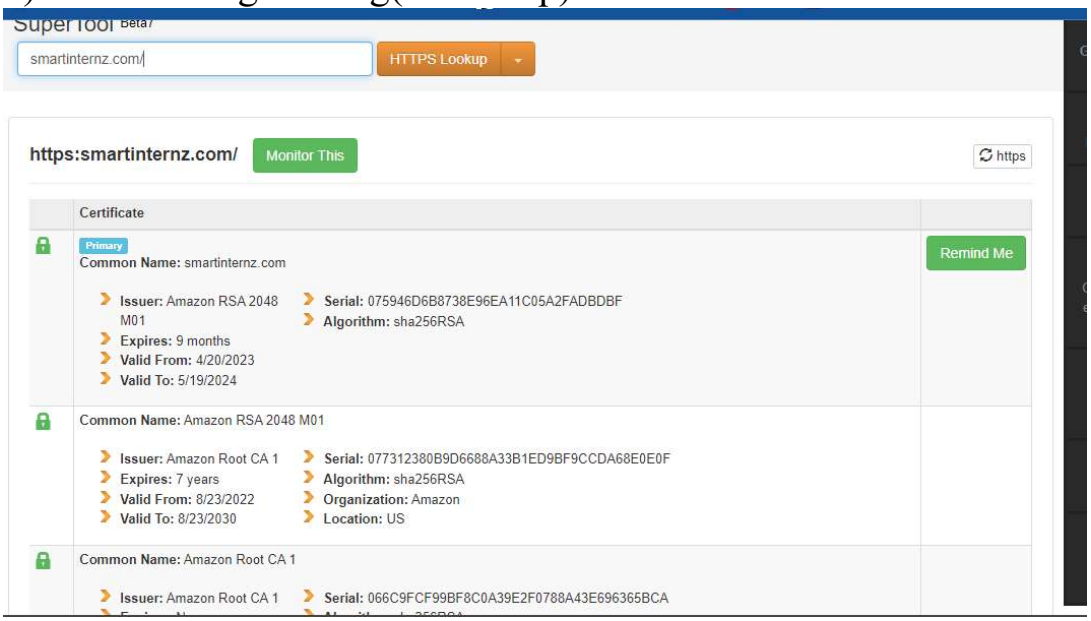
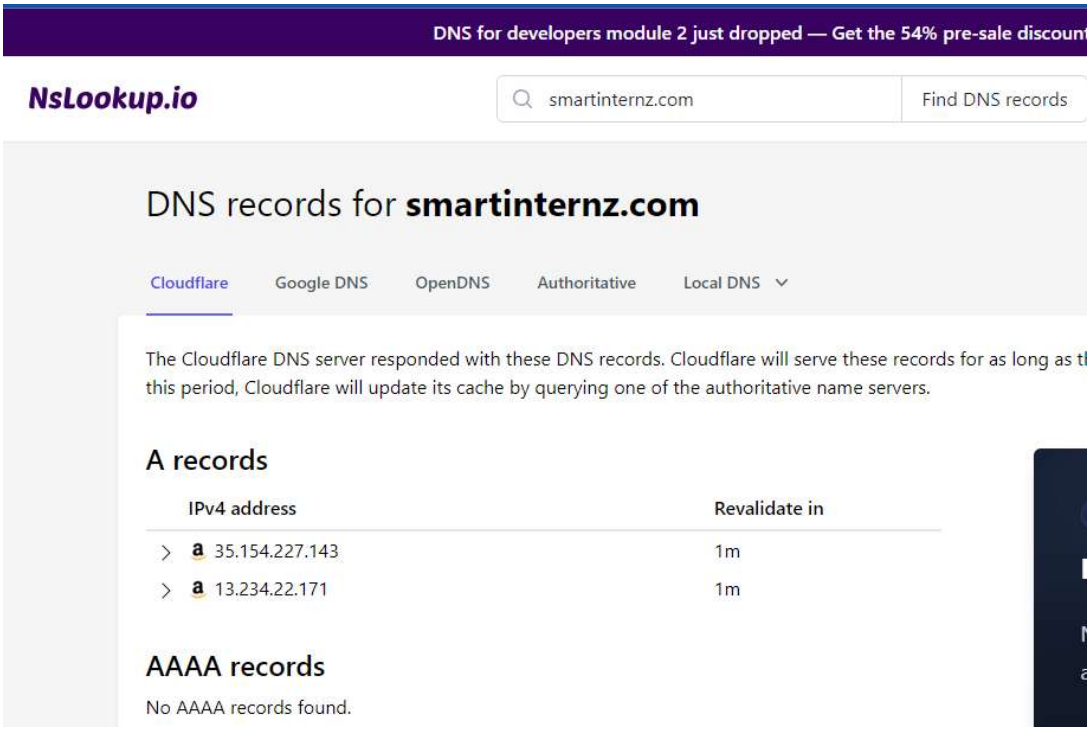
Kali Linux Tools

