

Promiscuous Mode Acer

Settings

Applications ▾Places ▾

Mi 12:54 • 1.29 GHz 33% net 0 KB/s 0 KB/s 37°C fan 0 rpm de 68%

Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Mon. Mode	Capture Filter
<input checked="" type="checkbox"/>	wlp4s0 10.149.26.85 fe80::b091:ad41:342f:1985	Ethernet	enabled	262144	2	disabled	
<input type="checkbox"/>	any	Linux cooked	enabled	262144	2	n/a	
<input type="checkbox"/>	Loopback: lo 127.0.0.1 ::1	Ethernet	enabled	262144	2	n/a	
<input type="checkbox"/>	virbr0 192.168.122.1	Ethernet	enabled	262144	2	n/a	
<input type="checkbox"/>	enp0s31f6	Ethernet	enabled	262144	2	n/a	
<input type="checkbox"/>	bluetooth0	Bluetooth HCI UART transport layer plus pseudo-header	enabled	262144	2	n/a	
<input type="checkbox"/>	nftlog	Linux netfilter log messages	enabled	262144	2	n/a	
<input type="checkbox"/>	nftqueue	Raw IPv4	enabled	262144	2	n/a	
<input type="checkbox"/>	usbmon1	unknown	enabled	262144	2	n/a	
<input type="checkbox"/>	usbmon2	unknown	enabled	262144	2	n/a	
<input type="checkbox"/>	Cisco remote capture: cl...	Remote capture dependent DLT	enabled	262144	2	n/a	
<input type="checkbox"/>	Random packet generat...	Generator dependent DLT	enabled	262144	2	n/a	
<input type="checkbox"/>	SSH remote capture: ssh...	Remote capture dependent DLT	enabled	262144	2	n/a	
<input type="checkbox"/>	UDP Listener remote ca...	Exported PDUs	enabled	262144	2	n/a	

☐ Capture on all interfaces

☒ Use promiscuous mode on all interfaces

Capture Filter:

▼

Compile selected BPFs

Capture Files

File:

Browse...

☐ Use multiple files ☒ Use pcapng format

☒ Next file every

1

—

+

megabyte(s)

▼

☐ Next file every

1

—

+

minute(s)

▼

☐ Ring buffer with

2

—

+

Files

Stop Capture Automatically After...

☐

1

—

+

packet(s)

☐

1

—

+

megabyte(s)

▼

☐

1

—

+

file(s)

☐

1

—

+

minute(s)

