

Microsoft Windows [Version 10.0.26120.4520]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Yahya>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . :
Link-local IPv6 Address : fe80::5237:79f1:1337:7c1a%2
IPv4 Address : 10.129.69.152
Subnet Mask : 255.255.255.0
Default Gateway : 10.129.69.228

C:\Users\Yahya>

C:\Users\Yahya>ping www.example.com

Pinging a1422.dscr.akamai.net [2.23.103.240] with 32 bytes of data:

Reply from 2.23.103.240: bytes=32 time=28ms TTL=58

Reply from 2.23.103.240: bytes=32 time=98ms TTL=58

Reply from 2.23.103.240: bytes=32 time=104ms TTL=58

Reply from 2.23.103.240: bytes=32 time=95ms TTL=58

Ping statistics for 2.23.103.240:

 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

 Minimum = 28ms, Maximum = 104ms, Average = 81ms

No.	http	Source	Destination	Protocol	Length	Info
3	http	86:70:93:61:96:16	2.23.103.233	HTTP	510	GET / HTTP/1.1
3	http2	86:70:93:61:96:16	10.129.69.152	HTTP	1032	HTTP/1.1 200 OK (text/html)
3	http3	86:70:93:61:96:16	2.23.103.233	HTTP	454	GET /favicon.ico HTTP/1.1
3584	17.470788	2.23.103.233	10.129.69.152	HTTP	242	HTTP/1.1 404 Not Found (text/html)
6588	69.442615	10.129.69.152	2.23.103.240	HTTP	454	GET /favicon.ico HTTP/1.1
6646	69.659931	2.23.103.240	10.129.69.152	HTTP	242	HTTP/1.1 404 Not Found (text/html)

3e. The IP address of PC is 10.129.69.152

3f. The version of HTTP is HTTP/1.1

```
> Frame 3543: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface \Device\NPF_{05950E6A-671C-450C-A8EB-437B968A5
> Ethernet II, Src: ChongqingFug_a4:50:eb (28:cd:c4:a4:50:eb), Dst: 86:70:93:61:96:16 (86:70:93:61:96:16)
> Internet Protocol Version 4, Src: 10.129.69.152, Dst: 2.23.103.233
> Transmission Control Protocol, Src Port: 49982, Dst Port: 80, Seq: 1, Ack: 1, Len: 456
> Hypertext Transfer Protocol
```

```
0000  86 70 93 61 96 16 28 cd c4 a4 50 eb 08 00 45 00  <--> P-a-( . .P--E-
0010  01 f0 f7 6d 40 00 00 06 47 81 00 81 45 98 02 17  . .m@---G---E---.
0020  67 e9 c3 3e 00 50 05 9b 1e 14 09 21 d0 6b 50 18  g-->P- . .!kP-
0030  00 ff 08 5c 00 00 47 45 54 20 2f 20 48 54 54 50  . .\`GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e  /1.1-Ho st: www.
0050  65 78 61 6d 70 6c 65 2e 63 6f 6d 0d 0a 43 6f 6e  example. com. Con
0060  66 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6e  nection: keep-al
0070  69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73  ive--Upg rade-Ins
0080  65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20  ecure-Re quest:
0090  31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  1--User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 64  ozilla/5.0 (Wind
00b0  6f 77 73 20 4e 54 28 31 30 2e 30 3b 20 57 69 6e  ows NT 1.0; Win
00c0  36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65  64; x64) AppleWebKit/537.36 (KHTML
00d0  62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54  like Gecko)
00e0  4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20  bkit/537.36 (KHTML
00f0  43 68 72 6f 6d 65 2f 31 33 39 2e 30 2e 30 2e 30  Chrome/1.39.0.0.0
0100  20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45  Safari/537.36 E
0110  64 67 2f 31 33 39 2e 30 2e 30 2e 30 0d 0a 41 63  dg/139.0.0.0. Ac
0120  63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c  cept: te xt/html,
0130  61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d  application/xhtml
0140  62 2b 78 6d 6c 61 70 78 6c 69 63 61 74 69 6f  l+xml,application
0150  62 2f 78 6d 6c 3b 71 3d 30 2e 39 2e 69 6d 61 67  n/xml;q=0.9,image
0160  65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62  e/avif,image/webp,image/apng,*/*
0170  70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a  ;q=0.8,application
0180  3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69  on/signat e-exchan
0190  6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e  ge;v=b3; q=0.7- A
01a0  67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41  accept-En coding:
01b0  63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20  gzip, de flate- A
01c0  67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41  accept-La nguage:
01d0  63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20  ccept-La nguage:
```

```
> Frame 3543: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface \Device\NPF_{05950E6A-671C-450C-A8EB-437B96BA5
< Ethernet II, Src: ChongqingFug_a4:50:eb (28:cd:c4:a4:50:eb), Dst: 86:70:93:61:96:16 (86:70:93:61:96:16)
  > Destination: 86:70:93:61:96:16 (86:70:93:61:96:16)
  > Source: ChongqingFug_a4:50:eb (28:cd:c4:a4:50:eb)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 10.129.69.152, Dst: 2.23.103.233
> Transmission Control Protocol, Src Port: 49982, Dst Port: 80, Seq: 1, Ack: 1, Len: 456
> Hypertext Transfer Protocol
```

