

Author: Agata GABARA

M00728162

WIRESHARK

Lab nr. 1 (12.02.2021)

We have download from wireshark.org the latest version of Wireshark (64 bit for computer).

Wireshark is open source and free packet analyser. The original name is Ethereal. It can be used for education, network analysis and troubleshooting. It was developed by Gerald Combs. It runs on Linux, macOS, BSD, Solaris and Microsoft Windows.

"Packet analysis, often referred to as packet sniffing or protocol analysis, describes the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network. Packet analysis is typically performed by a packet sniffer, a tool used to capture raw network data going across the wire. Packet analysis can help with the following: λ Understanding network characteristics λ Learning who is on a network λ Determining who or what is utilizing available bandwidth λ Identifying peak network usage times λ Identifying possible attacks or malicious activity λ Finding unsecured and bloated applications"¹ Wireshark works based on 3 process such as: collection², conversion³ and analysis⁴

Protocols:

"Common protocols include Transmission Control Protocol (TCP), Internet Protocol (IP), Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP). A protocol stack is a logical grouping of protocols that work together"⁵

Protocols can have easy or difficult structure.

¹ Chris Sanders, Practical Packet Analysis, p.26

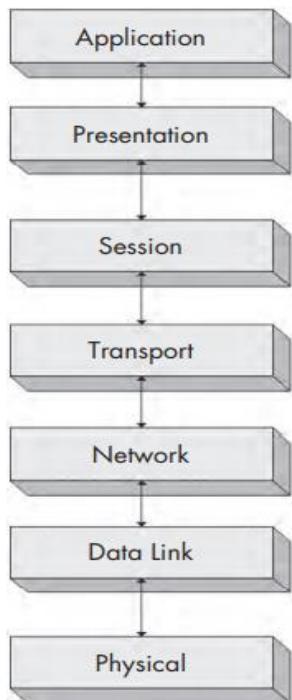
² collects raw binary data from the wire.

³ the captured binary data is converted into a readable form

⁴ the actual analysis of the captured and converted data

⁵ Chris Sanders, Practical Packet Analysis, p.24

OSI model



Source: Chris Sanders, Practical Packet Analysis, p.31

Layer 7- layer seen by end user, it provides the interface.

Layer 6- it handles with encryption and decryption.

Layer 5- it manages the sessions between the computers.

Layer 4- it provides the transport to lower layers.

Layer 3- one of the most complex OSI layers, logical addressing of network hosts.

Layer 2- it provides the means of transporting data across a physical network, provides the addressing scheme that can be used for devices identification (MAC address etc.)

Layer 1- physical medium, through which network

Types of protocols used in layers

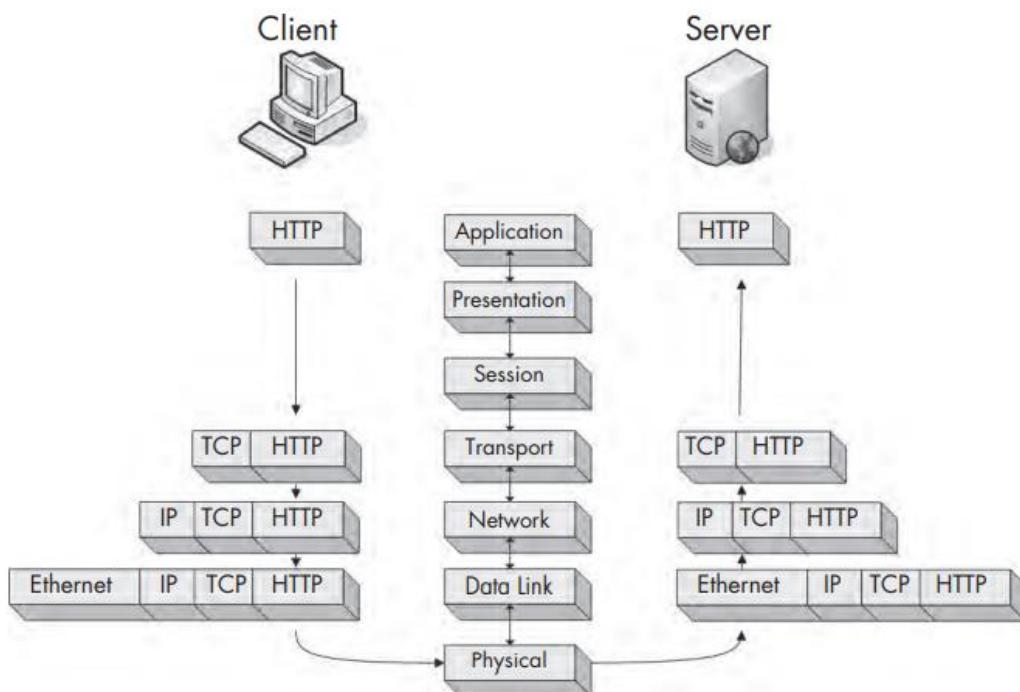
Layer	Protocol
Application	HTTP, SMTP, FTP, Telnet
Presentation	ASCII, MPEG, JPEG, MIDI
Session	NetBIOS, SAP, SDP, NWLink
Transport	TCP, UDP, SPX
Network	IP, IPX
Data link	Ethernet, Token Ring, FDDI, AppleTalk

"Each layer in the OSI model is capable of communicating with only the layers directly above and below it."⁶

Data encapsulation:

" Each layer in the stack is responsible for adding a header or footer—extra bits of information that allow the layers to communicate—to the data being communicated" (..) The encapsulation process creates a protocol data unit (PDU), which includes the data being sent and all header or footer information added to it."⁷ The packet = PDU with header and footer information from all layers.

Encapsulation of data between client and server.



Snapshots from Wireshark:

We have chosen WIFI and in the settings tick off the option which disables presenting what come from other network. At the bottom we see 7 headers such as: no, time, source, destination, protocol, length and info. Time is shown in seconds. The protocols are: DHCP⁸ v6, MDNS⁹, DNS¹⁰, TCP¹¹, TSL v.1.2¹² and others.

⁶ Chris Sanders, Practical Packet Analysis, p.31.

⁷ Chris Sanders, Practical Packet Analysis, p.32.

⁸ The Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks.

⁹ Multicast DNS

¹⁰ The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities

¹¹ The Transmission Control Protocol is one of the main protocols of the Internet protocol suite.

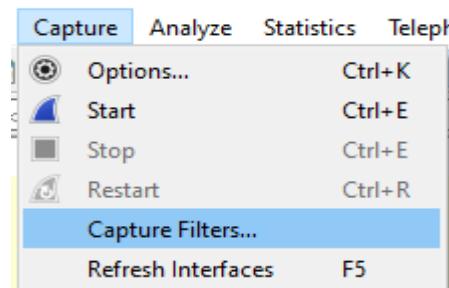
¹² Transport Layer Security

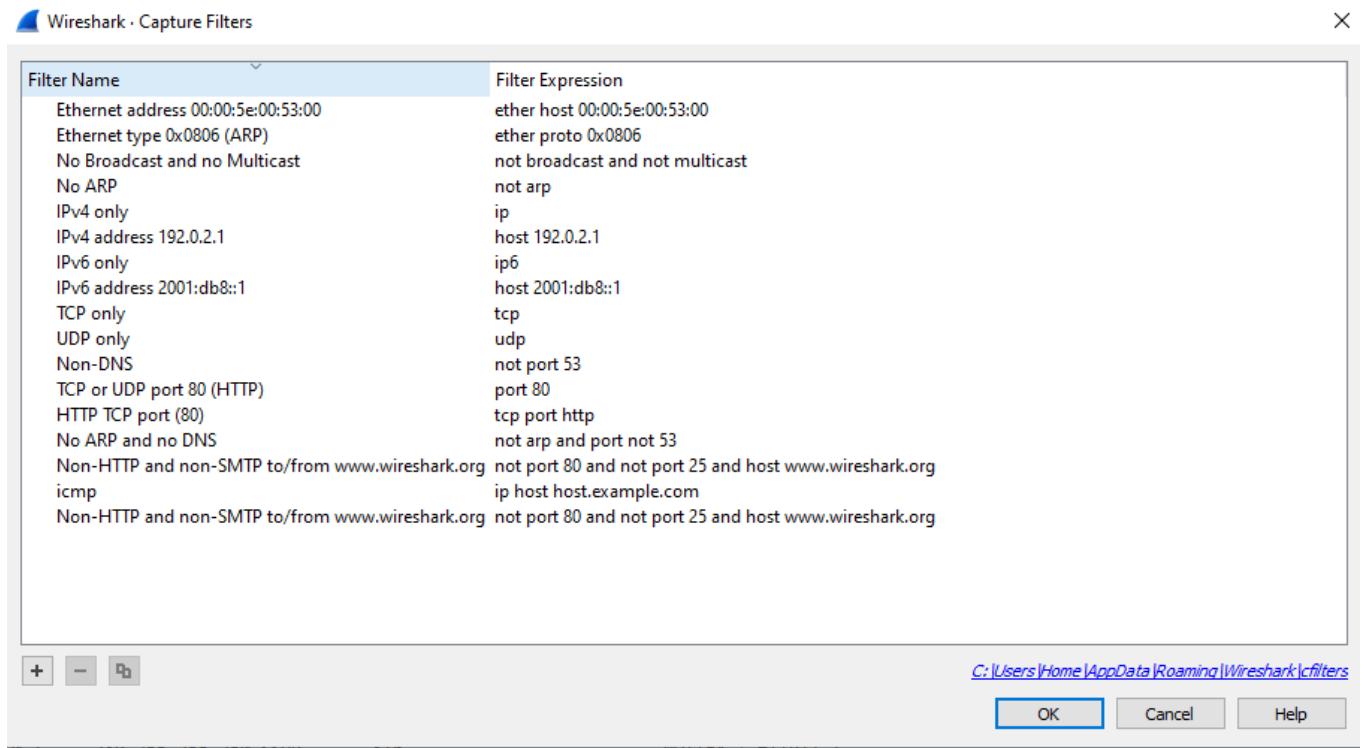
Description of basic windows program:



At the top is definition of filter of displaying. Below there is a window with captured packets. In the middle there is a content of highlighted packet. At the bottom there is a content of RAW highlighted packet. When we turned on packet capture, we could see the amount of information was transmitted by our network. The power of Wireshark is in its filters, which allows narrow the results down.

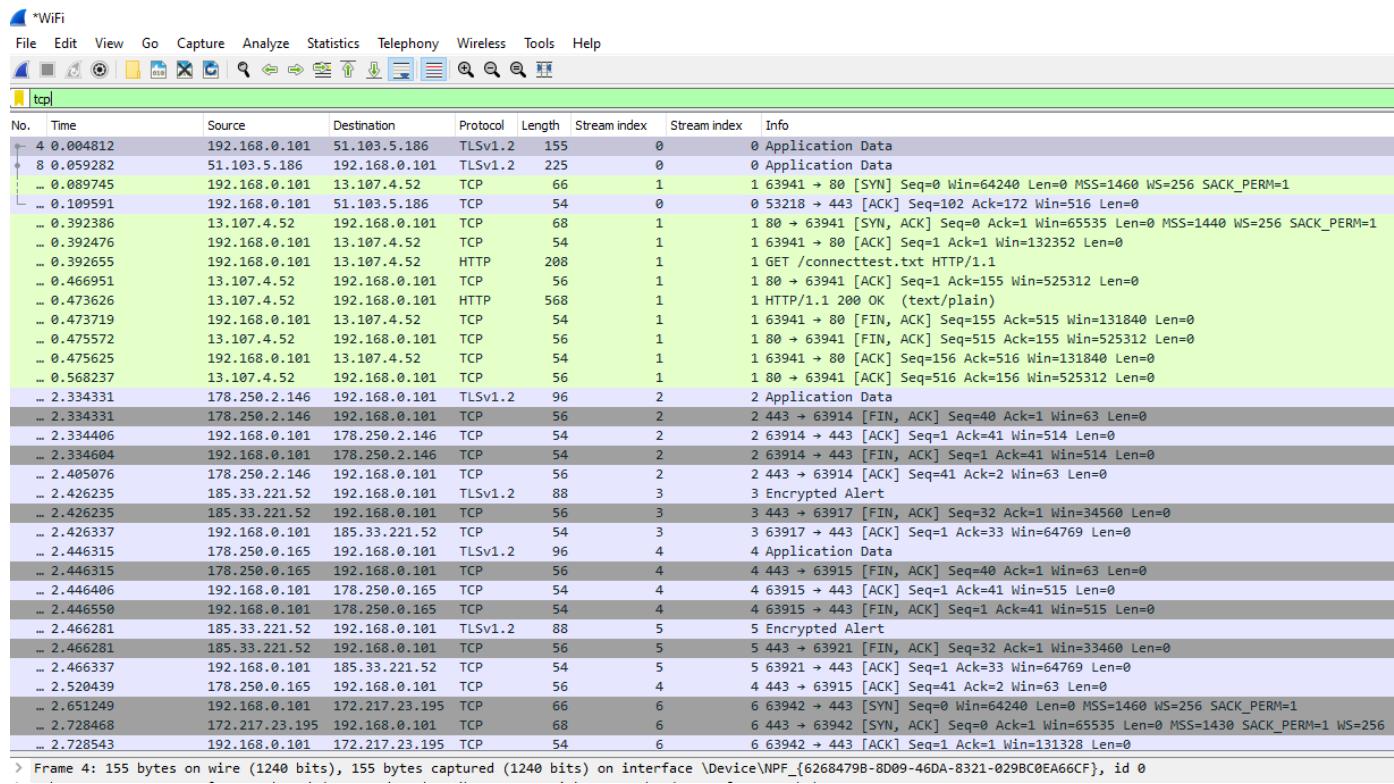
Filters: Options -> Capture Filters





We can choose what is interested in for us for example TCP or we can start write on the green field at the top, we have a menu with some options which we can choose.

No.	tcp.stream eq 0 tcp.port == 80 udp.port == 80	Destination	Protocol	Length	Stream index	Stream index	Info
0..	tcp	0.101	192.168.0.255	NBNS	92		Name query NB WPAD<00>
0..	tcp.options.cc	0.101	192.168.0.255	NBNS	92		Name query NB WPAD<00>
0..	tcp.options.ccecho	0.101	192.168.0.255	NBNS	92		Name query NB WPAD<00>
0..	tcp.options.ccnew	0.101	192.168.0.255	NBNS	92		Name query NB WPAD<00>
0..	tcp.options.echo	0.101	172.217.23.206	UDP	749		60524 → 443 Len=707
0..	tcp.options.echoreply	23.206	192.168.0.101	UDP	68		443 → 60524 Len=26
0..	tcp.options.eol	23.206	192.168.0.101	UDP	145		443 → 60524 Len=103
0..	tcp.options.experimental	23.206	192.168.0.101	UDP	68		443 → 60524 Len=26
0..	tcp.options.md5	0.101	172.217.23.206	UDP	75		60524 → 443 Len=33
0..	tcp.options.mss	:f5:28...	ff02::c	UDP/XML	718		63093 → 3702 Len=656
0..	tcp.options.nop	0.1	192.168.0.101	UDP	314		46612 → 52474 Len=272
0..	tcp.options.qs	0.1	192.168.0.101	UDP	314		46612 → 52474 Len=272
0..	tcp.options.rvbd.probe	0.1	192.168.0.101	UDP	323		46612 → 52474 Len=281
0..	tcp.options.rvbd.trpy	0.1	192.168.0.101	UDP	323		46612 → 52474 Len=281
0..	tcp.options.sack	0.1	192.168.0.101	UDP	378		46612 → 52474 Len=336
0..	tcp.options.sack_perm	0.1	192.168.0.101	UDP	378		46612 → 52474 Len=336
0..	tcp.options.scps	0.1	192.168.0.101	UDP	698		63093 → 3702 Len=656
0..	tcp.options.scpscor	0.101	239.255.255.250	UDP/XML			



Protocols:

Protocol	Protocol
LLMNR	TLSv1.3
LLMNR	TLSv1.3
TCP	TLSv1.3
TCP	TLSv1.3
TCP	TCP
AJP13	TLSv1.3
TCP	TLSv1.3
UDP	TLSv1.3
AJP13	TCP
TCP	TLSv1.3
TCP	TLSv1.3
TCP	TLSv1.3
TCP	TCP
AJP13	TCP
TCP	TCP
TCP	TLSv1.3

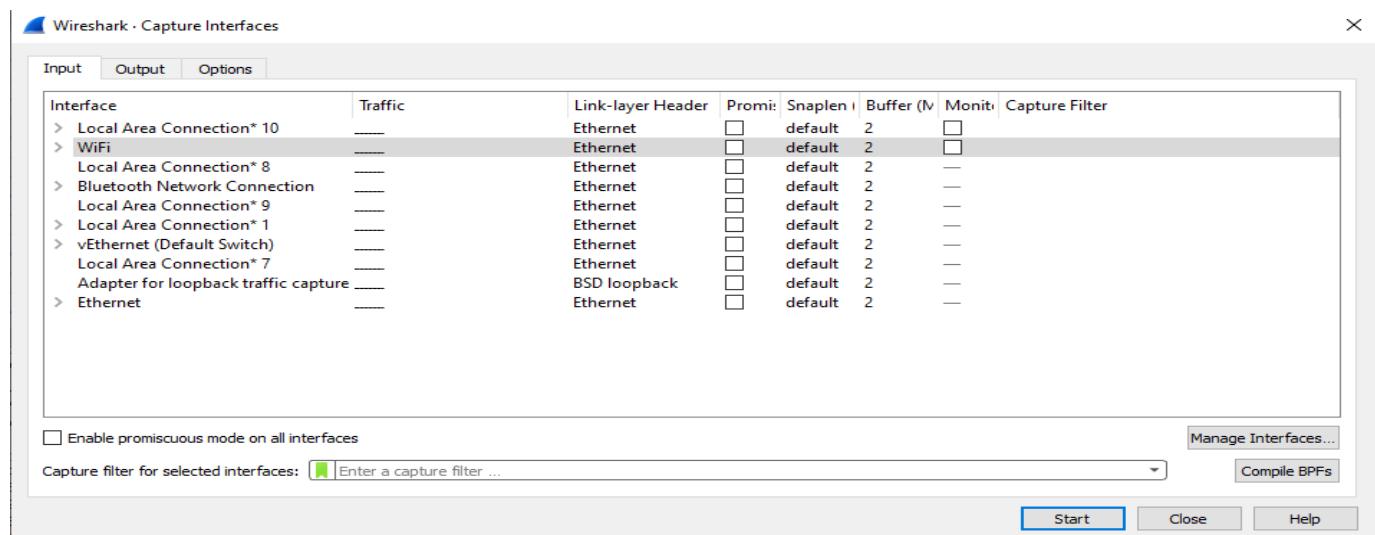
No.	Time	Source	Destination	Protocol	Length	Info
4810	390.979138	91.198.174.208	192.168.0.81	TCP	56	443 → 59146 [ACK] Seq=288315 Ack=2386 Win=42496 Len=0
4811	391.162636	192.168.0.81	192.168.0.69	AJP13	164	AJP13 Error? [TCP segment of a reassembled PDU]
4812	391.166796	192.168.0.69	192.168.0.81	TCP	164	8009 → 59168 [PSH, ACK] Seq=5800 Ack=920 Win=15680 Len=110
4813	391.208676	192.168.0.81	192.168.0.69	TCP	54	59168 → 8009 [ACK] Seq=920 Ack=5910 Win=131072 Len=0
4814	391.398827	192.168.0.81	74.125.71.188	TCP	55	[TCP Keep-Alive] 59116 → 5228 [ACK] Seq=789 Ack=4509 Win=13
4815	391.427468	74.125.71.188	192.168.0.81	TCP	66	[TCP Keep-Alive ACK] 5228 → 59116 [ACK] Seq=4509 Ack=790 Wi
4816	391.669048	192.168.0.81	192.168.0.69	TCP	55	[TCP Keep-Alive] 59117 → 8008 [ACK] Seq=248 Ack=1200 Win=13
4817	391.673350	192.168.0.69	192.168.0.81	TCP	66	[TCP Keep-Alive ACK] 8008 → 59117 [ACK] Seq=1200 Ack=249 Wi
4818	393.232839	192.168.0.81	216.58.204.35	TCP	55	[TCP Keep-Alive] 59138 → 443 [ACK] Seq=2802 Ack=4526 Win=13
4819	393.247254	216.58.204.35	192.168.0.81	TCP	66	[TCP Keep-Alive ACK] 443 → 59138 [ACK] Seq=4526 Ack=2803 Wi
4820	393.263829	192.168.0.81	216.58.204.67	TCP	55	[TCP Keep-Alive] 59147 → 443 [ACK] Seq=1664 Ack=4556 Win=13
4821	393.263943	192.168.0.81	142.250.178.14	TCP	55	[TCP Keep-Alive] 59137 → 443 [ACK] Seq=1879 Ack=5702 Win=13
4822	393.284340	216.58.204.67	192.168.0.81	TCP	66	[TCP Keep-Alive ACK] 443 → 59147 [ACK] Seq=4556 Ack=1665 Wi
4823	393.290674	142.250.178.14	192.168.0.81	TCP	66	[TCP Keep-Alive ACK] 443 → 59137 [ACK] Seq=5702 Ack=1880 Wi

Is it important to open Wireshark with the Promiscuous Mode turned off?

“Promiscuous mode” is a network interface mode in which the NIC reports every packet that it sees”¹³ It is not good as we should not see what other people in our neighbourhood doing as we don’t have permission to do it. “If you’re connected to a switch as opposed to a hub, broadcast traffic and multicast traffic will go to all ports, but unicast traffic does not. Check your switch to see if you can configure the port you’re using for Wireshark to have all traffic sent to it (“monitor” mode), and/or to “mirror” traffic from one port to another”¹⁴

At the bottom, we see a list, we have chosen WIFI and remember tick off option “enable promiscuous on all interfaces” in the left bottom corner.