▼

Display Options

☒ Update list of packets in real time

☒ Automatically scroll during live capture

☒ Hide capture info dialog

Name Resolution

☒ Resolve MAC addresses

☐ Resolve network-layer names

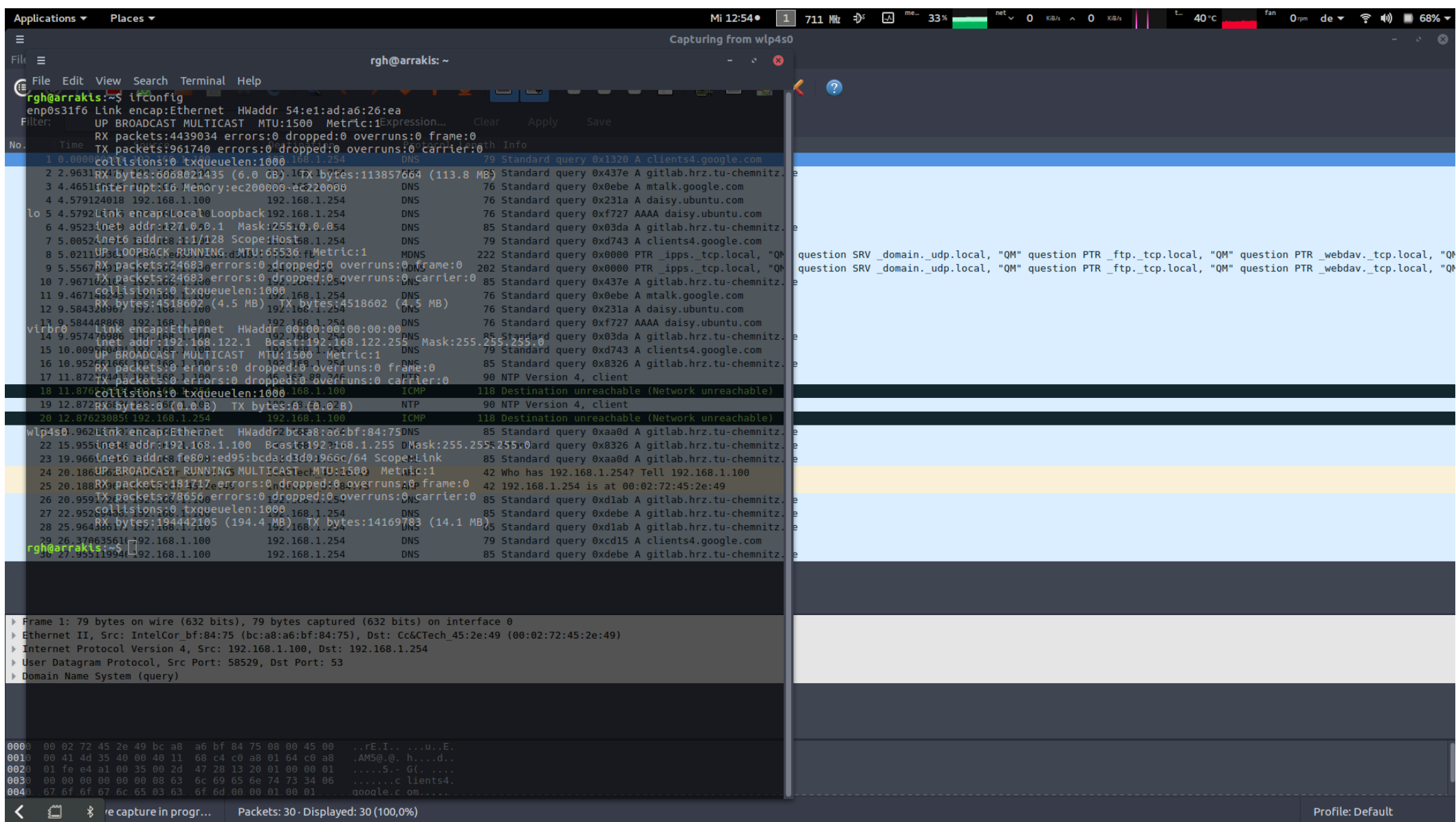
☐ Resolve transport-layer name

☒ Use external network name resolver

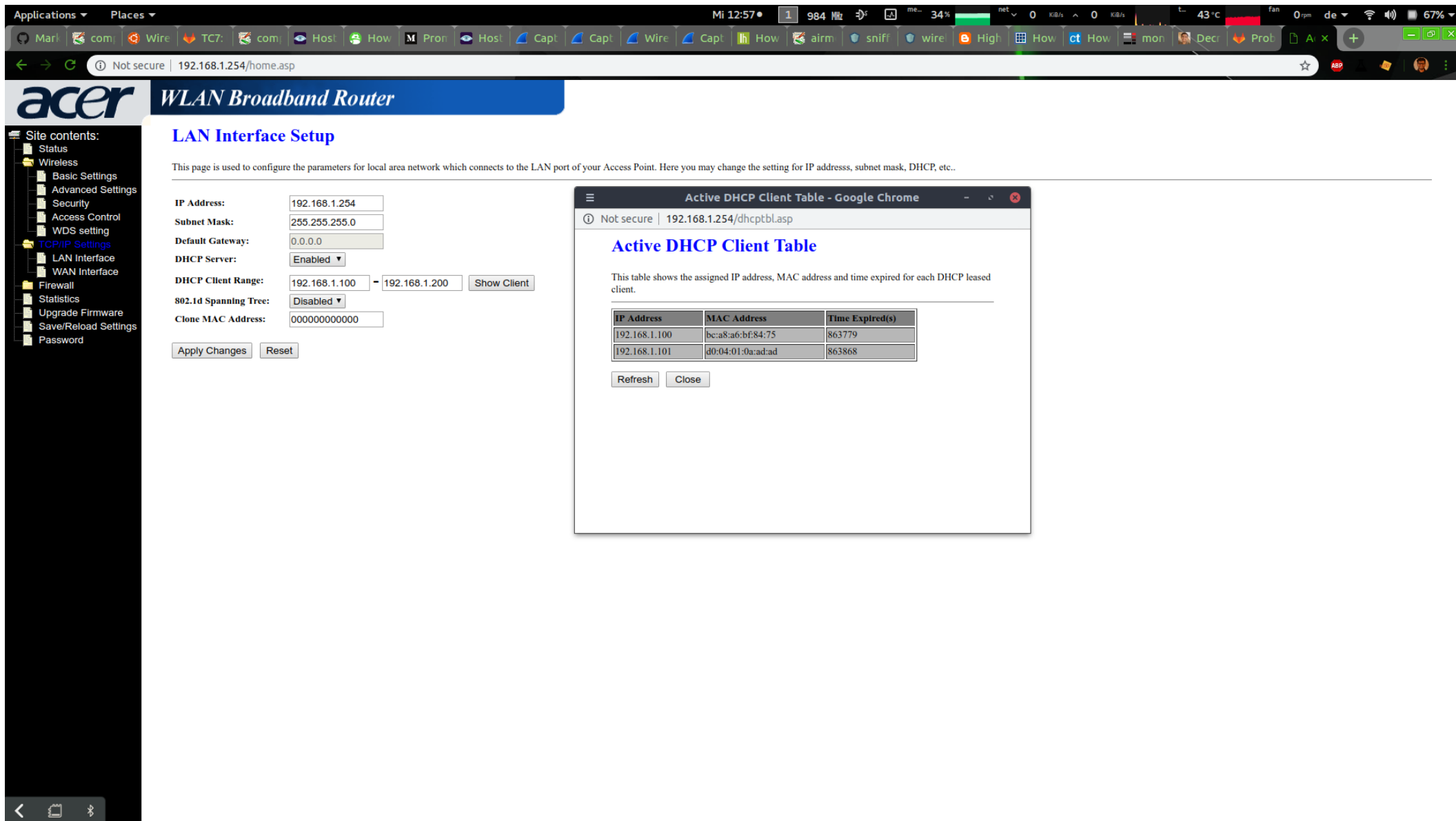
Start

Close

IP Address of computer.



IP Address of phone



Sniffing begins – mostly packets between router and computer.

Applications ▾ Places ▾ Mi 12:58 • 1 749 MHz 34% net 0 K/s 0 K/s 43°C fan 0 rpm de 67%