3b. MAC address of PC is 28:cd:c4:a4:50:eb

3d. The MAC address of gateway device is
86:70:93:61:96:16

28:cd:c4:a4:50:eb

Download Mac Details ↓

Vendor details

Address Prefix

28cdc4 ⓘ

Vendor / Company

CHONGQING FUGUI ELECTRONICS
CO.,LTD. ⓘ

Company Address

Building D21,No.1, East Zone 1st Road,Xiyong Town,Shapingba District Chongqing
Chongqing CN 401332 ⓘ

Is Private ?

No

Country Code

CN ⓘ

History

Download Results ↓

CHONGQING FUGUI ELECTRONICS
CO.,LTD.

Nov 5, 2019

Building D21,No.1, East Zone 1st
Road,Xiyong Town,Shapingba
District Chongqing Chongqing CN
401332

Detection Addition:

Vendor Address

2019

3c. vendor manufactured the network
card on PC => CHONGQING FUGUI
ELECTRONICS CO.,LTD.

Internet Protocol Version 4, Src: 10.129.69.152, Dst: 2.23.103.233

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 496

Identification: 0xf76d (63341)

> 010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x4781 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.129.69.152

Destination Address: 2.23.103.233

[Stream index: 23]

Transmission Control Protocol, Src Port: 49982, Dst Port: 80, Seq: 1, Ack: 1, Len: 456

Source Port: 49982

Destination Port: 80

[Stream index: 39]

[Stream Packet Number: 4]

> [Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 456]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 94051860

[Next Sequence Number: 457 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 153210987

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 255

[Calculated window size: 65280]

[Window size scaling factor: 256]

Checksum: 0x085c [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (456 bytes)

▼ Hypertext Transfer Protocol

➤ GET / HTTP/1.1\r\nHost: www.example.com\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/139.0.0.0 Safari/537.36 Edg/139.0.0.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1.0\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9,en-CA;q=0.8\r\n\r\n[\[Response in frame: 3545\]](#)
[\[Full request URI: http://www.example.com/\]](#)

3g. PC's operating system (OS) is Windows NT 10.0
(Windows 10)

3h. Browser language is en-US,en;q=0.9,en-CA;q=0.8



http

No.	Time	Source	Destination	Protocol	Length	Info
3543	17.036704	10.129.69.152	2.23.103.233	HTTP	510	GET / HTTP/1.1
3545	17.062429	2.23.103.233	10.129.69.152	HTTP	1032	HTTP/1.1 200 OK (text/html)
3569	17.245416	10.129.69.152	2.23.103.233	HTTP	454	GET /favicon.ico HTTP/1.1
3584	17.470788	2.23.103.233	10.129.69.152	HTTP	242	HTTP/1.1 404 Not Found (text/html)
6580	69.442615	10.129.69.152	2.23.103.240	HTTP	454	GET /favicon.ico HTTP/1.1
6646	69.659931	2.23.103.240	10.129.69.152	HTTP	242	HTTP/1.1 404 Not Found (text/html)

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 49982, Seq: 1, Ack: 457, Len: 978

