

## Experiment No 9

**Aim:** Study of packet sniffer tool “wireshark”:

- a) Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode.
- b) Explore how the packets can be traced based on different filters.

**Requirements:** Compatible version of Wireshark.

### **Theory:**

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

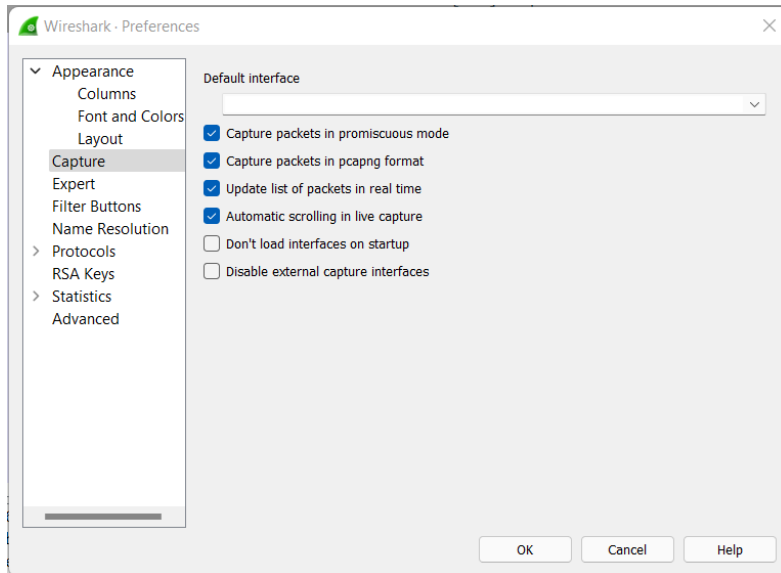
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

### **Intended purposes**

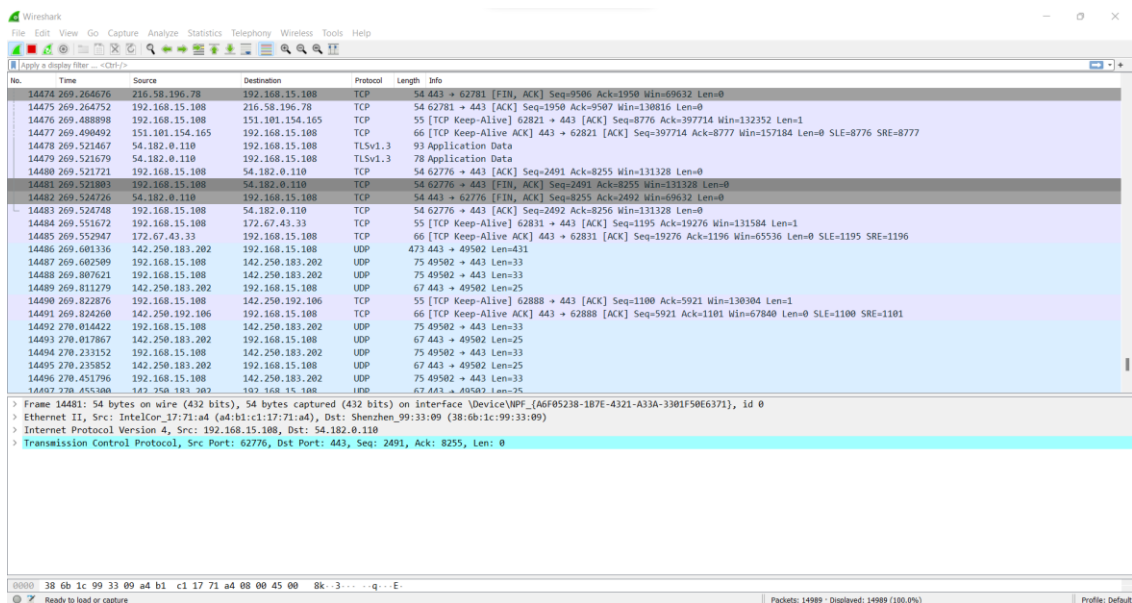
- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol internals*