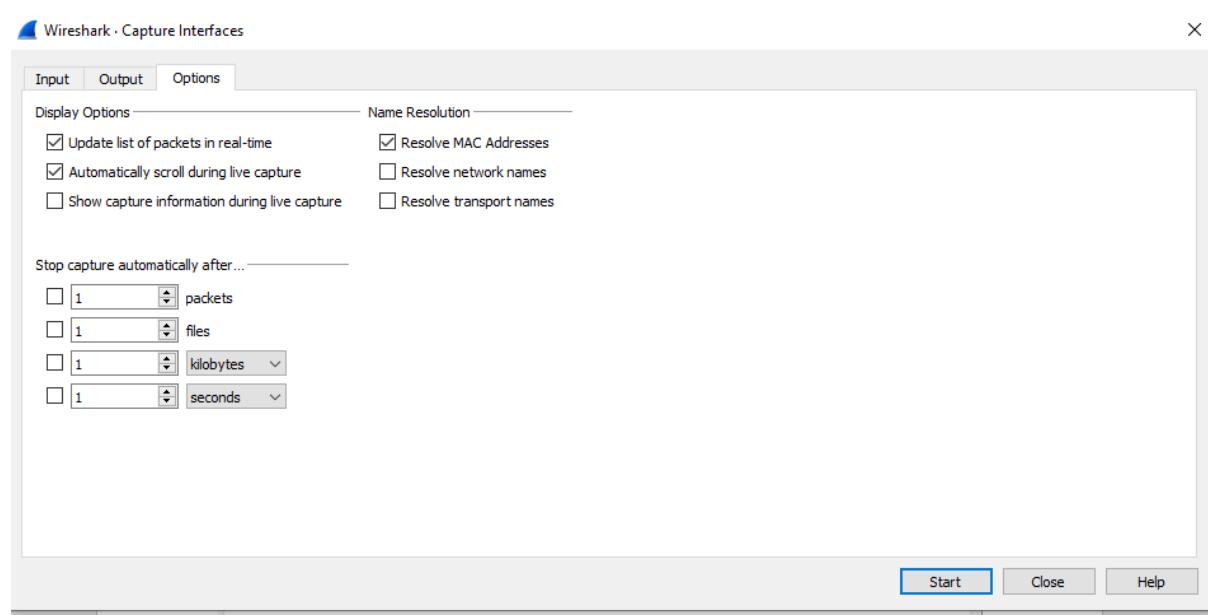
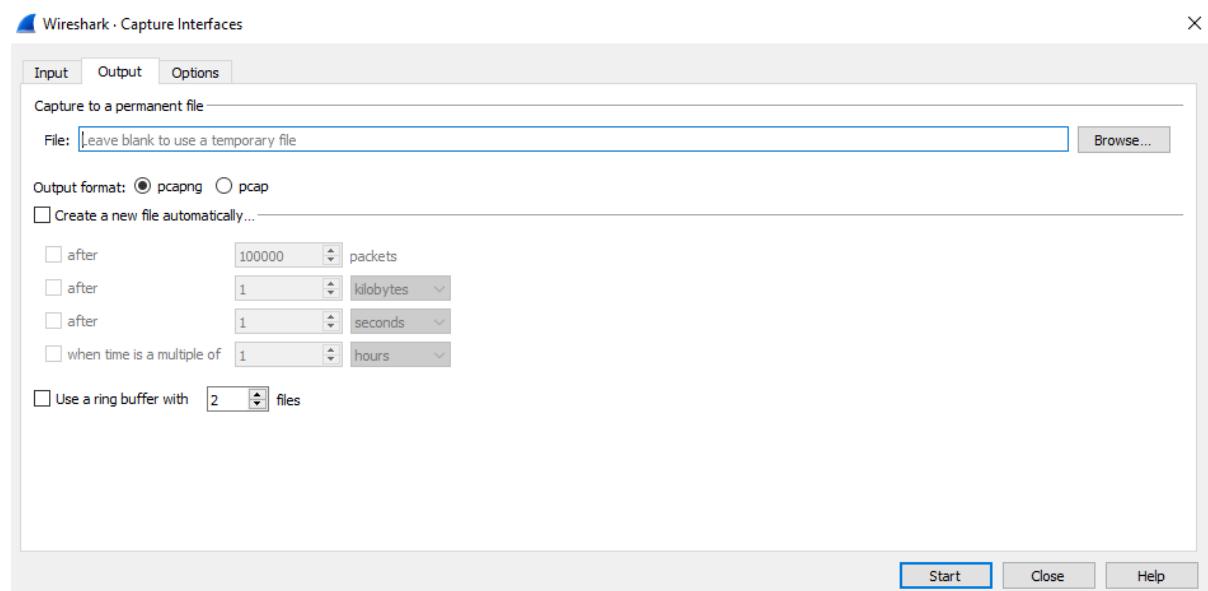
We see 3 tabs such as: input, output and options. In the first one we choose WIFI, we haven’t done any changes in 2 others, we have left how was fixed.



¹³ <https://www.networkworld.com/article/2231903/wireshark-and-promiscuous-mode.html>

¹⁴ <https://www.networkworld.com/article/2231903/wireshark-and-promiscuous-mode.html>

Without changes here:



In the case of having difficulties with this mode, we should use:

- to check NIC¹⁵'s manufacturer website if some issues happen,
- to check in Device Manager, the driver's settings to allow manually turn off this mode.

How can you follow a stream?

Following streams in Wireshark provides a different view on network traffic: instead of individual packets, one can see data flowing between client & server. Client part is marked as red, server one as blue in Wireshark.

¹⁵ Network Interface Card

I have chosen line 14 and click right mouse and I have chosen follow and TCP Stream (only one option is available)

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
14...	31.440...	192.168.0.81	173.194.183.138	TCP	66	21	62207 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

```

tcp.stream eq 21

No. Time Source Destination Protocol Length Stream index Info
14... 31.440... 192.168.0.81 173.194.183.138 TCP 66 21 62207 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 4071: 1462 bytes on wire (11696 bits), 1462 bytes captured (11696 bits) on interface \Device\NPF_{6268479B-8D09-46DA-8321-029BC0EA66CF}, id 0
> Ethernet II, Src: ARRISGro_c0:43:38 (40:0d:10:c0:43:38), Dst: IntelCor_81:b3:4d (a0:a8:cd:81:b3:4d)
> Internet Protocol Version 4, Src: 173.194.183.138, Dst: 192.168.0.81
✓ Transmission Control Protocol, Src Port: 443, Dst Port: 62207, Seq: 2692317, Ack: 13111, Len: 1408
  Source Port: 443
  Destination Port: 62207
  [Stream index: 21]
  [TCP Segment Len: 1408]
  Sequence number: 2692317 (relative sequence number)
  Sequence number (raw): 1057476565
  [Next sequence number: 2693725 (relative sequence number)]
  Acknowledgment number: 13111 (relative ack number)
  Acknowledgment number (raw): 573709965
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x010 (ACK)
  Window size value: 384
  [Calculated window size: 98304]
  [Window size scaling factor: 256]
  Checksum: 0xa6a9 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [timestamps]
  TCP payload (1408 bytes)
  [Reassembled PDU in frame: 4073]

```

After doing this at the top I have seen green field with info: tcp stream eq 21. TCP because I have chosen the line with this protocol. At the bottom, I need to find Transmission Control Protocol and analyse it. We are focus on STREAM INDEX which here has value 21. When I choose this stream index on mouse I can apply this as a column.

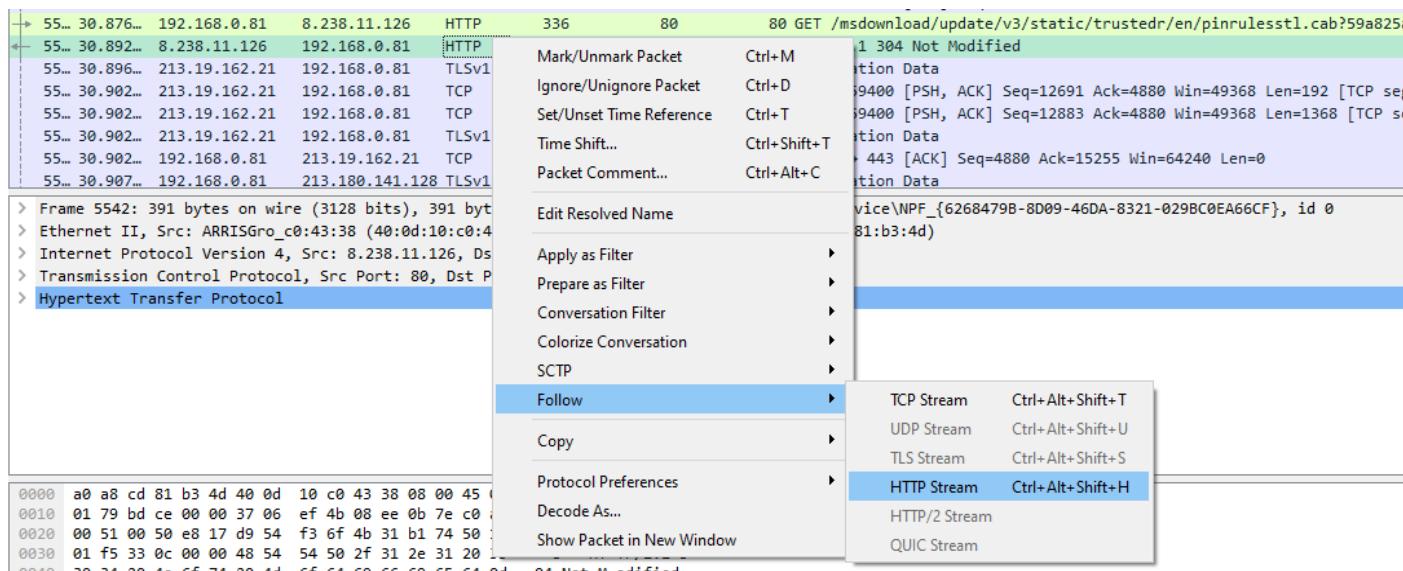
No.	Time	Source	Destination	Protocol	Length	Stream index
14...	31.440...	192.168.0.81	173.194.183.138	TCP	66	
> Frame 4071: 1462 bytes on wire (11696 bits), 1462 bytes captured (1:1) on interface Intel PRO/100 MT Desktop at 31.440000 seconds (rate 1462 bps)						
> Ethernet II, Src: ARRISGro_c0:43:38 (40:0d:10:c0:43:38), Dst: Intel PRO/100 MT Desktop (08:00:27:00:00:00)						
> Internet Protocol Version 4, Src: 173.194.183.138, Dst: 192.168.0.81						
Transmission Control Protocol, Src Port: 443, Dst Port: 62207, Seq: 10101 ...						
Source Port: 443						
Destination Port: 62207						
[Stream index: 21]						
[TCP Segmentation Offset] Expand Subtrees						
Sequence Number] Collapse Subtrees						
Sequence Number] Expand All						
Sequence Number] Collapse All						
[Next sequence number] [Previous sequence number] [Sequence number]						
Acknowledge Number] [Sequence number]						
Acknowledge Number] [Sequence number]						
Acknowledge Number] [Sequence number]						
Acknowledge Number] [Sequence number]						
Flags: 0						
Window Scale Factor] [Window Scale Factor]						
[Checksum] [Checksum]						
[Checksum] [Checksum]						
[Urgent pointer] [Urgent pointer]						
[SEQ/ACK] [SEQ/ACK]						
[Timestamp] [Timestamp]						
TCP payload] [TCP payload]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						
[Reassembly offset] [Reassembly offset]						

TCP Stream View:

.....m*aK..3.,^...:i.....FI.F ...{.....Jk.:...R.&..Q('T.L.. ZZ.....+./.,0...../.5....
.....%#.r5---sn-aig16ner.googlevideo.com.....
.....#.....h2.http/1.1.....
.....3.+..... Q.C%j.....>\.\. }
@.f.l.;..C.-..+.
!.....
.....z..v..@..yp|..~.i.W.[.._.....
.QnRCQ.f../ ..{.....Jk.:...R.&..Q('T.L.. ZZ.....3.\$.... !<.m.....IY\..Q..1..\.9.D..-U.+.....
0\k..Z....N..E..<..E..Z..|.S..U..|.S..B..|.S..3.b..|.ctjPH>..2m..&..}.....'..{..b..'.....
y.d..|.5..?..0..|.S..-..i.E..g*[..W..J..|.4..Z..0X:"w88..1.E..>..B..L..N..xT.. @..3I.V..Y..@..A..6..6..m.._..&y..Y..[.....j..-r..0..+.w[..Y..?DM2.#hi\$..r.{F.A].
[..Y0f..tG..7..L..W.g.....s..xx..oN.s.h..".m..6f..?..T..o..0..m..;..EU..+vc..m..;....Y)..u.%>.z..b..4.
.?.!....\$.8..?..Q1.85..3..k..x..}Hh..d..S..z7?..]!]..u..B.Z.. u..@/.....0F.z..<..{.g..]
Z..Ua.F..|.7..1;[xx.. .a..>..
.....
.BX..).36.v..n.s.|Q/X..!..].v..1..,[.....VYG..9..g.yq(H ..@..Q!.qt0.
.....j../.x..,/.In..X"S.s..|.J..|.i..\$Y..c.B..I.D.lG..`..1 ..
.....C..Z..Z[..... B.w.....
.73..|.1.S..Z..|.1.?..+k..m..e..>0..Mc%7.U.....Nw..o..8aR.Vs..!k..+6..G.:
.1q..G.....H.K.1
.S.%.. e.p.I.63....*.....
.N..W..J..W..5.....J..W..5.....|.@T..H..ZT..} ..H@..... X.w....y+..A..I.....!..d>[... (1....fB..!..He..1).z.....g
.....-..Yh..g..L..|[..L0..S..,r\$N..J..j..)U.
.|\.....m.S..=..%u..^.4.0...X1..55....g..|e..h^..V7.G.YzN..Cl:t..}.....^.. M..6..S..g..9..v.. Y.....9Umj..y.....I..0..J.. '2..\\...
0.Tm..q.B..].....
..P..|.DL2..|.r.D..|.D..{.Y..lg..|.J.f.P..&..B.m.n..{|&..... N6c..LB..'m<|f.m@P.vZ..+,1..?*U..4..%.!..a.0..|g..#.U.._I.q.0.....4..agn.....rq.
[..P..*{Z3..M..?..Se.....
!|c.jL..D]\$.#..x..t..TA..S1..#..]s..e..U..x..... <2..'.0..Yci.c.0]-
Y...H..&iek.w..0..#.S..@..]p.O.R.F..
.../..n..AW..S..7..Q1..Z..}..7..U..81..".awC..sN.._..1.S?..4..,...,..S..e..D..d..h..q)..,..e..#R".....i..\$.K..u..N..o..f[.9....(8..jr..5..Lk..,
..S..0..T7..f..b..>=ix..Vpu..se..D..|^..8..E..n..w1J..z..k8..}..F../~
4.K..~..t..@..x..<A%Aa..n}o..N..t..|.D..Y.Q..z..VJ..a..ja...
..L..[..%..ph.....
.....s..b..i.....V.M6\$. (T.....\.. 0cS
..C..0..i..z..R..dq..i..@..x..@..Q..1..c..6..|..
..7/....3BQ..v..|QY..=...&..7x8(..1..C..konL+..+..^C..Z..0..0..[s...
\$.b..t..|BL..Li..L..td0..^..j..m..p..};..&..+..

When we analysed, we could see 2 colours: red and blue. Blue is answer from the server, red is answer from the client side. All what we see it is called a **dialogue box**. It is difficult to understand what is in blue because it is **gzip compressed**.

HTTP Stream:



tcp.stream eq 80								
No.	Time	Source	Destination	Protocol	Length	Stream index	Stream index	Info
.. 30.670..	192.168.0.81	8.238.11.126	TCP	66	80	80	59415 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
.. 30.692..	8.238.11.126	192.168.0.81	TCP	66	80	80	80 80 + 59415 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128	
.. 30.692..	192.168.0.81	8.238.11.126	TCP	54	80	80	80 59415 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0	
.. 30.692..	192.168.0.81	8.238.11.126	HTTP	341	80	80	80 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?76b9e195bf080abe HTTP/1.1	
.. 30.714..	8.238.11.126	192.168.0.81	TCP	56	80	80	80 80 + 59415 [ACK] Seq=1 Ack=288 Win=64128 Len=0	
.. 30.714..	8.238.11.126	192.168.0.81	HTTP	389	80	80	80 HTTP/1.1 304 Not Modified	
.. 30.814..	192.168.0.81	8.238.11.126	HTTP	335	80	80	80 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?909c4a4c2f700f49 HTTP/1.1	
.. 30.833..	8.238.11.126	192.168.0.81	HTTP	392	80	80	80 HTTP/1.1 304 Not Modified	
.. 30.876..	192.168.0.81	8.238.11.126	HTTP	336	80	80	80 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?59a825ac88d45fbe HTTP/1.1	
.. 30.892..	8.238.11.126	192.168.0.81	HTTP	391	80	80	80 HTTP/1.1 304 Not Modified	

We see TCP Stream 80 at the bottom. All the screen is on green also stream index is 80 and the same value for all lines, which is normal behaviour. The protocol is HTTP. The last row shows more details. (synchronised, acknowledged, length, etc.)

When we click stream we see dialogue box.

Wireshark · Follow HTTP Stream (tcp.stream eq 80) · WiFi

```

GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?76b9e195bf080abe HTTP/1.1
Connection: Keep-Alive
Accept: /*
If-Modified-Since: Thu, 10 Dec 2020 22:11:52 GMT
If-None-Match: "084627641cf61:0"
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctld1.windowsupdate.com

HTTP/1.1 304 Not Modified
Date: Fri, 26 Feb 2021 19:46:26 GMT
Connection: keep-alive
Cache-Control: public, max-age=3600
ETag: "084627641cf61:0"
Expires: Fri, 26 Feb 2021 20:46:26 GMT
Last-Modified: Thu, 10 Dec 2020 22:11:52 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-CID: 3
X-CCC: UK
MSREGION: EMEA
Age: 9

GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?909c4a4c2f700f49 HTTP/1.1
Connection: Keep-Alive
Accept: /*
If-Modified-Since: Fri, 15 Jan 2021 00:46:38 GMT
If-None-Match: "0ebbae1d7ead61:0"
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctld1.windowsupdate.com

HTTP/1.1 304 Not Modified
Date: Fri, 26 Feb 2021 19:11:13 GMT
Connection: keep-alive
Cache-Control: public, max-age=3600
ETag: "0ebbae1d7ead61:0"
Expires: Fri, 26 Feb 2021 20:11:13 GMT
Last-Modified: Fri, 15 Jan 2021 00:46:38 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Age: 9

Packet 5447. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (1860 bytes)
Find: Filter Out This Stream

```

```

Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-CID: 3
X-CCC: UK
MSREGION: EMEA
Age: 2122

GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?59a825ac88d45fbe HTTP/1.1
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Fri, 02 Jun 2017 17:39:05 GMT
If-None-Match: "80424021c7dbd21:0"
User-Agent: Microsoft-CryptoAPI/10.0
Host: ctld1.windowsupdate.com

HTTP/1.1 304 Not Modified
Date: Fri, 26 Feb 2021 19:34:51 GMT
Connection: keep-alive
Cache-Control: public, max-age=3600
ETag: "80424021c7dbd21:0"
Expires: Fri, 26 Feb 2021 20:34:51 GMT
Last-Modified: Fri, 02 Jun 2017 17:39:05 GMT
Server: Microsoft-IIS/8.5
x-ccc: UK
x-cid: 3
X-Powered-By: ASP.NET
MSRegion: EMEA
Age: 704

3 client pkts, 3 server pkts, 5 turns.
Entire conversation (1860 bytes)
Find: Filter Out Th

```

Blue comes from client, red comes from the server. Content is also compressed, as we can't see more details (structure of html etc)

Summary:

"There is a difference between following a **TCP stream** and a **HTTP stream**. For example, if the data downloaded from the webserver is gzip compressed, following the TCP stream will display the compressed data, while following the HTTP stream will display the decompressed data"¹⁶

Can you filter to view packets only from specific sources or destinations?

Colour coding:

Purple – TCP traffic

Blue- UDP traffic

Black- packet with errors

¹⁶ <https://blog.didierstevens.com/2017/08/23/wireshark-follow-streams/>

Wireshark - Coloring Rules Default

Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3 icmpv6.type eq 4
ARP	arp
ICMP	icmp icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.4 && ip.ttl < 5 && !ipim && !ospf) (ip.dst == 224.0.0.24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp.eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad" sctp.checksum.status == "Bad"))
Checksum Errors	eth.fcs.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad" sctp.checksum.status == "Bad"
SMB	smb nbss nbns netbios
HTTP	http tcp.port == 80 http2
DCERPC	dcerpc
Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1
System Event	systemd_journal sysdig

Capture-> Capture Filters

Wireshark - Capture Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org
icmp	ip host host.example.com
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

<C:\Users\Home\AppData\Roaming\Wireshark\filters>

+ - OK Cancel Help

Analyse->Display Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}
New display filter	ip.addr == host.example.com
icmp	ip.addr == host.example.com
ping	icmp

Analyze Statistics Telephony Wireless Tools Help

- Display Filters...
- Display Filter Macros...
- Display Filter Expression...
- Apply as Column Ctrl+Shift+I
- Apply as Filter ▾
- Prepare a Filter ▾
- Conversation Filter ▾
- Enabled Protocols... Ctrl+Shift+E
- Decode As...
- Reload Lua Plugins Ctrl+Shift+L
- SCTP ▾
- Follow ▾
- Show Packet Bytes... Ctrl+Shift+O
- Expert Information

Index	Stream index	Info
0	0	59716 → 8
0	0	8009 → 59
0	0	59716 → 8
0	0	59716 → 8

CIP Connection → 59
 Ethernet → 8
 F5 TCP → 59
 F5 UDP → 8
 F5 IP → 8
 IEEE 802.15.4 → 8
IPv4 → 8
 IPv6 → 8
 TCP → 8
 UDP → 59
 ZigBee Network Layer → 8
 PN-IO AR → 8
 PN-IO AR (with data) → 8
 PN-CBA Err → 8

In the green field we see:

(ip.addr eq 192.168.0.81 and ip.addr eq 192.168.0.69) and (tcp.port eq 59716 and tcp.port eq 8009)

We see ip address: 192.168.0.81 and ip address 192.168.0.69 and we try investigate how to guess where there are come from. We have used command prompt appropriate command to get this info.

