```
tcpdump -w output.pcap -i en0
```

interface

```
tcpdump -w output.pcap -s 0 -i en0
```

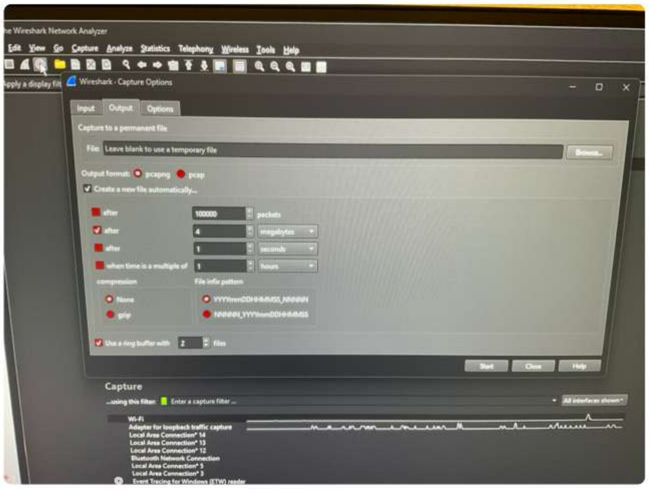
to capture the entire packet

☆ Press the File icon to access files that were saved from above.

Using Ring Buffers on Capturing:

- to have wireshark create files automatically

Step1: Select from where
Step2: Press on setting icon
Step3: Press "output"
Step4: Click the check box next to "Create a new file automatically"
Step5: Do the settings you want
Step6: click the check box next to "use a ring buffer with"
Step7: select the # of files



he Wireshark Network Analyzer
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filt
Wireshark - Capture Options
Input
Output
Options
Browse...
Start
Close
Help
Capture
All interfaces shown
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 14
Local Area Connection* 13
Local Area Connection* 12
Bluetooth Network Connection
Local Area Connection* 5
Local Area Connection* 3
Event Tracing for Windows (ETW) reader

Capture to a permanent file

File: Leave blank to use a temporary file

Output format: ● pcapng ○ pcap

☑ Create a new file automatically...

☐ after 100000 packets
☑ after 4 megabytes
☐ after 1 seconds
☐ when time is a multiple of 1 hours

compression: ● None ○ gzip

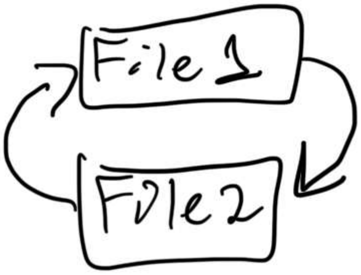
File infix pattern: ● YYYYmmDDHHMMSS_NNNNN ○ NNNNN_YYYYmmDDHHMMSS

☑ Use a ring buffer with 2 files

...using this filter: Enter a capture filter ...

What step 7 is doing is setting the amount of files that will be looped through.

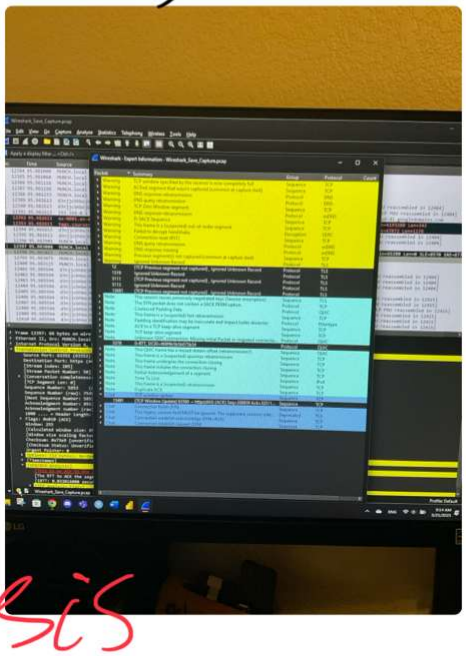
the 4 megabytes go to File 1, then 4mb go to File 2, 4mb are added to File 1, 4mb is added to File 2, ...



Analysis:

On the bottom left there is a circle with a color press it.