1)Information gathering(Nslookup)





It helps to find static ip/ip on which site is hosted

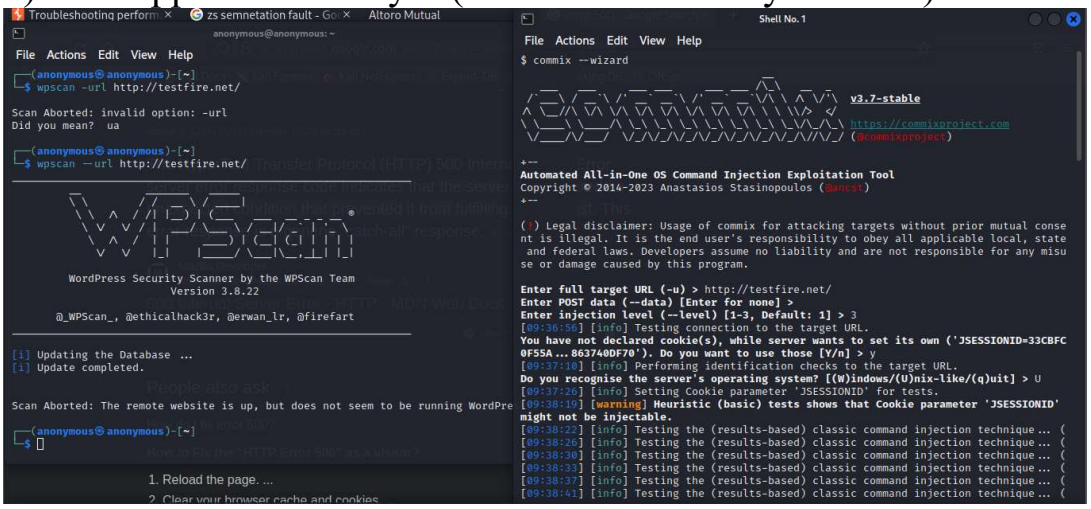
2)Vulnerability scan(Nmap)

```
┌──(anonymous㉿anonymous)-[~]
└─$ sudo nmap -Pn -O  35.154.227.143
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 02:04 IST
Nmap scan report for ec2-35-154-227-143.ap-south-1.compute.amazonaws.com (35.154.227.1
43)
Host is up (0.023s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE  SERVICE
25/tcp  closed smtp
80/tcp  open   http
110/tcp open   pop3
443/tcp open   https
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37
) (96%), Linux 3.2 (96%), Linux 4.4 (96%), Microsoft Windows XP SP3 or Windows 7 or Wi
ndows Server 2012 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT dev
ice (91%), BlueArc Titan 2100 NAS device (89%), DVTel DVT-9540DW network camera (88%),
 Toshiba e-STUDIO 280 printer (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 84.23 seconds
```

```
┌──(anonymous㉿anonymous)-[~]
└─$ sudo nmap -Pn -O  13.234.22.171
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-04 02:06 IST
Nmap scan report for ec2-13-234-22-171.ap-south-1.compute.amazonaws.com (13.234.22.171
)
Host is up (0.0012s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE  SERVICE
25/tcp  closed smtp
110/tcp open   pop3
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 30.32 seconds
```

It helps to find open ports (to perform attack) and version of packages related to port

3)Web Application analysis(WordPress Security Scanner)