Capturing from wlp4s0

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
265	153.9154570	192.168.1.100	192.168.1.254	DNS	81	Standard query 0x9fdb A 1.ubuntu.pool.ntp.org
266	153.9155717	192.168.1.100	192.168.1.254	DNS	81	Standard query 0x0393 AAAA 1.ubuntu.pool.ntp.org
267	153.9756194	192.168.1.100	192.168.1.254	DNS	82	Standard query 0x9ce4 A habitlab.herokuapp.com
268	154.0855473	192.168.1.100	192.168.1.254	DNS	75	Standard query 0xc94f A www.gstatic.com
269	154.0856763	192.168.1.100	192.168.1.254	DNS	74	Standard query 0x3bd1 A www.google.com
270	154.0857683	192.168.1.100	192.168.1.254	DNS	76	Standard query 0x703c A kite.zerodha.com
271	154.9650708	192.168.1.100	192.168.1.254	DNS	82	Standard query 0x7632 A habitlab.herokuapp.com
272	156.0984685	192.168.1.100	192.168.1.254	DNS	74	Standard query 0xdd84 A www.google.com
273	156.3214274	192.168.1.100	192.168.1.254	TCP	74	45180 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2369238986 TSecr=0 WS=128
274	156.3214918	192.168.1.100	192.168.1.254	TCP	74	45182 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2369238986 TSecr=0 WS=128
275	156.3255472	192.168.1.254	192.168.1.100	TCP	74	80 → 45180 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=27870 TSecr=2369238986 WS=1
276	156.3255872	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2369238990 TSecr=27870
277	156.3258895	192.168.1.100	192.168.1.254	HTTP	467	GET / HTTP/1.1
278	156.3277084	192.168.1.254	192.168.1.100	TCP	74	80 → 45182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=27870 TSecr=2369238986 WS=1
279	156.3277429	192.168.1.100	192.168.1.254	TCP	66	45182 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2369238993 TSecr=27870
280	156.3289583	192.168.1.254	192.168.1.100	TCP	66	80 → 45180 [ACK] Seq=1 Ack=402 Win=5792 Len=0 TSval=27871 TSecr=2369238991
281	156.3458133	192.168.1.254	192.168.1.100	TCP	89	80 → 45180 [PSH, ACK] Seq=1 Ack=402 Win=5792 Len=23 TSval=27872 TSecr=2369238991 [TCP segment of a reassembled PDU]
282	156.3458424	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [ACK] Seq=402 Ack=24 Win=29312 Len=0 TSval=2369239011 TSecr=27872
283	156.3477741	192.168.1.254	192.168.1.100	TCP	88	80 → 45180 [PSH, ACK] Seq=24 Ack=402 Win=5792 Len=22 TSval=27873 TSecr=2369239011 [TCP segment of a reassembled PDU]
284	156.3478009	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [ACK] Seq=402 Ack=46 Win=29312 Len=0 TSval=2369239013 TSecr=27873
285	156.3500701	192.168.1.254	192.168.1.100	TCP	141	80 → 45180 [PSH, ACK] Seq=46 Ack=402 Win=5792 Len=75 TSval=27873 TSecr=2369239013 [TCP segment of a reassembled PDU]
286	156.3500836	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [ACK] Seq=402 Ack=121 Win=29312 Len=0 TSval=2369239015 TSecr=27873
287	156.3523772	192.168.1.100	192.168.1.254	TCP	134	80 → 45180 [PSH, ACK] Seq=121 Ack=402 Win=5792 Len=68 TSval=27873 TSecr=2369239015 [TCP segment of a reassembled PDU]
288	156.3523921	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [ACK] Seq=402 Ack=189 Win=29312 Len=0 TSval=2369239017 TSecr=27873
289	156.3537967	192.168.1.254	192.168.1.100	HTTP	264	HTTP/1.0 302 Redirect (text/html)
290	156.3546774	192.168.1.100	192.168.1.254	TCP	66	45180 → 80 [RST, ACK] Seq=402 Ack=388 Win=30336 Len=0 TSval=2369239020 TSecr=27873
291	156.3599606	192.168.1.100	192.168.1.254	HTTP	475	GET /home.asp HTTP/1.1
292	156.3622386	192.168.1.100	192.168.1.254	TCP	66	80 → 45182 [ACK] Seq=1 Ack=410 Win=5792 Len=0 TSval=27874 TSecr=2369239025
293	156.3762528	192.168.1.254	192.168.1.100	TCP	115	80 → 45182 [PSH, ACK] Seq=1 Ack=410 Win=5792 Len=49 TSval=27875 TSecr=2369239025 [TCP segment of a reassembled PDU]
294	156.3762790	192.168.1.100	192.168.1.254	TCP	66	45182 → 80 [ACK] Seq=410 Ack=50 Win=29312 Len=0 TSval=2369239041 TSecr=27875
295	156.3804356	192.168.1.254	192.168.1.100	TCP	1039	80 → 45182 [PSH, ACK] Seq=50 Ack=410 Win=5792 Len=973 TSval=27876 TSecr=2369239041 [TCP segment of a reassembled PDU]
296	156.3804621	192.168.1.100	192.168.1.254	TCP	66	45182 → 80 [ACK] Seq=410 Ack=1023 Win=31232 Len=0 TSval=2369239045 TSecr=27876
297	156.3804726	192.168.1.254	192.168.1.100	HTTP	66	HTTP/1.0 200 OK (text/html)

Frame 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0

Ethernet II, Src: IntelCor_bf:84:75 (bc:a8:a6:bf:84:75), Dst: Cc&CTech_45:2e:49 (00:02:72:45:2e:49)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.254

