

CSCI 466: Networks

Lecture 6: Wireshark

Reese Pearsall
Fall 2023

Wireshark Lab 1 is released, due on **September 20th**

Cookies can be stolen using a variety of different attacks (XSS, Session Hijack, etc). Cookies are generally encrypted

Download Speed vs Upload Speed

Wireshark

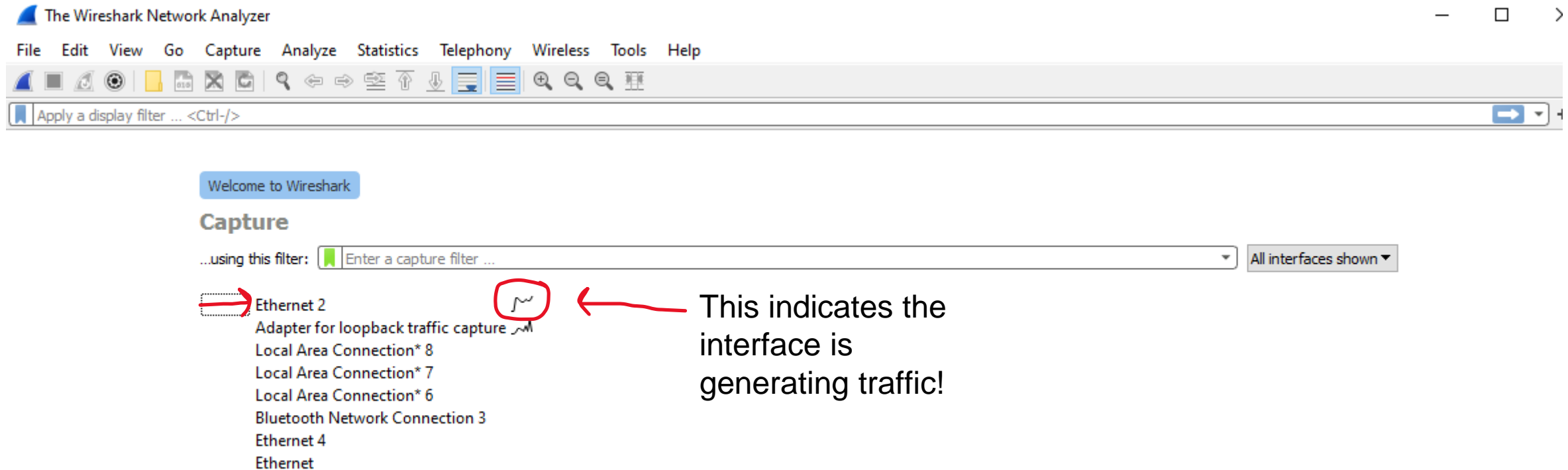
Wireshark is a free and open-source network packet analyzer

It captures packets that are leaving and arriving to your machine and provides details about them

You will use Wireshark to analyze real life network traffic for the labs



When you boot up Wireshark, you will need to select an **interface** to capture on



In general, you will select **ethernet** (wired connections) or **Wi-fi** (wireless connections)

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1948	5.275252	192.168.1.4	66.22.231.8	UDP	94	54038 → 50003 Len=52
1949	5.276205	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1950	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1951	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1952	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1953	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1954	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1955	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1956	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1957	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1958	5.296643	66.22.231.8	192.168.1.4	UDP	1174	50003 → 54038 Len=1132
1959	5.303321	66.22.231.8	192.168.1.4	UDP	1174	50003 → 54038 Len=1132
1960	5.303450	66.22.231.8	192.168.1.4	UDP	1174	50003 → 54038 Len=1132
1961	5.303546	66.22.231.8	192.168.1.4	UDP	1174	50003 → 54038 Len=1132
1962	5.303689	66.22.231.8	192.168.1.4	UDP	1174	50003 → 54038 Len=1132
1963	5.303776	66.22.231.8	192.168.1.4	UDP	1175	50003 → 54038 Len=1133