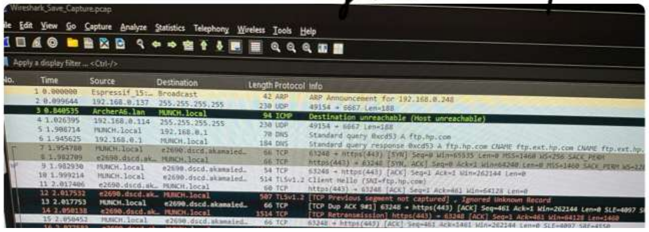
- ● serious problem
- ● warning
- ● Note
- ● chat


Wireshark · Expert Information · Wireshark_Save_Capture.pcap

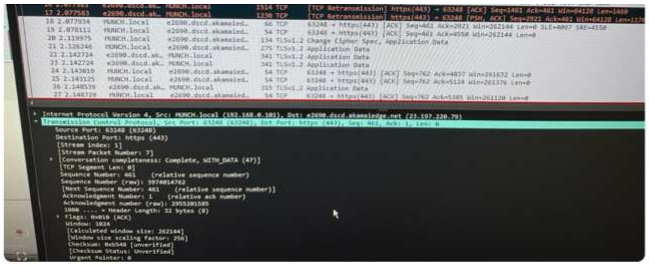
Export Analysis

LOCATING ERRORS:

Black lone with red text should pay more attention.
Or use analysis expert.


Wireshark_Save_Capture.pcap
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source            Destination          Length Protocol Info
    1 0.000000    Espressif_15:...  Broadcast               42 ARP      ARP Announcement for 192.168.0.248
    2 0.099644    192.168.0.137     255.255.255.255        230 UDP      49154 → 6667 Len=188
    3 0.840535    ArcherA6.lan      MUNCH.local             94 ICMP     Destination unreachable (Host unreachable)
    4 1.026395    192.168.0.114     255.255.255.255        230 UDP      49154 → 6667 Len=188
    5 1.908714    MUNCH.local       192.168.0.1             70 DNS      Standard query 0xcd53 A ftp.hp.com
    6 1.945625    192.168.0.1       MUNCH.local            184 DNS      Standard query response 0xcd53 A ftp.hp.com CNAME ftp.ext.hp.com CNAME ftp.ext.hp.
    7 1.954788    MUNCH.local       e2690.dscd.akamaied...  66 TCP      63248 → https(443) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
    8 1.982709    e2690.dscd.ak...  MUNCH.local             66 TCP      https(443) → 63248 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
    9 1.982930    MUNCH.local       e2690.dscd.akamaied...  54 TCP      63248 → https(443) [ACK] Seq=1 Ack=1 Win=262144 Len=0
   10 1.999214    MUNCH.local       e2690.dscd.akamaied... 514 TLSv1.2  Client Hello (SNI=ftp.hp.com)
   11 2.017406    e2690.dscd.ak...  MUNCH.local             60 TCP      https(443) → 63248 [ACK] Seq=1 Ack=461 Win=64128 Len=0
   12 2.017532    e2690.dscd.ak...  MUNCH.local            507 TLSv1.2  [TCP Previous segment not captured] , Ignored Unknown Record
   13 2.017753    MUNCH.local       e2690.dscd.akamaied...  66 TCP      [TCP Dup ACK 9#1] 63248 → https(443) [ACK] Seq=461 Ack=1 Win=262144 Len=0 SLE=4097 S
   14 2.050138    e2690.dscd.ak...  MUNCH.local           1514 TCP      [TCP Retransmission] https(443) → 63248 [ACK] Seq=1 Ack=461 Win=64128 Len=1460
   15 2.050452    MUNCH.local       e2690.dscd.akamaied...  66 TCP      63248 → https(443) [ACK] Seq=461 Ack=1461 Win=262144 Len=0 SLE=4097 SRE=4550
```

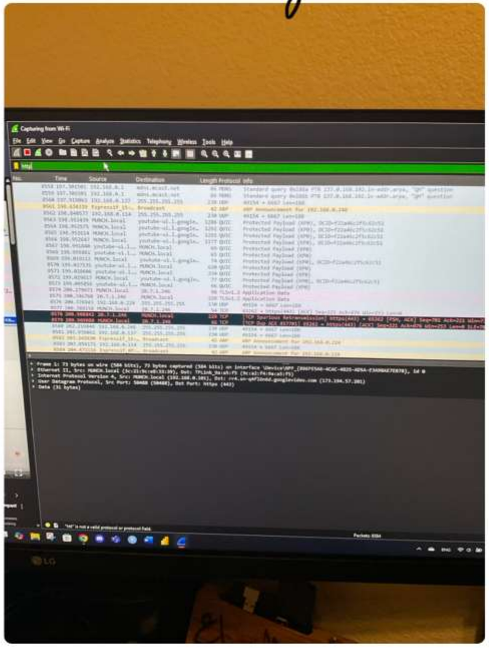