## Output:

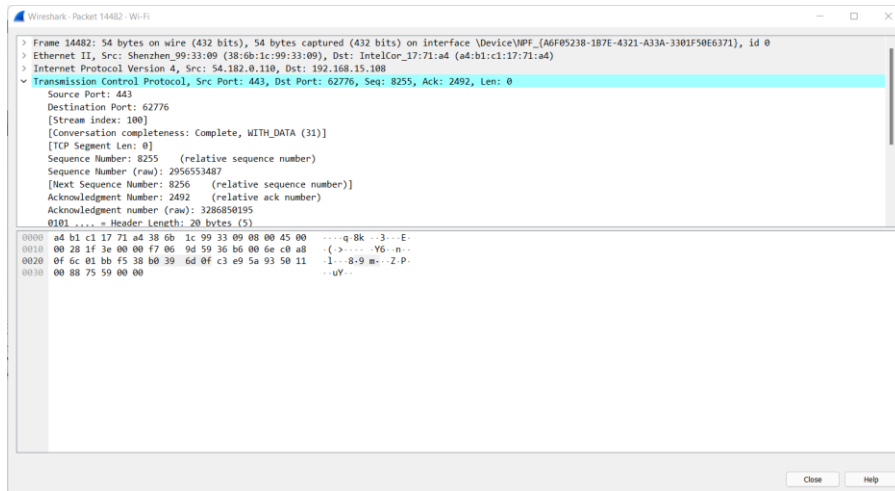
### Turning on promiscuous mode



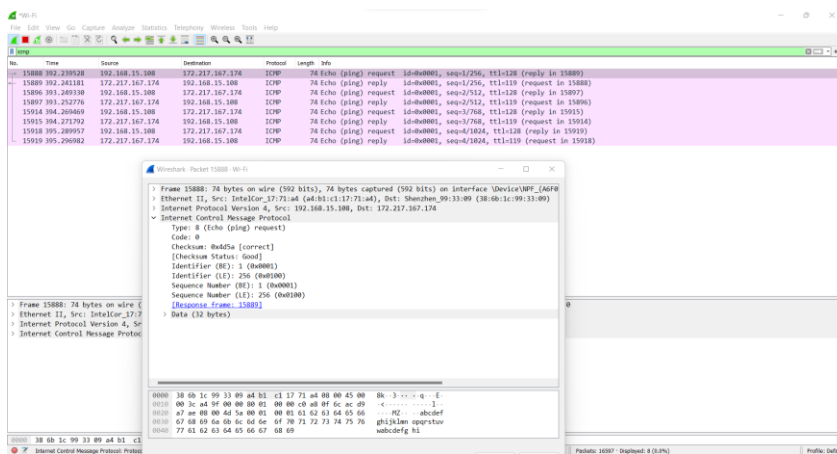
### Monitoring all packets routing through Wi-Fi