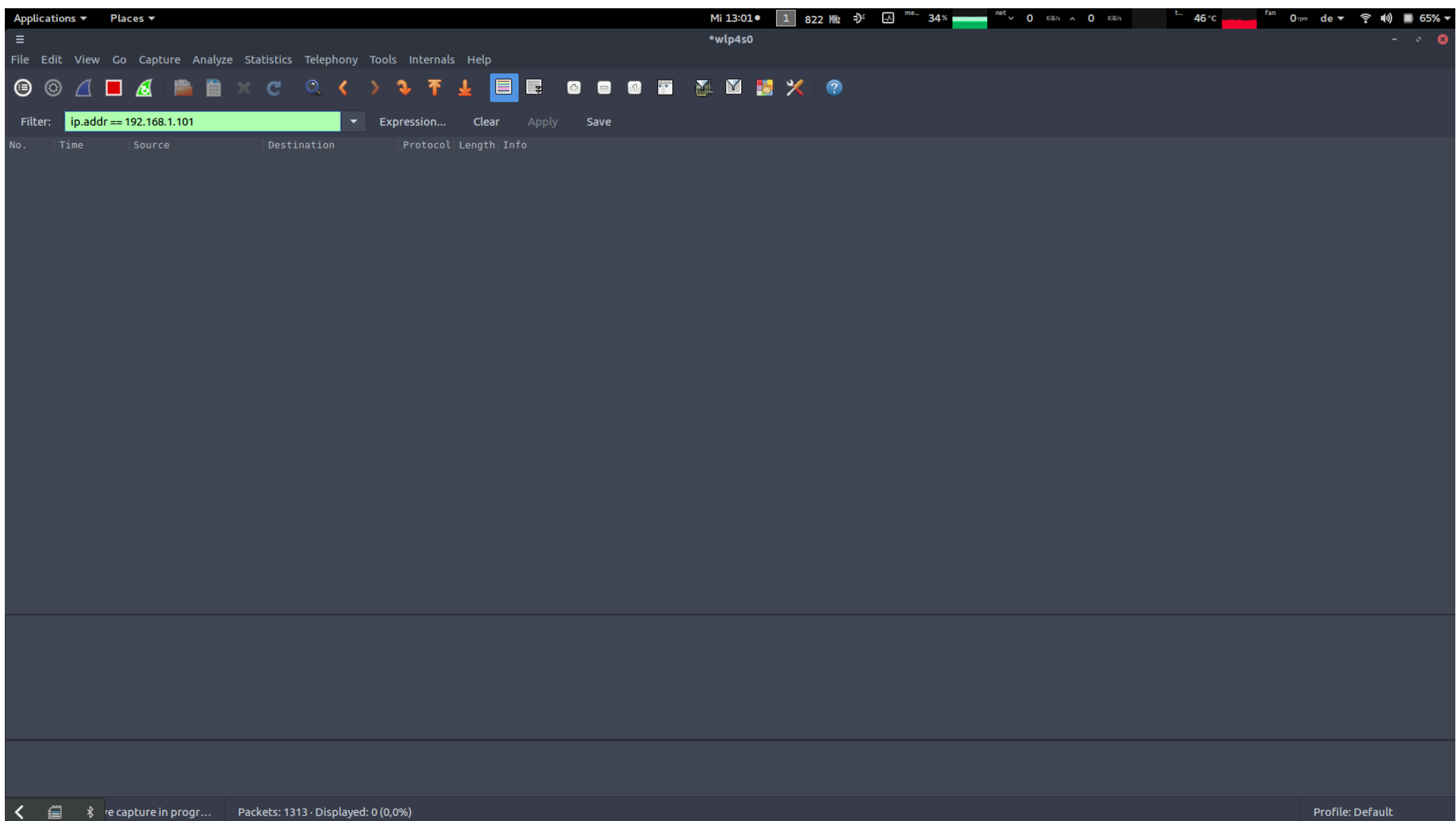
User Datagram Protocol, Src Port: 58529, Dst Port: 53

Domain Name System (query)

0000 00 02 72 45 2e 49 bc a8 a6 bf 84 75 08 00 45 00 ...rE.I...u..E.
0010 00 41 4d 35 40 00 00 11 68 c4 c0 a8 01 64 c0 a8 ..AMS@.@.h...d..
0020 01 fe e4 a1 00 35 00 2d 47 28 13 20 01 00 00 015.-G(.
0030 00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 34 06c lients4.
0040 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 ...oogle.c om....

⏪ 📄 📶 e capture in progr... Packets: 988 · Displayed: 988 (100,0%) Profile: Default

The source address is not shown properly for the phone



Not sure why only that ARP packet is visible via the promiscuous mode sniffing.

Applications

Places

Mi 13:41

700 MHz

me...

34%

net 0

KiB/s

3 KiB/s

34°C

fan 65...

de

59%

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter:

Expression...

Clear

Apply

Save

No.	Time	Source	Destination	Protocol	Length	Info
1228	364.25281286	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	192.168.1.254 is at 00:02:72:45:2e:49
1275	398.04477664	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	192.168.1.254 is at 00:02:72:45:2e:49
1310	425.69264978	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	192.168.1.254 is at 00:02:72:45:2e:49
1330	433.89013124	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	Who has 192.168.1.100? Tell 192.168.1.254
1369	454.38386234	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	192.168.1.254 is at 00:02:72:45:2e:49
1397	483.29380478	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	42	192.168.1.254 is at 00:02:72:45:2e:49
24	20.186836264	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
49	45.018861124	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
65	50.911291324	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
106	68.058874624	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
177	99.960579064	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
178	100.05886774	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
217	134.10683384	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
252	147.88482348	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
975	229.08285488	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
999	235.94970196	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
1053	264.15487096	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1097	286.94494128	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
1125	297.94692608	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1186	330.71489196	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1215	355.96312408	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
1227	364.25089748	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1274	398.04299996	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1309	425.69085608	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1331	433.89015268	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	192.168.1.100 is at bc:a8:a6:bf:84:75
1368	454.36295096	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
1396	483.29087788	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	42	Who has 192.168.1.254? Tell 192.168.1.100
96	64.317612636	Motorola_0a:ad:ad	Broadcast	ARP	42	Who has 192.168.1.254? Tell 192.168.1.101
8	5.021193301	fe80::ed95:bcda:d3d0::ff02::fb		MDNS	222	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question SRV _domain._udp.local, "QM" question PTR _ftp._tcp.local, "QM" question PTR _webdav._tcp.local, "QM" question PTR _http._tcp.local, "QM" question PTR _https._tcp.local, "QM" question PTR _ldap._tcp.local, "QM" question PTR _nntp._tcp.local, "QM" question PTR _rtsp._tcp.local, "QM" question PTR _sip._tcp.local, "QM" question PTR _smtp._tcp.local, "QM" question PTR _ssh._tcp.local, "QM" question PTR _telnet._tcp.local, "QM" question PTR _xmpp._tcp.local, "QM" question PTR _irc._tcp.local, "QM" question PTR _irc6._tcp.local, "QM" question PTR _irc7._tcp.local, "QM" question PTR _irc8._tcp.local, "QM" question PTR _irc9._tcp.local, "QM" question PTR _irc10._tcp.local, "QM" question PTR _irc11._tcp.local, "QM" question PTR _irc12._tcp.local, "QM" question PTR _irc13._tcp.local, "QM" question PTR _irc14._tcp.local, "QM" question PTR _irc15._tcp.local, "QM" question PTR _irc16._tcp.local, "QM" question PTR _irc17._tcp.local, "QM" question PTR _irc18._tcp.local, "QM" question PTR _irc19._tcp.local, "QM" question PTR _irc20._tcp.local, "QM" question PTR _irc21._tcp.local, "QM" question PTR _irc22._tcp.local, "QM" question PTR _irc23._tcp.local, "QM" question PTR _irc24._tcp.local, "QM" question PTR _irc25._tcp.local, "QM" question PTR _irc26._tcp.local, "QM" question PTR _irc27._tcp.local, "QM" question PTR _irc28._tcp.local, "QM" question PTR _irc29._tcp.local, "QM" question PTR _irc30._tcp.local, "QM" question PTR _irc31._tcp.local, "QM" question PTR _irc32._tcp.local, "QM" question PTR _irc33._tcp.local, "QM" question PTR _irc34._tcp.local, "QM" question PTR _irc35._tcp.local, "QM" question PTR _irc36._tcp.local, "QM" question PTR _irc37._tcp.local, "QM" question PTR _irc38._tcp.local, "QM" question PTR _irc39._tcp.local, "QM" question PTR _irc40._tcp.local, "QM" question PTR _irc41