> Frame 1: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface
 > Ethernet II, Src: Netgear_2b:78:46 (9c:3d:cf:2b:78:46), Dst: Giga-Byt_ae:b1:0f (e0:00:00:00:00:00)
 > Internet Protocol Version 4, Src: 66.22.231.8, Dst: 192.168.1.4
 > User Datagram Protocol, Src Port: 50003, Dst Port: 54038
 > Data (1126 bytes)

```

0000 e0 d5 5e ae b1 0f 9c 3d cf 2b 78 46 08 00 45 00  ..^....=..+xF...E..
0010 04 82 1e 98 40 00 34 11 39 08 42 16 e7 08 c0 a8  ....@.4. 9.B.....
0020 01 04 c3 53 d3 16 04 6e 05 6c 90 67 21 e6 59 bb  ...S...n.l!g!..Y..
0030 80 26 00 00 73 07 be de 00 03 94 4c 09 cb a2 1d  .&..s....L....
0040 e1 ba 0a 84 7f 0e 3b e7 f4 90 91 a2 e0 84 f5 70  .....;.....p....
0050 ca 5b 1a e2 ed f1 75 89 8b 0e 69 d7 79 2f c5 d7  .[.....u...i.y/..
0060 28 65 7d a3 f6 1e 5f 6e d0 fa f5 9a 94 e7 cd 32  (e)....n.....2...
0070 fb 4b 37 47 e9 d0 5c bf 15 87 10 ee ad a1 9d 8c  .K7G...\. ....
0080 79 b7 28 86 7e 8f a3 7d 12 92 fd 02 03 ce 05 09  y.(...)} .....
0090 a2 00 9e 62 11 3b 47 20 d4 b5 49 76 b5 5a 97 b3  ...b.;G ..Iv.Z...
00a0 25 e7 81 f2 dc 72 6c 43 35 15 b0 d0 df 60 50 a3  %....r!C 5....`P..
00b0 5e 6d 50 00 63 3f 8c 73 f3 b5 03 d9 3a 17 3d 20  ^mP.c?.s .....=
00c0 a1 e9 76 2a 5d 04 cb ed 74 a9 39 c9 a4 94 fd dd  ..v*]... t.9.....
00d0 67 b8 22 85 24 5b b5 a2 ae 48 ef 90 8a 9e dc 41  g.".$[...H....A..
00e0 6c da fe e8 9c 6e 40 2a 1e b3 10 9c 5f 29 92 cc  l.....n@* ...._)..
00f0 d2 5d 37 09 44 3d ce 69 d7 33 dc 3d 2e 26 ea 7d  .]7.D=..i .3=..&..
0100 fe 64 3f 27 17 06 66 62 a3 80 f8 e0 63 6f bb 3f  .d?...'fb ....co.?
0110 8a 55 d5 4b 22 12 b7 8e a2 d6 01 88 9f 26 9e d5  .U.K"... ..&...
0120 4a 98 72 16 ab 9f 2e 7e 44 c1 17 77 12 0b 88 e2  J.r....~ D..w....
0130 d0 66 30 98 c3 d3 bb 5b 7c ac 44 7a b3 91 14 50  .f0....[ |.Dz...P
  
```

Each row represents a single packet

Once an interface is selected, it will begin capturing packets!

Let's start generating some HTTP traffic!

We can do this via browsing the web, or through one of our other tools (curl, postman, etc)

If you use a web browser, I recommend using an incognito/private window

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1948	5.275252	192.168.1.4	66.22.231.8	UDP	94	54038 → 50003 Len=52
1949	5.276205	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1950	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1951	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1952	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1953	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1954	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1955	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1956	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1957	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1958	5.296643	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1959	5.303321	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1960	5.303450	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1961	5.303546	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1962	5.303689	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1963	5.303776	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152

< Frame 1: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface 0
 > Ethernet II, Src: Netgear_2b:78:46 (9c:3d:cf:2b:78:46), Dst: Giga-Byt_a
 > Internet Protocol Version 4, Src: 66.22.231.8, Dst: 192.168.1.4
 > User Datagram Protocol, Src Port: 50003, Dst Port: 54038
 > Data (1126 bytes)

This will issue an HTTP request to download an HTML file

Historical Documents:THE BILL OF RIGHTS

Not secure | wireshark.grydeske.net/file3.html

THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.


