

Sniffing & Spoofing

The basic concept of sniffing tools is as simple as wiretapping and Kali Linux has some popular tools for this purpose. In this chapter, we will learn about the sniffing and spoofing tools available in Kali.

Burpsuite

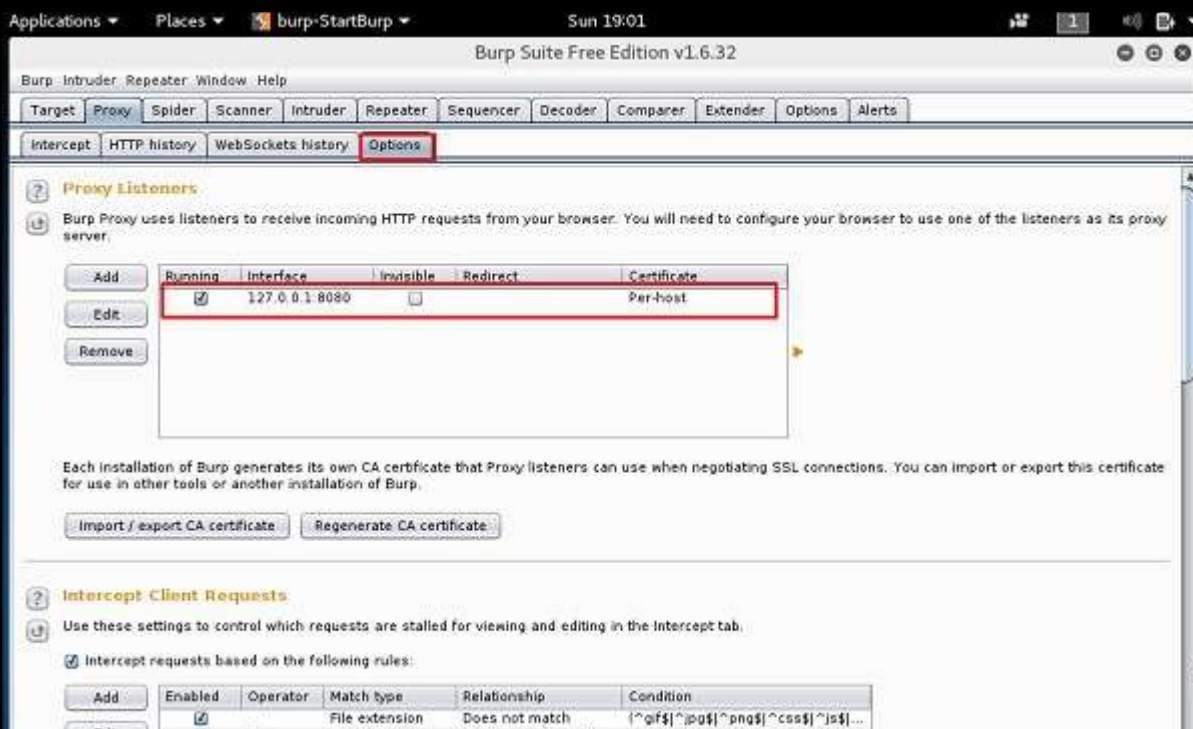
Burpsuite can be used as a sniffing tool between your browser and the web servers to find the parameters that the web application uses.

To open Burpsuite, go to Applications → Web Application Analysis → burpsuite.