Conclusion.

- I expected to see the same volume of message flow from the router to the phone as I saw between router and computer.
- But that didn't happen. I am not sure if this is because one device was a Linux based computer and the other an Android based phone.
- The same experiment I repeated with the “simple network” below:

ThinkPad 1	AP (Acer router)
ThinkPad 2 (Attacker)	ThinkPad 3

- Note that all the ThinkPads are on the same network which is created by the AP and I use Wireshark on ThinkPad 2 in promiscuous mode to track messages between ThinkPad 1 and ThinkPad 3. In this case also, I could not see the messages.

Monitoring mode Acer.

Setting up monitor mode for wireless adapter on the computer.

Applications ▾ Places ▾

root@arrakis: ~

File Edit View Search Terminal Help

Interface	Chipset	Driver
wlp4s0	Intel 4965/5xxx/6xxx/1xxx	

root@arrakis:~# airmon-ng check

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID	Name
986	avahi-daemon
1001	avahi-daemon
1096	NetworkManager
1637	wpa_supplicant
24416	dhclient

Process with PID 24416 (dhclient) is running on interface wlp4s0
root@arrakis:~# airmon-ng check kill

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID	Name
986	avahi-daemon
1001	avahi-daemon
1096	NetworkManager
1637	wpa_supplicant
24416	dhclient

Process with PID 24416 (dhclient) is running on interface wlp4s0
Killing all those processes...
root@arrakis:~# airmon-ng check

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID	Name
28016	avahi-daemon
28017	avahi-daemon

root@arrakis:~# airmon-ng check kill

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID	Name
28016	avahi-daemon
28017	avahi-daemon

root@arrakis:~#

Usage

usage: airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>

Where:

- <start|stop> indicates if you wish to start or stop the interface. (Mandatory)
- <interface> specifies the interface. (Mandatory)
- [channel] optionally set the card to a specific channel.
- <check|check kill> "check" will show any processes that might interfere with the aircrack-ng suite. It is strongly recommended that these processes be eliminated prior to using the aircrack-ng suite. "check kill" will check and kill off processes that might interfere with the aircrack-ng suite. For "check kill" see

Usage Examples

Typical Uses

Check status and/or listing wireless interfaces

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Atheros Communications, Inc. AR9271 802.11n

Checking for interfering processes

When putting a card into monitor mode, it will automatically check for interfering processes. It can also be done manually by running the following command:

```
~# airmon-ng check
```

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a short period of time, you may want to kill (some of) them!

PID	Name
718	NetworkManager
870	dhclient
1104	avahi-daemon
1105	avahi-daemon
1113	wpa_supplicant

Killing interfering processes

This command stops network managers then kill interfering processes left:

```
~# airmon-ng check kill
```

Killing these processes:

- Confirming the Card is in Monitor Mode
- Determining the Current Channel
- BSSIDs with Spaces, Special Characters
- How Do I Put My Card Back into Managed Mode?
- Usage Troubleshooting
 - General
 - Airmon-ng says the interface is not in monitor mode
 - My interface was put in monitor mode but tools says it is not
 - Interface athX number rising (ath0, ath1, ath2.... ath45...)
 - Interface ath1 created instead of ath0
 - Why do I get ioctl(SIOCGIFINDEX) failed?
 - Error message: "wlanconfig: command not found"
 - airmon-ng shows RT2500 instead of RT73
 - Error "add_iface: Permission denied"
 - check kill fails
 - SIOCSIFFLAGS: Unknown error 132