After writing ipconfig in command prompt I see this: (Command prompt runs as ADMIN)

```
c:\ Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 10:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Wireless LAN adapter WiFi:
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::dcf5:289b:f34c:bfbe%8
IPv4 Address. . . . . : 192.168.0.81
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Ethernet adapter vEthernet (Default Switch):
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::597f:e264:7392:4ae5%27
IPv4 Address. . . . . : 172.23.0.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
```

IPV4 Address is: 192.168.0.81

I put in command prompt **arp- a** command line and we see this:

```
C:\Users\Home>arp -a

Interface: 192.168.0.81 --- 0x8
Internet Address      Physical Address      Type
 192.168.0.1            40-0d-10-c0-43-38    dynamic
 192.168.0.69           f0-ef-86-4a-2e-15    dynamic
 192.168.0.255          ff-ff-ff-ff-ff-ff    static
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251             01-00-5e-00-00-fb    static
 224.0.0.252             01-00-5e-00-00-fc    static
 239.255.255.250         01-00-5e-7f-ff-fa    static

Interface: 169.254.61.64 --- 0x12
Internet Address      Physical Address      Type
 169.254.255.255        ff-ff-ff-ff-ff-ff    static
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251             01-00-5e-00-00-fb    static
 224.0.0.252             01-00-5e-00-00-fc    static
 239.255.255.250         01-00-5e-7f-ff-fa    static
 255.255.255.255         ff-ff-ff-ff-ff-ff    static

Interface: 172.23.0.1 --- 0x1b
Internet Address      Physical Address      Type
 172.23.15.255          ff-ff-ff-ff-ff-ff    static
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251             01-00-5e-00-00-fb    static
 239.255.255.250         01-00-5e-7f-ff-fa    static
```

We see that physical address¹⁷ can be static¹⁸ or dynamic¹⁹

We see 3 interfaces²⁰; first where we have dynamic and static, second one and third one with static only.

The available options after arp are:

¹⁷ is a memory address that is represented in the form of a binary number on the address bus circuitry.

¹⁸ Address which does not change.

¹⁹ dynamic IP addresses are subject to change, sometimes at a moment's notice. Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.

²⁰ 172... is class B type of address, 169 is automatic Private IP Address (APIPA)

```
C:\Users\Home>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.
```

Using other than arp – a option the results are shown below:

```
C:\Users\Home>arp -g

Interface: 192.168.0.81 --- 0x8
  Internet Address      Physical Address      Type
  192.168.0.1           40-0d-10-c0-43-38    dynamic
  192.168.0.69          f0-ef-86-4a-2e-15    dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22             01-00-5e-00-00-16    static
  224.0.0.251            01-00-5e-00-00-fb    static
  224.0.0.252            01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 169.254.61.64 --- 0x12
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff    static
  224.0.0.22             01-00-5e-00-00-16    static
  224.0.0.251            01-00-5e-00-00-fb    static
  224.0.0.252            01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 172.23.0.1 --- 0x1b
  Internet Address      Physical Address      Type
  172.23.15.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22             01-00-5e-00-00-16    static
  224.0.0.251            01-00-5e-00-00-fb    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
```

```
C:\Users\Home>arp -v

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212  00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                      .... Displays the arp table.
```

```
C:\Users\Home>arp -innet_adr

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.

-g          Same as -a.

-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.

inet_addr   Specifies an internet address.

-N if_addr  Displays the ARP entries for the network interface specified
           by if_addr.

-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.

-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.

eth_addr    Specifies a physical address.

if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
```

```
C:\Users\Home>arp -N_if_addr

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                      .... Displays the arp table.
```

```
C:\Users\Home>arp -s

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
           entries and entries on the loop-back interface will be shown.
inet_addr   Specifies an internet address.
-N if_addr   Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-AA-00-62-C6-09 .... Adds a static entry.
> arp -a                         .... Displays the arp table.
```

arp -d when Wireshark is running.

Any changes in command prompt after writing this command.

```
C:\WINDOWS\system32>arp -d
```

ipconfig/ flushdns

```
C:\WINDOWS\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\WINDOWS\system32>
```

Gratuitous ARP

- is a situation when ARP response was not initiated by ARP request,
- sent as a broadcast,

- it is different than traditional²¹ ARP behaviour,

By the use of ipconfig/all I have tried to find MAC address (physical add)

```
Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . .
  Description . . . . . : Intel(R) Dual Band Wireless-AC 7260
  Physical Address. . . . . : A0-A8-CD-81-B3-4D
  DHCP Enabled. . . . . : Yes
  Status. . . . . : Media connected
```

```
Windows IP Configuration

  Host Name . . . . . : DESKTOP-NKECTCQ
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
```

IP routing is not enabled.

arp gratuitous

no results in command prompt!

*

pathping -g host-list

```
C:\Users\Home>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                 [-p period] [-q num_queries] [-w timeout]
                 [-4] [-6] target_name

Options:
  -g host-list      Loose source route along host-list.
  -h maximum_hops  Maximum number of hops to search for target.
  -i address        Use the specified source address.
  -n               Do not resolve addresses to hostnames.
  -p period         Wait period milliseconds between pings.
  -q num_queries   Number of queries per hop.
  -w timeout        Wait timeout milliseconds for each reply.
  -4               Force using IPv4.
  -6               Force using IPv6.

C:\Users\Home>pathping -g host-list
Unable to resolve target system name host-list.
```

²¹ "where a node is requesting another node's MAC address"
<https://www.practicalnetworking.net/series/arp/gratuitous-arp/>

netstat

"displays network connections for TCP (both incoming and outgoing), routing table, and a number of network interface and network protocol statistics."²² We have seen TCP protocol, foreign addresses²³ and local address²⁴. The majority states²⁵ are established except of 3 lines.

```
C:\Users\Home>netstat

Active Connections

Proto  Local Address          Foreign Address        State
TCP    192.168.0.81:54115    40.67.254.36:https  ESTABLISHED
TCP    192.168.0.81:58313    5.62.54.63:http    ESTABLISHED
TCP    192.168.0.81:58317    52.97.202.98:https ESTABLISHED
TCP    192.168.0.81:58823    ws-in-f188:5228   ESTABLISHED
TCP    192.168.0.81:58825    192.168.0.69:8009 ESTABLISHED
TCP    192.168.0.81:58890    static:https     ESTABLISHED
TCP    192.168.0.81:59130    host:https      ESTABLISHED
TCP    192.168.0.81:59259    mrs04s10-in-f238:https ESTABLISHED
TCP    192.168.0.81:59260    lhr25s28-in-f3:https ESTABLISHED
TCP    192.168.0.81:59261    lhr25s28-in-f14:https ESTABLISHED
TCP    192.168.0.81:59266    lhr48s22-in-f4:https ESTABLISHED
TCP    192.168.0.81:59268    cpc25-finc13-2-0-cust8:http  TIME_WAIT
TCP    192.168.0.81:59269    93.184.221.240:http   TIME_WAIT
TCP    192.168.0.81:59270    cpc3-stme1-3-0-cust210:http TIME_WAIT
TCP    192.168.0.81:59271    52.114.75.150:https  ESTABLISHED
TCP    192.168.0.81:59272    13.107.21.200:https ESTABLISHED
TCP    192.168.0.81:59276    bingforbusiness:https ESTABLISHED
TCP    192.168.0.81:59277    bingforbusiness:https ESTABLISHED
TCP    192.168.0.81:59279    52.97.211.162:https ESTABLISHED
TCP    192.168.0.81:59280    52.97.211.162:https ESTABLISHED
TCP    192.168.0.81:59282    204.79.197.222:https ESTABLISHED
TCP    192.168.0.81:59285    152.199.19.161:https ESTABLISHED
TCP    192.168.0.81:59286    131.253.33.254:https ESTABLISHED
TCP    192.168.0.81:59287    51.140.152.167:https ESTABLISHED
```

nslookup.exe

```
C:\Users\Home>nslookup.exe
Default Server: cache1.service.virginmedia.net
Address: 194.168.4.100
```

We use for troubleshooting DNS servers. My internet provider is Virgin Media.

²² <https://en.wikipedia.org/wiki/Netstat>

²³ The address and **port** number of the remote end of the connection.

²⁴ The address details of the local end of the connection.

²⁵ State of the local socket. "The possible states are as follows: CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND, and TIME_WAIT"

net use

```
> net use
Server: use
Address: 92.242.132.24

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to use timed-out
>
```

“Execute the net use command alone to show detailed information about currently mapped drives and devices”²⁶

We can filter by writing in the field what exactly we are looking for; for example, I wrote TCP

No.	Time	Source	Destination	Protocol	Length	Stream index	Stream index	Info
1	0.000000	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=110 [TCP segm...
2	0.004431	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=1 Ack=111 Win=296 Len=110 [TCP se...
3	0.046793	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=111 Ack=111 Win=512 Len=0
4	1.779340	192.168.0.81	216.58.212.194	TLSv1.2	766	1	1	1 Application Data
5	1.779827	192.168.0.81	216.58.212.194	TLSv1.2	815	1	1	1 Application Data
6	1.801516	216.58.212.194	192.168.0.81	TCP	56	1	1	1 443 → 59923 [ACK] Seq=1 Ack=713 Win=694 Len=0
7	1.803092	192.168.0.81	216.58.212.194	TLSv1.2	759	1	1	1 Application Data
8	1.807154	216.58.212.194	192.168.0.81	TCP	56	1	1	1 443 → 59923 [ACK] Seq=1 Ack=1474 Win=705 Len=0
9	1.816352	216.58.212.194	192.168.0.81	TLSv1.2	141	1	1	1 Application Data
...	1.816873	192.168.0.81	216.58.212.194	TLSv1.2	93	1	1	1 Application Data
...	1.820784	216.58.212.194	192.168.0.81	TLSv1.2	124	1	1	1 Application Data
...	1.820784	216.58.212.194	192.168.0.81	TLSv1.2	85	1	1	1 Application Data
...	1.820867	192.168.0.81	216.58.212.194	TCP	54	1	1	1 59923 → 443 [ACK] Seq=2218 Ack=189 Win=512 Len=0
...	1.828788	216.58.212.194	192.168.0.81	TCP	60	1	1	1 443 → 59923 [ACK] Seq=189 Ack=2179 Win=716 Len=0
...	1.835451	216.58.212.194	192.168.0.81	TCP	60	1	1	1 443 → 59923 [ACK] Seq=189 Ack=2218 Win=716 Len=0
...	1.838160	216.58.212.194	192.168.0.81	TLSv1.2	124	1	1	1 Application Data
...	1.838160	216.58.212.194	192.168.0.81	TLSv1.2	85	1	1	1 Application Data
...	1.838160	216.58.212.194	192.168.0.81	TLSv1.2	93	1	1	1 Application Data
...	1.838198	192.168.0.81	216.58.212.194	TCP	54	1	1	1 59923 → 443 [ACK] Seq=2218 Ack=329 Win=511 Len=0
...	1.838597	192.168.0.81	216.58.212.194	TLSv1.2	93	1	1	1 Application Data
...	1.866801	216.58.212.194	192.168.0.81	TCP	60	1	1	1 443 → 59923 [ACK] Seq=329 Ack=2257 Win=716 Len=0
...	2.818592	192.168.0.81	216.58.212.194	TLSv1.2	545	2	2	2 Application Data
...	2.850497	216.58.212.194	192.168.0.81	TCP	56	2	2	2 443 → 59923 [ACK] Seq=1 Ack=492 Win=708 Len=0
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF_{6268479B-8D09-46DA-8321-029BC0EA66CF}, id 0								
> Ethernet II, Src: IntelCor_81:b3:4d (a0:a8:cd:81:b3:4d), Dst: Google_Google (f0:ef:86:4a:2e:15)								
> Internet Protocol Version 4, Src: 192.168.0.81, Dst: 192.168.0.69								
> Transmission Control Protocol, Src Port: 59716, Dst Port: 8009, Seq: 1, Ack: 1, Len: 110								
0000	f0 ef 86 4a 2e 15 a0 a8	cd 81 b3 4d 08 00 45 00	...J....	...M..E.				
0010	00 96 57 0f 40 00 80 06	21 6c c0 a8 00 51 c0 a8	..W@....	!l...Q...				
0020	00 45 e9 44 1f 49 41 5a	e0 75 e5 55 35 86 50 18	·E·D·IAZ	·u·U5·P·				
0030	02 00 d2 87 00 00 17 03	03 00 69 fd 0c a4 a1 b0i.....				
0040	c1 e0 26 fb 97 e2 c4 8b	b0 3a bc 52 b3 2e 62 6c	..&....	::R..bl				
0050	20 b9 fa f4 d0 70 f3 41	f1 4b 4c c3 82 5f bb 92p·A	·KL....				

²⁶ <https://www.lifewire.com/net-use-command-2618096>

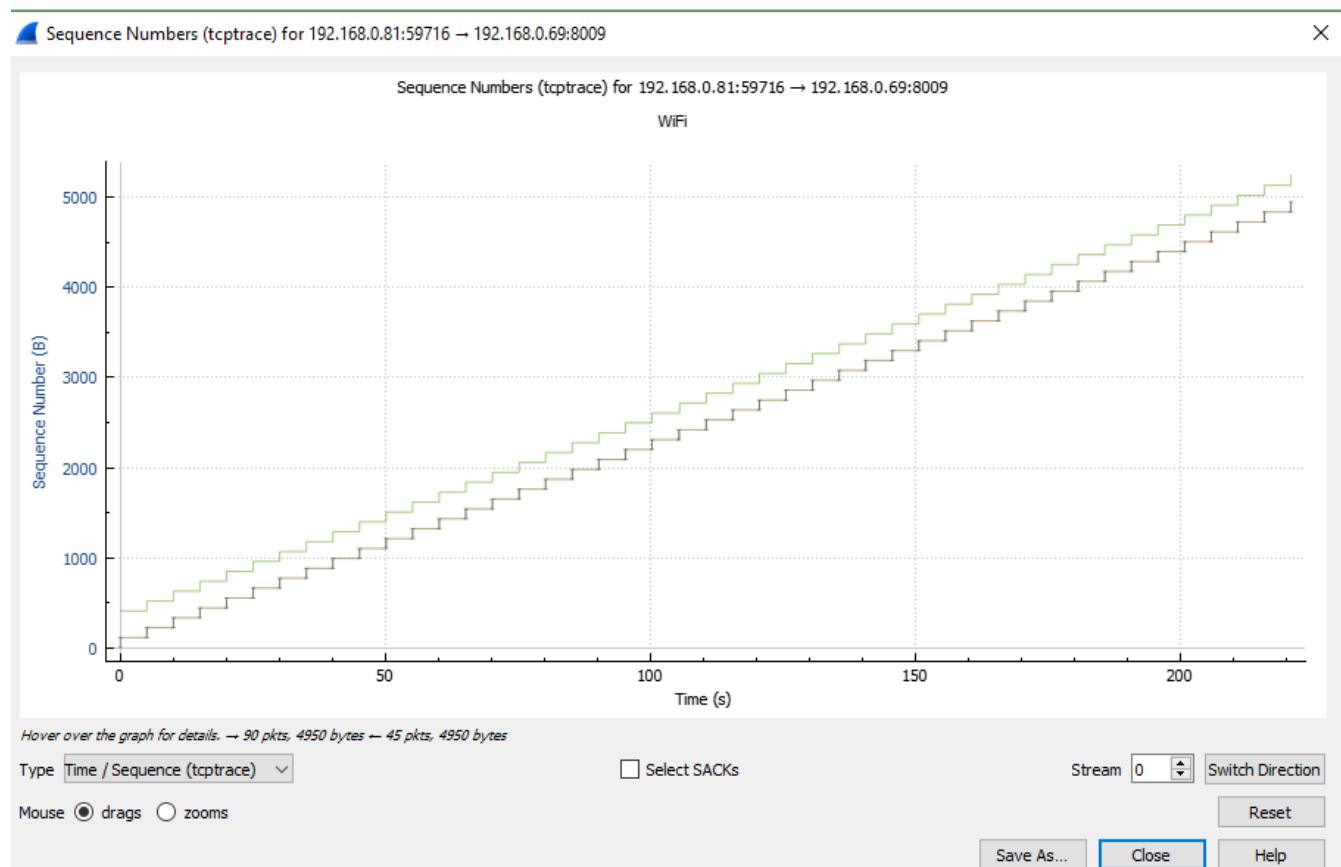
I have seen TCP protocol as filter has been used. We have a list what we are looking for we should select:

No.	tcp.stream == 0
1	tcp.stream eq 80
2	tcp.stream eq 21
3	tcp.stream eq 3
4	tcp.stream == 0
5	tcp.stream eq 1
6	tcp.port == 80 udp.port == 80
7	tcp
8	tcp.options.cc
9	tcp.options.ccecho
10	tcp.options.ccnew
11	tcp.options.echo
12	tcp.options.echoreply
13	tcp.options.eol
14	tcp.options.experimental
15	tcp.options.md5
16	tcp.options.mss
17	tcp.options.nop
18	tcp.options.qs
19	tcp.options.rvbd.probe
20	1.0.0.100 210.0.212.194 192.1
21	1 888160 216 58 212 194 192.1

For example `tcp.stream==0`

No.	Time	Source	Destination	Protocol	Length	Stream index	Stream index	Info
1	0.000000	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=110 [TCP segment of a reassembled PDU]
2	0.004431	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=1 Ack=111 Win=296 Len=110 [TCP segment of a reassembled PDU]
3	0.046793	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=111 Ack=111 Win=512 Len=0
4	0.0505497	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=512 Len=110 [TCP segment of a reassembled PDU]
5	0.010268	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=111 Ack=221 Win=296 Len=110 [TCP segment of a reassembled PDU]
6	0.052300	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=221 Ack=221 Win=511 Len=0
7	0.0161...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=221 Ack=221 Win=511 Len=110 [TCP segment of a reassembled PDU]
8	0.0022...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=221 Ack=331 Win=296 Len=110 [TCP segment of a reassembled PDU]
9	0.0063...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=331 Ack=331 Win=511 Len=0
10	0.023...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=331 Ack=331 Win=110 [TCP segment of a reassembled PDU]
11	0.027...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=331 Ack=441 Win=296 Len=110 [TCP segment of a reassembled PDU]
12	0.076...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=441 Ack=441 Win=511 Len=0
13	0.038...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=441 Ack=441 Win=511 Len=110 [TCP segment of a reassembled PDU]
14	0.043...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=441 Ack=551 Win=296 Len=110 [TCP segment of a reassembled PDU]
15	0.084...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=551 Ack=551 Win=510 Len=0
16	0.051...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=551 Ack=551 Win=510 Len=110 [TCP segment of a reassembled PDU]
17	0.060...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=551 Ack=661 Win=296 Len=110 [TCP segment of a reassembled PDU]
18	0.113...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=661 Ack=661 Win=510 Len=0
19	0.064...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=661 Ack=661 Win=110 [TCP segment of a reassembled PDU]
20	0.070...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=661 Ack=771 Win=296 Len=110 [TCP segment of a reassembled PDU]
21	0.113...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=771 Ack=771 Win=509 Len=0
22	0.083...	192.168.0.81	192.168.0.69	AJP13	164	0	0	0 AJP13 Error? [TCP segment of a reassembled PDU]
23	0.089...	192.168.0.69	192.168.0.81	AJP13	164	0	0	0 AJP13 Error? [TCP segment of a reassembled PDU]
24	0.130...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=881 Ack=881 Win=509 Len=0
25	0.090...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=881 Ack=881 Win=509 Len=110 [TCP segment of a reassembled PDU]
26	0.095...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=881 Ack=991 Win=296 Len=110 [TCP segment of a reassembled PDU]
27	0.135...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=991 Ack=991 Win=508 Len=0
28	0.107...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=991 Ack=991 Win=508 Len=110 [TCP segment of a reassembled PDU]
29	0.112...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=991 Ack=1101 Win=296 Len=110 [TCP segment of a reassembled PDU]
30	0.154...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=1101 Ack=1101 Win=508 Len=0
31	0.123...	192.168.0.81	192.168.0.69	TCP	164	0	0	0 59716 → 8009 [PSH, ACK] Seq=1101 Ack=1101 Win=508 Len=110 [TCP segment of a reassembled PDU]
32	0.128...	192.168.0.69	192.168.0.81	TCP	164	0	0	0 8009 → 59716 [PSH, ACK] Seq=1101 Ack=1211 Win=296 Len=110 [TCP segment of a reassembled PDU]
33	0.170...	192.168.0.81	192.168.0.69	TCP	54	0	0	0 59716 → 8009 [ACK] Seq=1211 Ack=1211 Win=508 Len=0

We have an option to have detailed info.



Should this software be freely available – considering its potential for misuse?

It is controversial subject; it can be used for the network analyses for education purpose, but from the other side allow the hackers to sniffer password, get personal information etc.

"That is also why securing and encrypting data is so important."²⁷ "Packet sniffing programs can be used to perform man-in-the-middle attacks (MITM). This type of attack occurs when "an attacker monitors network packets, modifies them, and inserts them back to the network" (Whitman, et al., 2008)"²⁸ We should focus on encryption as the best form of protection against any packet interception.

Week 20

ARP

The screenshots from my computer are attached in previous week. ARP means address resolution protocol, which is used by IP mainly by IPV4 to map IP network addresses to the

²⁷<https://www.ukessays.com/essays/information-technology/the-threat-of-packet-sniffers-information-technology-essay.php>

²⁸ Packet sniffing programs can be used to perform man-in-the-middle attacks (MITM). This type of attack occurs when "an attacker monitors network packets, modifies them, and inserts them back to the network" (Whitman, et al., 2008)

hardware addresses by use a data link protocol. Simple speaking arp helps to find an address of a computer in a network. The address resolution activity is related to an answer from the server which contains the address to a client. The hardware address is known as MAC²⁹ address. " Each computer network interface card is allocated a globally unique 6 byte link address when the factory manufactures the card (stored in a PROM)." ³⁰

Format of arp message

0	8	15_16	31
Hardware Type		Protocol Type	
HLEN	PLEN	Operation	
Sender HA (octets 0-3)			
Sender HA (octets 4-5)	Sender IP (octets 0-1)		
Sender IP (octets 2-3)	Target HA (octets 0-1)		
Target HA (octets 2-5)			
Target IP (octets 0-3)			

```
> arp -a
Unrecognized command: arp -a
> arp-a
Server: cache1.service.virginmedia.net
Address: 194.168.4.100

Non-authoritative answer:
Name:    arp-a
Address: 92.242.132.24
```

By the help of Powershell 5.0 We can see host name, physical address, IPV4, subnet mask etc.

