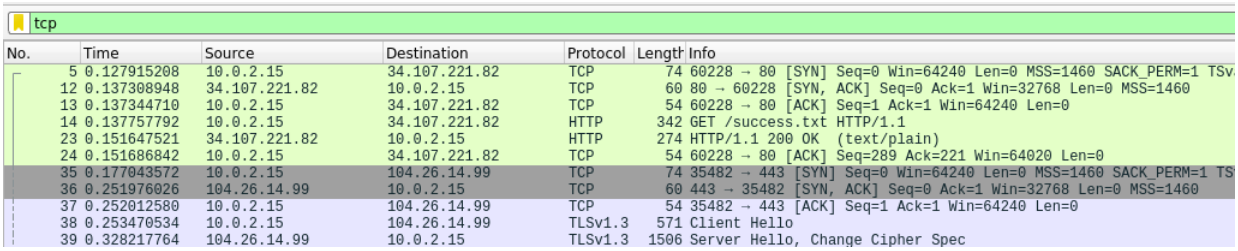
Security Lab
Lab Assignment No. 9

Aim: To study packet sniffer tools and wireshark.

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

Code and Output:

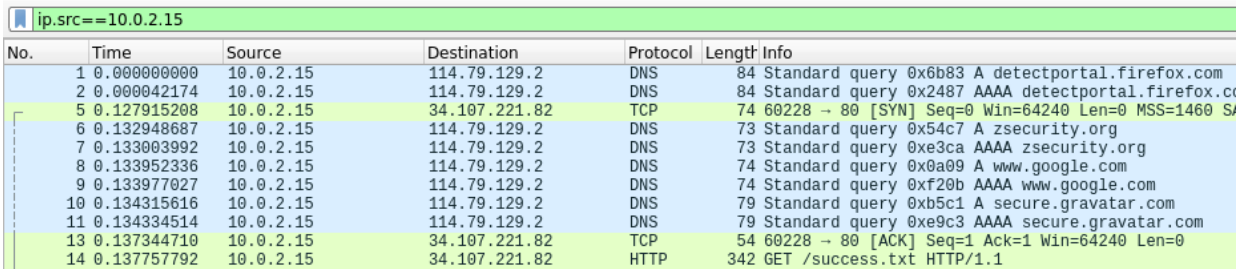
To monitor all TCP packets.
Command: tcp



tcp

No.	Time	Source	Destination	Protocol	Length	Info
5	0.127915208	10.0.2.15	34.107.221.82	TCP	74	60228 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSv
12	0.137308948	34.107.221.82	10.0.2.15	TCP	60	80 → 60228 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
13	0.137344710	10.0.2.15	34.107.221.82	TCP	54	60228 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14	0.137757792	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
23	0.151647521	34.107.221.82	10.0.2.15	HTTP	274	HTTP/1.1 200 OK (text/plain)
24	0.151686842	10.0.2.15	34.107.221.82	TCP	54	60228 → 80 [ACK] Seq=289 Ack=221 Win=64020 Len=0
35	0.177043572	10.0.2.15	104.26.14.99	TCP	74	35482 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TS
36	0.251976026	104.26.14.99	10.0.2.15	TCP	60	443 → 35482 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
37	0.252012580	10.0.2.15	104.26.14.99	TCP	54	35482 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
38	0.253470534	10.0.2.15	104.26.14.99	TLSv1.3	571	Client Hello
39	0.328217764	104.26.14.99	10.0.2.15	TLSv1.3	1506	Server Hello, Change Cipher Spec

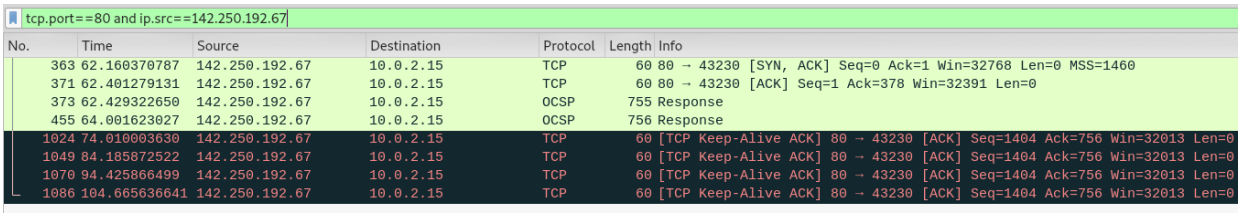
To monitor and display all incoming packets from a specific IP address.
Command: ip.src==<source_ip_address>
ip.src==10.0.2.15