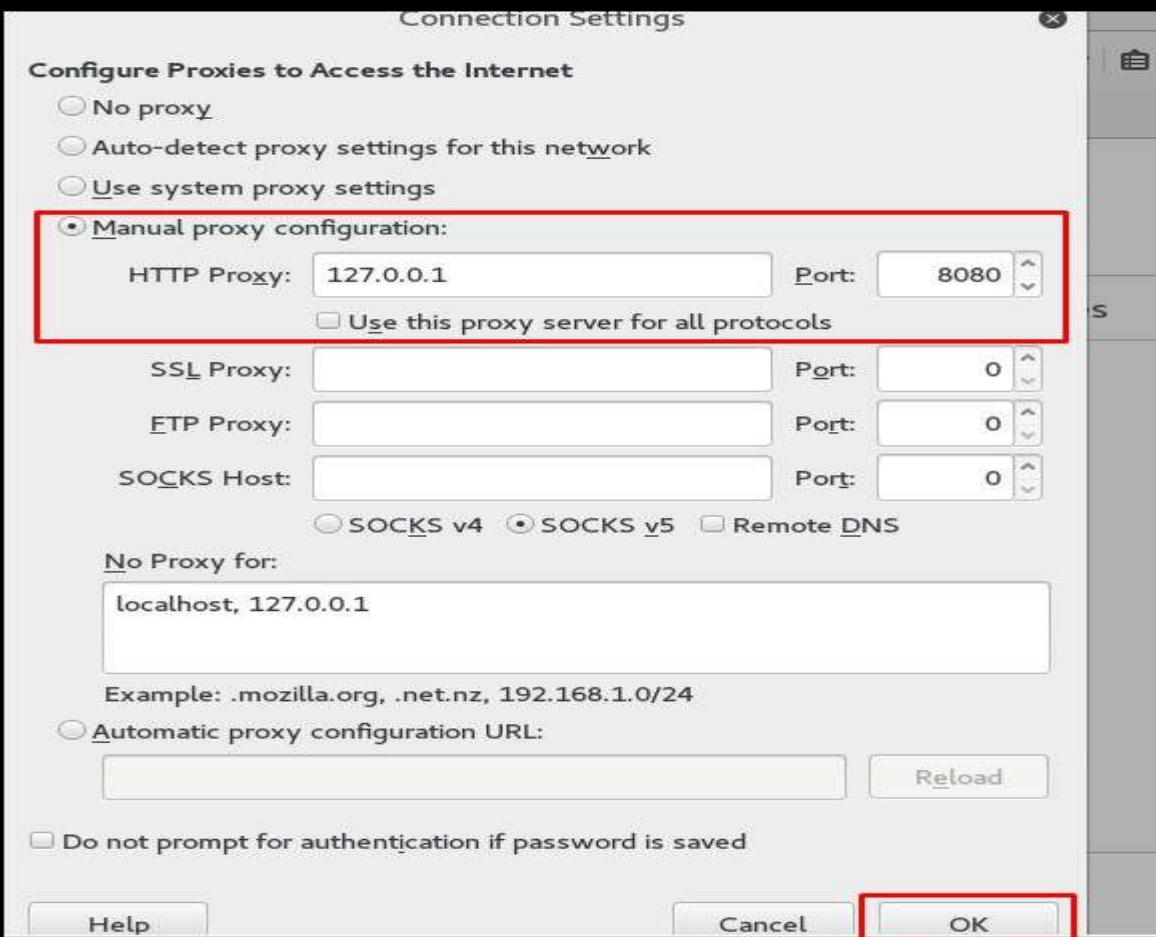


To make the setup of sniffing, we configure burpsuite to behave as a proxy. To do this, go to **Options** as shown in the following screenshot. Check the box as shown.

In this case, the proxy IP will be 127.0.0.1 with port 8080.



Then configure the browser proxy which is the IP of burpsuite machine and the port.