Mon0 is the monitor mode adapter.

```
Applications ▾ Places ▾ Mi 14:09 • 1 781 MB 38% net 0 KB/s 0 KB/s thermal 41°C fan 0 rpm de 50% ▾
root@arrakis: ~
File Edit View Search Terminal Help
root@arrakis:~# airmon-ng start wlan0
Interface Chipset Driver
wlan0 Intel 4965/5xxx/1xxx iwlwifi - [phy0]
(monitored mode enabled on wlan0)

root@arrakis:~# ifconfig
enp0s31f6 Link encap:Ethernet HWaddr 54:e1:ad:a6:26:8a
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:4439034 errors:0 dropped:0 overruns:0 frame:0
TX packets:961740 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6068021435 (6.0 GB) TX bytes:113857664 (113.8 MB)
Interrupt:16 Memory:ec200000-ec220000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:30720 errors:0 dropped:0 overruns:0 frame:0
TX packets:30720 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5007643 (5.0 MB) TX bytes:5007643 (5.0 MB)

mon0 Link encap:UNSPEC HWaddr BC-A8-A6-BF-84-75-3A-30-00-00-00-00-00-00-00-00
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

virbr0 Link encap:Ethernet HWaddr 00:00:00:00:00:00
inet addr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

wlan0 Link encap:Ethernet HWaddr bc:a8:a6:bf:84:75
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:182257 errors:0 dropped:0 overruns:0 frame:0
TX packets:83418 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:194570865 (194.5 MB) TX bytes:14660632 (14.6 MB)

root@arrakis:~#

# airmon-ng start wlan0
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
718 NetworkManager
670 dhclient
1104 avahi-daemon
1105 avahi-daemon
1106 avahi-daemon

# iwconfig
phy0 wlan0 ath9k_htc Atheros Communications, Inc. AR9271 802.11n
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

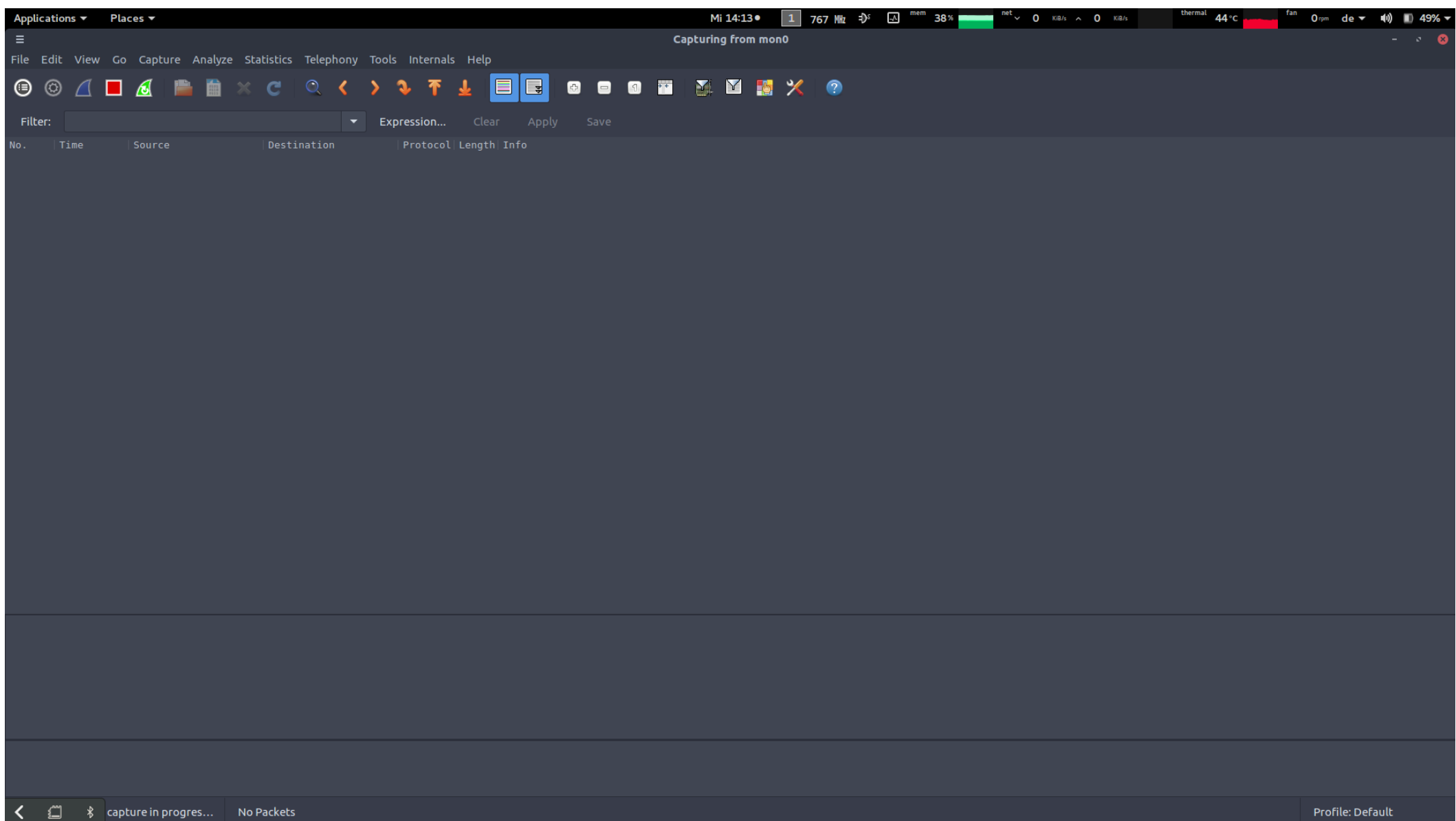
# iwconfig
lo no wireless extensions.

eth0 no wireless extensions.

wlan0 no wireless extensions.

ath0 IEEE 802.11b ESSID:"" Nickname:""
Mode:Managed Channel:0 Access Point: Not-Associated
Bit Rate:0 kb/s Tx-Power:0 dBm Sensitivity=0/3
```

When all the steps from the aironet guide are followed (which includes switching off the network-manager) there is no data captured.



But if I am also connected to the Acer router, then I can see following data but this kind of defeats the purpose of monitoring mode. More importantly, even in this case I cannot actually see the data which is sent from router to phone.