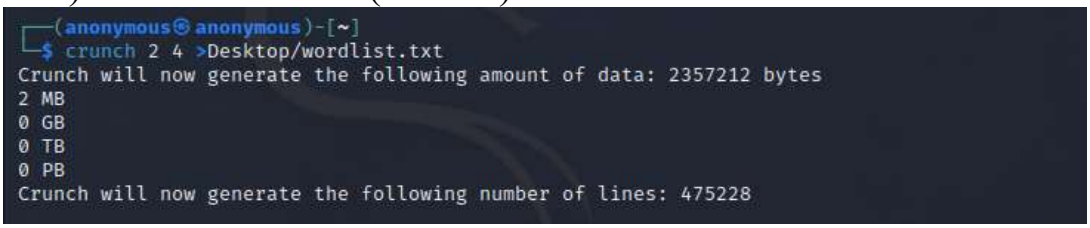


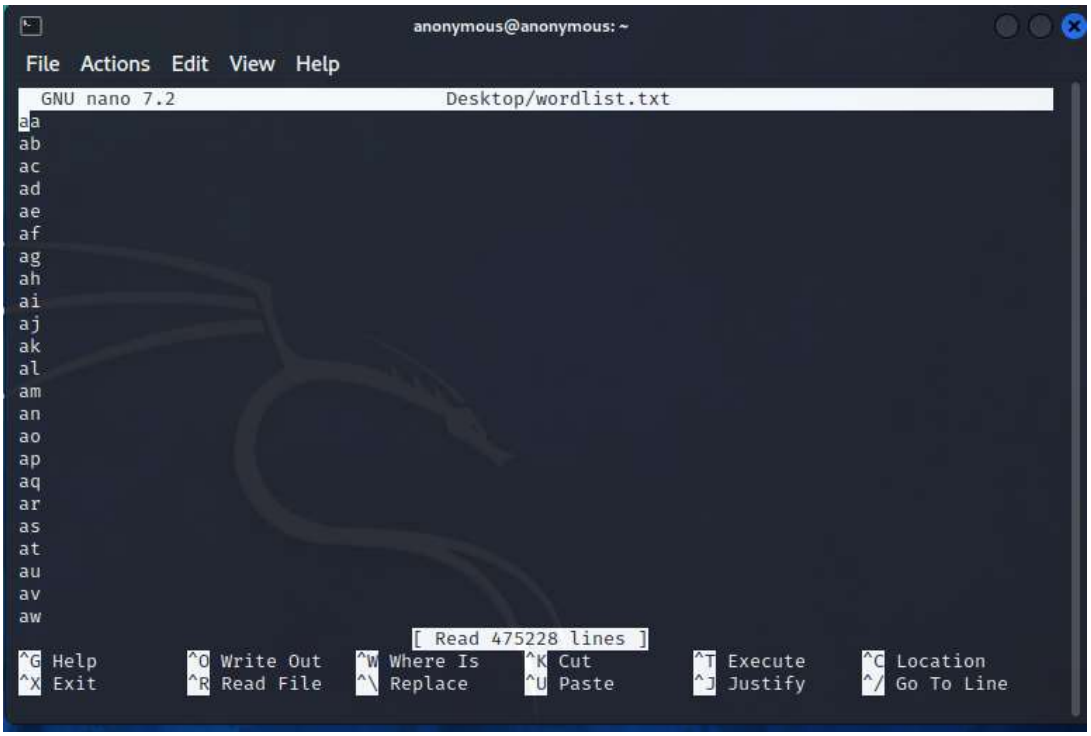
It scan the wordpress website and find vulnerability in it.

4)Database assessment(SqlMap)

Sqlmap find vulnerability to attack on databases of given url.