Amendment IV

<http://wireshark.grydeske.net/file3.html>

(must use HTTP, not HTTPS)

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1948	5.275252	192.168.1.4	66.22.231.8	UDP	94	54038 → 50003 Len=52
1949	5.276205	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1950	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1951	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1952	5.287137	66.22.231.8	192.168.1.4	UDP	1193	50003 → 54038 Len=1151
1953	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1954	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1955	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1956	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1957	5.287137	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1958	5.296643	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1959	5.303321	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1960	5.303450	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1961	5.303546	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1962	5.303689	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152
1963	5.303776	66.22.231.8	192.168.1.4	UDP	1194	50003 → 54038 Len=1152

> Frame 1: 1168 bytes on wire (9344 bits), 1168 bytes captured (9344 bits) on interface 0

> Ethernet II, Src: Netgear_2b:78:46 (9c:3d:cf:2b:78:46), Dst: Giga-Byt_a

> Internet Protocol Version 4, Src: 66.22.231.8, Dst: 192.168.1.4

> User Datagram Protocol, Src Port: 50003, Dst Port: 54038

> Data (1126 bytes)

Historical Documents:THE BILL

Not secure | wireshark.grydeske.net/file3.html

Incognito

THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

Once the page is loaded, press the red square button to stop collecting data

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

<

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface
 > Ethernet II, Src: Giga-Byte (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46 (94:69:76:2b:78:46)
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84
 > Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
 > Hypertext Transfer Protocol

0000 9c 3d cf 2b 78 46 e0 d5 5e ae b1 0f 08 00 45 00 ..+xF.. ^....E.
 0010 01 e7 98 61 40 00 80 06 00 00 c0 a8 01 04 34 d4 ...a@... ..4.
 0020 34 54 f1 af 00 50 c1 f5 f3 4c e2 1c 52 6f 50 18 4T...P...L..RoP.
 0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 .,...GE T /file3
 0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
 0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wi reshark.
 0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net..Co
 0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
 0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up grade-In
 0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
 00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1..User -Agent:
 00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
 00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi
 00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64) Apple
 00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH
 00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, lik e Gecko)
 0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e Chrome/ 116.0.0.
 0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36.
 0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht
 0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x

We can add a **display filter** to filter out any non-http traffic

Add the filter `http`

This will show only HTTP packets

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

< >

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
 > Ethernet II, Src: Giga-Byt_ea:b1:0f (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84
 > Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
 > Hypertext Transfer Protocol
 > GET /file3.html HTTP/1.1\r\n
 > [Expert Info (Chat/Sequence): GET /file3.html HTTP/1.1\r\n]
 > Request Method: GET
 > Request URI: /file3.html
 > Request Version: HTTP/1.1
 > Host: wireshark.grydeske.net\r\n
 > Connection: keep-alive\r\n
 > Upgrade-Insecure-Requests: 1\r\n
 > User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36\r\n
 > Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 > Accept-Encoding: gzip, deflate\r\n
 > Accept-Language: en-US,en;q=0.9\r\n

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ... GET /file3
 0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HTTP/1.1
 0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wireshark.
 0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske.net
 0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection: keep-a
 0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e liveUp grade-In
 0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-Requests:
 00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1User-Agent:
 00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
 00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi
 00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64) AppleW
 00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH
 00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, like Gecko)
 0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e Chrome/ 116.0.0.
 0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari/537.36
 0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 Accept: text/ht
 0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,application/x
 0140 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 html+xml, applica
 0150 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml;q=0.9,i
 0160 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f mage/avi f, image/