```
 16 2.077583   e2690.dscd.ak… MUNCH.local        1514 TCP     [TCP Retransmission] https(443) → 63248 [ACK] Seq=1461 Ack=461 Win=64128 Len=1460
 17 2.077583   e2690.dscd.ak… MUNCH.local        1230 TCP     [TCP Retransmission] https(443) → 63248 [PSH, ACK] Seq=2921 Ack=461 Win=64128 Len=1176
 18 2.077934   MUNCH.local    e2690.dscd.akamaied…  66 TCP     63248 → https(443) [ACK] Seq=461 Ack=2921 Win=262144 Len=0 SLE=4097 SRE=4550
 19 2.078113   MUNCH.local    e2690.dscd.akamaied…  54 TCP     63248 → https(443) [ACK] Seq=461 Ack=4550 Win=262144 Len=0
 20 2.119975   MUNCH.local    e2690.dscd.akamaied… 134 TLSv1.2 Change Cipher Spec, Application Data
 21 2.126246   MUNCH.local    e2690.dscd.akamaied… 275 TLSv1.2 Application Data
 22 2.142724   e2690.dscd.ak… MUNCH.local         341 TLSv1.2 Application Data
 23 2.142724   e2690.dscd.ak… MUNCH.local         341 TLSv1.2 Application Data
 24 2.143019   MUNCH.local    e2690.dscd.akamaied…  54 TCP     63248 → https(443) [ACK] Seq=762 Ack=4837 Win=261632 Len=0
 25 2.143125   MUNCH.local    e2690.dscd.akamaied…  54 TCP     63248 → https(443) [ACK] Seq=762 Ack=5124 Win=261376 Len=0
 26 2.148539   e2690.dscd.ak… MUNCH.local         315 TLSv1.2 Application Data
 27 2.148729   MUNCH.local    e2690.dscd.akamaied…  54 TCP     63248 → https(443) [ACK] Seq=762 Ack=5385 Win=261120 Len=0

› Internet Protocol Version 4, Src: MUNCH.local (192.168.0.101), Dst: e2690.dscd.akamaiedge.net (23.197.220.79)
˅ Transmission Control Protocol, Src Port: 63248 (63248), Dst Port: https (443), Seq: 461, Ack: 1, Len: 0
    Source Port: 63248 (63248)
    Destination Port: https (443)
    [Stream index: 1]
    [Stream Packet Number: 7]
  › [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 0]
    Sequence Number: 461    (relative sequence number)
    Sequence Number (raw): 3974014762
    [Next Sequence Number: 461    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2955201585
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0xb548 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

Applying dynamic Filters:

Filtering whole gathering Frames


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Length Protocol Info

Filtering Conversations:

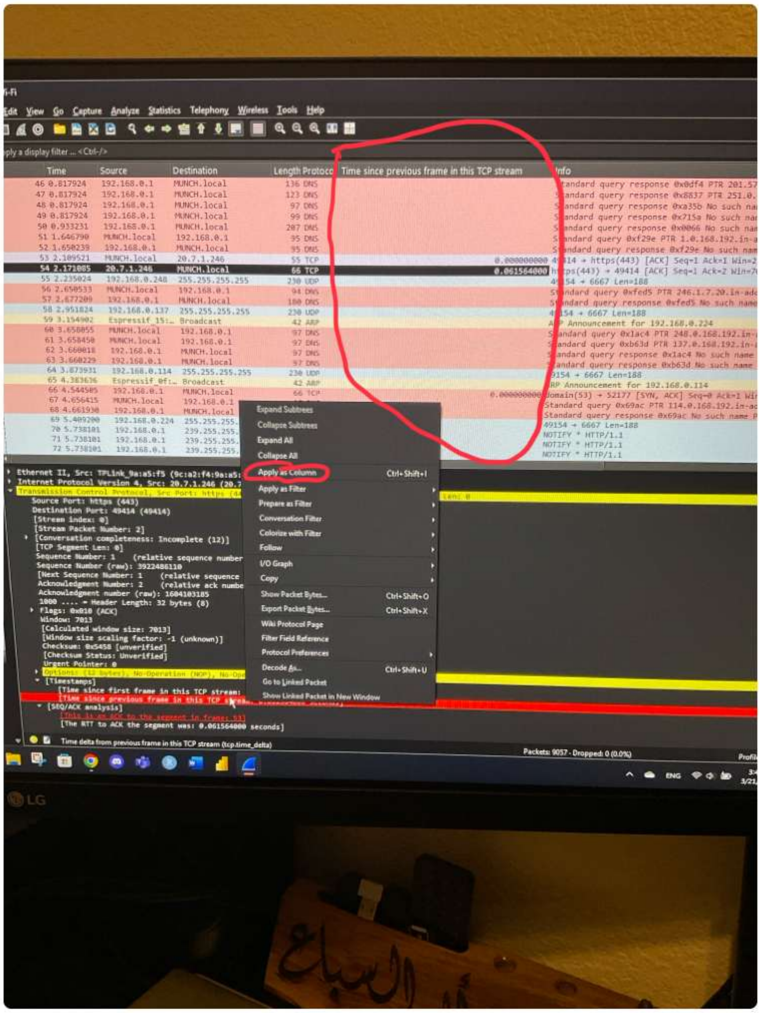
using Follow→TCP Stream
using Apply as Filter→selected/etc...
using Conversation Filter→IPv4/etc...
all on a specefic Frame.