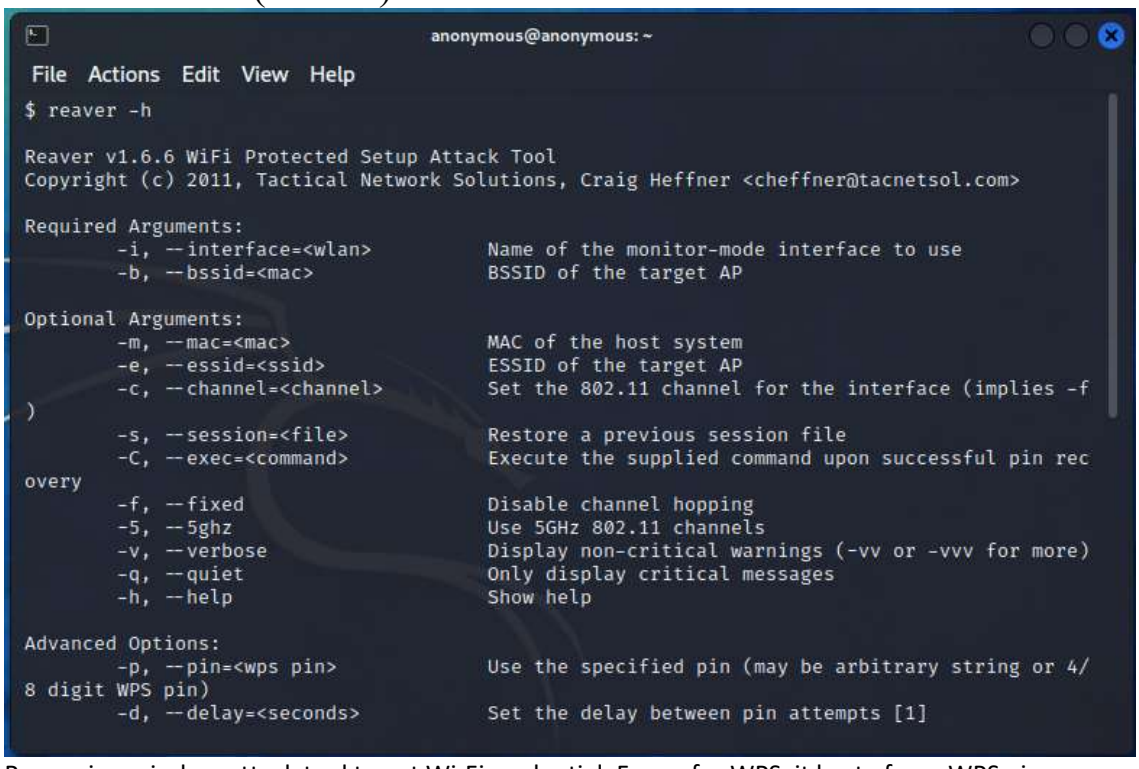
5)Password Attacks(Crunch)





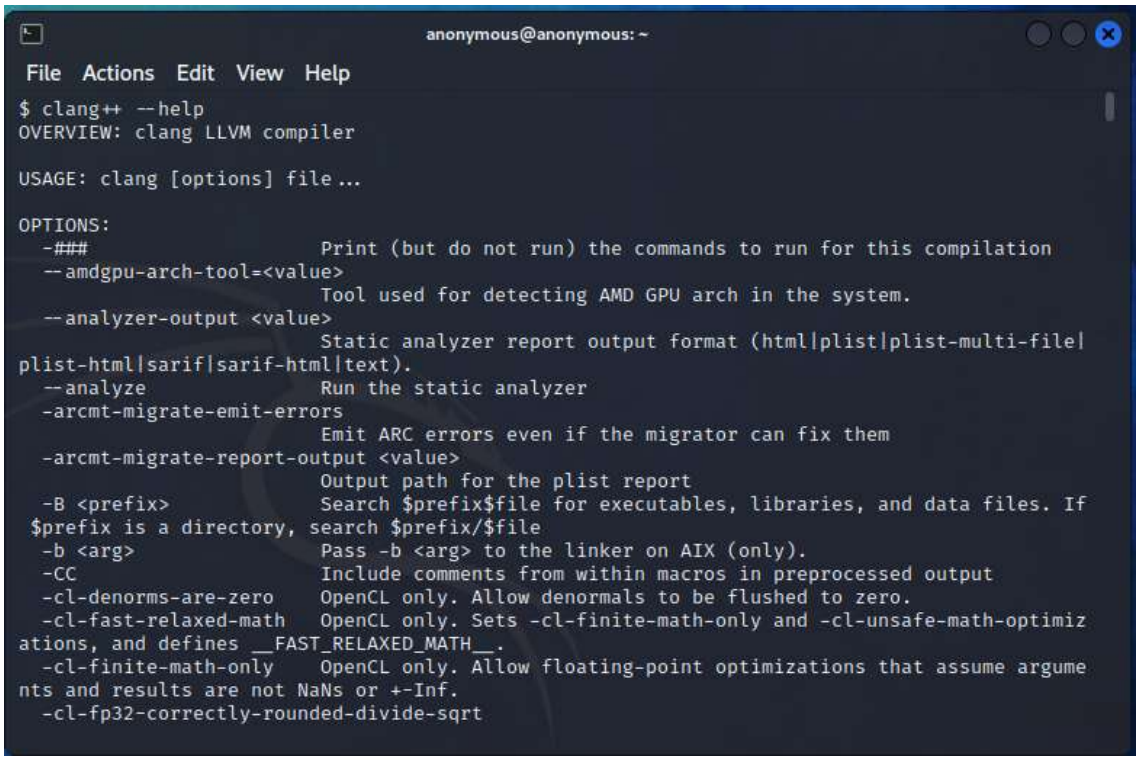
Crunch create a wordlist(dictionary) as user choice for brute force password attack