Click on the first packet

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface
> Ethernet II, Src: Giga-Byt_ea:b1:0f (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84
> Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼ Hypertext Transfer Protocol
 > GET /file3.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /file3.html HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /file3.html
 Request Version: HTTP/1.1
Host: wireshark.grydeske.net\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ... GET /file3
0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HTTP/1.1
0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wireshark.
0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske.net
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection: keep-a
0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e liveUp grade-In
0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-Requests:
00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1User-Agent:
00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi
00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64) AppleW
00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH
00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, like Gecko)
0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e Chrome/ 116.0.0.
0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari/537.36
0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 Accept: text/ht
0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,application/x
0140 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 html+xml, applica
0150 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml;q=0.9,i
0160 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f mage/avi f,image/

Click on the first packet

This pane shows detailed information about the entire packet (at all layers of the OSI)

We can click the “Hypertext Transfer Protocol” dropdown to view contents of the HTTP Request/Response

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

This is the HTTP Request (arrow pointing right)

HTTP Method

HTTP Version

Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
> Ethernet II, Src: Giga-Byte (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84
> Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼ Hypertext Transfer Protocol
 > GET /file3.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /file3.html HTTP/1.1\r\n
 Request Method: GET
 Request URI: /file3.html
 Request Version: HTTP/1.1
Host: wireshark.grydeske.net\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ... GET /file3
0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0ahtml HTTP/1.1
0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e ... Host: wireshark.
0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f ... grydeske.net
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 ... Connection: keep-a
0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e ... liveUp grade-In
0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a ... secure-Requests:
00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 ... 1>User-Agent:
00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e ... Mozilla/ 5.0 (Win
00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 ... dows NT 10.0; Wi
00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 ... n64; x64) AppleW
00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ... ebKit/53 7.36 (KH
00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 ... TML, like Gecko)
0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e ... Chrome/ 116.0.0.
0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d ... 0 Safari /537.36
0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 ... Accept: text/ht
0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ... ml,application/x
0140 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 ... html+xml, applica
0150 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 ... tion/xml;q=0.9,i
0160 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f ... mage/avi f,image/

Click on the first packet

This pane shows detailed information about the entire packet (at all layers of the OSI)

We can click the “Hypertext Transfer Protocol” dropdown to view contents of the HTTP Request/Response

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

Header Fields

URL of request

GET /file3.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /file3.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /file3.html

Request Version: HTTP/1.1

Host: wireshark.grydeske.net\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

[Full request URI: http://wireshark.grydeske.net/file3.html]

[HTTP request 1/2]

[Response in frame: 11675]

[Next request in frame: 11710]

0000 9c 3d cf 2b 78 46 e0 d5 5e ae b1 0f 08 00 45 00 ...+xF...^.....E..

0010 01 e7 98 61 40 00 80 06 00 00 c0 a8 01 04 34 d4 ...a@...4..

0020 34 54 f1 af 00 50 c1 f5 f3 4c e2 1c 52 6f 50 18 4T...P...L...RoP..

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ...GE T /file3..

0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..

0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wi reshark..

0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net..Co

0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a

0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up grade-In

0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:

00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1..User -Agent:

00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win

00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi

00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64) AppleW

00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH

00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, lik e Gecko)

0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e Chrome/ 116.0.0.

0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36.

