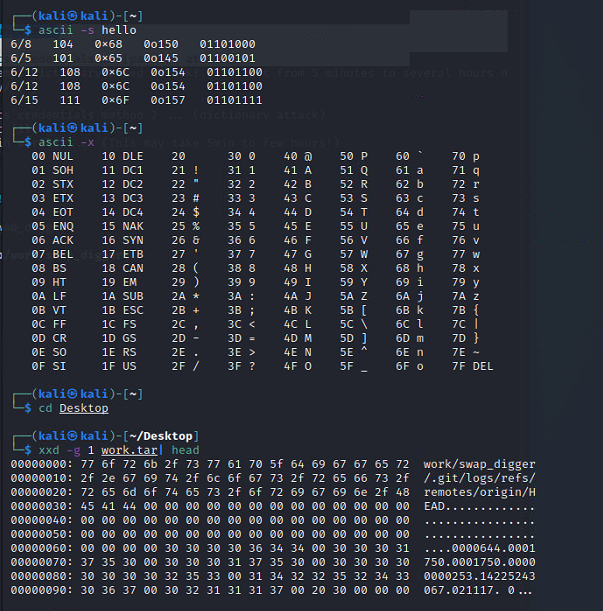
**Step 16**

Now we are going to display asci table using ascii tool, we can also asci values for “**hello**”



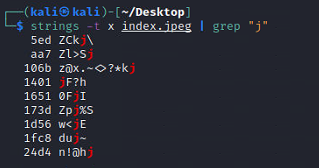
**Step 17**

**xxd** is linux built-in command that is used to display hexadecimal values and **head** command is used to output only header



**Step 18**

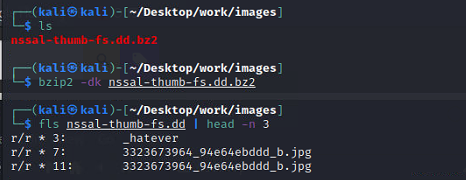
**String** is simple command that grep and display strings in a file

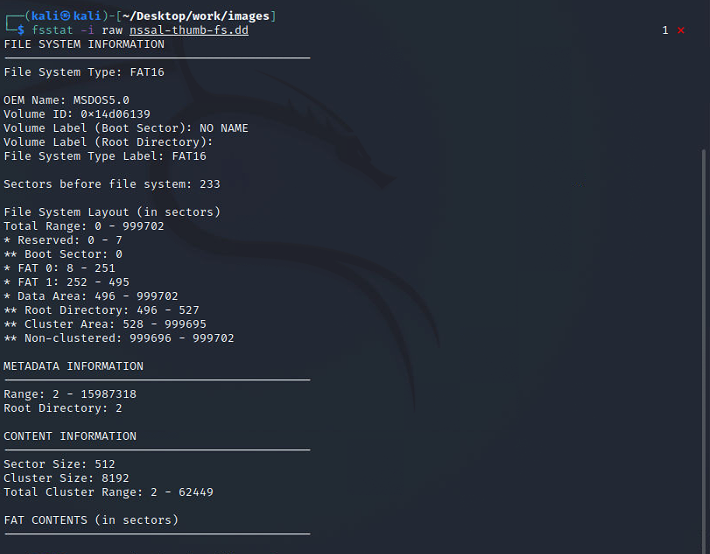


**Step 19 & 20**

The **Sleuth Kit** is a collection digital forensic tools that can be used to analyze disk images and recover files from them:

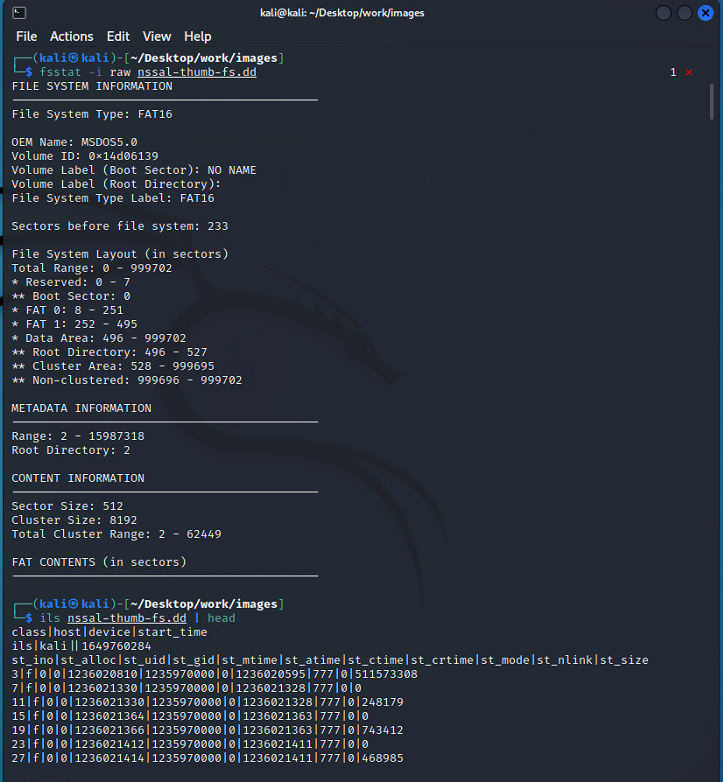
* **fsstat**: Display general details
* **fls**: List files and directories
* **ils**: List inode information
* **img\_cat**: Output contents of an image file
* **fiwalk**: Print the filesystem details