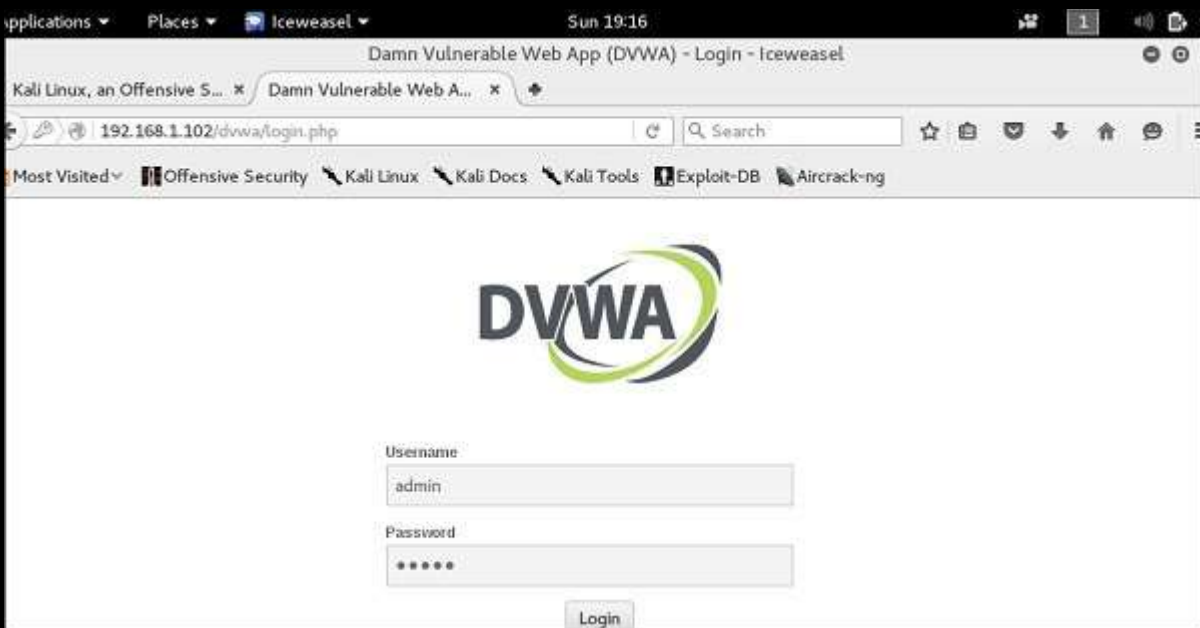


To start interception, go to Proxy → Intercept → click “Intercept is on”.

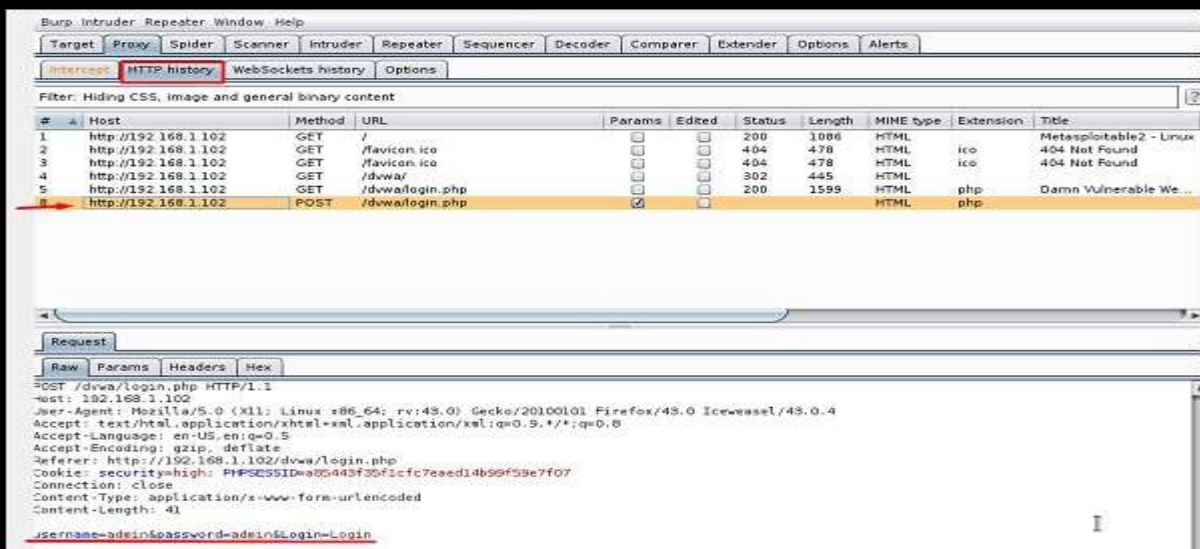
Continue to navigate on the webpage that you want to find the parameter to test for vulnerabilities.