0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht

0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x

Click on the first packet

This pane shows detailed information about the entire packet (at all layers of the OSI)

We can click the “Hypertext Transfer Protocol” dropdown to view contents of the HTTP Request/Response

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

The second packet is the HTTP Response (arrow pointing left)



```
> Frame 11675: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on i
> Ethernet II, Src: Netgear_2b:78:46 (9c:3d:cf:2b:78:46), Dst: Giga-Byt_ae:b1:0f
> Internet Protocol Version 4, Src: 52.212.52.84, Dst: 192.168.1.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 61871, Seq: 4381, Ack: 4
> [4 Reassembled TCP Segments (4749 bytes): #11672(1460), #11673(1460), #11674(14
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Connection: keep-alive\r\n
      Server: nginx\r\n
      Date: Fri, 08 Sep 2023 05:19:10 GMT\r\n
      Content-Type: text/html\r\n
      > Content-Length: 4500\r\n
```

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

Response Status Code

HTTP Version of Response

<

> Frame 11675: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on i

> Ethernet II, Src: Netgear_2b:78:46 (9c:3d:cf:2b:78:46), Dst: Giga-Byt_ae:b1:0f

> Internet Protocol Version 4, Src: 52.212.52.84, Dst: 192.168.1.4

> Transmission Control Protocol, Src Port: 80, Dst Port: 4381, Seq: 4381, Ack: 4

> [4 Reassembled TCP Segments (4749 bytes): #11672(1460), #11673(1460), #11674(14

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Connection: keep-alive\r\n

Server: nginx\r\n

Date: Fri, 08 Sep 2023 05:19:10 GMT\r\n

Content-Type: text/html\r\n

> Content-Length: 4500\r\n

0000	e0 d5 5e ae b1 0f 9c 3d	cf 2b 78 46 08 00 45 00	..^....= ..xF..E..
0010	01 99 4e a3 40 00 29 06	d6 e7 34 d4 34 54 c0 a8	..N.@.).. ..4·4T..
0020	01 04 00 50 f1 af e2 1c	63 8b c1 f5 f5 0b 50 18	...P.... c.....P·
0030	00 46 3d a1 00 00 68 65	20 43 6f 6e 73 74 69 74	·F=...he Constit
0040	75 74 69 6f 6e 2c 20 6f	66 20 63 65 72 74 61 69	ution, o f certai
0050	6e 20 72 69 67 68 74 73	2c 20 73 68 61 6c 6c 0a	n rights , shall·
0060	6e 6f 74 20 62 65 20 63	6f 6e 73 74 72 75 65 64	not be c onstrued
0070	20 74 6f 20 64 65 6e 79	20 6f 72 20 64 69 73 70	to deny or disp
0080	61 72 61 67 65 20 6f 74	68 65 72 73 20 72 65 74	arage ot hers ret
0090	61 69 6e 65 64 20 62 79	20 74 68 65 20 70 65 6f	ained by the peo
00a0	70 6c 65 2e 0a 0a 3c 2f	70 3e 3c 70 3e 3c 61 20	ple...</ p><p><a
00b0	6e 61 6d 65 3d 22 31 30	22 3e 3c 73 74 72 6f 6e	name="10 "><stron
00c0	67 3e 3c 68 33 3e 41 6d	65 6e 64 6d 65 6e 74 20	g><h3>Am endment
00d0	58 3c 2f 68 33 3e 3c 2f	73 74 72 6f 6e 67 3e 3c	X</h3></ strong><
00e0	2f 61 3e 0a 0a 3c 70 3e	3c 2f 70 3e 0a 3c 70 3e	/a>...<p> </p><p>
00f0	54 68 65 20 70 6f 77 65	72 73 20 6e 6f 74 20 64	The powe rs not d
0100	65 6c 65 67 61 74 65 64	20 74 6f 20 74 68 65 20	elegated to the
0110	55 6e 69 74 65 64 20 53	74 61 74 65 73 20 62 79	United S tates by
0120	20 74 68 65 20 43 6f 6e	73 74 69 74 75 74 69 6f	the Con stitutio

This pane will try to decode the contents of the HTTP request/HTTP response (HTML)

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

<

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
 > Ethernet II, Src: Giga-Byt_e:08:00:27:00:00, Dst: Netgear_2b:78:46
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84
 > Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
 Source Port: 61871
 Destination Port: 80
 [Stream index: 30]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 447]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 3254121292
 [Next Sequence Number: 448 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 3793506927
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x018 (PSH, ACK)
 Window: 1026