Source Port: 80
Destination Port: 49982
[Stream index: 39]
[Stream Packet Number: 6]
➤ [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 978]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 153210987
[Next Sequence Number: 979 (relative sequence number)]
Acknowledgment Number: 457 (relative ack number)
Acknowledgment number (raw): 94052316
0101 ... = Header Length: 20 bytes (5)
➤ Flags: 0x018 (PSH, ACK)
Window: 501
[Calculated window size: 64128]
[Window size scaling factor: 128]
Checksum: 0x1093 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
➤ [Timestamps]
➤ [SEQ/ACK analysis]
TCP payload (978 bytes)

▼ Hypertext Transfer Protocol

➤ HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: text/html\r\nETag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"\r\nLast-Modified: Mon, 13 Jan 2025 20:11:20 GMT\r\nVary: Accept-Encoding\r\nContent-Encoding: gzip\r\nCache-Control: max-age=1307\r\nDate: Sun, 13 Jul 2025 14:55:08 GMT\r\nContent-Length: 648\r\nConnection: keep-alive\r\n\r\n[Request in frame: 3543]
[Time since request: 0.025725000 seconds]
[Request URI: /]
[Full request URI: http://www.example.com/]
Content-encoded entity body (gzip): 648 bytes -> 1256 bytes
File Data: 1256 bytes

▼ Line-based text data: text/html (46 lines)

0000 28 cd c4 a4 50 eb 86 70 93 61 96 16 08 00 45 00 (...P..p..a...E.
0010 03 fa cf 9a 40 00 3a 06 b3 4a 02 17 67 e9 0a 81 ...@:.J.g...
0020 45 98 00 50 c3 3e 09 21 d8 6b 05 9b 1f dc 50 18 E..P->!..k...P.
0030 01 f5 10 93 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 41 63 63 65 70 74 2d 52 61 00 OK..A ccept-Ra
0050 66 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e nges: by tes..Con
0060 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f tent-Typ e: text/
0070 68 74 6d 6c 0d 0a 45 54 61 67 3a 20 22 38 34 32 html..ET ag: "842
0080 33 38 64 66 63 38 30 39 32 65 35 64 39 63 30 64 38dfc809 2e5d9c0d
0090 61 63 38 65 66 39 33 33 37 31 61 30 37 3a 31 37 acbef933 71a07:17
00a0 33 36 37 39 30 38 30 2e 31 32 31 31 33 34 22 36799008 .121134"
00b0 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a ..Last-M odified:
00c0 20 4d 6f 6e 2c 20 31 33 20 4a 61 6e 20 32 30 32 Mon, 13 Jan 202
00d0 35 20 32 30 3a 31 31 3a 32 30 20 47 4d 54 0d 0a 5 20:11: 20 GMT..
00e0 56 61 72 79 3a 20 41 63 63 65 70 74 2d 45 6e 63 Vary: Ac cept-Enc
00f0 6f 64 69 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d 45 oding..C ontent-E
0100 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 1a 0d 0a 43 ncoding: gzip..C
0110 61 63 68 65 62 43 6f 74 72 6f 6c 3a 20 6d 61 acce-Con trol: ma
0120 78 2d 61 67 65 3d 31 33 30 37 0d 0a 44 61 74 65 x-age=13 07..Date
0130 3a 20 53 75 66 2c 20 31 33 20 4a 75 6c 20 32 30 : Sun, 1 3 Jul 20
0140 32 35 20 31 34 3a 35 3a 30 38 20 47 4d 54 0d 25 14:55 :08 GMT..
0150 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a Content -Length:
0160 20 36 34 38 0d 0a 43 6f 6e 65 63 74 69 6f 6e 648..Co nnection:
0170 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 0a :keep-a live...
0180 1f 8b 08 00 00 00 00 00 00 00 7d 54 4d 73 db 20:..TMs..
0190 10 bd fb 57 6d 5f 4b 32 23 24 27 69 1a 8f 2d 69 ...Wl-K2 #\$'i..i..
01a0 fa 99 69 0f 69 0f 3d 12 b1 b2 98 08 50 01 ..i..i.=...i..
01b0 c9 f6 74 f2 fd bb 42 8e 23 37 99 9a 91 81 5d 78 ..t...B. #7...].x
01c0 bb ef 91 9b 10 2d 12 a6 f4 bb 16 a1 f6 aa 29 66 d9(....)f..
01d0 63 87 5c 14 33 a9 5f e6 a5 6f b0 f8 bc e5 aa 6d c.\.3..o..m
01e0 10 19 c5 a5 ce d2 d1 3a 1b 97 28 f4 1c ca 9a ..>...:...:(...
01f0 5b 87 3e 8f 5f b1 45 04 69 31 71 d6 de b7 0c [>>..._E..i.lq...
0200 f7 77 b2 cf a3 8f 46 7b d4 9e 0d 61 23 28 c7 59 ..w...F{..a#(....Y
0210 1a 79 dc fa 74 08 bf 3a 4b 8d 44 69 c2 3e ea ..y..t...:@...<..<
0220 25 6e 5a 63 6d 44 ff 46 0a 5f e7 02 7b 59 22 0b %Nzcd-F ..(Y".
0230 93 18 a4 96 5e f2 86 b9 92 37 98 9f 3d 41 39 bf^...7..-A9.
0240 23 32 43 06 fb a5 73 d1 e8 bb 33 62 07 7f c2 #2C...s ..3b..
0250 30 4c 79 79 bf b6 a6 d3 82 95 a6 31 76 09 af ab 0Ly... ..1v...
0260 39 b5 f3 d5 61 89 e2 76 2d f5 12 e6 4f a6 96 0b 9...a..v ..0...
0270 21 f5 fa c8 56 51 a6 ac e2 4a 36 bb 25 30 de 92 !..VQ... ..16..%0..
0280 9c cc ed 9c 47 15 c3 d8 b3 4e c6 f0 a1 91 fa fe ..G... N...
0290 86 97 b7 c1 74 4d 9b 62 88 6e 71 6d 10 7e 7e 8d ..tM.b..nqm~~~
02a0 68 fc bd 45 0d b7 5c bb 61 f2 05 9b 1e bd 2c 39 h..E..!..a...9
02b0 7c c3 0e c9 72 30 c4 f0 de 12 77 c2 a6 a5 cc a1 |...r0.. ..w...
02c0 95 d5 53 2e 61 f0 fe 85 ec 27 74 83 70 4b 78 ..S.a... ..t..pKx
02d0 3b 9f 7f db e7 0c 2f 51 01 ef bc 79 81 e8 39 aa ;.../Q...y..9..
02e0 d5 7f 45 13 d4 26 19 dc 19 2b 0d 32 cb 85 ee 1c ..E...&.. +2...
02f0 e9 94 5c 1e 01 98 2d 73 35 17 66 43 c8 ed 16 2e ..\\"..s 5..fc...