Investigating Latency:
-we can only capture by the time it takes
to get a respons.

- Time col. is only the start of the capture (duhh)

Step1: Press "Edit"
Step2: Press "Prefrences"
Step3: Press "Protocols"
Step4: in this example we select TCP
Step5: make sure "Calculate Stream packet number and timeStap" is checked. press OK
Step6: In TCP header look for "TimeStamp"

Time Deltas:
Look at image.


i-Fi
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pply a display filter ... <Ctrl-/>
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
I/O Graph
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
LG

	Time	Source	Destination	Length	Protocol	Time since previous frame in this TCP stream	Info
46	0.817924	192.168.0.1	MUNCH.local	136	DNS		tandard query response 0x0df4 PTR 201.57
47	0.817924	192.168.0.1	MUNCH.local	123	DNS		andard query response 0x8837 PTR 251.0.
48	0.817924	192.168.0.1	MUNCH.local	97	DNS		andard query response 0xa35b No such na
49	0.817924	192.168.0.1	MUNCH.local	99	DNS		andard query response 0x715a No such na
50	0.933231	192.168.0.1	MUNCH.local	207	DNS		andard query response 0x0066 No such na
51	1.646790	MUNCH.local	192.168.0.1	95	DNS		andard query 0xf29e PTR 1.0.168.192.in-a
52	1.650239	192.168.0.1	MUNCH.local	95	DNS		andard query response 0xf29e No such nam
53	2.109521	MUNCH.local	20.7.1.246	55	TCP	0.000000000	4914 → https(443) [ACK] Seq=1 Ack=1 Win=2
54	2.171085	20.7.1.246	MUNCH.local	66	TCP	0.061564000	https(443) → 49414 [ACK] Seq=1 Ack=2 Win=7
55	2.235024	192.168.0.248	255.255.255.255	230	UDP		4 54 → 6667 Len=188
56	2.650533	MUNCH.local	192.168.0.1	94	DNS		ndard query 0xfed5 PTR 246.1.7.20.in-add
57	2.677209	192.168.0.1	MUNCH.local	180	DNS		ndard query response 0xfed5 No such name
58	2.951824	192.168.0.137	255.255.255.255	230	UDP		4 54 → 6667 Len=188
59	3.154902	Espressif_15:…	Broadcast	42	ARP		P Announcement for 192.168.0.224
60	3.658055	MUNCH.local	192.168.0.1	97	DNS		andard query 0x1ac4 PTR 248.0.168.192.in-
61	3.658450	MUNCH.local	192.168.0.1	97	DNS		andard query 0xb63d PTR 137.0.168.192.in-
62	3.660018	192.168.0.1	MUNCH.local	97	DNS		andard query response 0x1ac4 No such name
63	3.660229	192.168.0.1	MUNCH.local	97	DNS		andard query response 0xb63d No such name
64	3.873931	192.168.0.114	255.255.255.255	230	UDP		9154 → 6667 Len=188
65	4.383636	Espressif_0f:…	Broadcast	42	ARP		RP Announcement for 192.168.0.114
66	4.544505	192.168.0.1	MUNCH.local	66	TCP	0.000000000	omain(53) → 52177 [SYN, ACK] Seq=0 Ack=1 Wi
67	4.656415	MUNCH.local	192.168.0.1				Standard query 0x69ac PTR 114.0.168.192.in-ad
68	4.661930	192.168.0.1	MUNCH.local				Standard query response 0x69ac No such name P
69	5.409200	192.168.0.224	255.255.255.				49154 → 6667 Len=188
70	5.738101	192.168.0.1	239.255.255.				NOTIFY * HTTP/1.1
71	5.738101	192.168.0.1	239.255.255.				NOTIFY * HTTP/1.1
72	5.738101	192.168.0.1	239.255.255.				NOTIFY * HTTP/1.1

```
> Ethernet II, Src: TPLink_9a:a5:f5 (9c:a2:f4:9a:a5:
> Internet Protocol Version 4, Src: 20.7.1.246 (20.7
v Transmission Control Protocol, Src Port: https (44                Len: 0
      Source Port: https (443)
      Destination Port: 49414 (49414)
      [Stream index: 0]
      [Stream Packet Number: 2]
    > [Conversation completeness: Incomplete (12)]
      [TCP Segment Len: 0]
      Sequence Number: 1    (relative sequence number
      Sequence Number (raw): 3922486110
      [Next Sequence Number: 1    (relative sequence
      Acknowledgment Number: 2    (relative ack numbe
      Acknowledgment number (raw): 1604103185
      1000 .... = Header Length: 32 bytes (8)
    > Flags: 0x010 (ACK)
      Window: 7013
      [Calculated window size: 7013]
      [Window size scaling factor: -1 (unknown)]
      Checksum: 0x5458 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    > Options: (12 bytes), No-Operation (NOP), No-Ope
    v [Timestamps]
        [Time since first frame in this TCP stream:
        [Time since previous frame in this TCP strea
    v [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 53]
        [The RTT to ACK the segment was: 0.061564000 seconds]
```