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ..,...GET /file3
 0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HTTP/1.1..
 0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wireshark.
 0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net..Co
 0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
 0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up grade-In
 0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
 00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1..User -Agent:
 00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win
 00c0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 dows NT 10.0; Wi
 00d0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64) AppleW
 00e0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/53 7.36 (KH
 00f0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, like Gecko)
 0100 20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e Chrome/ 116.0.0.
 0110 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36.
 0120 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 .Accept: text/ht
 0130 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,application/x
 0140 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 html+xml ,applica
 0150 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml;q=0.9,i
 0160 6d 61 67 65 2f 61 76 69 66 2f 69 6d 61 67 65 2f mages/avi f image/

By clicking on
 “Transmission
 Control Protocol”
 we can see
 information about
 the transport
 layer

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11861	28.909214	52.212.52.84	192.168.1.4	HTTP	1111	HTTP/1.1 200 OK (text/plain)

This traffic is happening on port 61871 on our local machine

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0

> Ethernet II, Src: Giga-Byte Ethernet (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84

> Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, Len: 501

Source Port: 61871

Destination Port: 80

[Stream index: 30]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 447]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3254121292

[Next Sequence Number: 448 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3793506927

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 1026

0030	04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33	..,...GET /file3
0040	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HTTP/1.1
0050	48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e	Host: wireshark.
0060	67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f	grydeske.net..Co
0070	6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61	nnnection: keep-a
0080	6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e	live..Up grade-In
0090	73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a	secure-Requests:
00a0	20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20	1..User-Agent:
00b0	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e	Mozilla/ 5.0 (Win
00c0	64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69	dows NT 10.0; Wi
00d0	6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57	n64; x64) AppleW
00e0	65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48	ebKit/53.7.36 (KH
00f0	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29	TML, like Gecko)
0100	20 43 68 72 6f 6d 65 2f 31 31 36 2e 30 2e 30 2e	Chrome/ 116.0.0.
0110	30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d	0 Safari /537.36
0120	0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74	.Accept: text/ht
0130	6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,application/x
0140	68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61	html+xml ,applica
0150	74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69	tion/xml;q=0.9,i
0160	6d 61 67 65 2f 61 76 69 66 2f 69 6d 61 67 65 2f	mage/svg+xml

By clicking on “Transmission Control Protocol” we can see information about the transport layer

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.srcport == 61871 || tcp.dstport == 61871

No.	Time	Source	Destination	Protocol	Length	Info
11499	28.088056	192.168.1.4	52.212.52.84	TCP	66	61871 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11583	28.264776	52.212.52.84	192.168.1.4	TCP	66	80 → 61871 [SYN, ACK] Seq=0 Ack=1 Win=35844 Len=0 MSS=1460 SACK_PERM WS=
11584	28.264843	192.168.1.4	52.212.52.84	TCP	54	61871 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11671	28.451302	52.212.52.84	192.168.1.4	TCP	60	80 → 61871 [ACK] Seq=1 Ack=448 Win=35840 Len=0
11672	28.453488	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=1 Ack=448 Win=35840 Len=1460 [TCP segment of a reas
11673	28.455657	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=1461 Ack=448 Win=35840 Len=1460 [TCP segment of a
11674	28.455657	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=2921 Ack=448 Win=35840 Len=1460 [TCP segment of a
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11680	28.455720	192.168.1.4	52.212.52.84	TCP	54	61871 → 80 [ACK] Seq=448 Ack=4750 Win=262656 Len=0
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11789	28.723309	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=4750 Ack=846 Win=35840 Len=1460 [TCP segment of a
11790	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=6210 Ack=846 Win=35840 Len=1460 [TCP segment of a
11791	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=7670 Ack=846 Win=35840 Len=1460 [TCP segment of a
11792	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=9130 Ack=846 Win=35840 Len=1460 [TCP segment of a
11793	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=10590 Ack=846 Win=35840 Len=1460 [TCP segment of a

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on i

> Ethernet II, Src: Giga-Byt_ae:b1:0f (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84

> Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, L

Source Port: 61871

Destination Port: 80

[Stream index: 30]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 447]

0020 34 54 f1 af 00 50 c1 f5 f3 4c e2 1c 52 6f 50 18 41 P...L..RoP.