6)Wireless Attacks (Reaver)



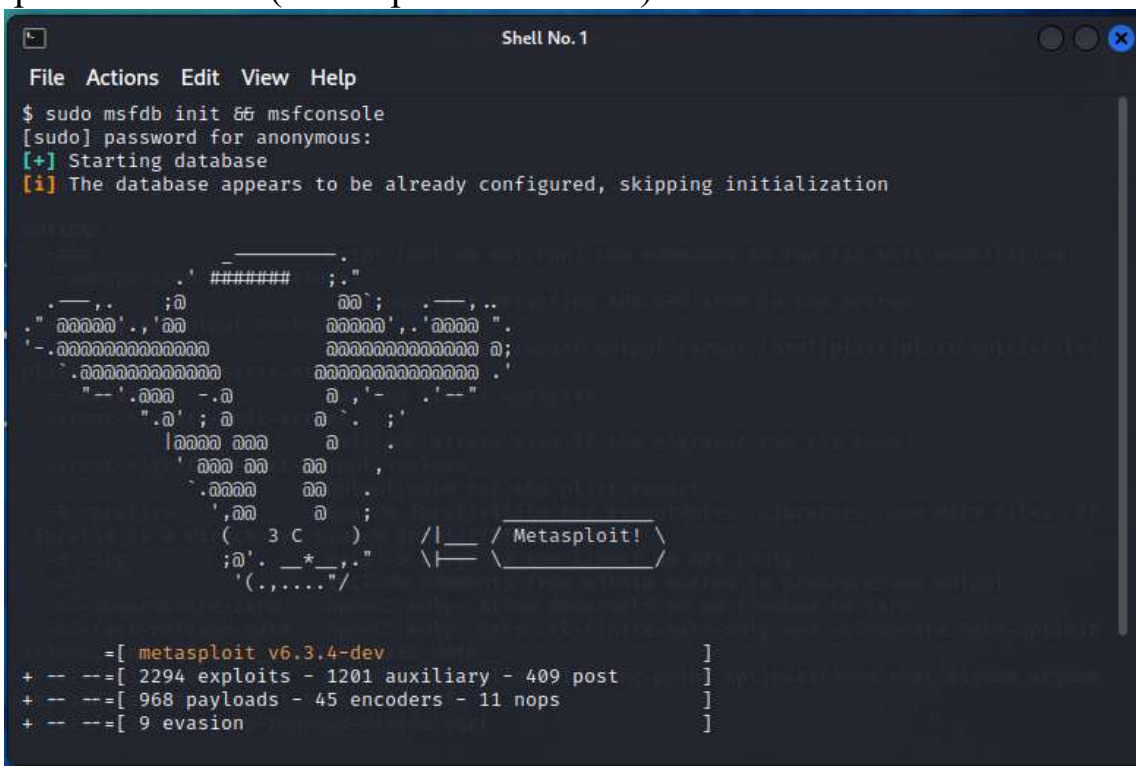
Reaver is a wireless attack tool to get Wi-Fi credential. For ex for WPS ,it brute force WPS pin and can set to wait for particular time to continue again

7)Reverse Engineering(Clang++)