In this case, it is metasploitable machine with IP 192.168.1.102



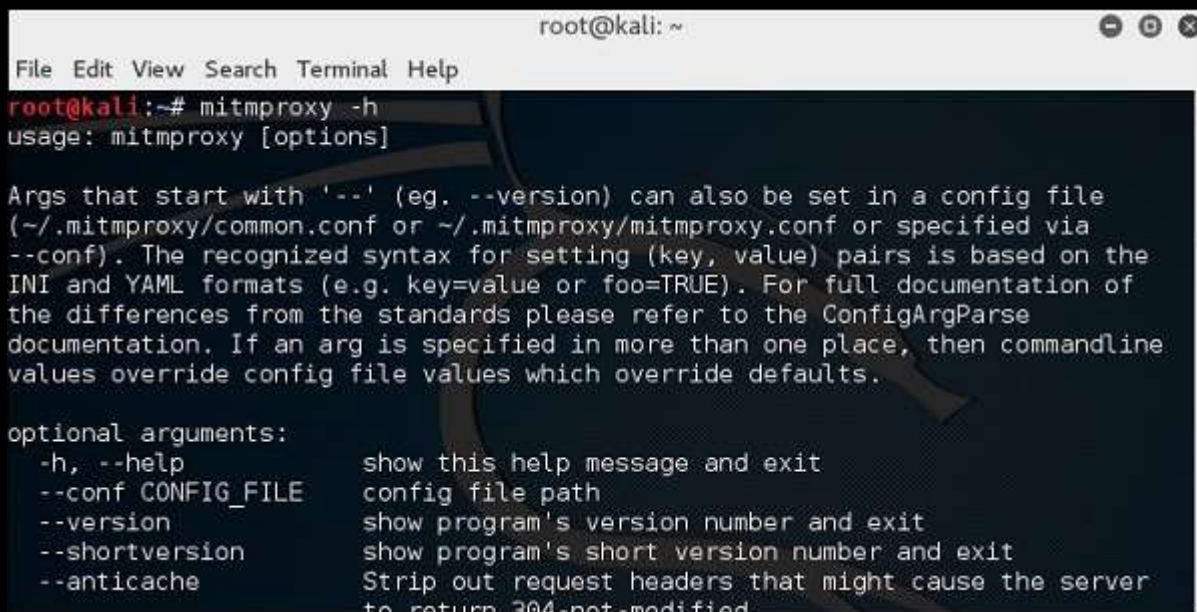
Go to “HTTP History”. In the following screenshot, the line marked in red arrow shows the last request. In Raw and the hidden parameter such as the Session ID and other parameter such as user name and password has been underlined in red.



Mitmproxy

mitmproxy is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected and edited on the fly.

To open it, go to the terminal and type “**mitmproxy -parameter**” and for getting help on commands, type “**mitmproxy -h**”.

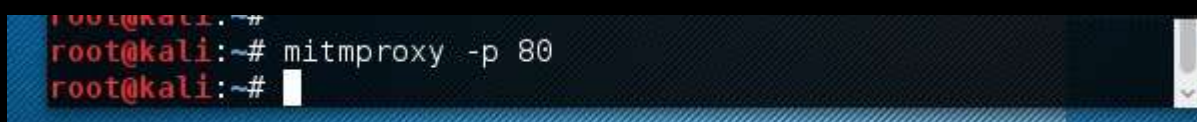
A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'mitmproxy -h' has been executed, displaying the usage and optional arguments. The output text is as follows:

```
root@kali:~# mitmproxy -h
usage: mitmproxy [options]

Args that start with '--' (eg. --version) can also be set in a config file
(~/mitmproxy/common.conf or ~/mitmproxy/mitmproxy.conf or specified via
--conf). The recognized syntax for setting (key, value) pairs is based on the
INI and YAML formats (e.g. key=value or foo=TRUE). For full documentation of
the differences from the standards please refer to the ConfigArgParse
documentation. If an arg is specified in more than one place, then commandline
values override config file values which override defaults.

optional arguments:
  -h, --help            show this help message and exit
  --conf CONFIG_FILE    config file path
  --version              show program's version number and exit
  --shortversion         show program's short version number and exit
  --anticache            Strip out request headers that might cause the server
                        to return 304-not-modified.
```