ip.src==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	114.79.129.2	DNS	84	Standard query 0x6b83 A detectportal.firefox.com
2	0.000042174	10.0.2.15	114.79.129.2	DNS	84	Standard query 0x2487 AAAA detectportal.firefox.c
5	0.127915208	10.0.2.15	34.107.221.82	TCP	74	60228 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
6	0.132948687	10.0.2.15	114.79.129.2	DNS	73	Standard query 0x54c7 A zsecurity.org
7	0.133003992	10.0.2.15	114.79.129.2	DNS	73	Standard query 0xe3ca AAAA zsecurity.org
8	0.133952336	10.0.2.15	114.79.129.2	DNS	74	Standard query 0x0a09 A www.google.com
9	0.133977027	10.0.2.15	114.79.129.2	DNS	74	Standard query 0xf20b AAAA www.google.com
10	0.134315616	10.0.2.15	114.79.129.2	DNS	79	Standard query 0xb5c1 A secure.gravatar.com
11	0.134334514	10.0.2.15	114.79.129.2	DNS	79	Standard query 0xe9c3 AAAA secure.gravatar.com
13	0.137344710	10.0.2.15	34.107.221.82	TCP	54	60228 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14	0.137757792	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1

To check all requests to and response received from a particular HTTP Web server.
Command: tcp.port==80 and ip.src==142.250.192.167



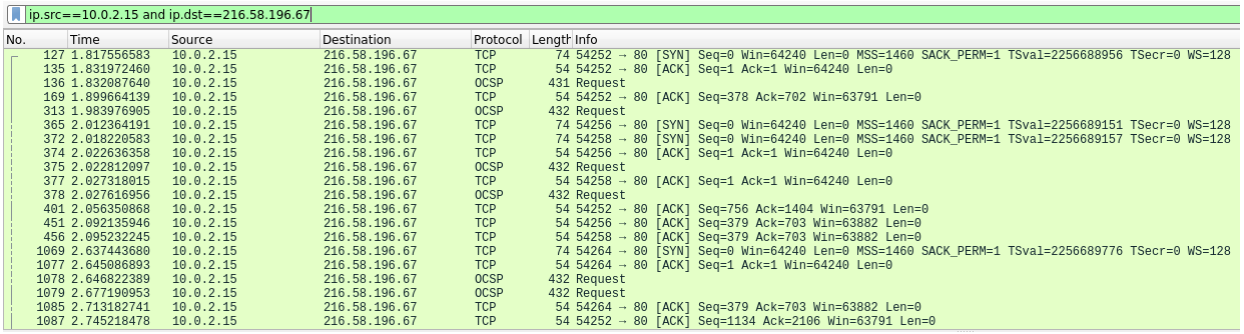
tcp.port==80 and ip.src==142.250.192.67

No.	Time	Source	Destination	Protocol	Length	Info
363	62.160370787	142.250.192.67	10.0.2.15	TCP	60	80 → 43230 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
371	62.401279131	142.250.192.67	10.0.2.15	TCP	60	80 → 43230 [ACK] Seq=1 Ack=378 Win=32391 Len=0
373	62.429322650	142.250.192.67	10.0.2.15	OCSP	755	Response
455	64.001623027	142.250.192.67	10.0.2.15	OCSP	756	Response
1024	74.010003630	142.250.192.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 43230 [ACK] Seq=1404 Ack=756 Win=32013 Len=0
1049	84.185872522	142.250.192.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 43230 [ACK] Seq=1404 Ack=756 Win=32013 Len=0
1070	94.425866499	142.250.192.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 43230 [ACK] Seq=1404 Ack=756 Win=32013 Len=0
1086	104.665636641	142.250.192.67	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 43230 [ACK] Seq=1404 Ack=756 Win=32013 Len=0

To monitor all packets exchanged between 2 IP addresses.