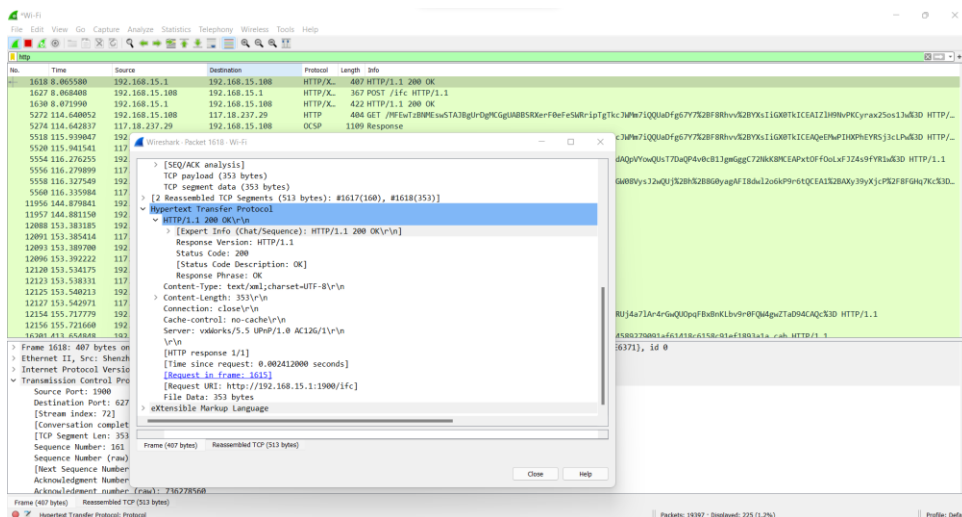
## TCP packet



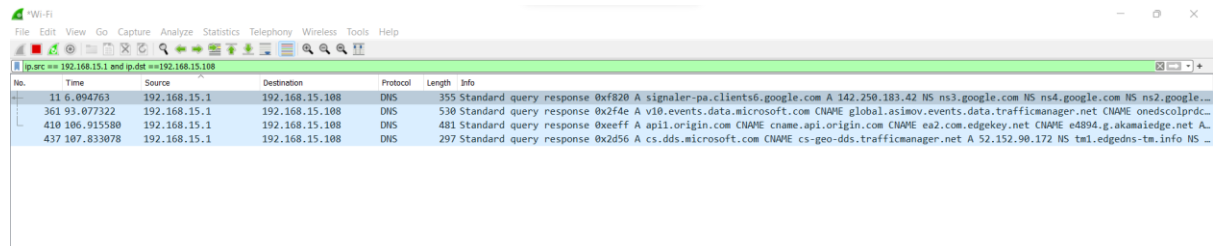
## Filter ICMP packet



HTTP packet



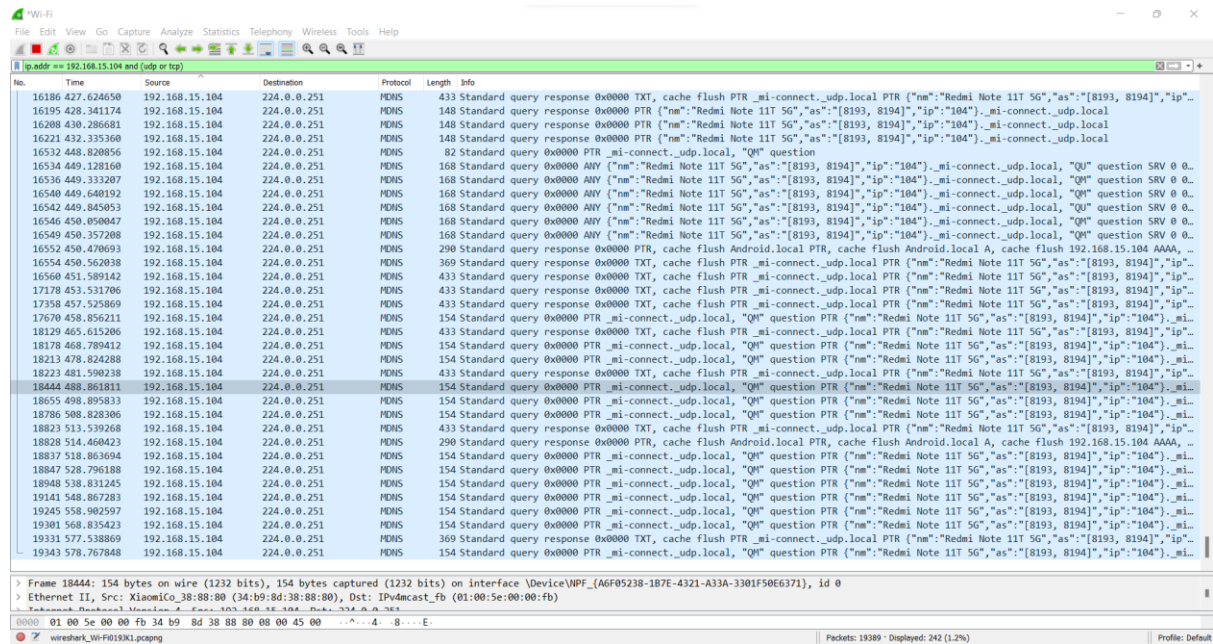
## Filter source and destination IP



Wi-Fi packet capture window showing a filter for source and destination IP. The filter is set to `ip.src == 192.168.15.1 and ip.dst == 192.168.15.108`. The packet list shows several DNS queries and responses between these two IP addresses.