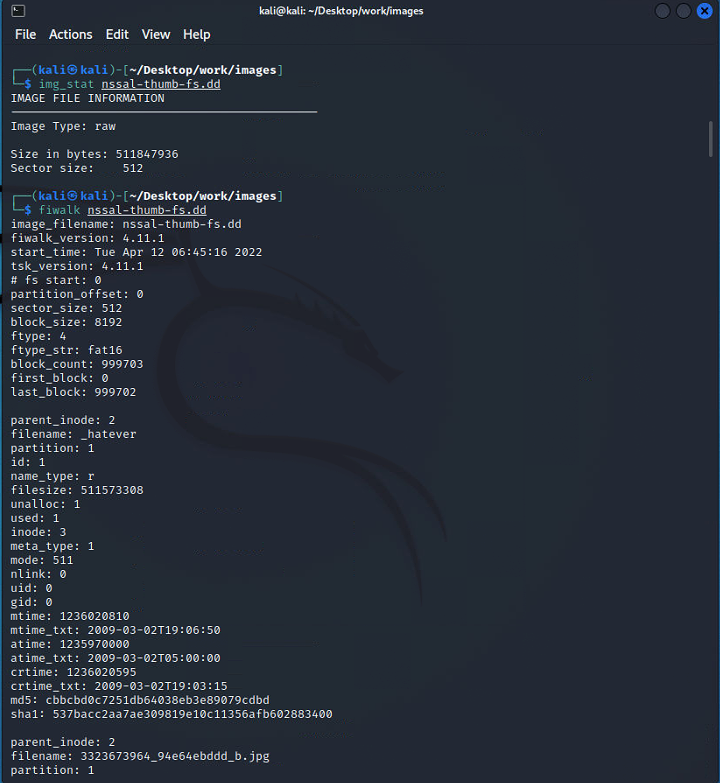


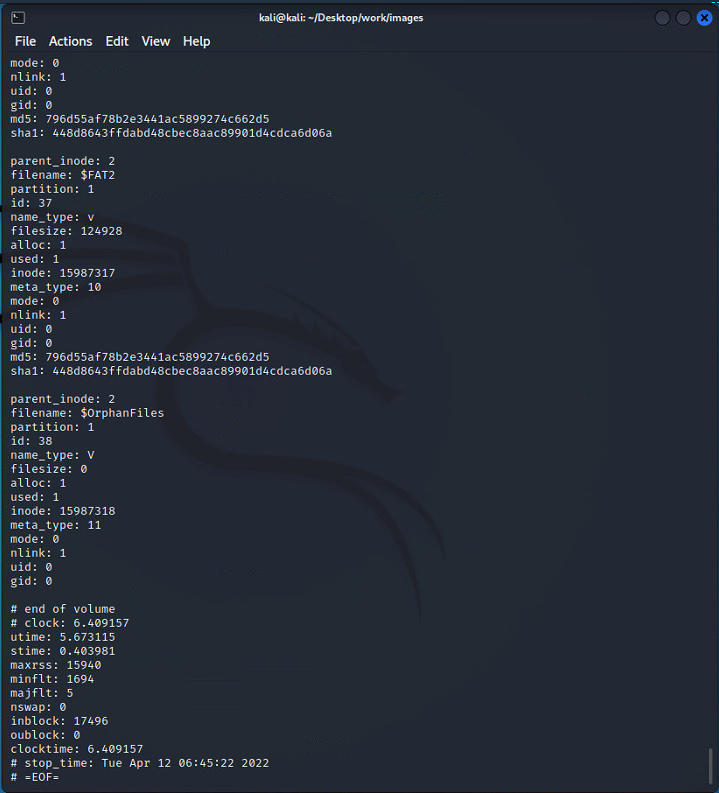
**fsstat**: Display general details

**ils**: List inode information



**fiwalk**: Print the filesystem details





SUMMARY

This lab was all about learning **Linux Forensics** from Identifying devices using different tool to using STK (**Sleuth Toolkit**). In the First part, we learned to do identification of devices using **p0f** tool. In the Second part, we learned about **arp-scan** and **nmap** scan, as they are used for network and device information gathering. In the Third part, we used **swap\_digger**, which is another amazing tool for information gathering of a device, it extracts passwords and much more. In the Fourth part, we tried to do password dumping using **mimipenguin** tool that is available on github. In Fifth part, we did Digital Forensics using **rkhunter** tool, **chkrootkit**, **ascii**, **xxd** and **strings**. In the last part, we used **Sleuth Toolkit** to analyze disk images and recover files.