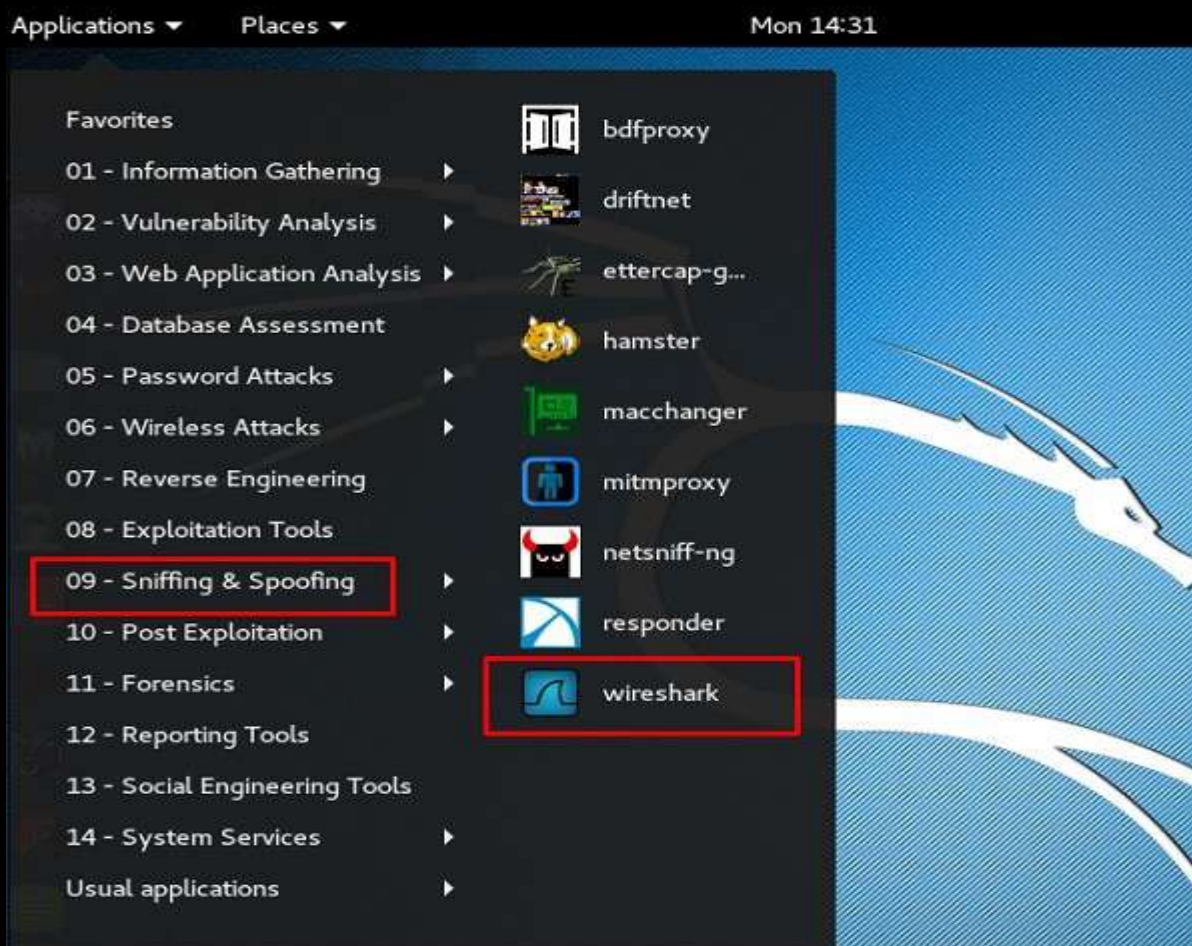
To start the mitmproxy, type “**mitmproxy -p portnumber**”. In this case, it is “**mitmproxy -p 80**”.

A terminal window showing the command 'mitmproxy -p 80' being entered at the prompt 'root@kali:~#'. The prompt is highlighted in red, and the command is in white text on a dark background.