No.	Time	Source	Destination	Protocol	Length	Info
11	6.094763	192.168.15.1	192.168.15.108	DNS	355	Standard query response 0x7820 A signaler-pa.clients6.google.com A 142.250.183.42 NS ns3.google.com NS ns4.google.com NS ns2.google...
361	93.077322	192.168.15.1	192.168.15.108	DNS	530	Standard query response 0x2f4e A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdc...
410	106.915580	192.168.15.1	192.168.15.108	DNS	481	Standard query response 0xe0ff A api1.origin.com CNAME cname.api.origin.com CNAME ea2.com.edgekey.net CNAME e4894.g.akamaiedge.net A...
437	107.833078	192.168.15.1	192.168.15.108	DNS	297	Standard query response 0x2d56 A cs.dds.microsoft.com CNAME cs-geo-dds.trafficmanager.net A 52.152.90.172 NS tml.edgedns-tm.info NS...

## Filter IP and protocols



Wi-Fi packet capture window showing a filter for IP and protocols. The filter is set to `ip.addr == 192.168.15.104 and (udp or tcp)`. The packet list shows a large number of DNS queries and responses between 192.168.15.104 and 224.0.0.251.

No.	Time	Source	Destination	Protocol	Length	Info
16186	427.624650	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
16195	428.341174	192.168.15.104	224.0.0.251	MDNS	148	Standard query response 0x0000 PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local
16200	430.206681	192.168.15.104	224.0.0.251	MDNS	148	Standard query response 0x0000 PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local
16221	432.235360	192.168.15.104	224.0.0.251	MDNS	148	Standard query response 0x0000 PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local
16532	448.820856	192.168.15.104	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question
16534	449.128160	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QU" question SRV 0 0...
16536	449.333207	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QM" question SRV 0 0...
16540	449.640192	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QM" question SRV 0 0...
16542	449.845053	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QU" question SRV 0 0...
16546	450.090847	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QM" question SRV 0 0...
16549	450.357208	192.168.15.104	224.0.0.251	MDNS	168	Standard query 0x0000 ANY ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi-connect._udp.local, "QM" question SRV 0 0...
16552	450.470693	192.168.15.104	224.0.0.251	MDNS	290	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 192.168.15.104 AAAA, ...
16554	450.562038	192.168.15.104	224.0.0.251	MDNS	369	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
16560	451.589142	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
17178	453.531706	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
17358	457.525869	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
17670	458.856211	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18120	465.615206	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
18178	468.789412	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18213	478.824288	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18223	481.590238	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
18444	488.861811	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18655	498.895833	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18786	508.828306	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18823	513.539268	192.168.15.104	224.0.0.251	MDNS	433	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
18828	514.460423	192.168.15.104	224.0.0.251	MDNS	290	Standard query response 0x0000 PTR, cache flush Android.local PTR, cache flush Android.local A, cache flush 192.168.15.104 AAAA, ...
18837	518.863694	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18847	528.796188	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
18948	538.831245	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
19141	548.867283	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
19245	558.902597	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
19301	568.835423	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...
19331	577.538869	192.168.15.104	224.0.0.251	MDNS	369	Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":...
19343	578.767848	192.168.15.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _mi-connect._udp.local, "QM" question PTR ("nm":"Redmi Note 11T 5G","as":["8193, 8194"],"ip":["104"]]._mi...

Frame 18444: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface \Device\NPF\_{AGF05238-1B7E-4321-A33A-3301F50E6371}, id 0  
> Ethernet II, Src: XiaomiCo\_38:88:80 (34:b9:8d:38:88:80), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
...  
0000 01 00 5e 00 00 fb 34 b9 8d 38 88 80 08 00 45 00 ...  
Packets: 19389 - Displayed: 242 (1.2%)