Time delta from previous frame in this TCP stream (tcp.time_delta)

Packets: 9057 · Dropped: 0 (0.0%)

Detailed Displayed Filter:

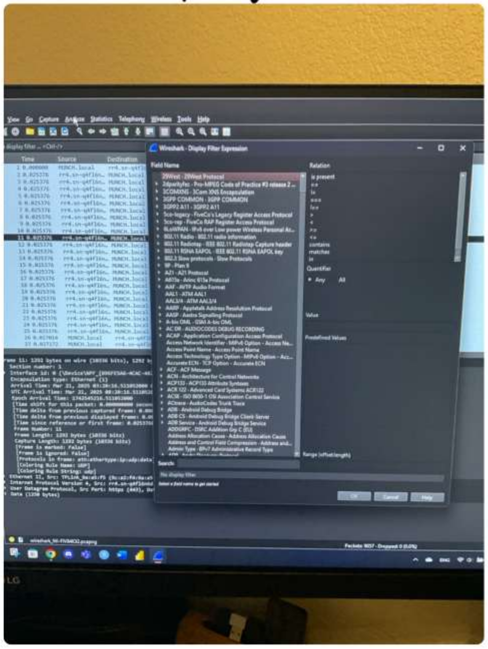
- the Filter on the top can be as Specefic as you want
- you can use "and", "or", "not"

Locating Response Code:

- you can search for errors

Using Expression Filter:

Step 1: press "Analyze"
Step 2: press "Display Filter Expression"


View Go Capture Analyze Statistics Telephony Wireless Tools Help
display filter ... <Ctrl-/>
Time Source Destination

```
1 0.000000  MUNCH.local  rr4.sn-q4fl6n...
2 0.025376  rr4.sn-q4fl6n...  MUNCH.local
3 0.025376  rr4.sn-q4fl6n...  MUNCH.local
...
26 0.027014  MUNCH.local  rr4.sn-q4fl...
27 0.027172  MUNCH.local  rr4.sn-q4fl...
```

```
Frame 11: 1292 bytes on wire (10336 bits), 1292 by
  Section number: 1
  Interface id: 0 (\Device\NPF_{...
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 21, 2025 01:20:16.511052000
  UTC Arrival Time: Mar 21, 2025 08:20:16.51105
  Epoch Arrival Time: 1742545216.511052000
  [Time shift for this packet: 0.000000000 secon
  [Time delta from previous captured frame: 0.00
  [Time delta from previous displayed frame: 0.0
  [Time since reference or first frame: 0.025376
  Frame Number: 11
  Frame Length: 1292 bytes (10336 bits)
  Capture Length: 1292 bytes (10336 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:data
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: TPLink_...
Internet Protocol Version 4, Src: rr4.sn-q4fl6nds
User Datagram Protocol, Src Port: https (443), Ds
Data (1250 bytes)
```

Wireshark · Display Filter Expression

Field Name

- 29West · 29West Protocol
- 2dparityfec · Pro-MPEG Code of Practice #3 release 2 ...
- 3COMXNS · 3Com XNS Encapsulation
- 3GPP COMMON · 3GPP COMMON
- 3GPP2 A11 · 3GPP2 A11
- 5co-legacy · FiveCo's Legacy Register Access Protocol
- 5co-rap · FiveCo RAP Register Access Protocol
- 6LoWPAN · IPv6 over Low power Wireless Personal Ar...
- 802.11 Radio · 802.11 radio information
- 802.11 Radiotap · IEEE 802.11 Radiotap Capture header
- 802.11 RSNA EAPOL · IEEE 802.11 RSNA EAPOL key
- 802.3 Slow protocols · Slow Protocols
- 9P · Plan 9
- A21 · A21 Protocol
- A615a · Arinc 615a Protocol
- AAF · AVTP Audio Format
- AAL1 · ATM AAL1
- AAL3/4 · ATM AAL3/4
- AARP · Appletalk Address Resolution Protocol
- AASP · Aastra Signalling Protocol
- A-bis OML · GSM A-bis OML
- AC DR · AUDIOCODES DEBUG RECORDING
- ACAP · Application Configuration Access Protocol
- Access Network Identifier · MIPv6 Option · Access Ne...
- Access Point Name · Access Point Name
- Access Technology Type Option · MIPv6 Option · Acc...
- Accurate ECN · TCP Option · Accurate ECN
- ACF · ACF Message
- ACN · Architecture for Control Networks
- ACP133 · ACP133 Attribute Syntaxes
- ACR 122 · Advanced Card Systems ACR122
- ACSE · ISO 8650-1 OSI Association Control Service
- ACtrace · AudioCodes Trunk Trace
- ADB · Android Debug Bridge
- ADB CS · Android Debug Bridge Client-Server
- ADB Service · Android Debug Bridge Service
- ADDGRPC · DSRC Addition Grp C (EU)
- Address Allocation Cause · Address Allocation Cause
- Address and Control Field Compression · Address and...
- Admin Type · IPv7 Administrative Record Type