Command: ip.src==<source_ip_address> and ip.dst==<destination_ip_address>

ip.src==10.0.2.15 and ip.dst==216.68.196.67

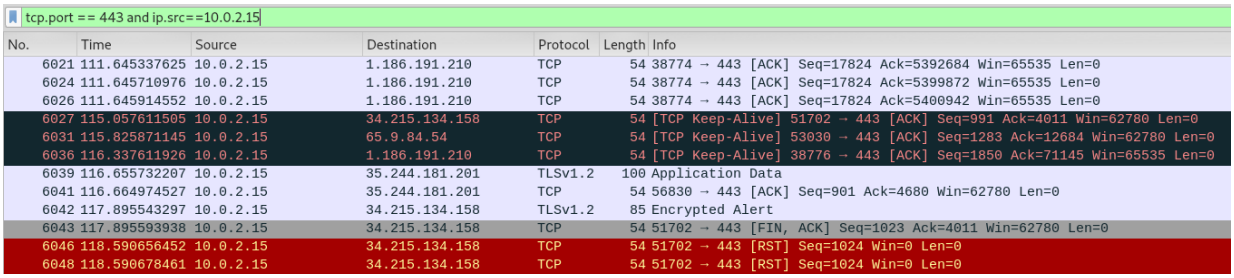


ip.src==10.0.2.15 and ip.dst==216.58.196.67

No.	Time	Source	Destination	Protocol	Length	Info
127	1.817556583	10.0.2.15	216.58.196.67	TCP	74	54252 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2256688956 TSecr=0 WS=128
135	1.831972460	10.0.2.15	216.58.196.67	TCP	54	54252 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
136	1.832087640	10.0.2.15	216.58.196.67	OCSP	431	Request
169	1.899664139	10.0.2.15	216.58.196.67	TCP	54	54252 → 80 [ACK] Seq=378 Ack=702 Win=63791 Len=0
313	1.983976905	10.0.2.15	216.58.196.67	OCSP	432	Request
365	2.012364191	10.0.2.15	216.58.196.67	TCP	74	54256 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2256689151 TSecr=0 WS=128
372	2.018220583	10.0.2.15	216.58.196.67	TCP	74	54258 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2256689157 TSecr=0 WS=128
374	2.022636358	10.0.2.15	216.58.196.67	TCP	54	54256 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
375	2.022812097	10.0.2.15	216.58.196.67	OCSP	432	Request
377	2.027318015	10.0.2.15	216.58.196.67	TCP	54	54258 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
378	2.027616956	10.0.2.15	216.58.196.67	OCSP	432	Request
401	2.056350868	10.0.2.15	216.58.196.67	TCP	54	54252 → 80 [ACK] Seq=756 Ack=1404 Win=63791 Len=0
451	2.092135946	10.0.2.15	216.58.196.67	TCP	54	54256 → 80 [ACK] Seq=379 Ack=703 Win=63882 Len=0
456	2.095232245	10.0.2.15	216.58.196.67	TCP	54	54258 → 80 [ACK] Seq=379 Ack=703 Win=63882 Len=0
1069	2.637443680	10.0.2.15	216.58.196.67	TCP	74	54264 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2256689776 TSecr=0 WS=128
1077	2.645086893	10.0.2.15	216.58.196.67	TCP	54	54264 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1078	2.646822389	10.0.2.15	216.58.196.67	OCSP	432	Request
1079	2.677190953	10.0.2.15	216.58.196.67	OCSP	432	Request
1085	2.713182741	10.0.2.15	216.58.196.67	TCP	54	54264 → 80 [ACK] Seq=379 Ack=703 Win=63882 Len=0
1087	2.745218478	10.0.2.15	216.58.196.67	TCP	54	54252 → 80 [ACK] Seq=1134 Ack=2106 Win=63791 Len=0

Check all incoming requests to an HTTPS Web Server.

Command: tcp.port==443 and ip.src==10.0.2.15



tcp.port == 443 and ip.src==10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
6021	111.645337625	10.0.2.15	1.186.191.210	TCP	54	38774 → 443 [ACK] Seq=17824 Ack=5392684 Win=65535 Len=0
6024	111.645710976	10.0.2.15	1.186.191.210	TCP	54	38774 → 443 [ACK] Seq=17824 Ack=5399872 Win=65535 Len=0
6026	111.645914552	10.0.2.15	1.186.191.210	TCP	54	38774 → 443 [ACK] Seq=17824 Ack=5400942 Win=65535 Len=0
6027	115.057611505	10.0.2.15	34.215.134.158	TCP	54	[TCP Keep-Alive] 51702 → 443 [ACK] Seq=991 Ack=4011 Win=62780 Len=0
6031	115.825871145	10.0.2.15	65.9.84.54	TCP	54	[TCP Keep-Alive] 53030 → 443 [ACK] Seq=1283 Ack=12684 Win=62780 Len=0
6036	116.337611926	10.0.2.15	1.186.191.210	TCP	54	[TCP Keep-Alive] 38776 → 443 [ACK] Seq=1850 Ack=71145 Win=65535 Len=0
6039	116.655732207	10.0.2.15	35.244.181.201	TLSv1.2	100	Application Data
6041	116.664974527	10.0.2.15	35.244.181.201	TCP	54	56830 → 443 [ACK] Seq=901 Ack=4680 Win=62780 Len=0
6042	117.895543297	10.0.2.15	34.215.134.158	TLSv1.2	85	Encrypted Alert
6043	117.895593938	10.0.2.15	34.215.134.158	TCP	54	51702 → 443 [FIN, ACK] Seq=1023 Ack=4011 Win=62780 Len=0
6046	118.590656452	10.0.2.15	34.215.134.158	TCP	54	51702 → 443 [RST] Seq=1024 Win=0 Len=0
6048	118.590678461	10.0.2.15	34.215.134.158	TCP	54	51702 → 443 [RST] Seq=1024 Win=0 Len=0

Conclusion: Thus, we have studied packet sniffer tools and understood the installation of Wireless (Network protocol analyzer) and analyzed the traffic.