Applications ▾ Places ▾ Mi 14:17 • 1 693 MHz 38% net 0 K/s 0 K/s 49°C fan 0 rpm de 48%

*mon0

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
316	65.308600256	192.168.1.100	192.168.1.254	DNS	118	Standard query 0x2a23 A safebrowsing.googleapis.com
317	67.296110418	192.168.1.100	192.168.1.254	DNS	118	Standard query 0x018c A safebrowsing.googleapis.com
318	68.081777676	Cisco_6c:88:70	IntelCor_bf:84:75	802.11	309	Probe Response, SN=2567, FN=0, Flags=...R..., BI=102, SSID=eduroam
319	68.081816371	Cisco_6c:88:74	IntelCor_bf:84:75	802.11	314	Probe Response, SN=2568, FN=0, Flags=...R..., BI=102, SSID=tuc-special
320	68.081829291	Cisco_6c:88:71	IntelCor_bf:84:75	802.11	305	Probe Response, SN=2569, FN=0, Flags=...R..., BI=102, SSID=lab
321	68.081843631	Cisco_6c:88:73	IntelCor_bf:84:75	802.11	290	Probe Response, SN=2570, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
322	68.097769736	192.168.1.100	192.168.1.254	DNS	116	Standard query 0xb095 A gitlab.hrz.tu-chemnitz.de
323	68.319132081	Cisco_7c:db:d2	Broadcast	802.11	305	Beacon frame, SN=1237, FN=0, Flags=..., BI=102, SSID=\000
324	68.329797081	Cisco_6c:9a:20	IntelCor_bf:84:75	802.11	309	Probe Response, SN=3812, FN=0, Flags=...R..., BI=102, SSID=eduroam
325	68.329887561	Cisco_6c:9a:24	IntelCor_bf:84:75	802.11	314	Probe Response, SN=3813, FN=0, Flags=...R..., BI=102, SSID=tuc-special
326	68.329909436	Cisco_6c:9a:24	IntelCor_bf:84:75	802.11	314	Probe Response, SN=3813, FN=0, Flags=...R..., BI=102, SSID=tuc-special
327	68.329928501	Cisco_6c:9a:21	IntelCor_bf:84:75	802.11	305	Probe Response, SN=3814, FN=0, Flags=...R..., BI=102, SSID=lab
328	68.329949761	Cisco_7c:db:d4	IntelCor_bf:84:75	802.11	314	Probe Response, SN=1595, FN=0, Flags=...R..., BI=102, SSID=tuc-special
329	68.329985831	Cisco_6c:9a:23	IntelCor_bf:84:75	802.11	290	Probe Response, SN=3815, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
330	68.330044821	Cisco_7c:db:d1	IntelCor_bf:84:75	802.11	305	Probe Response, SN=1596, FN=0, Flags=...R..., BI=102, SSID=lab
331	68.330125191	Cisco_7c:db:d3	IntelCor_bf:84:75	802.11	290	Probe Response, SN=1597, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
332	68.335046301	Cisco_6c:9a:21	Broadcast	802.11	311	Beacon frame, SN=2298, FN=0, Flags=..., BI=102, SSID=lab
333	68.343657201	Cisco_7c:db:d1	Broadcast	802.11	311	Beacon frame, SN=1238, FN=0, Flags=..., BI=102, SSID=lab
334	68.610881361	Cc&Tech_45:2e:49	IntelCor_bf:84:75	802.11	105	Probe Response, SN=2430, FN=0, Flags=..., BI=100, SSID=Acer
335	68.614954521	Cisco_44:49:a4	IntelCor_bf:84:75	802.11	314	Probe Response, SN=3291, FN=0, Flags=...R..., BI=102, SSID=tuc-special
336	68.614995631	Cisco_7c:bd:01	IntelCor_bf:84:75	802.11	305	Probe Response, SN=1238, FN=0, Flags=...R..., BI=102, SSID=lab
337	68.615026621	Cisco_7c:bd:03	IntelCor_bf:84:75	802.11	290	Probe Response, SN=1239, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
338	68.615060191	Cisco_7c:bd:03	IntelCor_bf:84:75	802.11	290	Probe Response, SN=1239, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
339	68.633160581	Cc&Tech_45:2e:49	Broadcast	802.11	145	Beacon frame, SN=2431, FN=0, Flags=..., BI=100, SSID=Acer
340	68.696323541	192.168.1.100	192.168.1.254	DNS	120	Standard query 0x71d4 A clientservices.googleapis.com
341	69.516031951	Cisco_6c:88:7f	IntelCor_bf:84:75	802.11	308	Probe Response, SN=2714, FN=0, Flags=...R..., BI=102, SSID=eduroam
342	69.516068451	Cisco_6c:88:7b	IntelCor_bf:84:75	802.11	313	Probe Response, SN=2715, FN=0, Flags=...R..., BI=102, SSID=tuc-special
343	69.516089321	Cisco_6c:88:7e	IntelCor_bf:84:75	802.11	304	Probe Response, SN=2716, FN=0, Flags=...R..., BI=102, SSID=lab
344	69.516113161	Cisco_6c:88:7c	IntelCor_bf:84:75	802.11	289	Probe Response, SN=2717, FN=0, Flags=...R..., BI=102, SSID=tu-chemnitz.de
345	69.775714771	192.168.1.100	192.168.1.254	DNS	120	Standard query 0x614a A clientservices.googleapis.com
346	70.235297411	192.168.1.100	192.168.1.254	DNS	105	Standard query 0x8151 A ntp.ubuntu.com
347	70.235858751	192.168.1.100	192.168.1.254	DNS	105	Standard query 0x7771 AAAA ntp.ubuntu.com
348	70.240378191	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xa5d2 A clients1.google.com

▶ Frame 400: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0

▶ Radiotap Header v0, Length 13

▶ 802.11 radio information

▶ IEEE 802.11 Data, Flags:T

▶ Logical-Link Control

▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.254

▶ User Datagram Protocol, Src Port: 40964, Dst Port: 53

▶ Domain Name System (query)

```
0000 00 00 0d 00 04 80 02 00 16 00 00 00 08 01 00 .....
0010 00 00 02 72 45 2e 49 bc a8 a6 bf 84 75 00 02 72 ...rE.I. ....u..r
0020 45 2e 49 00 4f aa aa 03 00 00 00 08 00 45 00 00 E.I.O. ....E..
0030 4b e7 d5 40 00 40 11 ce 19 c0 a8 01 64 c0 a8 01 K..@.. ....d...
0040 fe a0 04 00 35 00 37 19 ca 35 de 01 00 00 01 00 ...5...5..
```

< /wireshark_mon0... Packets: 417 · Displayed: 417 (100,0%) · Dropped: 0 (0,0%) Profile: Default

In my view the settings are correct...