Frame (1032 bytes) Uncompressed entity body (1256 bytes)

Packets: 8028 · Displayed: 6 (0.1%)

Profile: Default

ip.addr eq 10.129.69.152 and ip.addr eq 2.23.103.233

No.	Time	Source	Destination	Protocol	Length	Info
3520	17.004070	10.129.69.152	2.23.103.233	TCP	66	49982 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3521	17.004753	10.129.69.152	2.23.103.233	TCP	66	49983 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3539	17.035381	2.23.103.233	10.129.69.152	TCP	66	80 → 49983 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3540	17.035381	2.23.103.233	10.129.69.152	TCP	66	80 → 49982 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3541	17.035550	10.129.69.152	2.23.103.233	TCP	54	49983 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3542	17.035654	10.129.69.152	2.23.103.233	TCP	54	49982 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3543	17.036704	10.129.69.152	2.23.103.233	HTTP	510	GET / HTTP/1.1
3544	17.062429	2.23.103.233	10.129.69.152	TCP	54	80 → 49982 [ACK] Seq=1 Ack=457 Win=64128 Len=0
3545	17.062429	2.23.103.233	10.129.69.152	HTTP	1032	HTTP/1.1 200 OK (text/html)
3551	17.112259	10.129.69.152	2.23.103.233	TCP	54	49982 → 80 [ACK] Seq=457 Ack=979 Win=64512 Len=0
3569	17.245416	10.129.69.152	2.23.103.233	HTTP	454	GET /favicon.ico HTTP/1.1
3573	17.270421	2.23.103.233	10.129.69.152	TCP	54	80 → 49982 [ACK] Seq=979 Ack=857 Win=64128 Len=0
3583	17.470788	2.23.103.233	10.129.69.152	TCP	1514	80 → 49982 [ACK] Seq=979 Ack=857 Win=64128 Len=1460 [TCP PDU reassembled in 3584]
3584	17.470788	2.23.103.233	10.129.69.152	HTTP	242	HTTP/1.1 404 Not Found (text/html)
3585	17.470929	10.129.69.152	2.23.103.233	TCP	54	49982 → 80 [ACK] Seq=857 Ack=2627 Win=65280 Len=0
4011	26.022933	10.129.69.152	2.23.103.233	TCP	54	49983 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65280 Len=0
4012	26.023084	10.129.69.152	2.23.103.233	TCP	54	49982 → 80 [FIN, ACK] Seq=857 Ack=2627 Win=65280 Len=0
4044	26.058211	2.23.103.233	10.129.69.152	TCP	54	80 → 49983 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
4045	26.058211	2.23.103.233	10.129.69.152	TCP	54	80 → 49982 [FIN, ACK] Seq=2627 Ack=858 Win=64128 Len=0
4051	26.058511	10.129.69.152	2.23.103.233	TCP	54	49983 → 80 [ACK] Seq=2 Ack=2 Win=65280 Len=0
4052	26.058543	10.129.69.152	2.23.103.233	TCP	54	49982 → 80 [ACK] Seq=858 Ack=2628 Win=65280 Len=0
6786	74.366545	10.129.69.152	2.23.103.233	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 6788)
6788	74.416512	2.23.103.233	10.129.69.152	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=58 (request in 6786)
6794	75.377330	10.129.69.152	2.23.103.233	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 6795)
6795	75.412606	2.23.103.233	10.129.69.152	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=58 (request in 6794)
6900	76.392008	10.129.69.152	2.23.103.233	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 6901)
6901	76.488347	2.23.103.233	10.129.69.152	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=58 (request in 6900)
6917	77.402210	10.129.69.152	2.23.103.233	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 6918)
6918	77.427216	2.23.103.233	10.129.69.152	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=58 (request in 6917)

