Topic-WireShark

Functionalities implemented:
i_Traffic Analysis
ii_PortScan
iii_Packet Sniffing
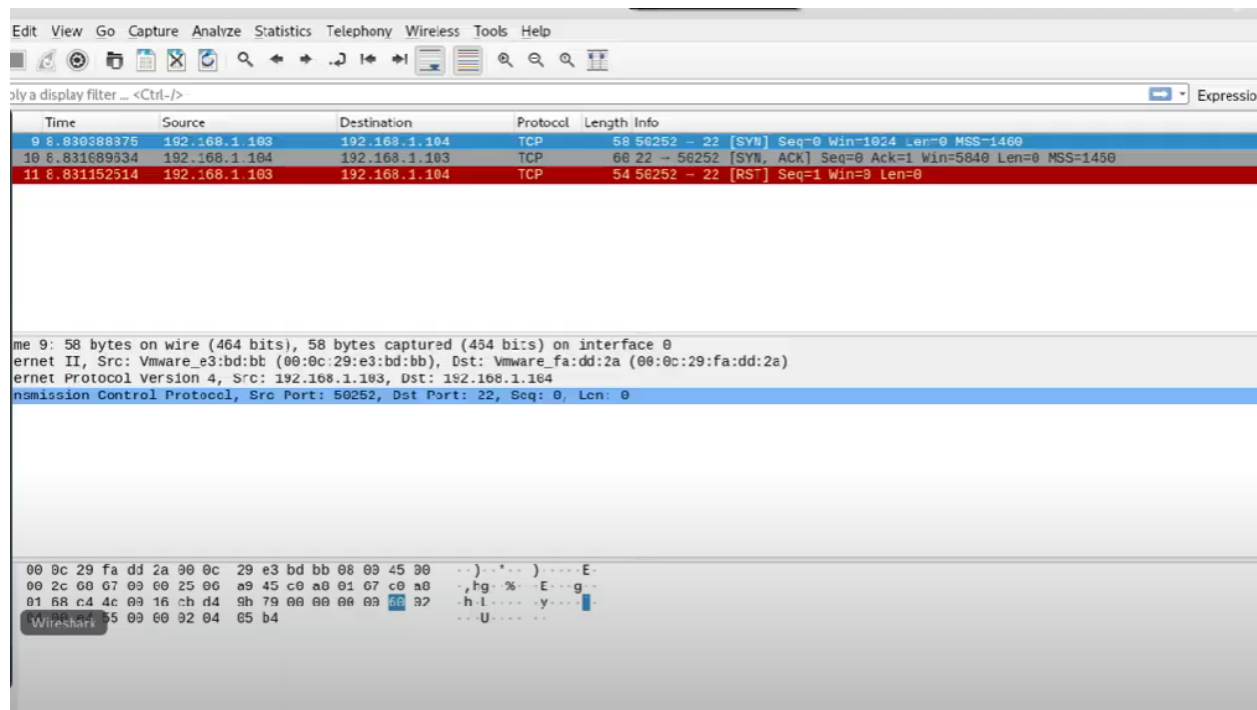
Traffic Analysis Screenshot:

Port Scan Screenshot:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.10

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.103	14.49.100.37	TCP	78	54460 → 80 [ACK] Seq=1 Ack=1 Win=5093 Len=0 TSval=4191317101 TSecr=474
2	0.006283568	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=7241 Ack=1 Win=59 Len=1448 TSval=47463029 TSecr=4
3	0.008201963	192.168.1.103	14.49.100.37	TCP	78	[TCP Dup ACK 1#1] 54460 → 80 [ACK] Seq=1 Ack=1 Win=5093 Len=0 TSval=41
4	0.022617929	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=8689 Ack=1 Win=59 Len=1448 TSval=47463029 TSecr=4
5	0.023164320	192.168.1.103	14.49.100.37	TCP	78	[TCP Dup ACK 1#2] 54460 → 80 [ACK] Seq=1 Ack=1 Win=5093 Len=0 TSval=41
6	0.024283506	14.49.100.37	192.168.1.103	TCP	1514	[TCP Fast Retransmission] 80 → 54460 [ACK] Seq=1 Ack=1 Win=59 Len=1448
7	0.024318499	192.168.1.103	14.49.100.37	TCP	66	54460 → 80 [ACK] Seq=1 Ack=10137 Win=5048 Len=0 TSval=4191317126 TSecr
8	0.028218552	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=10137 Ack=1 Win=59 Len=1448 TSval=47463932 TSecr=
9	0.030721654	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=11585 Ack=1 Win=59 Len=1448 TSval=47463932 TSecr=
10	0.030747966	192.168.1.103	14.49.100.37	TCP	66	54460 → 80 [ACK] Seq=1 Ack=13033 Win=5093 Len=0 TSval=4191317133 TSecr
11	0.031281900	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=13033 Ack=1 Win=59 Len=1448 TSval=47463932 TSecr=
12	0.036805563	14.49.100.37	192.168.1.103	TCP	1514	80 → 54460 [ACK] Seq=14481 Ack=1 Win=59 Len=1448 TSval=47463933 TSecr=

▸ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Ethernet II, Src: Vmware_e3:bd:bb (00:0c:29:e3:bd:bb), Dst: BestItWo_4b:56:a0 (00:1e:a6:4b:56:a0)
▸ Internet Protocol Version 4, Src: 192.168.1.103, Dst: 14.49.100.37
▸ Transmission Control Protocol, Src Port: 54460, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

```
0000  00 1e a6 4b 56 a0 00 0c  29 e3 bd bb 08 00 45 00   ···KV··· )····E·
0010  00 40 ae b7 40 00 40 06  57 9b c0 a8 01 67 0e 31   ·@··@·@· W····g·1
0020  64 25 d4 bc 00 50 5d 5c  df cd 51 07 84 67 b0 10   d%···P]\ ··Q··g·
0030  13 e5 34 98 00 00 01 01  08 0a f9 d2 6c 6d 02 d4   ··4····· ····lm·
0040  3a 72 01 01 05 0a 51 07  0a 0f 51 07 20 af         :r····Q· ··Q··
```

Packet Sniffing:

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
15	1.499691000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB WPAD<00>
16	1.504609000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB WPAD<00>
17	1.504650000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB ISATAP<00>
18	1.506625000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB WPAD<00>
19	1.506799000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB WPAD<00>
20	1.520710000	192.168.0.100	192.168.0.255	NBNS	92	Name query NB WPAD<00>
21	1.539518000	fe80::64b3:bb08:7792:3b23	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation fo
22	2.676392000	fe80::64b3:bb08:7792:3b23	ff02::1:3	LLMNR	84	Standard query 0x8cbe A
23	2.676491000	192.168.0.100	224.0.0.252	LLMNR	64	Standard query 0x8cbe A
24	2.686343000	fe80::64b3:bb08:7792:3b23	ff02::1:3	LLMNR	84	Standard query 0xfb76 A
25	2.686441000	192.168.0.100	224.0.0.252	LLMNR	64	Standard query 0xfb76 A
26	2.701590000	fe80::64b3:bb08:7792:3b23	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation fo
27	2.703160000	fe80::64b3:bb08:7792:3b23	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation fo
28	2.723050000	fe80::64b3:bb08:7792:3b23	ff02::1:3	LLMNR	84	Standard query 0x001a A
29	2.723155000	192.168.0.100	224.0.0.252	LLMNR	64	Standard query 0x001a A
30	2.727440000	fe80::64b3:bb08:7792:3b23	ff02::1:3	LLMNR	84	Standard query 0x9fd6 A
31	2.727560000	192.168.0.100	224.0.0.252	LLMNR	64	Standard query 0x9fd6 A
32	2.736134000	fe80::64b3:bb08:7792:3b23	ff02::1:3	LLMNR	84	Standard query 0xcaa6 A

⊞ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_91:c3:5d (1c:c1:de:91:c3:5d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.255 (192.168.0.255)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
⊞ NetBIOS Name Service