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ..,..GE T /file3

0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..

0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wi reshark.

0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net..Co

0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a

0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live..Up grade-In

0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:

00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1..User -Agent:

00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win

Let's change our filter to `tcp.srcport == 61871 || tcp.dstport == 61871`

This will only show traffic where the source port or destination port is 61871

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.srcport == 61871 || tcp.dstport == 61871

No.	Time	Source	Destination	Protocol	Length	Info
11499	28.088056	192.168.1.4	52.212.52.84	TCP	66	61871 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11583	28.264776	52.212.52.84	192.168.1.4	TCP	66	80 → 61871 [SYN, ACK] Seq=0 Ack=1 Win=35844 Len=0 MSS=1460 SACK_PERM WS=
11584	28.264843	192.168.1.4	52.212.52.84	TCP	54	61871 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
11585	28.265019	192.168.1.4	52.212.52.84	HTTP	501	GET /file3.html HTTP/1.1
11671	28.451302	52.212.52.84	192.168.1.4	TCP	60	80 → 61871 [ACK] Seq=1 Ack=448 Win=35840 Len=0
11672	28.453488	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=1 Ack=448 Win=35840 Len=1460 [TCP segment of a reas
11673	28.455657	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=1461 Ack=448 Win=35840 Len=1460 [TCP segment of
11674	28.455657	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=2921 Ack=448 Win=35840 Len=1460 [TCP segment of a
11675	28.455657	52.212.52.84	192.168.1.4	HTTP	423	HTTP/1.1 200 OK (text/html)
11680	28.455720	192.168.1.4	52.212.52.84	TCP	54	61871 → 80 [ACK] Seq=448 Ack=4750 Win=262656 Len=0
11710	28.537098	192.168.1.4	52.212.52.84	HTTP	452	GET /favicon.ico HTTP/1.1
11789	28.723309	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=4750 Ack=846 Win=35840 Len=1460 [TCP segment of a
11790	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=6210 Ack=846 Win=35840 Len=1460 [TCP segment of
11791	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=7670 Ack=846 Win=35840 Len=1460 [TCP segment of a
11792	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [PSH, ACK] Seq=9130 Ack=846 Win=35840 Len=1460 [TCP segment of
11793	28.723859	52.212.52.84	192.168.1.4	TCP	1514	80 → 61871 [ACK] Seq=10590 Ack=846 Win=35840 Len=1460 [TCP segment of a

> Frame 11585: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on i

> Ethernet II, Src: Giga-Byt_ae:b1:0f (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 52.212.52.84

> Transmission Control Protocol, Src Port: 61871, Dst Port: 80, Seq: 1, Ack: 1, L

Source Port: 61871

Destination Port: 80

[Stream index: 30]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 447]

0020 34 54 f1 af 00 50 c1 f5 f3 4c e2 1c 52 6f 50 18 4T...P...L...RoP...

0030 04 02 2c ae 00 00 47 45 54 20 2f 66 69 6c 65 33 ...GE T /file3

0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1

0050 48 6f 73 74 3a 20 77 69 72 65 73 68 61 72 6b 2e Host: wi reshark.

0060 67 72 79 64 65 73 6b 65 2e 6e 65 74 0d 0a 43 6f grydeske .net Co

0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a

0080 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e live Up grade-In

0090 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:

00a0 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 1 User -Agent:

00b0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (Win

The first three packets is us establishing a TCP connection before we send our fist HTTP request!