Relation

- is present
- ==
- !=
- ===
- !==
- >
- <
- >=
- <=
- contains
- matches
- in

Quantifier

● Any ○ All

Value

Predefined Values

Range (offset:length)

Search

No display filter

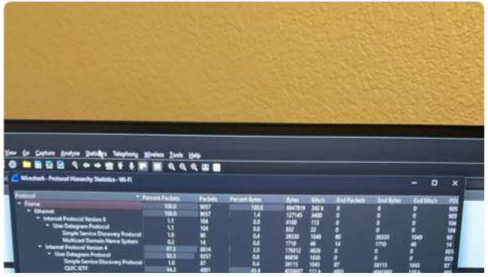
Select a field name to get started

OK Cancel Help

wireshark_Wi-FiVB4CO2.pcapng
Packets: 9057 · Dropped: 0 (0.0%)
LG

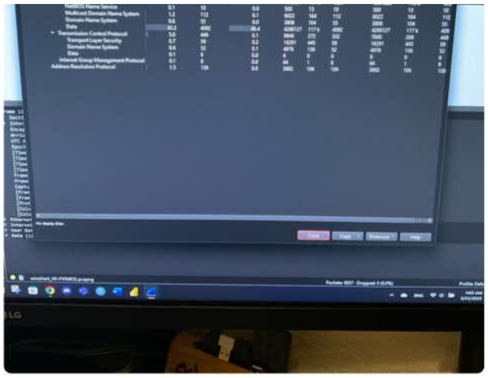
Locating suspicious Traffic in the Capture:

Step 1: Statics
Step 2: Protocal Hierarchy


View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Protocol Hierarchy Statistics · Wi-Fi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	9057	100.0	8847819	242 k	0	0	0	9057
Ethernet	100.0	9057	1.4	127145	3480	0	0	0	9057
Internet Protocol Version 6	1.1	104	0.0	4160	113	0	0	0	104
User Datagram Protocol	1.1	104	0.0	832	22	0	0	0	104
Simple Service Discovery Protocol	1.0	90	0.4	38330	1049	90	38330	1049	90
Multicast Domain Name System	0.2	14	0.0	1710	46	14	1710	46	14
Internet Protocol Version 4	97.3	8814	2.0	176212	4826	0	0	0	8814
User Datagram Protocol	92.3	8357	0.8	66856	1830	0	0	0	8357
Simple Service Discovery Protocol	1.0	87	0.4	38113	1043	87	38113	1043	87
QUIC IETF	44.2	4001	45.9	[illegible]	111 k	4001	[illegible]	[illegible]	[illegible]



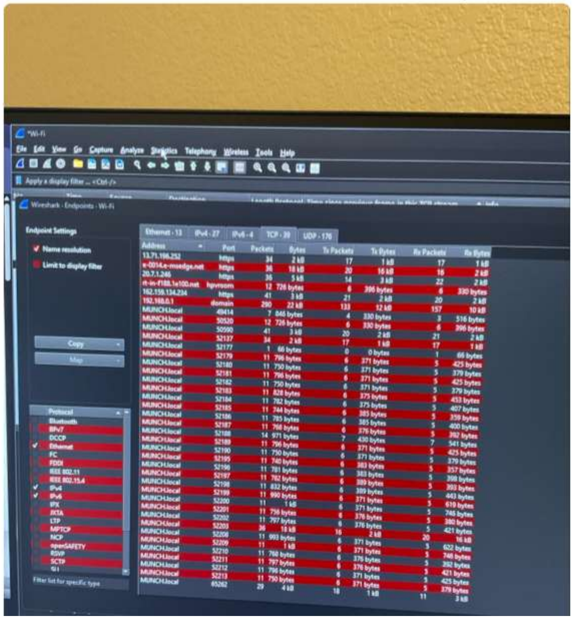
NetBIOS Name Service	0.1	10	0.0	500	13	10	500	13	10
Multicast Domain Name System	1.2	112	0.1	6022	164	112	6022	164	112
Domain Name System	0.6	55	0.0	3806	104	55	3806	104	55
Data	45.2	4092	48.4	4288127	117 k	4092	4288127	117 k	409
▾ Transmission Control Protocol	5.0	449	0.1	9940	272	332	7600	208	449
Transport Layer Security	0.7	59	0.2	16291	445	59	16291	445	59
Domain Name System	0.6	52	0.1	4976	136	52	4976	136	52
Data	0.1	6	0.0	6	0	6	6	0	6
Internet Group Management Protocol	0.1	8	0.0	64	1	8	64	1	8
Address Resolution Protocol	1.5	139	0.0	3892	106	139	3892	106	139