²⁹ Medium Access Control

³⁰ <https://erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>

```
PS C:\WINDOWS\system32> ipconfig /all

Windows IP Configuration

 Host Name . . . . . : DESKTOP-NKECTCQ
 Primary Dns Suffix . . . . . :
 Node Type . . . . . : Hybrid
 IP Routing Enabled. . . . . : No
 WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

 Media State . . . . . : Media disconnected
 Connection-specific DNS Suffix . . . . . :
 Description . . . . . : Intel(R) Ethernet Connection I218-LM
 Physical Address. . . . . : EC-F4-BB-4B-67-A6
 DHCP Enabled. . . . . : Yes
 Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Npcap Loopback Adapter:

 Connection-specific DNS Suffix . . . . . :
 Description . . . . . : Npcap Loopback Adapter
 Physical Address. . . . . : 02-00-4C-4F-4F-50
 DHCP Enabled. . . . . : Yes
 Autoconfiguration Enabled . . . . . : Yes
 Link-local IPv6 Address . . . . . : fe80::8893:6b3b:c872:3d40%18(PREFERRED)
 Autoconfiguration IPv4 Address. . . . . : 169.254.61.64(PREFERRED)
 Subnet Mask . . . . . : 255.255.0.0
 Default Gateway . . . . . :
 DHCPv6 IAID . . . . . : 704774220
 DHCPv6 Client DUID. . . . . : 00-01-00-01-24-22-22-D4-EC-F4-BB-4B-67-A6
 DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
 NetBIOS over Tcpip. . . . . : Enabled
```

```
Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address. . . . . : 00-15-5D-DD-4C-D3
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f8f4:fd19:ec7c:b8ad%25(Preferred)
IPv4 Address. . . . . : 172.27.128.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 419435869
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-22-22-D4-EC-F4-BB-4B-67-A6
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
PS C:\WINDOWS\system32>
```

The same info by command line:

```
Ethernet adapter vEthernet (Default Switch):

Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Hyper-V Virtual Ethernet Adapter
Physical Address . . . . . : 00-15-5D-DD-4C-D3
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f8f4:fd19:ec7c:b8ad%25(PREFERRED)
IPv4 Address. . . . . : 172.27.128.1(PREFERRED)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 419435869
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-22-22-D4-EC-F4-BB-4B-67-A6
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

C:\WINDOWS\system32>s
```

DHCP

Dynamic Host Configuration Protocol

- network management protocol,
- used on IP local area networks,
- must be present on the network,
- “a device connected to the network requests an IP address from the DHCP server using the DHCP protocol;”³¹
- uses User Datagram Protocol.

“DHCP can assign much more than just the IP address, but assigning the IP address is a primary purpose. Other information commonly assigned by DHCP includes the following: Subnet mask Default gateway DNS server address”³²

“Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually; IP addresses for computers that are removed from the network must be manually reclaimed. With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network”³³

³¹ https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

³² CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 120

³³ <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>

Benefits of DHCP: reliable IP address configuration, reduced network administration.

Ipcconfig /all We are looking for DHCP enabled etc.

DHCP Configuration

```

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
  Description . . . . . : Bluetooth Device (Personal Area Network)
  Physical Address. . . . . : A0-A8-CD-81-B3-51
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

  Connection-specific DNS Suffix . :
  Description . . . . . : Hyper-V Virtual Ethernet Adapter
  Physical Address. . . . . : 00-15-5D-DD-4C-D3
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::f8f4:fd19:ec7c:b8ad%25(PREFERRED)
  IPv4 Address. . . . . : 172.27.128.1(PREFERRED)
  Subnet Mask . . . . . : 255.255.240.0
  Default Gateway . . . . . :
  DHCPv6 IAID . . . . . : 419435869
  DHCPv6 Client DUID. . . . . : 00-01-00-01-24-22-22-D4-EC-F4-BB-4B-67-A6
  DNS Servers . . . . . :
    fec0:0:0:ffff::1%1
    fec0:0:0:ffff::2%1
    fec0:0:0:ffff::3%1
  NetBIOS over Tcpip. . . . . : Enabled

C:\WINDOWS\system32>
```

```

DHCPv6 IAID . . . . . : 419435869
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-22-22-D4-EC-F4-BB-4B-67-A6
```

“**DHCPv6** uses basically the same scheme, but makes the Client ID mandatory and imposes structure on it. The Client ID in DHCPv6 consists of two parts: a DHCP Unique Identifier (DUID) and an Identity Association Identifier (IAID). The DUID identifies the client **system** (rather than just an interface, as in DHCPv4), and the IAIID identifies the interface on that system”³⁴

³⁴<https://docs.oracle.com/cd/E19253-01/816-4554/clientid/index.html>

Renew DHCP-Assigned Address Lease

```
C:\WINDOWS\system32>ipconfig /renew
Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
```

Release DHCP-Assigned Address

As media is disconnected any further steps cannot be done.

```
C:\WINDOWS\system32>ipconfig /release
Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter vEthernet (Default Switch):
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::f8f4:fd19:ec7c:b8ad%25
  IPv4 Address. . . . . : 172.27.128.1
  Subnet Mask . . . . . : 255.255.240.0
  Default Gateway . . . . . :

Ethernet adapter Npcap Loopback Adapter:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::8893:6b3b:c872:3d40%18
  Autoconfiguration IPv4 Address. . . : 169.254.61.64
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :
```

```
Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
```

```
Wireless LAN adapter WiFi:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::dcf5:289b:f34c:bfbe%6
  Default Gateway . . . . . :
```

Ethernet adapter Bluetooth Network Connection:

```
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
```

```
C:\WINDOWS\system32>
```

DNS

A Gratuitous ARP if possible explained – with source and destination explained.

Ping I have tried ping www.google.com

```
C:\WINDOWS\system32>ping google.com

Pinging google.com [216.58.213.110] with 32 bytes of data:
Reply from 216.58.213.110: bytes=32 time=18ms TTL=115
Reply from 216.58.213.110: bytes=32 time=20ms TTL=115
Reply from 216.58.213.110: bytes=32 time=15ms TTL=115
Reply from 216.58.213.110: bytes=32 time=23ms TTL=115

Ping statistics for 216.58.213.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 23ms, Average = 19ms
```

- use to troubleshoot connectivity, name resolution and reachability.
- TTL³⁵= time to live (115 seconds)
- there is no loss of data (0%) 4 packets have been sent and 4 have been received.
- At the bottom there is a statistic shows approximate round trip times in milli-seconds; minimum was 15 milliseconds.

Ping www.google.com /t

Parameter	Description
/t	Specifies ping continue sending echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL+ENTER. To interrupt and quit this command, press CTRL+C.

³⁵ “It is a value on an **ICMP** packet that prevents that packet from propagating back and forth between hosts ad infinitum. Each router that touches the packet decrements the **TTL**. If the **TTL** ever reaches zero, the packet is discarded. It's also a measure of how many hops the packet took”, https://answers.microsoft.com/en-us/windows/forum/windows_xp-networking/what-is-it-ttl-which-shows-on-ping-report-and-the/5eb539d8-b9bc-4a16-bc3e-92fa5ca0bd16

```
microsoft Windows [Version 10.0.19042.804]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.google.com /t

Pinging www.google.com [216.58.204.228] with 32 bytes of data:
Reply from 216.58.204.228: bytes=32 time=28ms TTL=116
Reply from 216.58.204.228: bytes=32 time=21ms TTL=116
Reply from 216.58.204.228: bytes=32 time=26ms TTL=116
Reply from 216.58.204.228: bytes=32 time=19ms TTL=116
Reply from 216.58.204.228: bytes=32 time=19ms TTL=116
Reply from 216.58.204.228: bytes=32 time=19ms TTL=116
Reply from 216.58.204.228: bytes=32 time=18ms TTL=116
Reply from 216.58.204.228: bytes=32 time=26ms TTL=116
Reply from 216.58.204.228: bytes=32 time=18ms TTL=116
Reply from 216.58.204.228: bytes=32 time=23ms TTL=116
Reply from 216.58.204.228: bytes=32 time=19ms TTL=116
Reply from 216.58.204.228: bytes=32 time=25ms TTL=116
```

and it will continue until will be disrupted.

Ping www.google.com /a

/a Specifies reverse name resolution be performed on the destination IP address. If this is successful, ping displays the corresponding host name.

```
C:\WINDOWS\system32>ping www.google.com /a

Pinging www.google.com [216.58.204.228] with 32 bytes of data:
Reply from 216.58.204.228: bytes=32 time=21ms TTL=116
Reply from 216.58.204.228: bytes=32 time=40ms TTL=116
Reply from 216.58.204.228: bytes=32 time=21ms TTL=116
Reply from 216.58.204.228: bytes=32 time=17ms TTL=116

Ping statistics for 216.58.204.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 40ms, Average = 24ms
```

Ping www.google.com /4

/n <count> Specifies the number of echo Request messages be sent. The default is 4.

```
C:\WINDOWS\system32>ping www.google.com /4

Pinging www.google.com [216.58.204.228] with 32 bytes of data:
Reply from 216.58.204.228: bytes=32 time=21ms TTL=116
Reply from 216.58.204.228: bytes=32 time=21ms TTL=116
Reply from 216.58.204.228: bytes=32 time=17ms TTL=116
Reply from 216.58.204.228: bytes=32 time=19ms TTL=116

Ping statistics for 216.58.204.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 21ms, Average = 19ms
```

Ping www.google.com /R

/R Specifies the round-trip path is traced (available on IPv6 only).

```
C:\WINDOWS\system32>ping www.google.com /R
ping request could not find host www.google.com. Please check the name and try again.
```

Because available on IPV6, I have used IPV4 that is why it doesn't go through.

Tracert

- diagnostic tool,
- track in real time,
- keeps records time taken for each hop the packet makes during route to the destination.

```
Tracing route to google.com [216.58.213.110]
over a maximum of 30 hops:

 1  3 ms    3 ms    2 ms  192.168.0.1
 2  *        *        *      Request timed out.
 3  21 ms   23 ms   13 ms  hari-core-2a-xe-823-0.network.virginmedia.net [82.2.243.25]
 4  *        *        *      Request timed out.
 5  26 ms   13 ms   20 ms  tele-ic-7-ae2-0.network.virginmedia.net [62.253.175.34]
 6  14 ms   13 ms   15 ms  74-14-250-212.static.virginm.net [212.250.14.74]
 7  14 ms   24 ms   23 ms  108.170.246.161
 8  17 ms   32 ms   14 ms  216.239.57.121
 9  20 ms   17 ms   17 ms  lhr25s02-in-f14.1e100.net [216.58.213.110]

Trace complete.
```

I have tracert www.google.com

- ** appear when “that the router at that hop doesn't respond to the type of packet you were using for the traceroute”
- max 30 hops
- ms= milliseconds

- 192.168.0.1 is Default Gateway : 192.168.0.1
 (after checking ipconfig /all in command prompt)

Virgin Media is an internet provider

“This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer”³⁶

Tracert 11.1.0.1

```
Tracing route to 11.1.0.1 over a maximum of 30 hops

 1      3 ms      2 ms      2 ms  192.168.0.1
 2      *          *          *      Request timed out.
 3     10 ms     11 ms     11 ms  hari-core-2a-xe-823-0.network.virginmedia.net [82.2.243.25]
 4      *          *          *      Request timed out.
 5     17 ms     25 ms     20 ms  m686-mp2.cvx1-b.lis.dial.ntli.net [62.254.42.174]
 6     13 ms     15 ms     12 ms  213.46.174.86
 7     15 ms     14 ms     31 ms  100ge11-2.core1.lon2.he.net [184.104.195.109]
 8     84 ms     81 ms     81 ms  100ge15-2.core1.nyc5.he.net [184.105.81.41]
 9    104 ms     98 ms     99 ms  100ge10-1.core2.ash1.he.net [184.105.81.150]
10      *          *          *      Request timed out.
11      *          *          *      Request timed out.
12      *
```

192.168.0.1 is a default gateway

The packet travels through 2 routers 192.168.0.1 and 213.46.174.86 to get to host 11.1.0.1.

* ** appear when “that the router at that hop doesn't respond to the type of packet you were using for the traceroute”

tracert 22.110.0.1

Tracing route to 22.110.0.1 over a maximum of 30 hops.

³⁶ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tracert>

```
C:\WINDOWS\system32>tracert 22.110.0.1

Tracing route to 22.110.0.1 over a maximum of 30 hops

 1   3 ms    4 ms    2 ms  192.168.0.1
 2   *         *         * Request timed out.
 3  13 ms    12 ms   19 ms hari-core-2a-xe-823-0.network.virginmedia.net [82.2.243.25]
 4   *         *         * Request timed out.
 5  23 ms    18 ms   13 ms m686-mp2.csv1-b.lis.dial.ntli.net [62.254.42.174]
 6  12 ms    13 ms   13 ms 213.46.174.86
 7  14 ms    22 ms   33 ms 100ge11-2.core1.lon2.he.net [184.104.195.109]
 8  83 ms    84 ms   82 ms 100ge15-2.core1.nyc5.he.net [184.105.81.41]
 9  98 ms    94 ms   99 ms 100ge10-1.core2.ash1.he.net [184.105.81.150]
10   *         *         * Request timed out.
11   *         *         * Request timed out.
12   *         *         * Request timed out.
13   *         *         * Request timed out.
14   *         *         * Request timed out.
15   *         *         * Request timed out.
16   *         *         * Request timed out.
17
```

IP Internet Protocol

” is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication”³⁷

My Public IPv4 Is: 77.101.226.166	
Your IPv6 is: Not Detected	
My IP Location Info <small>?</small>	My IP Hostname
City: London State: England Country: United Kingdom of Great Britain and Northern Ireland Postal Code: WC2N Time Zone: +00:00	ISP: Virgin Media Limited Host Name: cpc93828-hari18-2-0-cust677.20-2.cable.virginm.net 5089

³⁷[https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20\(IP,interface%20identification%20and%20location%20addressing](https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20(IP,interface%20identification%20and%20location%20addressing)

IP Address Lookup	
IP:	77.101.226.166
IP Address	77.101.226.166
ASN	5089
City	London
State/Region	England
Country Code	United Kingdom of Great Britain and Northern Ireland
Postal Code	WC2N
ISP	Virgin Media Limited

IP WHOIS Lookup

To clarify, Lookup IP WHOIS information using the IP WHOIS Lookup tool for any allocated IP address. This tool will provide you with the [IP Address](#) owners contact information. To clarify, the results will also show the Regional Internet Registry (RIR) who assigns the IP, the assigned owner, location, contact information, and abuse reporting details. Furthermore, other important information includes how many IP Addresses are in the block or blocks assigned to the owner of the IP you're researching.

IPv4

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.

Both IP addresses and subnet masks are composed of 32 bits. They are typically presented as four decimal numbers divided by dots (also known as dotted decimal notation), but they can also be represented in binary. For example, consider the IP address of 192.168.1.5 with a subnet mask of 255.255.255.0. Both can be represented in binary as follows:

192.168.1.5 = 1100 0000.1010 1000.0000 0001.0000 0101

255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000³⁸

After ipconfig/all in command

Ethernet adapter Ethernet (Default Switch):

IPv4 Address.: 172.31.48.1(Preferred)

Wireless LAN adapter WiFi:

³⁸ CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 120

IPv4 Address.: 172.31.48.1(Preferred)

172,1,48 and 1 is composed of 8 bits each number;

For example:

172= 0 1 1 1 1 0 1 0

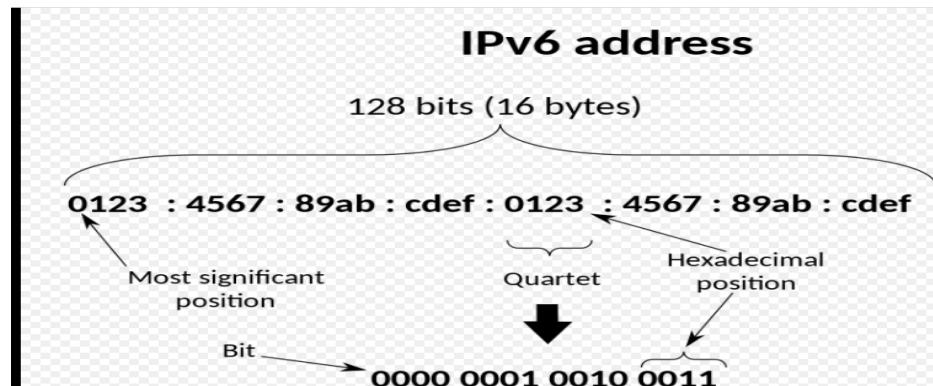
1=0 0 0 0 0 0 0 1

48=0 0 1 1 0 0 0 1

1=0 0 0 0 0 0 0 1

At the end we have 32 bits (IPV4)

IPV6:



"the address size was increased from 32 bits in IPv4 to 128 bits, thus providing up to 2^{128} (approximately 3.403×10^{38}) addresses"³⁹ ... " IPv6 has facilities that automatically change the routing prefix of entire networks, should the global connectivity or the routing policy change, without requiring internal redesign or manual renumbering."⁴⁰

" IPv6 addresses can omit leading zeroes and use zero compression to shorten the way the address is displayed without changing the actual address. IPv6 addresses use 32 hexadecimal characters. Each hexadecimal character represents four bits for a total of 128 bits (4×128)"⁴¹

"Instead of displaying groups of zeros, you can use a double colon to replace one or more such zero-value groups. For example, either of the following two IPv6 addresses represents the same address:

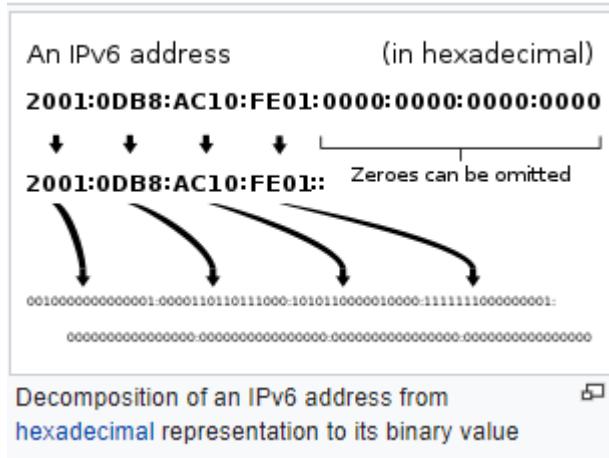
³⁹[https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20\(IP,interface%20identification%20and%20location%20addressing](https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20(IP,interface%20identification%20and%20location%20addressing)

⁴⁰[https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20\(IP,interface%20identification%20and%20location%20addressing](https://en.wikipedia.org/wiki/IP_address#:~:text=An%20Internet%20Protocol%20address%20(IP,interface%20identification%20and%20location%20addressing)

⁴¹ CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 116

FC00::042A:0000:0000:07F5

FC00:0000:0000:0000:042A::07F5''42



Each number is made up of 16 nr. hexadecimal representation.

C:\WINDOWS\system32>netsh interface ipv6

The following commands are available:

Commands in this context:

6to4 - Changes to the 'netsh interface ipv6 6to4' context.

? - Displays a list of commands.

- Adds a configuration entry to a table

- Adds a configuration entry to a table.
- Deletes a configuration entry from a table.

delete - Deletes a configuration entry in
dump - Displays a configuration script

- Displays a configuration script.
- Displays a list of commands.

`isctan` - Changes to the 'ctan' interface.

- Changes to the netsh interface
reset - Reset the IP configurations

reset - Reset the IP configurations.
set - Sets configuration information.

`set` - Sets configuration in Pipeline information

The following sections contain some possible

The following statement is true:

To view help for a command, type the command, followed by a space, and then type ?

⁴² CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 116

```
C:\WINDOWS\system32>netsh interface ipv6 dump

# -----
# IPv6 Configuration
# -----
pushd interface ipv6

reset
set interface interface="Ethernet (Kernel Debugger)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="WiFi" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Ethernet" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Local Area Connection* 1" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Local Area Connection* 10" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Bluetooth Network Connection" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Npcap Loopback Adapter" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="vEthernet (Default Switch)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled

popd
# End of IPv6 configuration


# -----
# ISATAP Configuration
# -----
pushd interface isatap

popd
# End of ISATAP configuration


# -----
# 6to4 Configuration
# -----
pushd interface 6to4

reset
```

```
C:\WINDOWS\system32>netsh interface ipv6 show

The following commands are available:

Commands in this context:
show addresses - Shows current IP addresses.
show compartments - Shows compartment parameters.
show destinationcache - Shows destination cache entries.
show dnsservers - Displays the DNS server addresses.
show dynamicportrange - Shows dynamic port range configuration parameters.
show excludedportrange - Shows all excluded port ranges.
show global    - Shows global configuration parameters.
show interfaces - Shows interface parameters.
show ipstats   - Displays IP statistics.
show joins     - Displays multicast groups joined.
show neighbors  - Shows neighbor cache entries.
show offload    - Displays the offload information.
show potentialrouters - Shows potential routers.
show prefixpolicies - Shows prefix policy entries.
show privacy   - Shows privacy configuration parameters.
show route     - Shows route table entries.
show siteprefixes - Shows site prefix table entries.
show subinterfaces - Shows subinterface parameters.
show tcpstats   - Displays TCP statistics.
show teredo     - Shows Teredo state.
show tfofallback - Shows per-network TCP Fastopen fallback state.
show udpstats   - Displays UDP statistics.
```

```

show udpstats - Displays UDP statistics.

C:\WINDOWS\system32>netsh interface ipv6 show addresses

Interface 1: Loopback Pseudo-Interface 1

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Preferred infinite infinite ::1

Interface 7: WiFi

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Preferred infinite infinite fe80::dcf5:289b:f34c:bfbe%7

Interface 14: Ethernet

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Deprecated infinite infinite fe80::7035:57aa:2413:1799%14

Interface 13: Local Area Connection* 1

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Deprecated infinite infinite fe80::54ac:18bf:dfaе:aad7%13

Interface 8: Local Area Connection* 10

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Deprecated infinite infinite fe80::e561:5094:732c:800%8

Interface 20: Bluetooth Network Connection

Addr Type DAD State Valid Life Pref. Life Address
----- -----
Other Deprecated infinite infinite fe80::2cce:d60:818b:f99d%20

Interface 27: vEthernet (Default Switch)

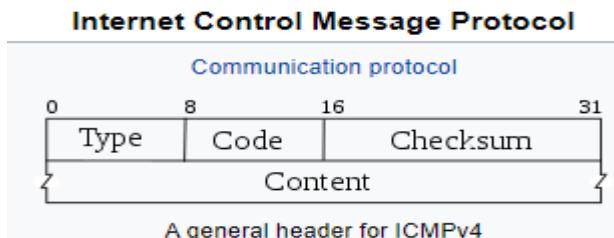
Addr Type DAD State Valid Life Pref. Life Address
----- -----

```

ICMP = Internet Control Message Protocol (ICMP)

- supporting protocol in the internet protocol suite,
- “is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address”⁴³

⁴³ https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol



"The ICMP packet is encapsulated in an IPv4 packet. The packet consists of header and data sections"⁴⁴

ICMP header format																																	
Offsets	Octet	0							1							2							3										
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Type							Code							Checksum																	
4	32	Rest of header																															

```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow
Ok.
```

```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name= "All ICMP V4" protocol=icmpv4:any,any dir=in action=allow
Ok.
```

```
C:\WINDOWS\system32>netsh advfirewall firewall add rule name= "Open Port 80" dir=in action=allow protocol=TCP localport=80
Ok.
```

Spoofing attack:

= to identify as another by falsifying data.

" IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network"⁴⁵

TCP/IP protocols do not have enough mechanisms for authentication of the source of a message.

ARP cache poisoning = ARP poison routing

Attacker sends ARP messages onto a LAN. "(...) the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic

⁴⁴ https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

⁴⁵ https://en.wikipedia.org/wiki/Spoofing_attack

meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic”⁴⁶

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.0.81 --- 0x7
Internet Address      Physical Address      Type
 192.168.0.1           40-0d-10-c0-43-38    dynamic
 192.168.0.69          f0-ef-86-4a-2e-15    dynamic
 192.168.0.255         ff-ff-ff-ff-ff-ff    static
 224.0.0.2              01-00-5e-00-00-02    static
 224.0.0.22             01-00-5e-00-00-16    static
 224.0.0.251            01-00-5e-00-00-fb    static
 224.0.0.252            01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 169.254.61.64 --- 0x12
Internet Address      Physical Address      Type
 169.254.255.255       ff-ff-ff-ff-ff-ff    static
 224.0.0.2              01-00-5e-00-00-02    static
 224.0.0.22             01-00-5e-00-00-16    static
 224.0.0.251            01-00-5e-00-00-fb    static
 224.0.0.252            01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 172.31.48.1 --- 0x1b
Internet Address      Physical Address      Type
 172.31.63.255          ff-ff-ff-ff-ff-ff    static
 224.0.0.2              01-00-5e-00-00-02    static
 224.0.0.22             01-00-5e-00-00-16    static
 224.0.0.251            01-00-5e-00-00-fb    static
 224.0.0.252            01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Week 21

IPV4 Packet Structure:

“IPv4 addresses use 32 bits and are displayed in dotted decimal format, such as 192.168.1.1”

⁴⁷ IPv4 addresses are matched with a subnet mask. For example, in the case of **IPV4 192.168.1.1** is from **Class C** (private address) which allow us to know what is the subnet mask, in this case **the subnet is 255.255.255.0** We can differentiate classes: A, B and C.

” Class A—1 to 126 (subnet mask 255.0.0.0)

Class B—128 to 191 (subnet mask 255.255.0.0)

⁴⁶ https://en.wikipedia.org/wiki/ARP_spoofing

⁴⁷ CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 116

Class C—192 to 223 (subnet mask 255.255.255.0)”⁴⁸

” Public vs. private vs. APIPA

IP addresses used on the Internet are public IP addresses. IP addresses used on internal networks are private IP addresses. Automatic Private IP Addressing (APIPA) addresses are randomly selected private addresses that always start with 169.254. Private IP addresses are formally defined in Request for Comments (RFC) 1918, with the following ranges: 10.0.0.0 through 10.255.255.255 (Class A private IP addresses) 172.16.0.0 through 172.31.255.255 (Class B private IP addresses) 192.168.0.0 through 192.168.255.255 (Class C private IP addresses)”

Features:

- **Version:** 4 for IPV4
- **Header Length:** the length of IP's header
- **Service's type:** a precedence flag and its type. (prioritize traffic)
- **Total length:** IP's header length + data.
- **Identification:** a unique number used to packet's identification.
- **Flags:** helpful when we need to identify if a packet is a part of sequence of highlighted packets.
- **Fragment offset:** it is helpful when we need reassemble the packets in correct order.
- **TTL** (time to live) – shows the packet lifetime, it describes in hops or seconds. It reduces the lifespan of data in network.
- **Protocol:** defines the header of transport layer which encapsulates the IPV4 header.
- **Header Checksum:** checks if IP header is damaged or not.
- **Source IP address:** IP address of the host which was responsible for packet transfer.
- **Destination IP Address:** destination of IP address.
- **Options:** related to source routing and timestamps.
- **Data:** transmitted data.

Screenshots from Wireshark and analyses:

(The highlight on blue it is what we are analysing. We see 9 categories in the header such as: no, time, source, destination, protocol, length, stream node, stream index, info. “TCP-Transmission Control Protocol (TCP) provides end to end reliability for the delivery of data.”⁴⁹ TCP provides formal connectivity before the data’s transmitting)

No.	Time	Source	Destination	Protocol	Length	Stream index	Stream index	Info
...	20.102682	192.168.1.130	216.58.213.4	TCP	54	10	10	63778
Info: 63778 → 443 [ACK] Seq=10479 Ack=181348 Win=131328 Len=0								

The source is: 192.168.1.30 *(When we open command prompt we can find this info: ipconfig /all

⁴⁸ CompTIA A+, Rapid Review, Darril Gibson, Microsoft, page 115.

⁴⁹ Ch. Sanders, “Practical Packet Analysis”, p.151

IPv4 Address. : 192.168.1.130(Preferred)

We have seen IPv4⁵⁰ address is our source in Wireshark.

Destination: 216.58.213.4

Protocol: TCP (Transmission Control Protocol allows exchange messages in network)

Length: 54 (size of frame is 54)

Stream index: 10 (it runs from 6-196)

Another screen

tcp.stream eq 0								
No.	Time	Source	Destination	Protocol	Length	Stream index	Stream index	Info
1	0.000000	192.168.0.101	3.235.82.194	TLSv1.2	271	0	0	0 Application Data
2	0.159936	3.235.82.194	192.168.0.101	TCP	54	0	0	0 443 → 54194 [ACK] Seq=1 Ack=218 Win=27 Len=0
3	0.160498	3.235.82.194	192.168.0.101	TLSv1.2	249	0	0	0 Application Data
4	0.204943	192.168.0.101	3.235.82.194	TCP	54	0	0	0 54194 → 443 [ACK] Seq=218 Ack=196 Win=517 Len=0
...	28.882237	192.168.0.101	3.235.82.194	TLSv1.2	84	0	0	0 Application Data
...	29.085511	3.235.82.194	192.168.0.101	TCP	54	0	0	0 443 → 54194 [ACK] Seq=196 Ack=248 Win=27 Len=0
...	30.098451	192.168.0.101	3.235.82.194	TLSv1.2	271	0	0	0 Application Data

```
> Frame 65: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6268479B-8D09-46DA-8321-029BC0EA66CF}, id 0
> Ethernet II, Src: Tp-LinkT_86:97:b6 (18:a6:f7:86:97:b6), Dst: IntelCor_81:b3:4d (a0:a8:cd:81:b3:4d)
< Internet Protocol Version 4, Src: 3.235.82.194, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 40
        Identification: 0x2d9e (11678)
    > Flags: 0x4000, Don't fragment
        Fragment offset: 0
        Time to live: 42
        Protocol: TCP (6)
        Header checksum: 0xb78 [validation disabled]
        [Header checksum status: Unverified]
        Source: 3.235.82.194
        Destination: 192.168.0.101
    > Transmission Control Protocol, Src Port: 443, Dst Port: 54194, Seq: 196, Ack: 248, Len: 0

0000 a0 a8 cd 81 b3 4d 18 a6 f7 86 97 b6 08 00 45 00  ....M....E...
0010 00 28 2d 9e 40 00 2a 06 0b 78 03 eb 52 c2 c0 a8  .(-@.*. x..R...
0020 00 65 01 bb d3 b2 bb cc b9 24 b8 e0 eb c7 50 10  .e.....$....P.
0030 00 1b a8 f7 00 00  ..... 
```

Analyses:

Protocol is TCP, length is 54, stream index =0. 54 bytes has been captured. Ethernet II has been used to do it. Source: Tp-LinkT is the name of my WIFI. TTL=42 means 42 seconds was the lifespan of the packet. Header checksum – validation was disabled. Fragmented offset 0 means we haven't started reassemble the packet in order. Destination 192.168.0.101 is default gateway and IPV4, after calling

⁵⁰ Is used for identifying devices which are connected to network, 32-bit number, it consists of 2 parts: network portion and host portion.

ipconfig in command prompt:

```
Wireless LAN adapter WiFi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::dcf5:289b:f34c:bfbe%6
IPv4 Address . . . . . : 192.168.0.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

We can use also in command prompt command:

netsh show wlan networks mode=bssid

```
C:\Users\Home>netsh wlan show networks mode=bssid

Interface name : WiFi
There are 1 networks currently visible.

SSID 1 : TP-LINK_8697B7
    Network type          : Infrastructure
    Authentication        : WPA2-Personal
    Encryption            : CCMP
    BSSID 1               : 18:a6:f7:86:97:b6
    Signal                : 99%
    Radio type            : 802.11n
    Channel               : 3
    Basic rates (Mbps)   : 6.5 16 19.5 117
    Other rates (Mbps)   : 18 19.5 24 36 39 48 54 156
```

We can see the name of network, what is used for authentication in this case is WPA2, which is good because it is better than WPA. Encryption CCMP which is standard encryption protocol. It is good signal 99% out 100%, channel 3 (we have 13 ones used in Poland) 2 indicators referring to rates, it is in Mbps (megabits per second, it is related to reference to download and upload speeds)

The next command is:

Netsh wlan show interfaces

```
C:\Users\Home>netsh wlan show interfaces

There is 1 interface on the system:

  Name : WiFi
  Description : Intel(R) Dual Band Wireless-AC 7260
  GUID : 6268479b-8d09-46da-8321-029bc0ea66cf
  Physical address : a0:a8:cd:81:b3:4d
  State : connected
  SSID : TP-LINK_8697B7
  BSSID : 18:a6:f7:86:97:b6
  Network type : Infrastructure
```

BSSID is “the MAC address of the radio interface the client device is currently connected to”
⁵¹ MAC is the abbreviation of Media Access Control, unique number associated with NIC (Network Interface Card) SSID is the name of my WIFI, it is visible because I haven’t changed what was set by the default. State connected means I have net connection.

TCP:

Source port 443 means: is used for secure web browser communication, name =https (http protocol over TLS/SSL) “Web servers offering to accept and establish secure connections listen on this port for connections from web browsers desiring strong communication security.”⁵²

Destination port 54194 means: “TCP guarantees delivery of data packets on port 54194 in the same order in which they were sent. Guaranteed communication over TCP port 54194 is the main difference between TCP and UDP. UDP port 54194 would not have guaranteed communication as TCP. UDP on port 54194 provides an unreliable service and datagrams may arrive duplicated, out of order, or missing without notice.”⁵³

Sequence 196 means: number of the first byte of data in TCP transferred packet.

And len 0 means: because 192.168.0.1 only acknowledges the data, there is no data transfer in this case.

Abbreviations:

SYN – means synchronise, it happened when clients request a connection.

SYN/ACK – synchronise/acknowledgement, there are bits in TCP header; SYN starts TCP session, ACK highlights the ACK number in TCP header is acknowledging the data.

⁵¹<https://help.datto.com/s/article/KB115005592546#:~:text=The%20BSSID%20is%20the%20MAC,MAC%20addresses%20assigned%20to%20it>

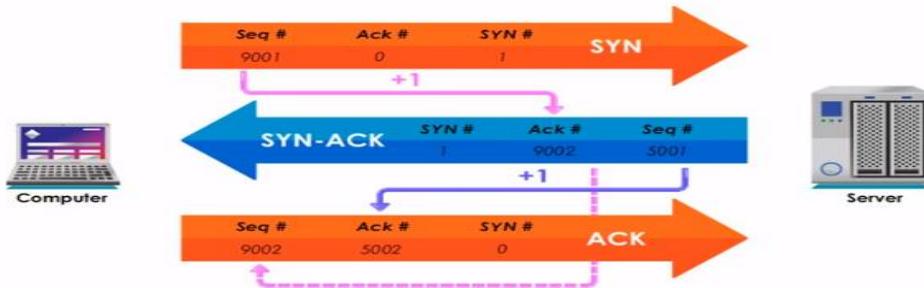
⁵² https://www.grc.com/port_443.htm

⁵³ <https://www.adminsub.net/tcp-udp-port-finder/54194>

3-way handshake:

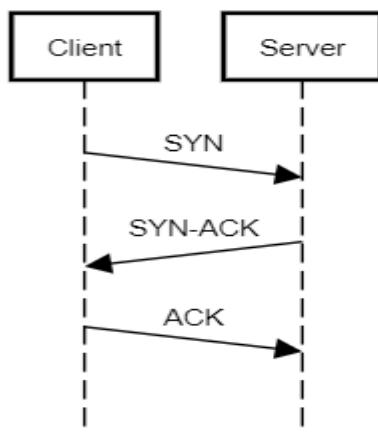
TCP is a connection between 2 hosts such as: server and client. "The TCP defines a 3-way handshake mechanism to initiate the connection."⁵⁴

- Client starts by sending SYN packet.
- Server responds with a packet included ACK (acknowledgment) that it received client SYN and SYN was directed to the client.
- Client should reply with ACK that SYN has been received.



based on: <https://www.youtube.com/watch?v=xMtP5ZB3wSk>

3-way handshake



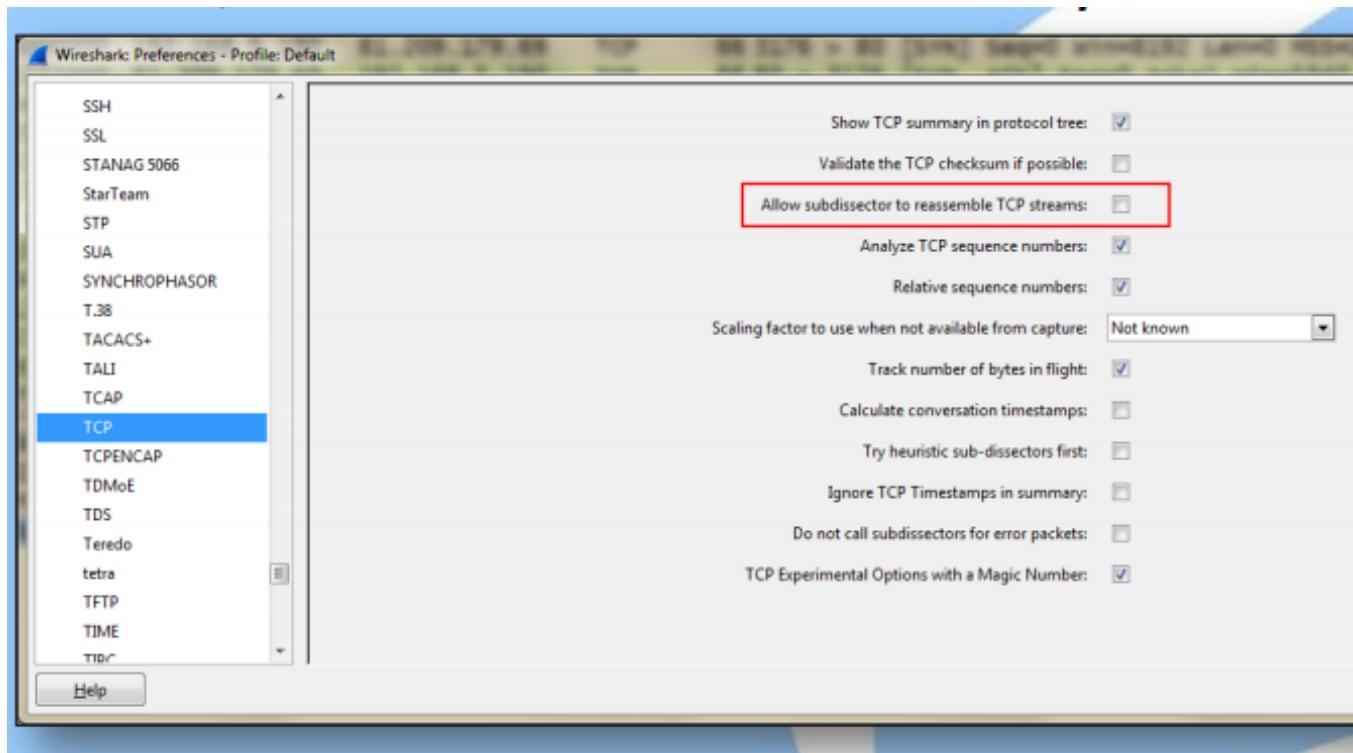
based on: <https://codeburst.io/basic-tcp-analysis-with-wireshark-b99ed54fa499>

For example, in Wireshark we can see this 3 handshake, we have 3 lines and on each one we can notice status such as: on the first SYN only, on the second SYN and ACK and on third just ACK.

Source	Destination	Protocol	Length	Info
172.16.16.128	212.58.226.142	TCP	66 2826 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	
212.58.226.142	172.16.16.128	TCP	66 80 → 2826 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1406 SACK_PERM=1 WS=12	
172.16.16.128	212.58.226.142	TCP	54 2826 → 80 [ACK] Seq=1 Ack=1 Win=16872 Len=0	

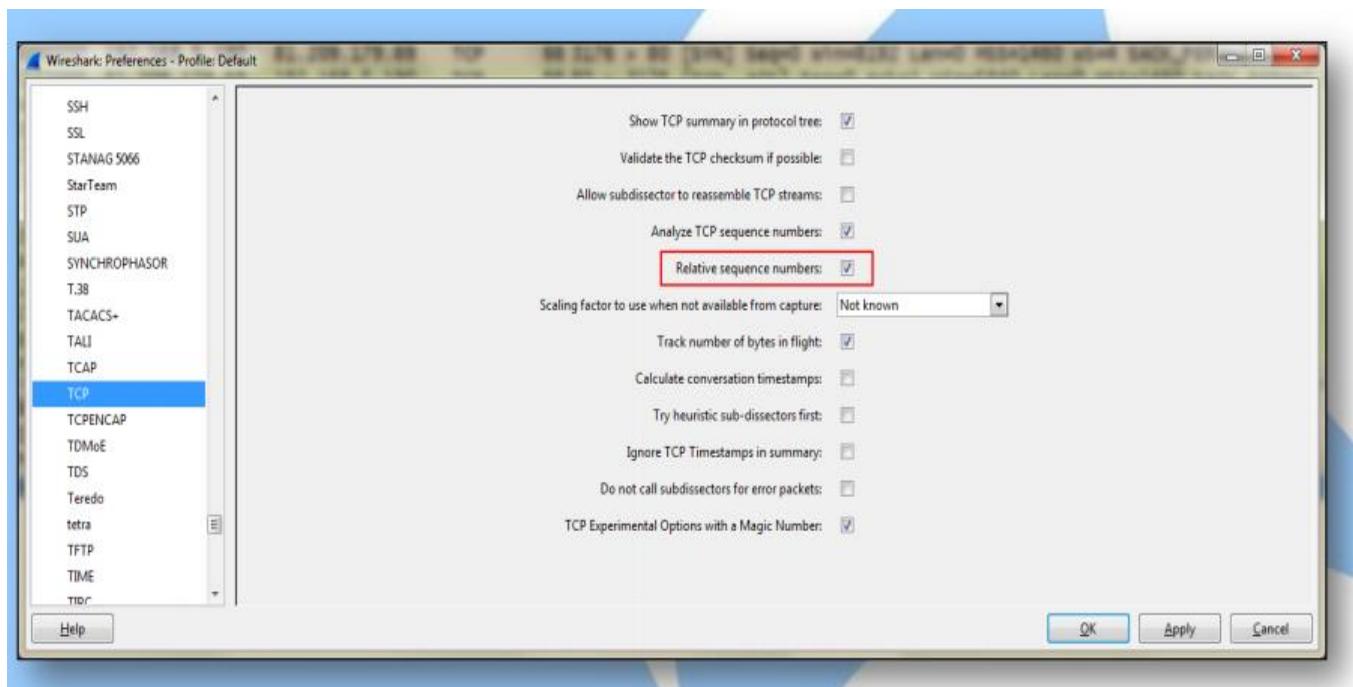
⁵⁴ <https://codeburst.io/basic-tcp-analysis-with-wireshark-b99ed54fa499>

It is important to turn on reassemble TCP streams.



Based on: B5-TCP Analysis First step, presentation Power Point, slide 13/34.

Later turn on: RELATIVE SEQUENCE NUMBERS



Based on: B5-TCP Analysis First step, presentation Power Point, slide 13/34.

Sequence Numbers – The Rules

1. Each TCP sequence starts with random number
2. It is increased by 1 for each byte transmitted
3. SYN and FIN flags count as 1 Byte („Phantom Byte“)

Based on: B5-TCP Analysis First step, presentation Power Point, slide 13/34.

For instance:



Based on: B5-TCP Analysis First step, presentation Power Point, slide 13/34.

We can observe on this schema that AckNo and SeqNo has been increased by 1. Moreover, we should also consider that every direction has own number and relative sequence numbers look identical for 2 directions.

Wireshark – screenshots:

192.168.0.101	13.107.4.52	TCP	66	19	19 50290 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13.107.4.52	192.168.0.101	TCP	68	19	19 80 → 50290 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
192.168.0.101	13.107.4.52	TCP	54	19	19 50290 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
192.168.0.101	13.107.4.52	HTTP	208	19	19 GET /connecttest.txt HTTP/1.1
13.107.4.52	192.168.0.101	TCP	56	19	19 80 → 50290 [ACK] Seq=1 Ack=155 Win=525312 Len=0
13.107.4.52	192.168.0.101	HTTP	568	19	19 HTTP/1.1 200 OK (text/plain)
192.168.0.101	13.107.4.52	TCP	54	19	19 50290 → 80 [FIN, ACK] Seq=155 Ack=515 Win=131840 Len=0
13.107.4.52	192.168.0.101	TCP	56	19	19 80 → 50290 [FIN, ACK] Seq=515 Ack=155 Win=525312 Len=0
192.168.0.101	13.107.4.52	TCP	54	19	19 50290 → 80 [ACK] Seq=156 Ack=516 Win=131840 Len=0
13.107.4.52	192.168.0.101	TCP	56	19	19 80 → 50290 [ACK] Seq=516 Ack=156 Win=525312 Len=0