Applications ▾ Places ▾ Mi 14:20 • 1 796 MHz 38% net 0 K/s 0 K/s 47°C fan 0 rpm de 46%

*mon0

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
374	74.12180157	192.168.1.254	192.168.1.100	ICMP	190	Destination unreachable (Network unreachable)
375	74.70195614	192.168.1.100	192.168.1.254	DNS	120	Standard query 0x614a A clientservices.googleapis.com
376	75.11915679	192.168.1.100	176.9.102.215	NTP	121	NTP Version 4, client
377	75.14432443	192.168.1.100	192.168.1.254	DNS	105	Standard query 0x8151 A ntp.ubuntu.com
378	75.14815315	192.168.1.100	192.168.1.254	DNS	105	Standard query 0x7771 AAAA ntp.ubuntu.com
379	75.24079031	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xa5d2 A clients1.google.com
380	76.12246520	192.168.1.100	131.188.3.221	NTP	121	NTP Version 4, client
381	76.13148730	192.168.1.254	192.168.1.100	ICMP	190	Destination unreachable (Network unreachable)
382	76.24210695	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xc9bd A clients1.google.com
383	76.69369472	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xff28 A clientservices.googleapis.com
384	77.30337922	192.168.1.100	192.168.1.254	DNS	118	Standard query 0x153d A safebrowsing.googleapis.com
385	78.16479692	Cc&CTech_45:2e:49	IntelCor_bf:84:75	ARP	114	Who has 192.168.1.100? Tell 192.168.1.254
386	78.16557380	IntelCor_bf:84:75	Cc&CTech_45:2e:49	ARP	114	Who has 192.168.1.100? Tell 192.168.1.254
387	78.70203459	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
388	79.70021415	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xff28 A clientservices.googleapis.com
389	80.14958879	192.168.1.100	192.168.1.254	DNS	118	Standard query 0x153d A safebrowsing.googleapis.com
390	80.15009660	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xc9bd A clients1.google.com
391	80.24520461	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xff28 A clientservices.googleapis.com
392	81.24602329	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xc9bd A clients1.google.com
393	81.69787070	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
394	83.70470778	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xff28 A clientservices.googleapis.com
395	84.70185628	192.168.1.100	192.168.1.254	DNS	110	Standard query 0xc9bd A clients1.google.com
396	85.15412852	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
397	85.15504007	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
398	85.24937118	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
399	86.24995379	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
400	86.70297252	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
401	88.24234929	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
402	88.70502094	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
403	89.70358873	192.168.1.100	192.168.1.254	DNS	120	Standard query 0xc9bd A clients1.google.com
404	90.15739135	192.168.1.100	192.168.1.254	DNS	112	Standard query 0xc8a A 2.ubuntu.pool.ntp.org
405	90.15796491	192.168.1.100	192.168.1.254	DNS	112	Standard query 0xc8a A 2.ubuntu.pool.ntp.org
406	91.2	192.168.1.100	192.168.1.254	DNS	112	Standard query 0xc8a A 2.ubuntu.pool.ntp.org

Edit Interface Settings

Capture

Interface: mon1

IP address: none

Link-layer header type: 802.11 plus radiotap header Buffer size: 2 mebibyte(s)

☒ Capture packets in promiscuous mode

☒ Capture packets in monitor mode

☐ Limit each packet to 262144 bytes

Capture Filter: Compile BPF

Help Cancel OK

Wireshark: Capture Options

Capture	Interface	Link-layer header	Prom. Mode	Snappn [B]	Buffer [MiB]	Mon. Mode	Capture Filter
<input type="checkbox"/>	wlp4s0 192.168.1.100 fe80::ed95:bcd:d3d0:966c	Ethernet	enabled	262144	2	disabled	
<input checked="" type="checkbox"/>	mon1	802.11 plus radiotap header	enabled	262144	2	disabled	

☐ Capture on all interfaces

☒ Use promiscuous mode on all interfaces

Capture Filter: Compile selected BPFs

Manage Interfaces

Display Options Profile: Default

Conclusion.

I think the thinkpad computer is capable of wireless monitoring mode – because I read in aircrack-ng user guide that otherwise I would have seen errors in the airmmon-ng steps. I didn't see them.

- I went through quite a few “tutorials” and “walkthroughs” for monitor mode packet capture using Wireshark and no one actually mentions whether the network-manager should be on or off.
- The airmmon-ng guide says that it should be off but that is not aircrack-ng toolset. Not sure how that mixes with Wireshark.
- For now I feel that if I am connected to the same network which I am trying to “monitor”, then it doesn't really mean I am “monitoring”. Defeats the definition.
- Also, Wireshark actually offers an automatic “monitor mode”. When using this mode, after trying several times, I could not actually see any data between the phone and the router. I expected to see at least DNS protocol packets and some TCP packets when connection is made.

Overall Conclusion

- This is very similar to what I observed earlier with the GoPros.
- Not able to see data communication between other devices (in this case, the phone and in GoPro's case, the communication between Smart Remote and GoPros) in Promiscuous mode.
- Monitor mode doesn't produce any results when I am not connected to the network using Wireshark. Even if I am – and I believe this is the intended way of using it, it doesn't actually show any useful data.
- The experiment was also repeated using the “simple network” as follows:

- | |
|-----------------------------------|
| ThinkPad 1 (connected to Acer AP) |
|-----------------------------------|

Acer AP

- | |
|---------------------------------------|
| ThinkPad 2 (not connected to Acer AP) |
|---------------------------------------|

ThinkPad 3 (connected to Acer AP)

- Results were exactly same in this network as well.