Expert information Errors:
the color thing on the bottom

Obtaining Files:
step 1: Find a file on the info
step 2: press "File"
step 3: press "Export.... "

Exporting Captured Objects:
File → Export Object → what you want.

Statistics:
statistics → Endpoints
seeing connections and ports.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Endpoints · Wi-Fi
Endpoint Settings
Copy
Map
Filter list for specific type
Ethernet · 13
IPv4 · 27
IPv6 · 4
TCP · 39
UDP · 176

☑ Name resolution
☐ Limit to display filter

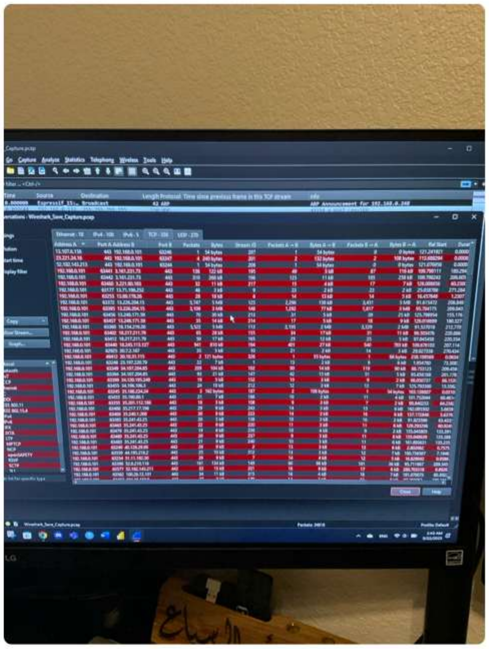
	Protocol
	Bluetooth
	BPv7
	DCCP
✓	Ethernet
	FC
	FDDI
	IEEE 802.11
	IEEE 802.15.4
✓	IPv4
✓	IPv6
	IPX
	JXTA
	LTP
	MPTCP
	NCP
	openSAFETY
	RSVP
	SCTP
	SLL

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
13.71.196.252	https	34	2 kB	17	1 kB	17	1 kB
e-0014.e-msedge.net	https	36	18 kB	20	16 kB	16	2 kB
20.7.1.246	https	36	5 kB	14	3 kB	22	2 kB
rt-in-f188.1e100.net	hpvroom	12	726 bytes	6	396 bytes	6	330 bytes
162.159.134.234	https	41	3 kB	21	2 kB	20	2 kB
192.168.0.1	domain	290	22 kB	133	12 kB	157	10 kB
MUNCH.local	49414	7	846 bytes	4	330 bytes	3	516 bytes
MUNCH.local	50520	12	726 bytes	6	330 bytes	6	396 bytes
MUNCH.local	50590	41	3 kB	20	2 kB	21	2 kB
MUNCH.local	52137	34	2 kB	17	1 kB	17	1 kB
MUNCH.local	52177	1	66 bytes	0	0 bytes	1	66 bytes
MUNCH.local	52179	11	796 bytes	6	371 bytes	5	425 bytes
MUNCH.local	52180	11	750 bytes	6	371 bytes	5	379 bytes
MUNCH.local	52181	11	796 bytes	6	371 bytes	5	425 bytes
MUNCH.local	52182	11	750 bytes	6	371 bytes	5	379 bytes
MUNCH.local	52183	11	828 bytes	6	375 bytes	5	453 bytes
MUNCH.local	52184	11	782 bytes	6	375 bytes	5	407 bytes
MUNCH.local	52185	11	744 bytes	6	385 bytes	5	359 bytes
MUNCH.local	52186	11	785 bytes	6	385 bytes	5	400 bytes
MUNCH.local	52187	11	768 bytes	6	376 bytes	5	392 bytes
MUNCH.local	52188	14	971 bytes	7	430 bytes	7	541 bytes
MUNCH.local	52189	11	796 bytes	6	371 bytes	5	425 bytes
MUNCH.local	52190	11	750 bytes	6	371 bytes	5	379 bytes
MUNCH.local	52195	11	740 bytes	6	383 bytes	5	357 bytes
MUNCH.local	52196	11	781 bytes	6	383 bytes	5	398 bytes
MUNCH.local	52197	11	782 bytes	6	389 bytes	5	393 bytes
MUNCH.local	52198	11	832 bytes	6	389 bytes	5	443 bytes
MUNCH.local	52199	11	990 bytes	6	371 bytes	5	619 bytes
MUNCH.local	52200	11	1 kB	6	371 bytes	5	745 bytes
MUNCH.local	52201	11	756 bytes	6	376 bytes	5	380 bytes
MUNCH.local	52202	11	797 bytes	6	376 bytes	5	421 bytes
MUNCH.local	52203	36	18 kB	16	2 kB	20	16 kB
MUNCH.local	52208	11	993 bytes	6	371 bytes	5	622 bytes
MUNCH.local	52209	11	1 kB	6	371 bytes	5	748 bytes
MUNCH.local	52210	11	768 bytes	6	376 bytes	5	392 bytes
MUNCH.local	52211	11	797 bytes	6	376 bytes	5	421 bytes
MUNCH.local	52212	11	796 bytes	6	371 bytes	5	425 bytes
MUNCH.local	52213	11	750 bytes	6	371 bytes	5	379 bytes
MUNCH.local	65262	29	4 kB	18	1 kB	11	3 kB