```

Capture Length: 56 bytes (448 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:vssmonitoring]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Tp-LinkT_86:97:b6 (18:a6:f7:86:97:b6), Dst: IntelCor_81:b3:4d (a0:a8:cd:81:b3:4d)
> Internet Protocol Version 4, Src: 13.107.4.52, Dst: 192.168.0.101
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 50290, Seq: 516, Ack: 156, Len: 0
  Source Port: 80
  Destination Port: 50290
  [Stream index: 19]
  [TCP Segment Len: 0]
  Sequence number: 516    (relative sequence number)
  Sequence number (raw): 4024584630
  [Next sequence number: 516    (relative sequence number)]
  Acknowledgment number: 156    (relative ack number)
  Acknowledgment number (raw): 2817646949
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window size value: 2052
  [Calculated window size: 525312]
  [Window size scaling factor: 256]
  Checksum: 0x4d71 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
> VSS Monitoring Ethernet trailer, Source Port: 0

▼ Flags: 0x010 (ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0.... .... = Congestion Window Reduced (CWR): Not set
  .... .0... .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0.... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....A.....]
  Window size value: 2052
  [Calculated window size: 525312]
  [Window size scaling factor: 256]
  Checksum: 0x4d71 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0

▼ [SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 2281]
  [The RTT to ACK the segment was: 0.070218000 seconds]
  [iRTT: 0.072353000 seconds]
  - - - - -
  ▼ [Timestamps]
    [Time since first frame in this TCP stream: 0.194863000 seconds]
    [Time since previous frame in this TCP stream: 0.059957000 seconds]
▼ VSS Monitoring Ethernet trailer, Source Port: 0
  Src Port: 0

```

Analysis based on <https://www.youtube.com/watch?v=HCHFX5O1laQ>

Conclusions:

Initial packet is:

```

192.168.0.101 13.107.4.52   TCP      66      19      19 50290 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13.107.4.52   192.168.0.101  TCP      68      19      19 80 → 50290 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1448 WS=256 SACK_PERM=1
192.168.0.101 13.107.4.52   TCP      54      19      19 50290 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0

```

The port which we want to achieve is 80. Stream index =19, Sequence number = 516 (relative).

Windows size value =2052, this is where I am advertising the size of my TCP receive buffer; I can receive 2052 bytes at once, acknowledged.

Calculated Window Size --=525312, ($2052 \times 256 = 525312$; windows size value * Windows size scaling factor)

Flags:

0 means false, only acknowledgement **=1** means true, all others are false, have not been set.

It is important to catch TCP handshake because we can calculate true window, we can have delta time (time between packets) and initial roundtrip time (Go to Edit -> Preferences -> User Interface -> Columns. Click "Add", name it "Relative Time" and select "Relative Time" as Field Type)

Timestamp

“While packets are captured, each packet is timestamped. These timestamps will be saved to the capture file, so they will be available for later analysis”⁵⁵

Ghost (Phantom) byte = “causes the sequence number and acknowledgment number fields to increment by 1 even though no data is exchanged. This phantom byte can be confusing when you have just learned that the sequence number field increments only when data is sent.”⁵⁶

TCP Connection Teardown⁵⁷:

In brief:

⁵⁵ <https://cse.sc.edu/~pokeefe/tutorials/wireshark/ChWorkTimeFormatsSection.html>

⁵⁶ <https://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/>

⁵⁷ based on <https://www2.hawaii.edu/~esb/1998fall.ics451/nov02.html>

Independent shutdown on every side,
 Closure the connection on condition that second side send FIN,
 FIN packets have been acknowledged.

More detailed:

Every handshake has teardown, it happened when connection between 2 sides is closed. FIN is the indicator which defines end of connection. 4 packets are used in this process.

Process:

- 1) Host A sends FIN and ACK flag set.
- 2) Host B responds with ACK packet and send own FIN/ACK.
- 3) Host A responds with ACK packet and ending the communication.

Tcp_teardown in Wireshark

TCP resets:

RST flag is used to signalise that was disruption, the connection was failed or finished suddenly.

Window in Wireshark to look what is happening: Tcp_refuseconnection.pcapng in Wireshark

RESET – can happen in any point of TCP connection. This is abortive release.

Analysis:

No.	Time	Delta	Source	Destination
1	15:02:46.543503	0.000000	192.168.1.1	66.163.43.11
2	15:02:46.543710	0.000207	66.163.43.11	192.168.1.1
3	15:02:47.042699	0.498989	192.168.1.1	66.163.43.11
4	15:02:47.068309	0.025610	66.163.43.11	192.168.1.1

Length	Time to live	Info
66	128	50249 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
60	64	https(443) → 50249 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66	128	[TCP Retransmission] 50249 → https(443) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66	58	[TCP Port numbers reused] https(443) → 50249 [SYN, ACK] Seq=4203465782 Ack=1

The client starts from 443 SYN there was no connection (RST) we try again and after this was retransmission (TCP Retransmission) after that 25 milliseconds later the connection was successful; we can observe SYN ACK and connection being established. In line 13 we can see that client sent FIN to a server. It happened after some seconds of inactivity.

4	15:02:47.068309	0.025610	66.163.43.11	192.168.1.1	66	58	[TCP Port numbers reused] https(443) → 50249 [SYN, ACK] Seq=4203465783
5	15:02:47.068374	0.000065	192.168.1.1	66.163.43.11	54	128	50249 → https(443) [ACK] Seq=1 Ack=4203465783 Win=65536 Len=0
6	15:02:47.068908	0.000534	192.168.1.1	66.163.43.11	571	128	Client Hello[Packet size limited during capture]
7	15:02:47.089617	0.020709	66.163.43.11	192.168.1.1	60	58	https(443) → 50249 [ACK] Seq=4203465783 Ack=518 Win=44032 Len=0
8	15:02:47.090574	0.000957	66.163.43.11	192.168.1.1	214	58	[Packet size limited during capture]
9	15:02:47.091440	0.000866	192.168.1.1	66.163.43.11	270	128	Change Cipher Spec, Encrypted Handshake Message
10	15:02:47.110930	0.019490	66.163.43.11	192.168.1.1	116	58	Application Data[Packet size limited during capture]
11	15:02:47.111884	0.000954	66.163.43.11	192.168.1.1	96	58	Application Data
12	15:02:47.111936	0.000052	192.168.1.1	66.163.43.11	54	128	50249 → https(443) [ACK] Seq=734 Ack=4203466047 Win=65280 Len=0
13	15:03:00.397503	13.285567	192.168.1.1	66.163.43.11	54	128	50249 → https(443) [FIN, ACK] Seq=734 Ack=4203466047 Win=65280 Len=0

The reset was sent by a firewall (TTL=64) it did not get to a server.

Delta	Source	Destination	Length	Time to live	Info
0.000207	66.163.43.11	192.168.1.1	60	64	https(443) → 50249 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

We can see a second connection, lines 15,16,17 we have a handshake.

14	15:03:00.397556	0.000053	192.168.1.1	66.163.43.11	54	128	50249 → https(443) [RST, ACK] Seq=735 Ack=4203465783
15	15:03:57.408771	57.011215	192.168.1.1	164.209.248.50	66	128	50736 → https(443) [SYN] Seq=0 Win=8192 Len=0
16	15:03:57.449930	0.041159	164.209.248.50	192.168.1.1	66	49	https(443) → 50736 [SYN, ACK] Seq=0 Ack=1 Win=1
17	15:03:57.449989	0.000059	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [ACK] Seq=1 Ack=1 Win=657
18	15:03:57.450340	0.000351	192.168.1.1	164.209.248.50	287	128	Client Hello[Packet size limited during capture]
19	15:03:57.492258	0.041918	164.209.248.50	192.168.1.1	60	241	https(443) → 50736 [ACK] Seq=1 Ack=234 Win=1
20	15:03:57.495206	0.002948	164.209.248.50	192.168.1.1	1486	241	[Packet size limited during capture]
21	15:03:57.496205	0.000999	164.209.248.50	192.168.1.1	1486	241	[Packet size limited during capture]
22	15:03:57.496235	0.000030	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [ACK] Seq=234 Ack=2865 Win=1
23	15:03:57.496271	0.000036	164.209.248.50	192.168.1.1	339	241	[Packet size limited during capture]
24	15:03:57.500789	0.004518	192.168.1.1	164.209.248.50	180	128	Client Key Exchange
25	15:03:57.501059	0.000270	192.168.1.1	164.209.248.50	601	128	Application Data[Packet size limited during capture]
26	15:03:57.540714	0.039655	164.209.248.50	192.168.1.1	60	241	https(443) → 50736 [ACK] Seq=3150 Ack=907 Win=1
27	15:03:57.541666	0.000952	164.209.248.50	192.168.1.1	105	241	Change Cipher Spec, Encrypted Handshake Message
28	15:03:57.552299	0.010633	164.209.248.50	192.168.1.1	414	241	Application Data[Packet size limited during capture]
29	15:03:57.552337	0.000038	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [ACK] Seq=907 Ack=3561 Win=1
30	15:04:03.554243	6.001906	164.209.248.50	192.168.1.1	85	241	Encrypted Alert
31	15:04:03.554462	0.000219	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [FIN, ACK] Seq=907 Ack=3592 Win=1
32	15:04:03.593006	0.038544	164.209.248.50	192.168.1.1	60	241	https(443) → 50736 [FIN, ACK] Seq=3592 Ack=908 Win=1
33	15:04:03.593063	0.000057	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [ACK] Seq=908 Ack=3593 Win=1
30	15:04:03.554243	6.001906	164.209.248.50	192.168.1.1	85	241	Encrypted Alert
31	15:04:03.554462	0.000219	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [FIN, ACK] Seq=907 Ack=3592 Win=65024 Len=0
32	15:04:03.593006	0.038544	164.209.248.50	192.168.1.1	60	241	https(443) → 50736 [FIN, ACK] Seq=3592 Ack=908 Win=16896 Len=0
33	15:04:03.593063	0.000057	192.168.1.1	164.209.248.50	54	128	50736 → https(443) [ACK] Seq=908 Ack=3593 Win=65024 Len=0

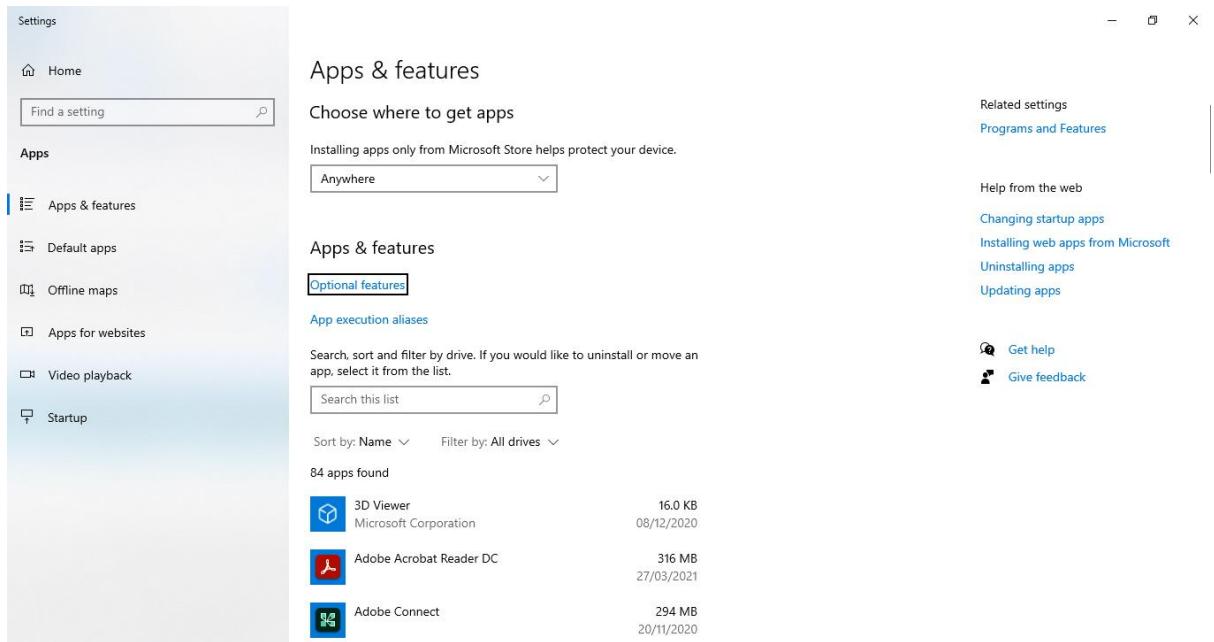
30 15:04:03.554243 6.001906 164.209.248.50 192.168.1.1 85 241 Encrypted Alert

There is encrypted alert (line 30); TCP can get FIN, it is time to teardown and allows resource to be used for something else.

Week 22

Tips against computer slowlessness:

- Uninstall unused programs,



- Delete temporary files,

Recycle Bin			
	Name	Original Location	Date Deleted
Quick access	IMG_20210329_140147	C:\Users\Home\Desktop	02/04/2021 09:49
Desktop	IMG_20210329_140154	C:\Users\Home\Desktop	02/04/2021 09:49
Downloads	IMG_20210329_140203	C:\Users\Home\Desktop	02/04/2021 09:49
Documents	IMG_20210329_140206	C:\Users\Home\Desktop	02/04/2021 09:49
Pictures	IMG_20210329_140215	C:\Users\Home\Desktop	02/04/2021 09:49
CERTYF	IMG_20210329_140220	C:\Users\Home\Desktop	02/04/2021 09:49
cv	IMG_20210329_140220 (1)	C:\Users\Home\Desktop	02/04/2021 09:49
karl	IMG_20210329_140224	C:\Users\Home\Desktop	02/04/2021 09:49
NIEMIECKI	k9	C:\Users\Home\Desktop	02/04/2021 09:56
OneDrive - Middlesex University			
6 SIGMA			

- Buy solid SSD,

Sponsored ⓘ

WD_BLACK SN750 500GB High-Performance NVMe Internal Gaming SSD

★★★★★ 16,421

£59⁹⁸ £98.99

prime FREE delivery



Transcend 128 GB M.2 SATA III SSD Type 2260 MLC

★★★★★ 1,429

£70¹⁵

Only 5 left in stock.



"The first question is whether you should choose a SATA drive or a more modern M.2 model. SATA SSDs use the same data and power connectors as a regular hard disk, so they're pretty much guaranteed to work with any system made in the past ten years. The catch is that the SATA interface is limited to around 550MB/sec - and on older systems, some or all ports may only support half that data rate."⁵⁸

- Stop unnecessary start-ups,
- Buy more RAM,
- Run disk clean up, AVAST CLEANUP PREMIUM

⁵⁸ <https://www.itpro.co.uk/ssds/29494/how-to-pick-the-perfect-ssd-for-your-needs-and-budget>

The screenshot shows the Avast Cleanup Premium application interface. At the top, there's a large circular progress meter indicating "92% TUNED UP" out of 100%. Below the meter are four circular icons with checkmarks: Maintenance (LAST RUN: 4 HOURS AGO), Speed up (67% OPTIMIZED, 4 optimizations found), Free up space (ALL CLEANED), and Fix problems (2 PROBLEMS FIXED). A sidebar on the right contains icons for Notifications, Menu, and other system functions.

Maintenance

87 Issues to fix & 649.2 MB to clean up

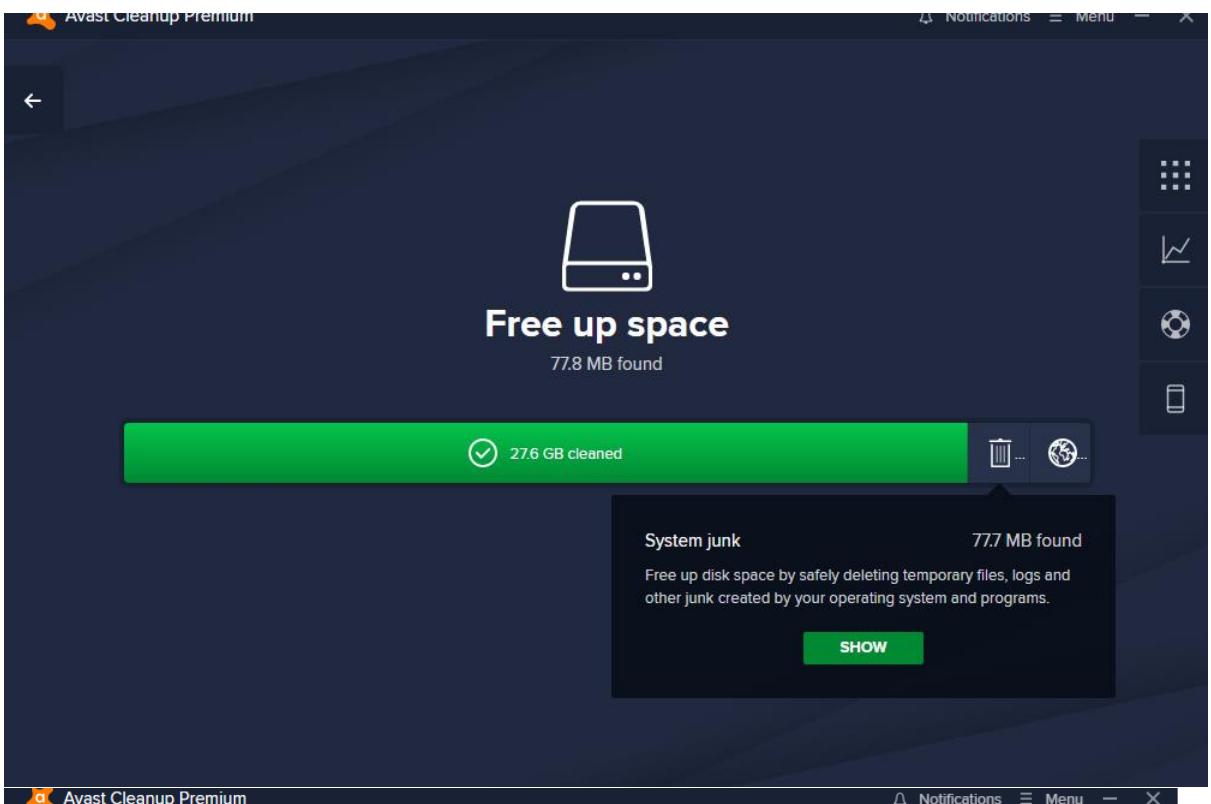
<input checked="" type="checkbox"/>	Broken registry items	38 issues >
<input checked="" type="checkbox"/>	Broken shortcuts	48 issues >
<input checked="" type="checkbox"/>	System junk	391.1 MB >
<input checked="" type="checkbox"/>	Browser cache	258.1 MB >
<input checked="" type="checkbox"/>	Tracking & other cookies	1 issue >
<input type="checkbox"/>	Browsing & download history	2,263 items >

FIX & CLEAN

Cancel

The screenshot shows the Avast Cleanup Premium interface. At the top, a banner indicates "Speed up" with a clock icon and "4 optimizations found". A progress bar shows "67% optimized". Below this, a section titled "Background & startup programs" shows "2 programs" that are slowing down the PC. A "SHOW" button is present. The main content area is titled "Background & startup programs" and shows "10 programs sleeping". A dropdown menu lists these programs with their status: "Sleeping" or "Temporarily awake", and a "Wake" link to manage them.

Program	Status	Action
Adobe Acrobat Reader ...	Sleeping	Wake
Chromium	Sleeping	Wake
Dell Touchpad	Sleeping	Wake
Microsoft Edge Update	Sleeping	Wake
Microsoft Office Professi...	Temporarily awake	Wake
Microsoft OneDrive	Sleeping	Wake



This screenshot shows the "System junk" cleanup screen. The title is "System junk" with "77.7 MB found". It says "Free up disk space by safely deleting temporary files, logs and other junk created by your operating system and programs." A "SHOW" button is visible. Below this, there's a table of junk types:

Name	Items	Size
<input checked="" type="checkbox"/> Program log files	Ignore	1 12.3 KB >
<input checked="" type="checkbox"/> Program temp files	Ignore	3 29.4 KB >
<input checked="" type="checkbox"/> Windows cache files	Ignore	1 20.0 MB >
<input checked="" type="checkbox"/> Windows history files	Ignore	2 1.3 KB >
<input checked="" type="checkbox"/> Windows log files	Ignore	7 33.1 KB >

At the bottom, there are buttons for "Select recommended" (with a dropdown arrow), "20.0 MB selected", and "CLEAN NOW". The date "20/11/2020" is at the very bottom.

Fix problems



2 problems fixed

✓ 2 problems fixed

! All of your programs are up-to-date [Show](#)

! All disks scanned [Show](#)

> No problems ignored

Outdated programs

✓ 5 programs up-to-date

 Adobe Reader
Current version 21.001.20145.

 Java Runtime Environment 8 (32 Bit)
Current version 8.0.2710.9.

 Notepad++
Current version 7.9.3.0.

 VLC Media Player (64 Bit)
Current version 3.0.12.0.

 WinRAR Archiver (64 Bit)
Current version 6.0.0.0.

> No programs ignored

Automatic Updates [ON](#) 

The image consists of two vertically stacked screenshots of a mobile application named "Disk Doctor".

Top Screenshot: This screen shows the results of a disk scan. At the top center is the title "Disk Doctor" in white. Below it is a large green checkmark icon inside a circle. The text "All disks have been fixed" is displayed in green at the bottom of the main content area. On the left side, there is a small back arrow icon. On the right side, there is a "Rescan" button with a circular arrow icon. The main content area includes a section header "1 disk scanned" with a checkmark icon and a dropdown arrow. Below this is a row for "Local Disk (C:)": it shows a small disk icon, a checkmark indicating "No issues found", and the date "18 days ago". To the right of this row are two buttons: "Details" and "Scan now".

Bottom Screenshot: This screen shows the process of scanning a disk. The title "Scanning 'Local Disk (C:)' for errors..." is at the top in white. Below it is a search icon (magnifying glass over a folder). A horizontal progress bar is shown, with a green segment indicating "11%" completion. At the bottom is a rectangular button labeled "STOP".

- Vacuum,
- Updates

Windows Update

 **Updates available**
Last checked: Today, 11:45

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.43.0)
Status: Downloading - 62%

Optional quality update available
2021-03 Cumulative Update Preview for Windows 10 Version 20H2 for x64-based Systems (KB5000842)

[Download and install](#)

 **Pause updates for 7 days**
Visit Advanced options to change the pause period

 **Change active hours**
Currently 08:00 to 17:00

 **View update history**
See what updates are installed on your device

 **Advanced options**
Additional update controls and settings

Looking for info about the latest updates?
[Learn more](#)

Related links
[Check Storage](#)
[OS build and System info](#)

 [Get help](#)
 [Give feedback](#)

- Think about new PC

For example, this type of Dell



Dell Precision 15 7550, Xeon, 128GB RAM, 2TB SSD, UHD, Quadro T2000, Dell WTY
Seller refurbished

£3,719.99 [Buy it now](#)

[Add to Watchlist](#)

Condition: Seller refurbished : ?		Item Weight: 2.450000	
Seller notes: "Certified Manufacturer Refurbished As New (Unused)"		Processor: Intel Xeon W-10885M (8 Core), 2.4 GHz (5.3 GHz Max Turbo)	
Brand:	Dell	Type:	SSD
Hard Drive Capacity:	2 TB Solid State Drive (M.2 SSD)	Storage Type:	4GB NVIDIA Quadro T2000
Most Suitable For:	Business Use	Graphics Processing Type:	English UK (QWERTY), Keyboard
Manufacturer Colour:	Grey	Features:	Precision 15 7550 Mobile Workstation
RAM Size:	128 GB	Colour:	Grey
Manufacturer Warranty:	3 Years	Model:	2.4 GHz
MPN:	EPC147324	Processor Speed:	3840 x 2160
Series:	Dell Precision 15 7000 Series	Maximum Resolution:	DDR 4 SDRAM
Screen Size:	15.6 inch	Memory Type:	5056375278990
Connectivity:	2x USB 3.2, 2x USB 3.2 TB Type-C, 1x HDMI, 1x mDP, 1x RJ45	EAN:	
GPU:	4GB NVIDIA Quadro T2000	Condition Description:	Certified Manufacturer Refurbished As New (Unused)
Operating System:	Windows 10 Pro	UPC:	Does Not Apply
ISBN:	Does Not Apply		

Features:

RAM size: 128 GB

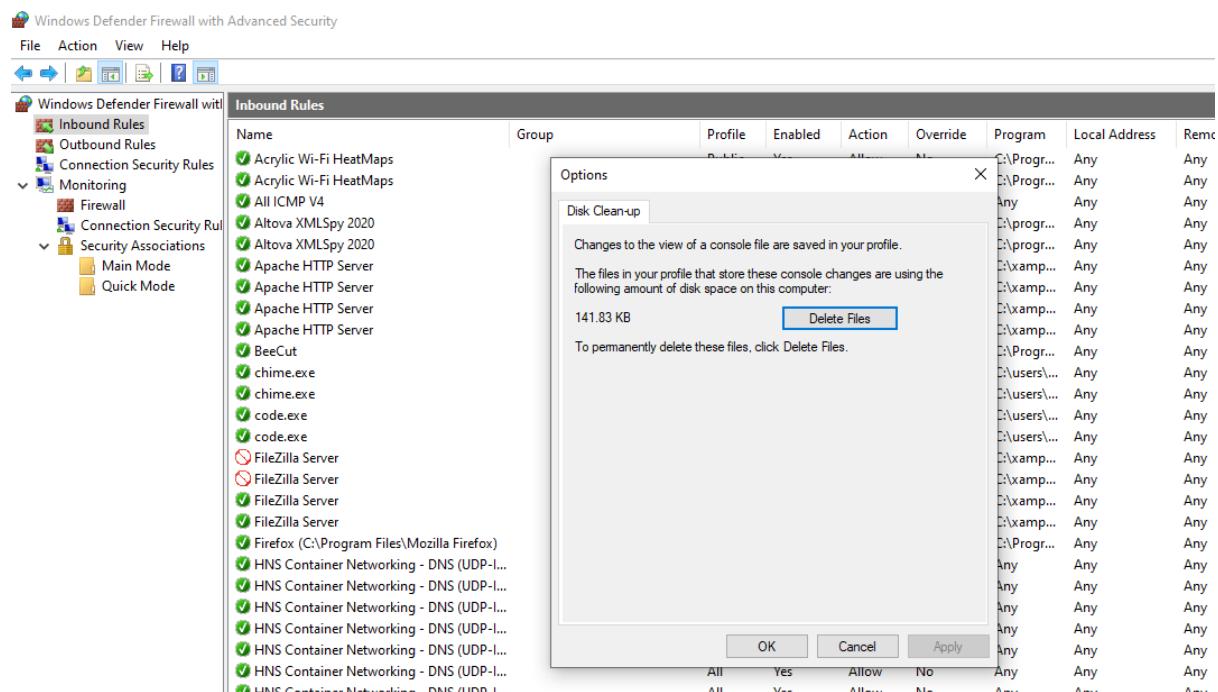
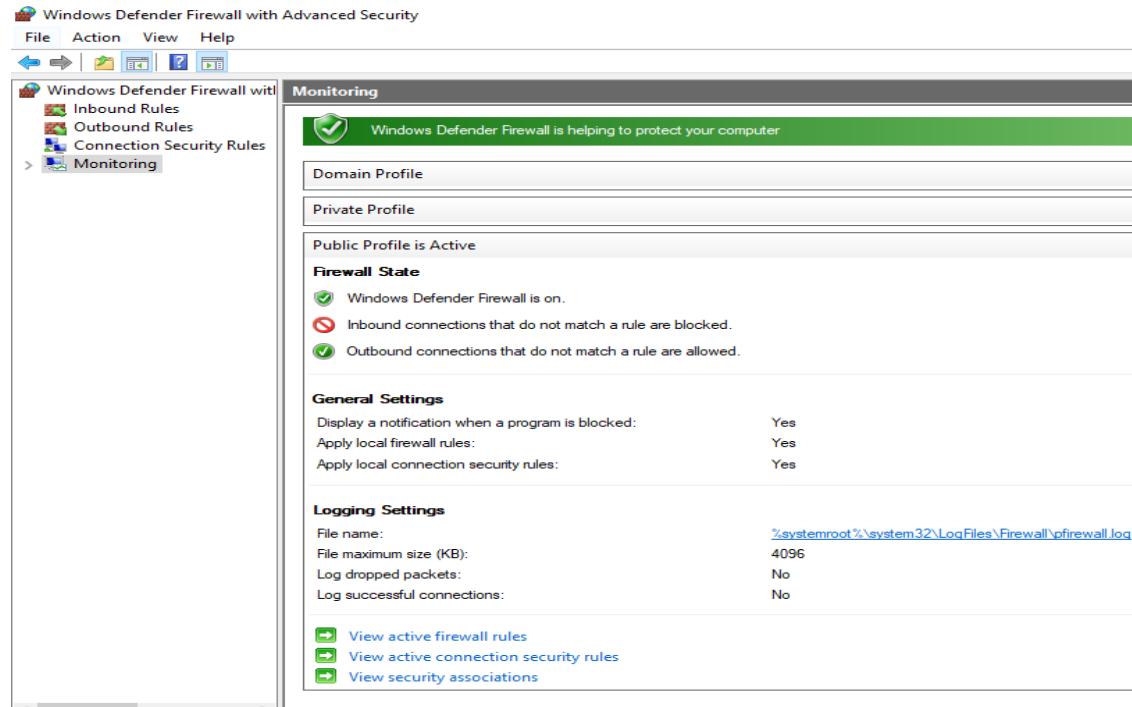
GPU: 4GB NVIDIA Quadro T2000

Storage type: SSD

Memory type: DDR 4 SDRAM

How else might you identify adware, a worm or data mining on your machine?

Windows Defender:



Windows Security

Windows Security

The screenshot shows the Windows Security interface. On the left is a sidebar with navigation links: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main area is titled "Security at a glance" with a sub-section "See what's happening with the security and health of your device and take any actions needed." It displays four cards: "Virus & threat protection" (Quick scan due, "Scan now" button), "Account protection" (No action needed), "Firewall & network protection" (No action needed), and "App & browser control" (No action needed). Below these are three more cards: "Device security" (View status and manage hardware security features), "Device performance & health" (No action needed), and "Family options" (Manage how your family uses their devices).

Windows Security

The screenshot shows the "Virus & threat protection" page. The sidebar remains the same. The main content starts with a heading "Protection for your device against threats." Below it is a section titled "Current threats" with a "Quick scan running..." status (Estimated time remaining: 00:00:32, 2708 files scanned) and a "Cancel" button. A message encourages users to "Feel free to keep working while we scan your device." There are two sections: "Virus & threat protection settings" (No action needed, "Manage settings" link) and "Virus & threat protection updates" (Security intelligence up to date, Last update: 02/04/2021 11:46). At the bottom is a "Settings" link.

🛡️ Virus & threat protection

Protection for your device against threats.

⌚ Current threats

No current threats.

Last scan: 02/04/2021 12:29 (quick scan)

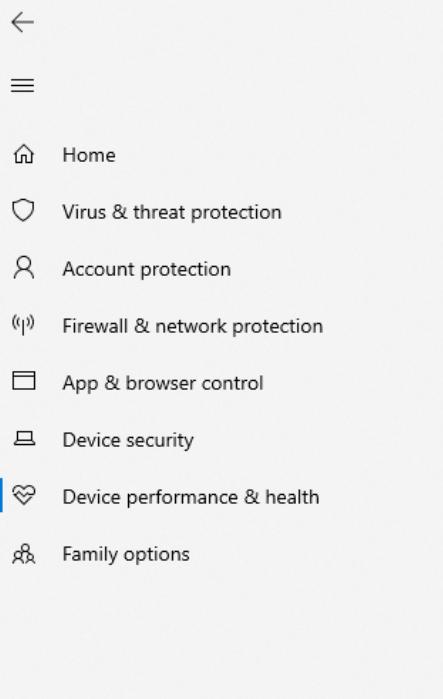
0 threats found.

Scan lasted 1 minutes 51 seconds

41405 files scanned.

Quick scan

Windows Security



♡ Device performance & health

Reports on the health of your device.

📋 Health report

Last scan: 02/04/2021 12:31

✔️ Windows Time service
No issues

✔️ Storage capacity
No issues

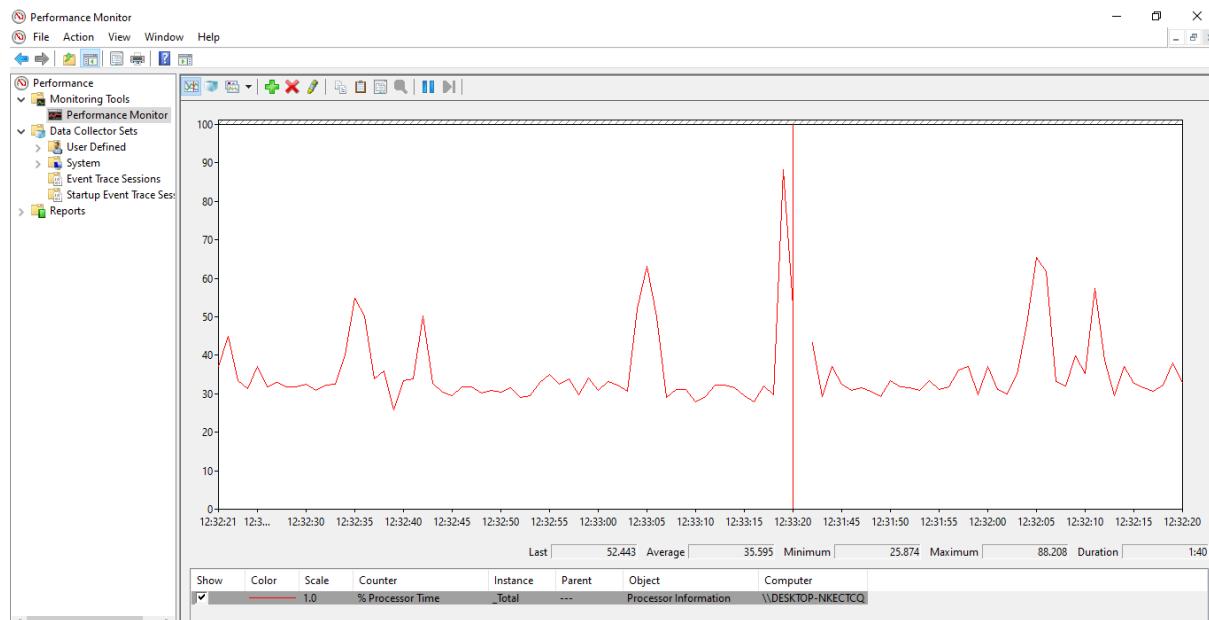
✔️ Battery life
No issues

✔️ Apps and software
No issues

Performance monitor

See how computer deals with all

For example



Clear browsing data in Google Chrome

The screenshot shows the Google Chrome settings page with the 'History' tab selected. A 'Clear browsing data' dialog box is open, showing the 'Advanced' tab. The 'Time range' is set to 'All time'. The dialog lists several items for clearing data, each with a checked checkbox:

- Browsing history: 31 items (and more on synced devices)
- Download history: None
- Cookies and other site data: From 514 sites (you won't be signed out of your Google Account)
- Cached images and files: 72.2 MB
- Passwords and other sign-in data: 268 passwords (for mdx.ac.uk, linkedin.com and 266 more, synced)
- Auto-fill form data

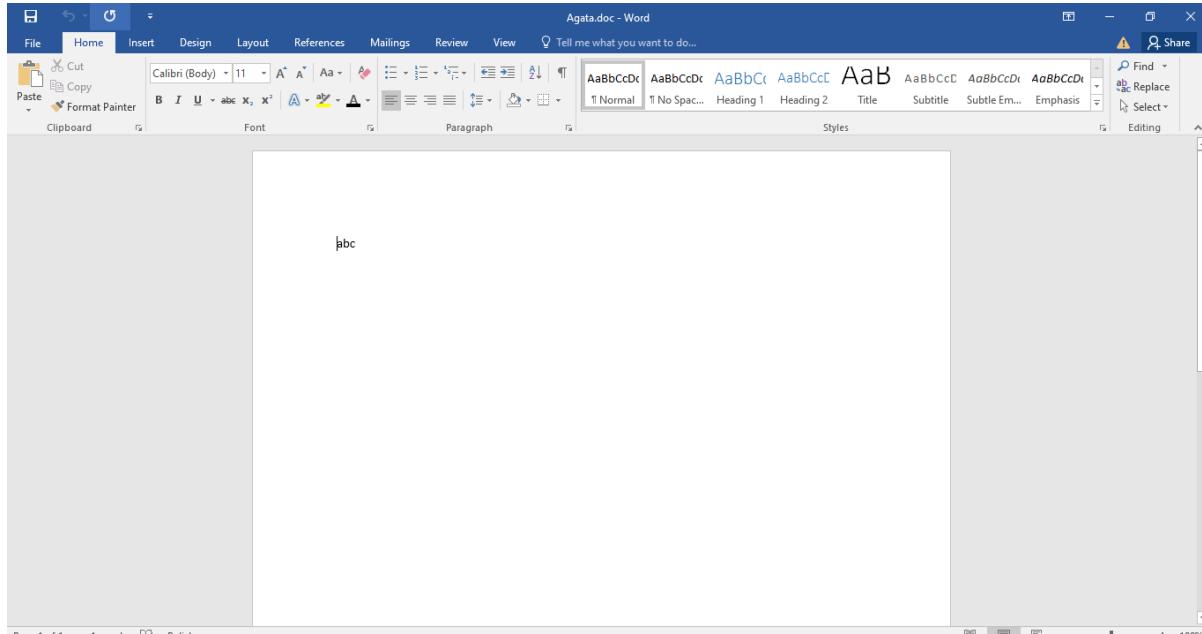
At the bottom of the dialog are 'Cancel' and 'Clear data' buttons.

Find an image for Windows 3.1 that runs in Virtual Box – Install it – look at the difference between Win10 and Win3.1

Week 23

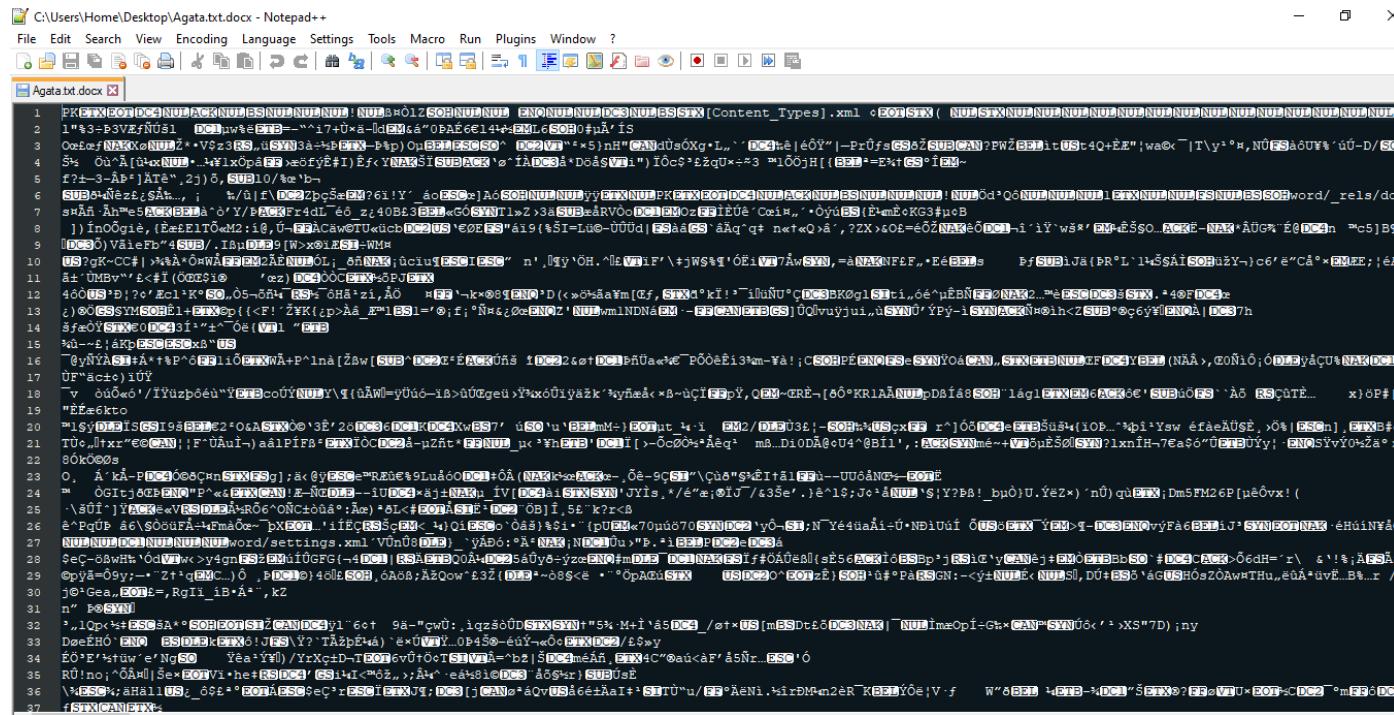
1. Change a .doc extension on a word document to .txt and view in notepad or a similar simple editor

Agata.doc



In Notepad opening the same document

In Notepad ++



2. Try the same with a .docx document



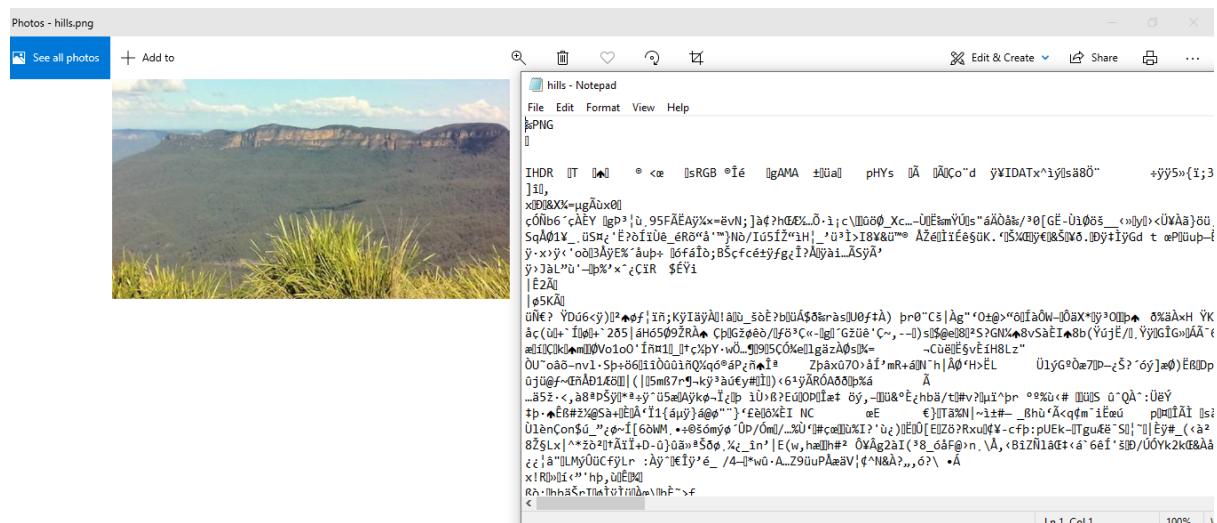
3. Change a .docx extension on a word document to .zip and try to extract.

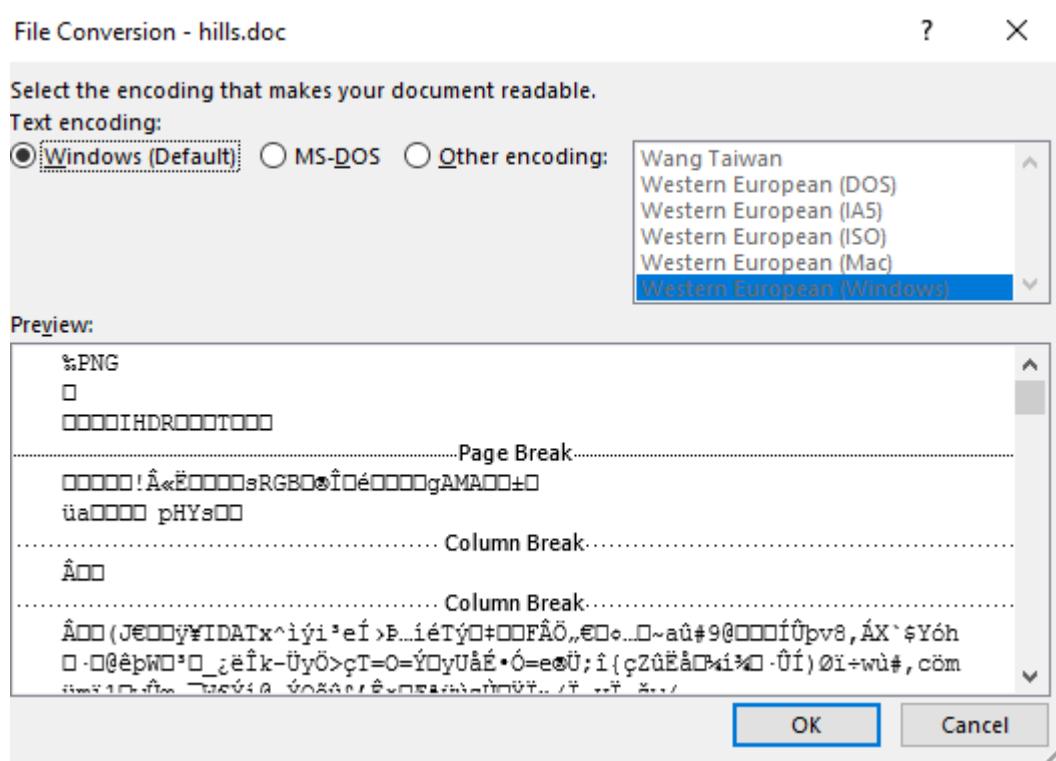


Could you recover a message? NO

- 4) Try changing a .jpg extension to .txt, open the file in notepad or a similar simple editor

How can we tell this is a jpg file from the data in the file?