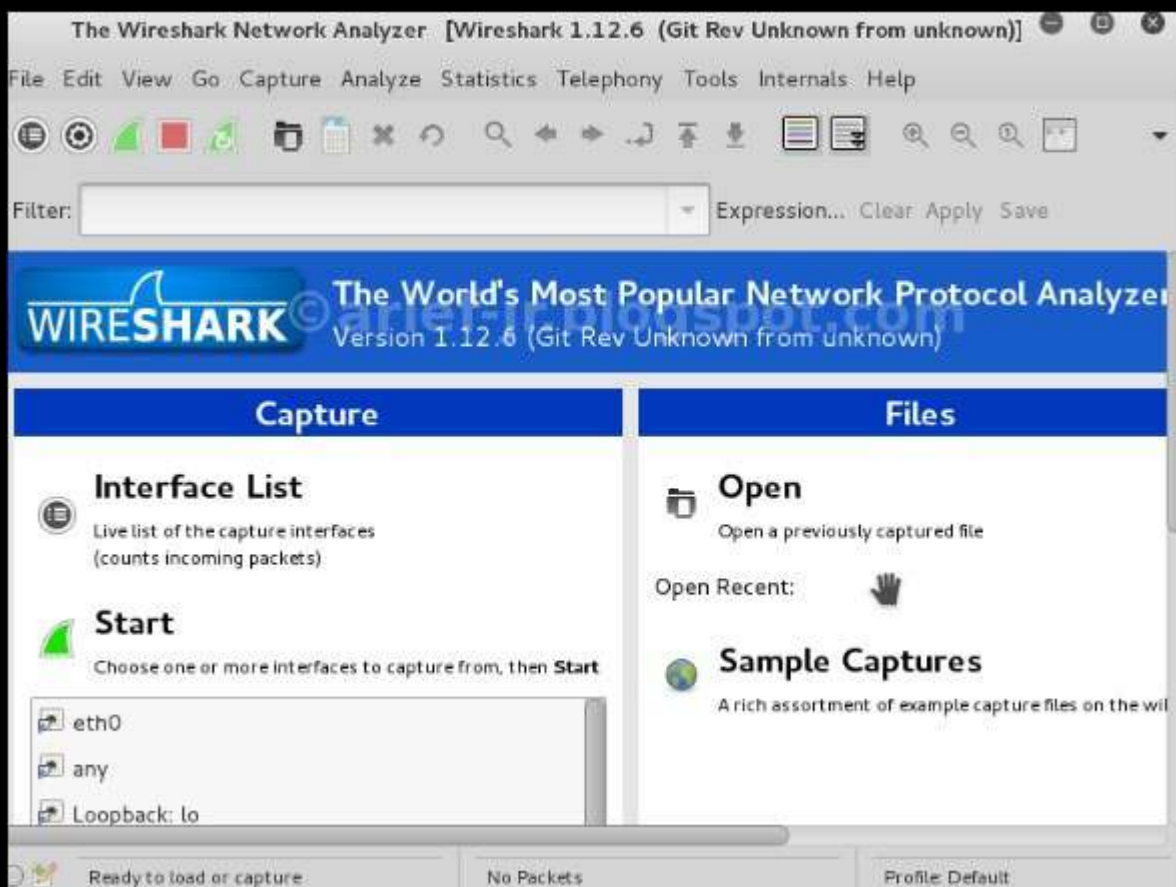
```
root@kali:~# mitmproxy -p 80
root@kali:~#
```

Wireshark

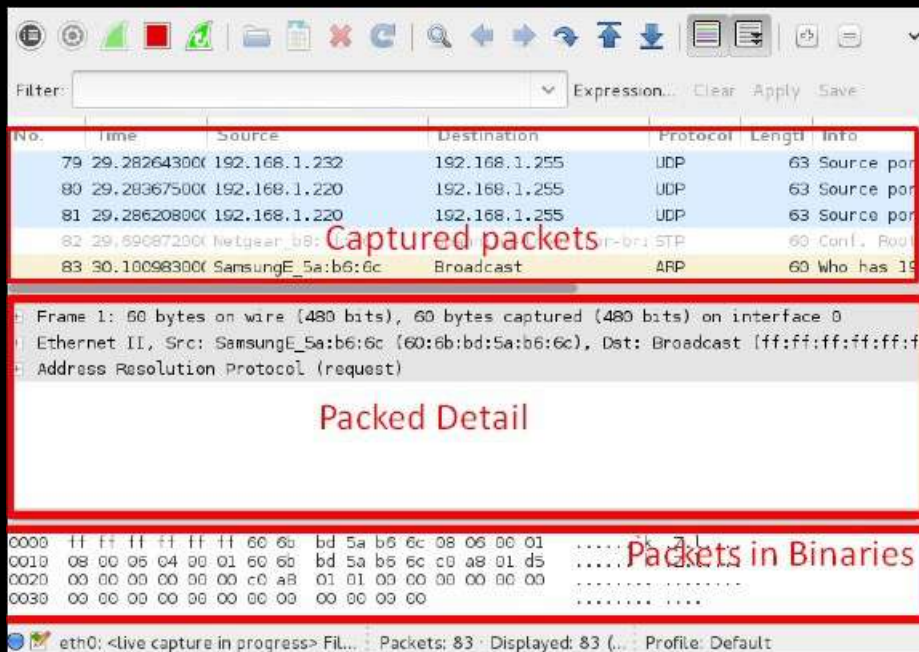
Wireshark is one of the best data packet analyzers. It analyzes deeply the packets in frame level. You can get more information on Wireshark from their official webpage: <https://www.wireshark.org/>. In Kali, it is found using the following path - Applications → Sniffing & Spoofing → wireshark.



Once you click wireshark, the following GUI opens up.