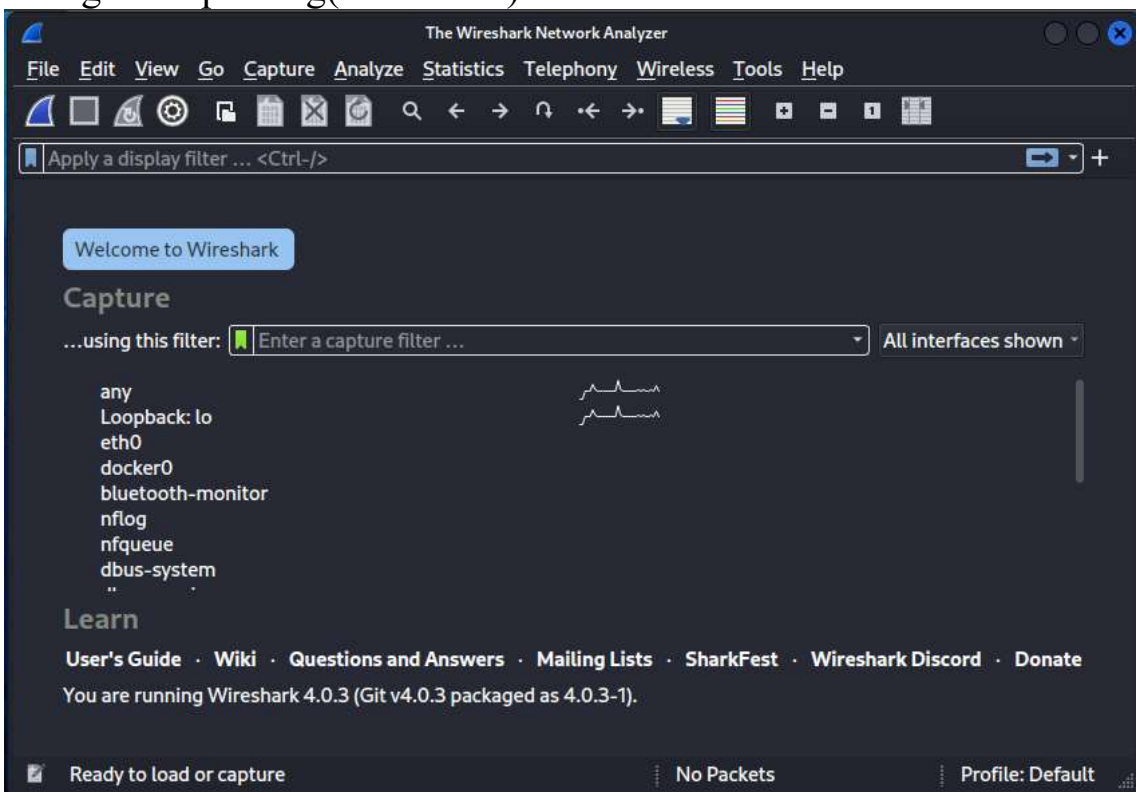


Clang++ helps to analyse packages to retrieve information code or process of development. TO develop crack of a software ,reverse engineering is done ,the according to code malicious dll or package is created to crack it

8)Exploitation Tools(Metaslpoit framework)

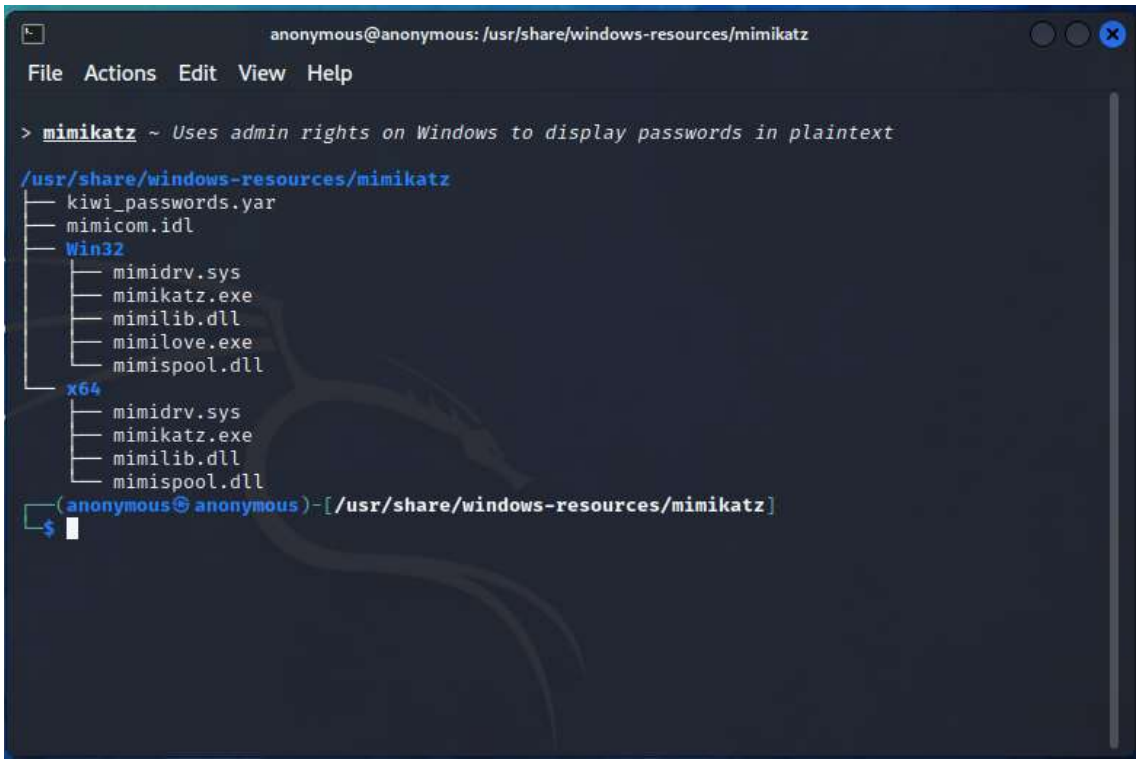


9)Sniffing and Spoofing(Wireshark)