```
%PNG
□
□□□IHDR□□□T□□□
```

6. What metadata can be hidden in a word document?

"Most Word documents contain hidden metadata that shows the history of the document. Metadata is data about the document or file that is embedded within the file's details. That data shows when the document was first created, who authored the document, total editing time, and the last time the document was modified."⁵⁹

Agata.doc - Word

Info

Agata
Desktop

Protect Document
Control what types of changes people can make to this document.

Inspect Document
Before publishing this file, be aware that it contains:
■ Document properties and author's name

Manage Document
Check in, check out, and recover unsaved changes.
There are no unsaved changes.

Properties

Size	11.1KB
Pages	1
Words	1
Total Editing Time	9 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	Today, 16:56
Created	Today, 16:56
Last Printed	

Related People

Author	Home
Last Modified By	Home

Related Documents

[Open File Location](#)

[Show All Properties](#)

Document Inspector

Review the inspection results.

- Comments, Revisions, Versions, and Annotations**
No items were found.
- Document Properties and Personal Information**
The following document information was found:
* Document properties
* Author [Remove All](#)
- Task Pane Add-ins**
We did not find any Task Pane add-ins.
- Embedded Documents**
No embedded documents were found.
- Macros, Forms, and ActiveX Controls**
No macros, forms, or ActiveX controls were found.
- Collapsed Headings**
No collapsed headings were found.
- Custom XML Data**
No custom XML data was found.

Note: Some changes cannot be undone.

[Reinspect](#) [Close](#)

Remove all and we can send.

7. How can you access this?

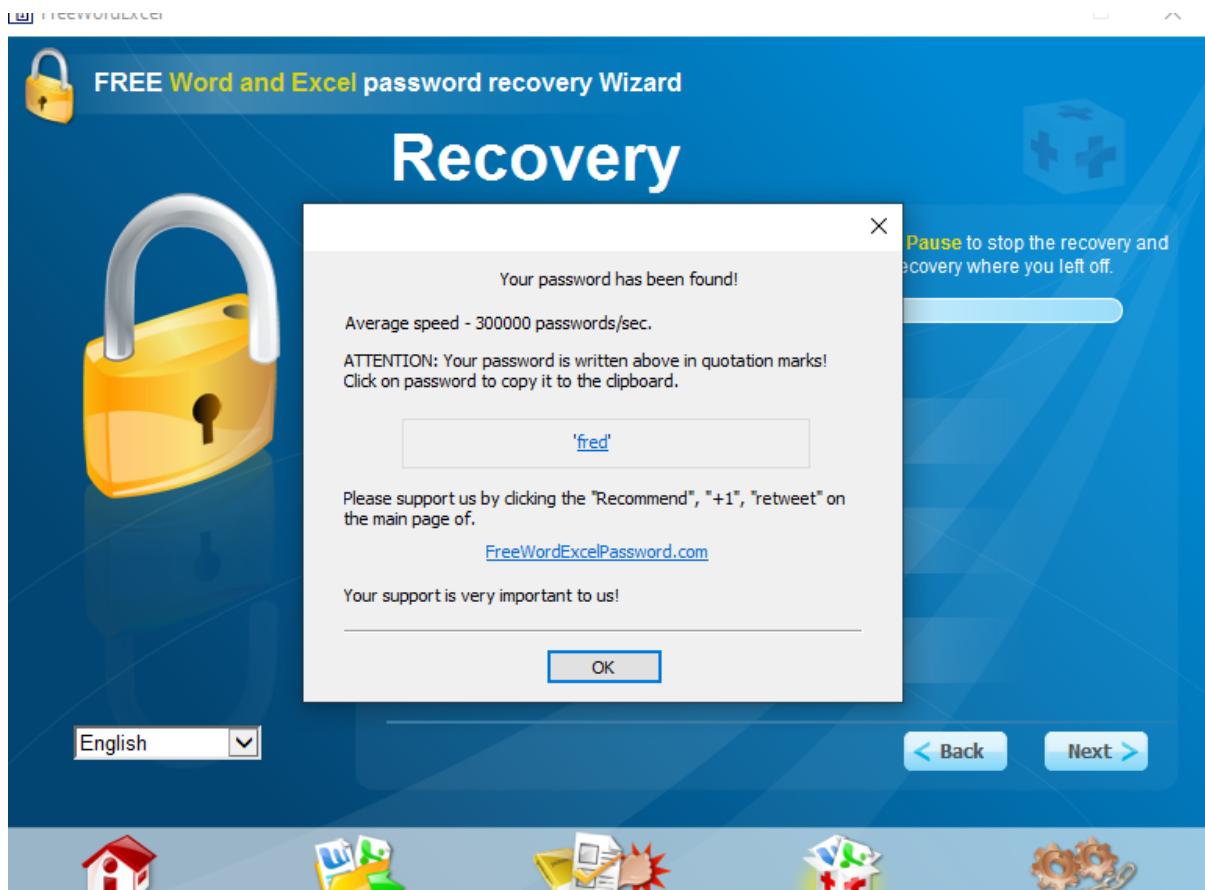
I have tried opening Test 1 by FreeWordExcel

Dictionary Attack:



Brute Force Attack





Test 2

By brute force attack



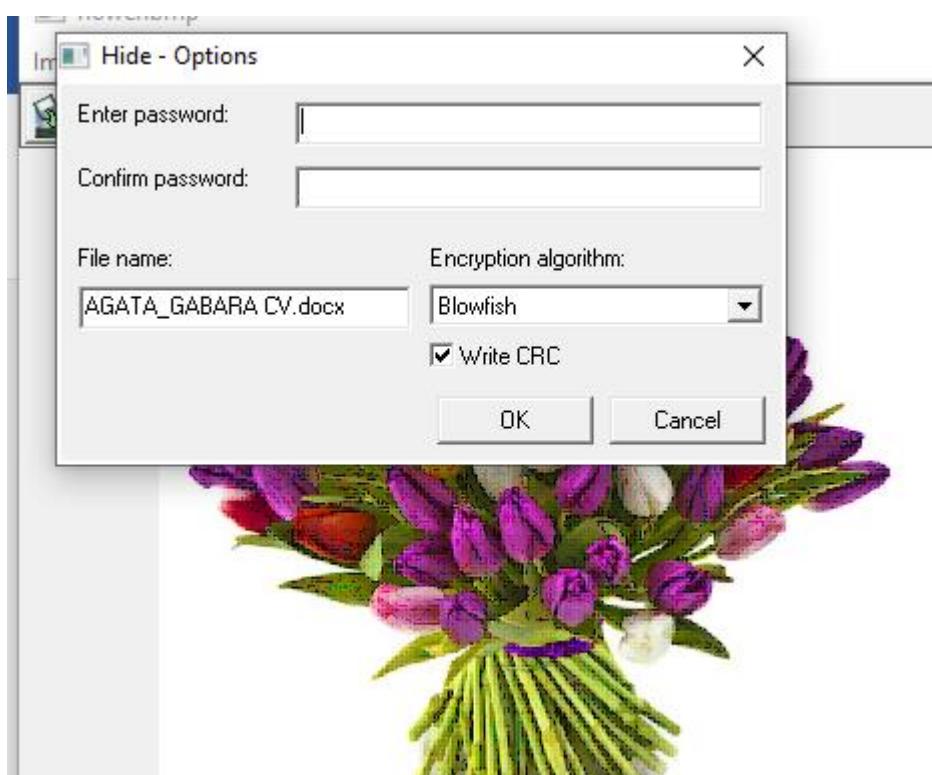
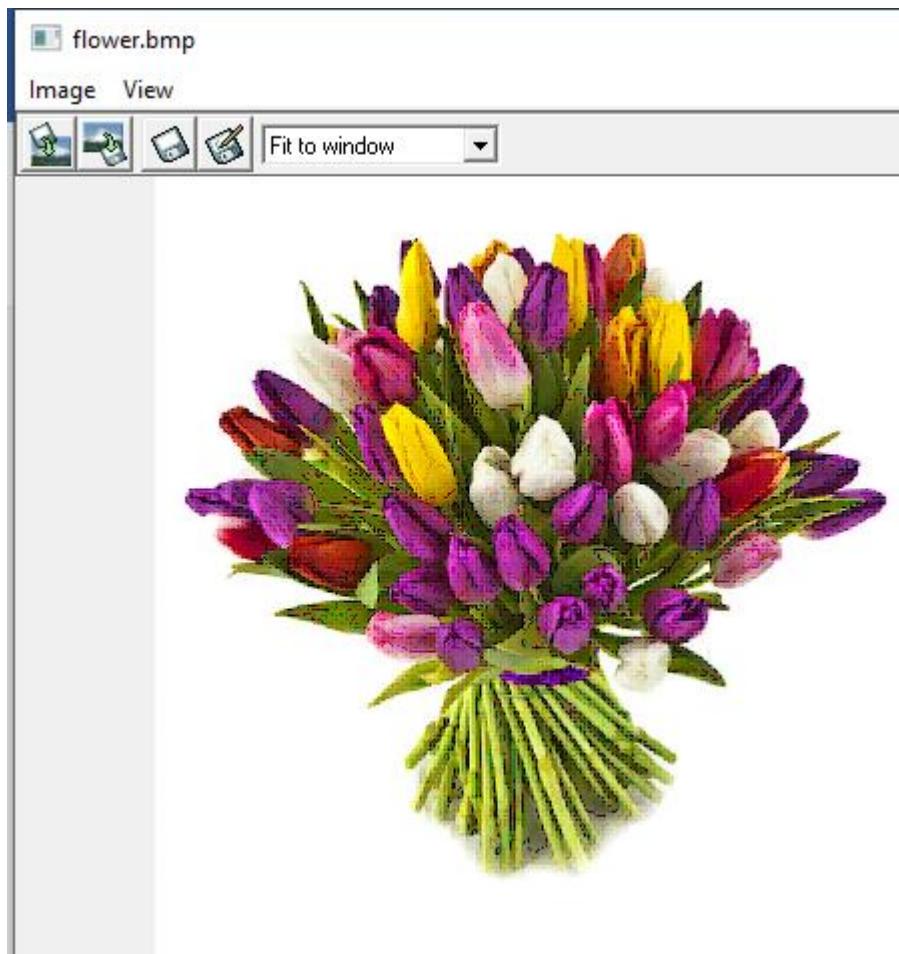
"Hide in Picture"

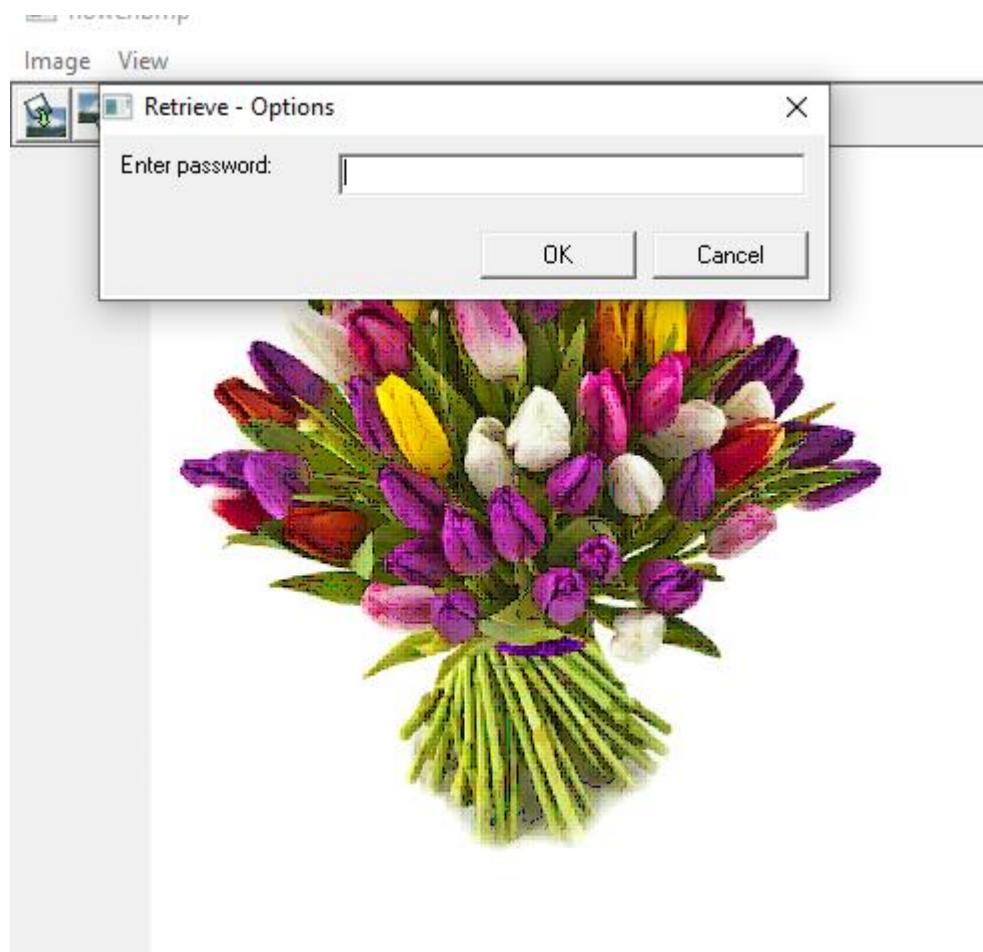
- type of steganography program, it allows hide any kind of file inside bitmap pictures.
- it doesn't look suspiciously,
- it is possible to set a password to hide files, without the password it is not possible to discover if something was hidden.

I have created flowers with extension bmp and save on desktop and I open a program and hide inside flowers my doc file called AGATA_GABARA CV

I set up a password and when I choose option retrieve I need to put a password to check if something was hidden or not. In the case of wrong password, it is communique that nothing was hidden.

Screenshots:





What types of files can you hide? images, text files, video files, software files, .exe, .bat

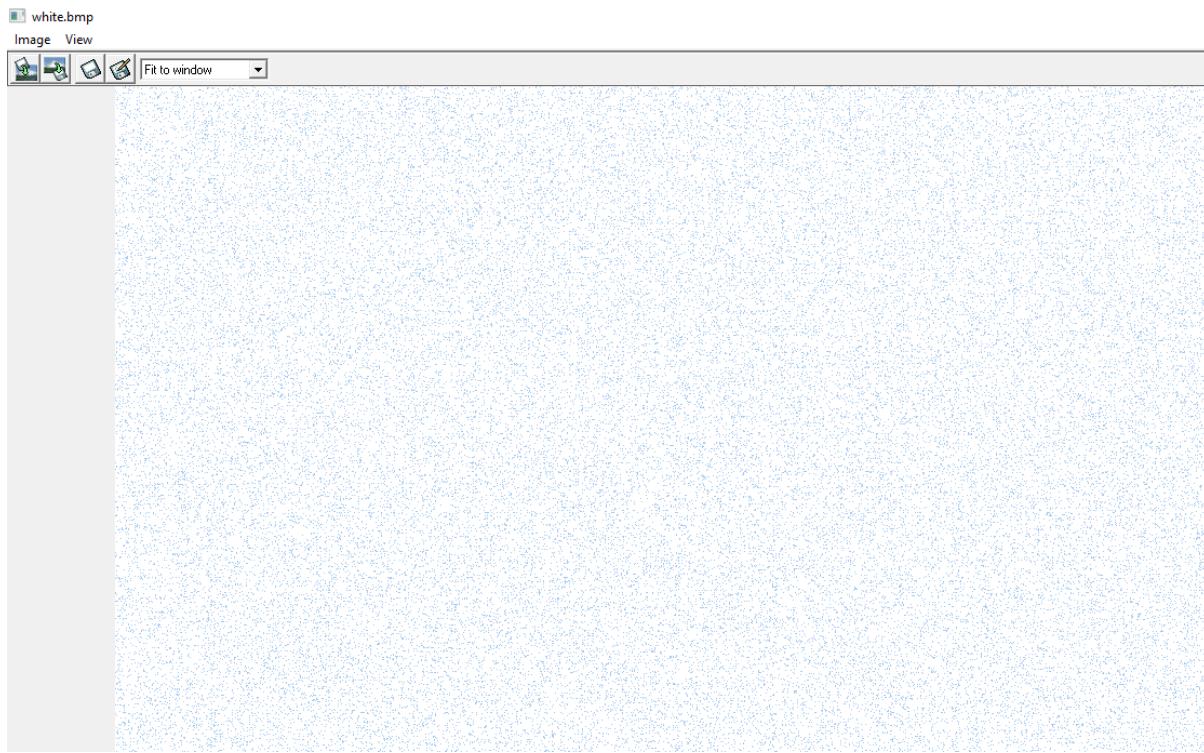
What difference does the size ratio of the marked file to embedded file make?

How can you tell if this software is Robust or Fragile? fragile, because it does not have an encryption,

What happens if you mark a file that is all white or black?

I have white bmp and I hide word file

I see this:



The background is not white it includes some blue dots.

In the case of black



There are some dots on the black background.

How secure is steganography as a protection system? it is not safe and it is not encryption.

Have there been any recent stories about steganography in the real world?

2010 – Russian spy hid codes in online photos

“In 2011, a suspected al-Qaeda member was arrested in Berlin, Germany in May. This suspect

was he found with a memory card with a password-protected folder. Examiners discovered hidden files were contained in the protected folder. However, as the German newspaper Die Zeit reported, digital forensics examiners from the German Federal Criminal Police (BKA) claimed to have eventually uncovered its contents (Gallagher, 2012). The examiners reported that a video was uncovered and appeared to be a pornographic video. Within that video, forensic examiners were able to reveal 141 separate text files (Gallagher, 2012). They claim that the documents contained details regarding al-Qaeda operations and future operating plans. Among these documents were three documents labelled "Future Works," "Lessons Learned," and "Report on Operations" (Gallagher, 2012)^{2⁶⁰}

"A Russian hacker group named Advanced Persistent Threat (APT) 29, used steganography in 2015 to disguise communication within pictures on GitHub (Bell, 2015). 2⁶¹

Can you think of any novel or interesting applications of steganography?

Creation tools:

- QuickStego
- OpenStego
- Xiao Steganography
- Camouflage
- Our Secret
- Steganofile
- Steghide
- OpenPuff
- SteganPEG
- SilentEye

Week 24 DRP

Part 1 Main goals of this plan

The major goals of this plan are the following:

- To minimize disruption impact.
- To keep update personnel with all emergency procedures.
- To deliver smooth restoration of service.

⁶⁰[www.researchgate.net/publication/326098434 Digital steganography and its existence in cybercrime](http://www.researchgate.net/publication/326098434_Digital_steganography_and_its_existence_in_cybercrime)

⁶¹[www.researchgate.net/publication/326098434 Digital steganography and its existence in cybercrime](http://www.researchgate.net/publication/326098434_Digital_steganography_and_its_existence_in_cybercrime)

- Update the software accordingly.
- Keep staff duties per plan.
- Limit extra costs.

Part 2 Personnel

First Name, Last Name	Position in company	Address	Mobile / Email

Part 3 VHD – features

Name	Number	Manufacturer	Length	Comments

Part 4 Inventory

Name	Serial Number	Cost	Manufacturer	Own/leased

- Personal computers
- USB cables
- VCR players
- Video capture devices
- Video playback machines
- Software
- Telephones
- Printers
- Heaters
- Chairs
- Tables
- Lamps

This list will be checked every ... months.

Part 5 Backup procedures

- Personal Computer
 - It is recommended that all personal computers should be backed up. Copies of the personal computer files should be uploaded to the server on ... (date) at ... (time). It corresponds with the normal saving data system procedure.

- Carbonite (Cloud backup solution)
 - It is recommended that all should be send to the cloud. It will be saved on the server. It is recommended to choose full back up; Carbonite offers 3 types of backup such as: full, incremental and differential. It is recommending also add encryption key and set email notification on the status of backup.

(based on: <https://www.youtube.com/watch?v=pmxlbEWTdhs>)

Part 6 Disaster recovery procedures

At this stage we should differentiate 3 types of procedures such as: emergency response guideline, backup operations guideline and recovery one.

Emergency Dealing

To evidence emergency response to natural disaster, or any other activity in order to save lives and reduce damages.

Backup Dealing

To ensure that essential data processing tasks can be executed after the disruption.

Recovery Dealing

To enable quick data's restoration process after a disaster.

Example of checklist

1) Initiation schedule.

- Inform management,
- Contact disaster team,
- Define the level of disaster,
- Put into practice application recovery plan,
- Progress's observation,
- Keep updated other staff

2) Follow –up checklist.

- Tasks of each member,
- List all staff mobile numbers and emails,
- Define applications to be run,
- Check what was backup recently and what was not and make notes accordingly,
- Take copies of system and operational documentation and procedural manuals,
- Inform insurance provider about the disaster and make steps accordingly.

Recovery guidelines after an accident.

- a) Inform Disaster Recovery Services of the need to utilize service and of recovery plan selection.

These telephone numbers are in service from ... am until ... pm Monday through Friday.

Disaster notification number:

1. Inform power and telephone service suppliers and plan any essential service connections.
2. Inform immediately on condition that any related plans will change.

Part 7 System's restoring

Before You Start: localize the tapes, equipment, and information from the off-site storage location.

- All tapes from the most recent complete save operation
- The most recent tapes from saving security data (SAVSECDTA or SAVSYS)
- PTF list
- Tape list from daily, weekly and most recent save operation.
- The Backup and Recovery book
- Telephone directory
- Modem manual
- Tool kits

Part 8 Rebuilding

- Disaster recovery plan,
- Run recovery test (highlight of areas which should be under test)
- Record of plan changes