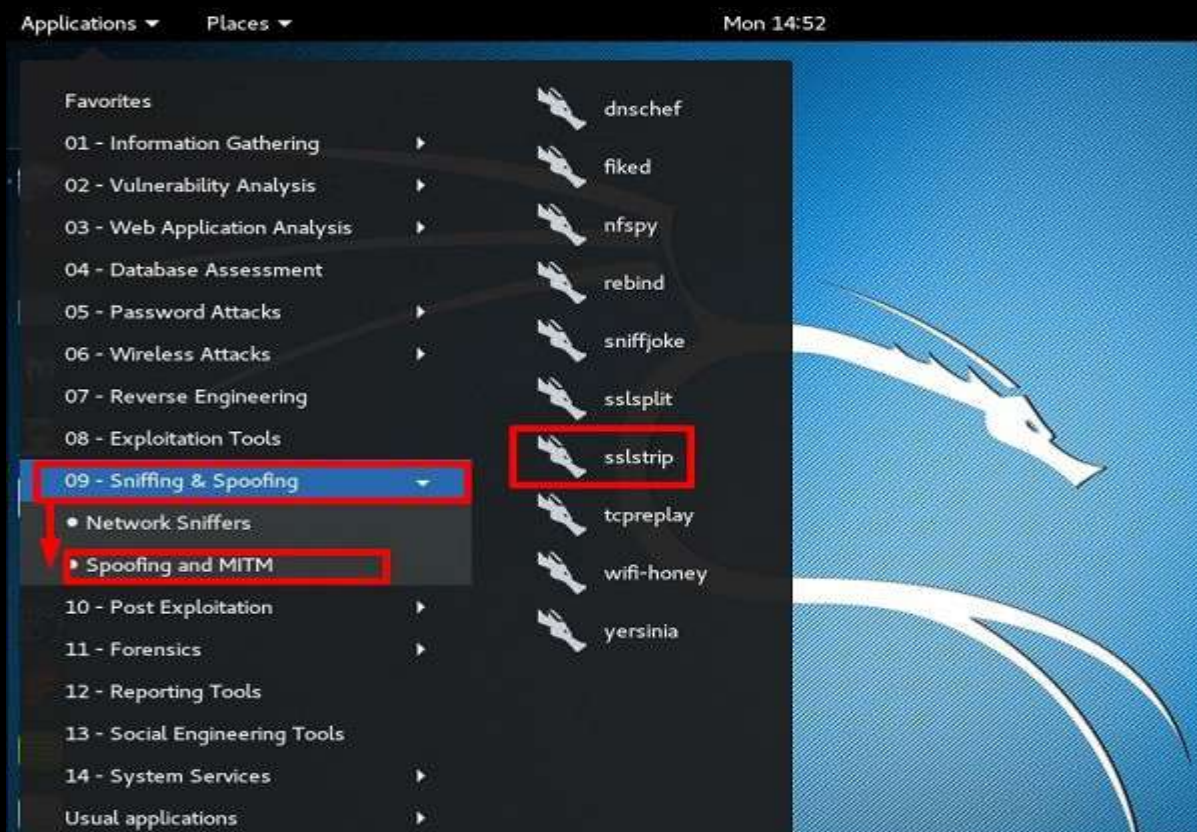
Click "Start" and the packet capturing will start as shown in the following screenshot.



sslstrip

Sslstrip is a MITM attack that forces a victim's browser to communicate in plain-text over HTTP, and the proxies modifies the content from an HTTPS server. To do this, sslstrip is "stripping" https:// URLs and turning them into http:// URLs.

To open it, go to Applications → 09-Sniffing & Spoofing → Spoofing and MITM → sslstrip.




```
sslstrip 0.9 by Moxie Marlinspike
Usage: sslstrip <options>

Options:
-w <filename>, --write=<filename> Specify file to log to (optional).
-p , --post                        Log only SSL POSTs. (default)
-s , --ssl                        Log all SSL traffic to and from server.
-a , --all                        Log all SSL and HTTP traffic to and from server.
-l <port>, --listen=<port>        Port to listen on (default 10000).
-f , --favicon                    Substitute a lock favicon on secure requests.
-k , --killsessions              Kill sessions in progress.
-h                                Print this help message.

root@kali:~#
```

To set it up, write to forward all the 80 port communication to 8080.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@kali:~# route -n
```

Then, start the **sslstrip** command for the port needed.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# sslstrip -l 8080
```