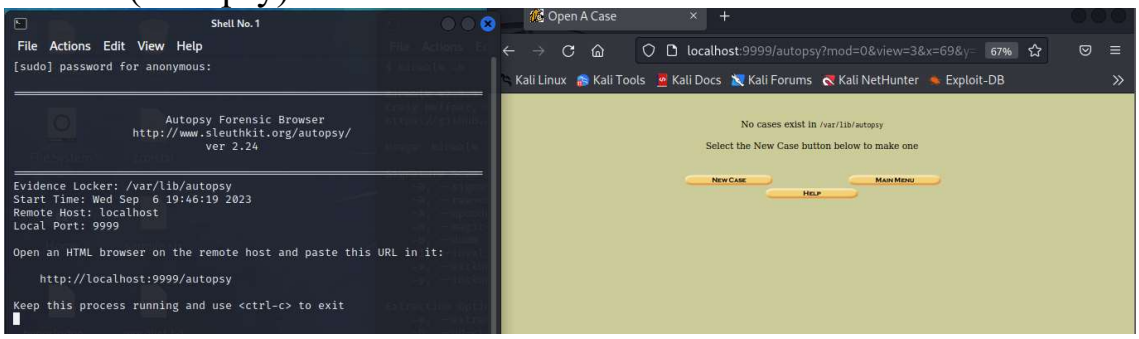
Wireshark helps to analyze or live monitoring of network to know the traffic or data transmission over network layer of packets. If data is transmitted by http, sniffer will get the actual data sent through it.

10)Post Exploitation(Mimikatz)



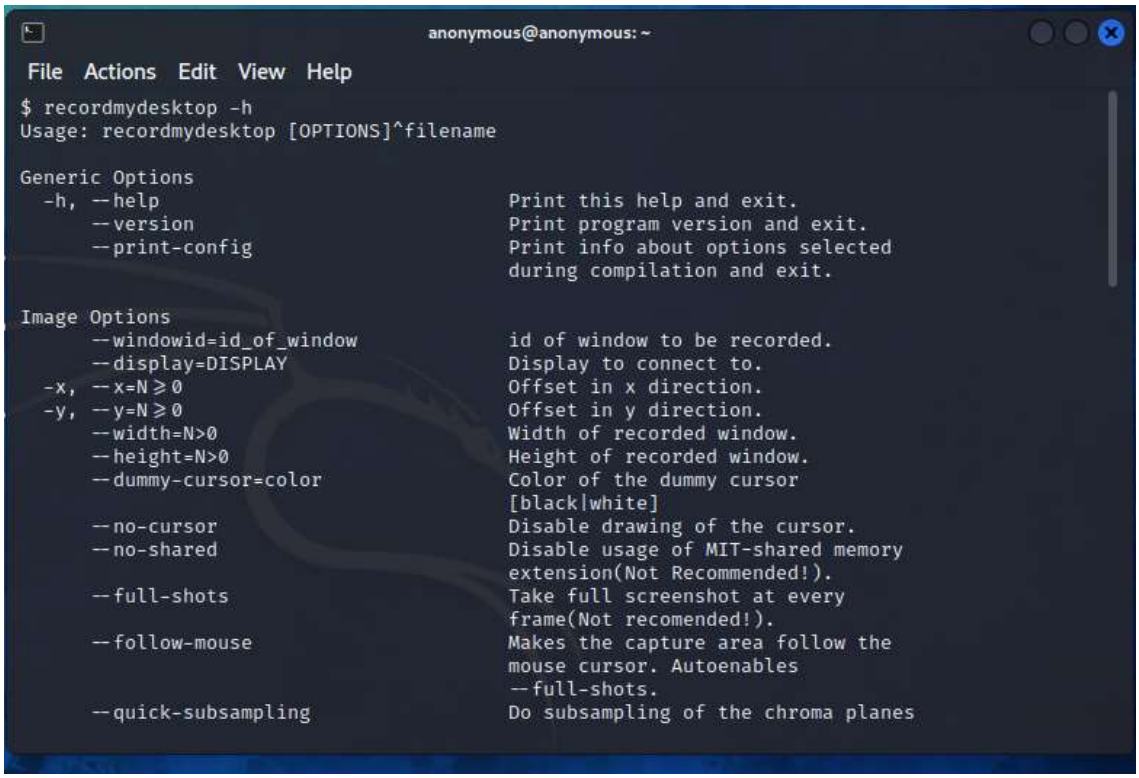
After execution of attack, if anyone want to trace , foot printing mimikatz can be used. It save the data in memory and perform operation to know how it peform. Sometimes it also help to retrieve password as password are saved in memory for useful purpose.