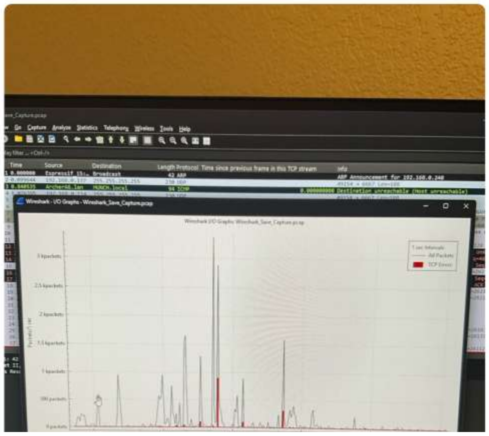
wireshark_Wi-FIVB4K32.pcapng
Packets: 9057 · Dropped: 0 (0.0%)
LG

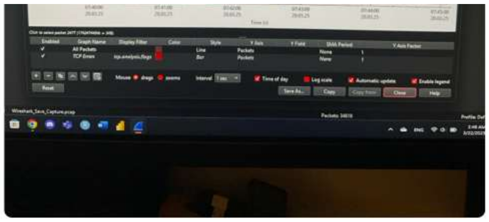
End Points

Conversations:
Statistics → conversation
- shows addresses
- shows the whole interaction.
- shows the bytes (packs) that go A → B & B → A
- Also show Duration (time)


Capture.pcap
Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Length Protocol Time since previous frame in this TCP stream Info
0.000000 Espressif_15:.. Broadcast 42 ARP ARP Announcement for 192.168.0.240
Conversations · Wireshark_Save_Capture.pcap
Ethernet · 13 IPv4 · 105 IPv6 · 1 TCP · 356 UDP · 270
Address A Port A Address B Port B Packets Bytes Stream ID Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration
Copy
Follow Stream...
Graph...
LG

Graphing:
Statistic → graphs (I/O graph)
- it can be edited and used in reports


Save_Capture.pcap
Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source Destination Length Protocol Time since previous frame in this TCP stream Info
1 0.000000 Espressif_15:.. Broadcast 42 ARP ARP Announcement for 192.168.0.240
2 0.099944 192.168.0.177 255.255.255.255 238 UDP
3 0.840535 Archer46.lan MUNCH.local 94 ICMP 0.000000000 Destination unreachable (Host unreachable)
Wireshark · I/O Graphs · Wireshark_Save_Capture.pcap
Wireshark I/O Graphs: Wireshark_Save_Capture.pcap
3 kpackets
2.5 kpackets
2 kpackets
1.5 kpackets
1 kpackets
500 packets
0 packets
Packets/1 sec
1 sec intervals
All Packets
TCP Errors



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
✓	All Packets		🟥	Line	Packets		None	1
✓	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec ☑ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Wireshark_Save_Capture.pcap

Identifying Active conversations:
- in conversation look at packet amount and Byte.

Self Analysis

Using GeoIP: Download.

Identify packets By location: Filtering For
- end points show more info, location.

Mapping packet location using GeoIP: creates a map.

Using protocol Hierarchies:
Stat → Protocol Hierarchy
showing how to read.

Locating suspicious traffic using :
- apply filters on the Hierarchy pages.

Graphing Analysis Flags:
- you can press on the IO graph to look at errors

Voice over IP Telaphony:
"sip" in the filter
4223 errors
"Telephony" tab.

Identifying VoIP calls

Locating Conversations:

Telephony → VOIP Calls

Using VOIP Stats:

Ladder Diagrams: SIP

Getting audio: SIP

Advanced: cmd

tshark