11)Forensic(Autopsy)



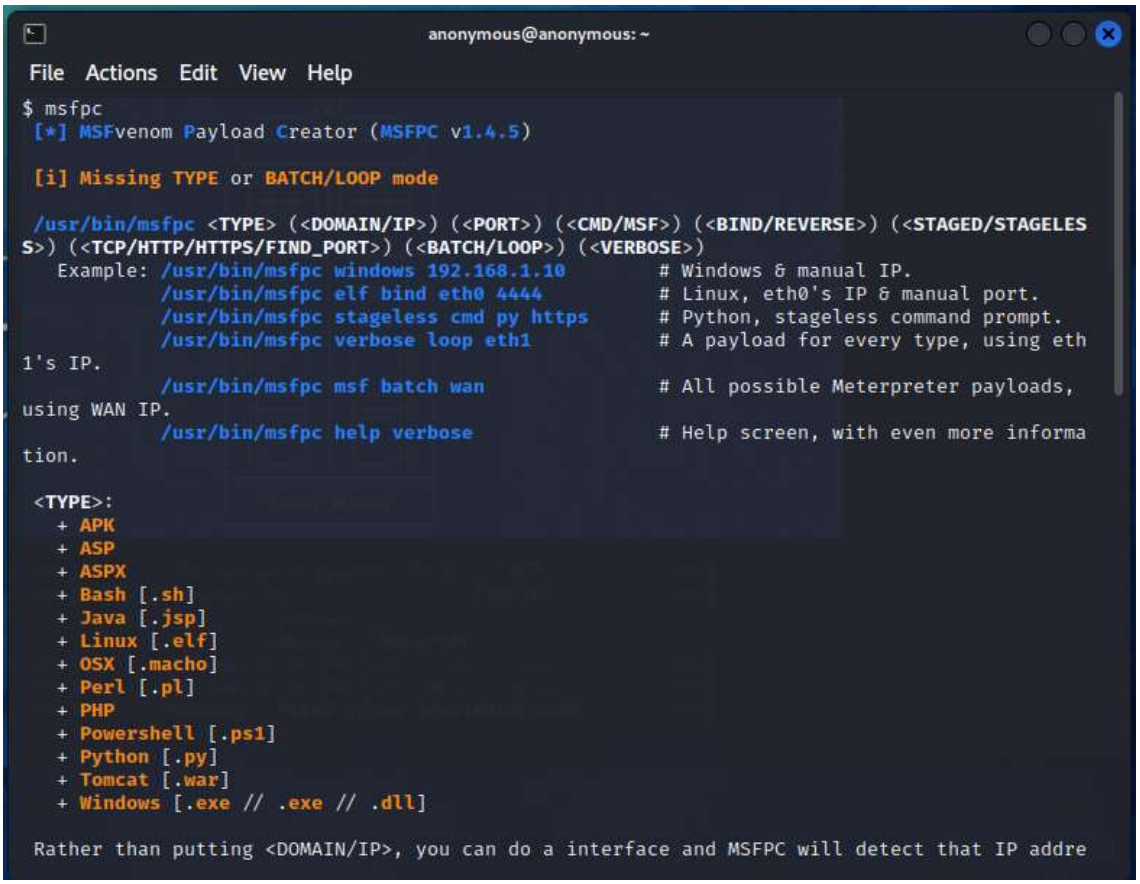
Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.

12)Reporting Tools(RecordmyDesktop)



Recordmydesktop is report creation in form of video with version of os with customized recording area of screen.

13)Social Engineering Tools(MSF Payload Creator)



To create malware for social engineering after reconnaissance, MSF payload creator is one of the tool customized malware of defined OS and file type.