3a. TCP 3-way handshake interaction

> Frame 3545: 1032 bytes on wire (8256 bits), 1032 bytes captured (8256 bits) on interface \Device\NPF_{05950E6A-671C-450C-A8EB-437B96B
> Ethernet II, Src: 86:70:93:61:96:16 (86:70:93:61:96:16), Dst: ChongqingFug_a4:50:eb (28:cd:c4:a4:50:eb)
> Internet Protocol Version 4, Src: 2.23.103.233, Dst: 10.129.69.152
> Transmission Control Protocol, Src Port: 80, Dst Port: 49982, Seq: 1, Ack: 457, Len: 978
> Hypertext Transfer Protocol
> Line-based text data: text/html (46 lines)

0000	28 cd c4 a4 50 eb	86 70 93 61 96 16 08 00 45 00	(...P...p...a...E...
0010	03 fa cf 9a 40 00 3a 06	b3 4a 02 17 67 e9 0a 81	...@... J...g...
0020	45 98 00 50 c3 3e 09 21	d0 6b 05 9b 1f dc 50 18	E...P->! k...P...
0030	01 f5 10 93 00 48 54	54 50 2f 31 2e 31 20 32HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 41	63 63 65 70 74 2d 52 61	00 OK... A ccept-Ra
0050	6e 67 65 73 3a 20 62 79	74 65 73 0d 0a 43 6f 6e	nges: by tes... Con
0060	74 65 6e 74 2d 54 79 70	65 3a 20 74 65 78 74 2f	tent-Typ e: text/
0070	68 74 6d 6c 0d 0a 45 54	61 67 3a 26 22 38 34 32	html... ET ag: "842
0080	33 38 64 66 33 30 39	32 65 35 64 39 63 30 64	38dfc809 2e5d9c0d
0090	61 63 38 65 66 39 33	37 31 61 30 37 3a 31 37	ac8ef933 71a07:17
00a0	33 36 37 39 39 30 38 30	2e 31 32 31 31 33 34 22	36799080 .121134"

Frame (1032 bytes) Uncompressed entity body (1256 bytes)

Packets: 8028 · Displayed: 29 (0.4%)

Profile: Default

NETWORK TRAFFIC ANALYSIS REPORT

Introduction

This report analyzes the HTTP and TCP traffic captured during a session where the client PC accessed <http://www.example.com/>. The analysis focuses on key network parameters that can help improve performance, security, and network management (Kurose & Ross, 2021). The captured data provides insights into the client's network configuration and communication patterns.

Analysis Findings

a. TCP 3-way Handshake Interaction

The TCP 3-way handshake occurs in packets 3520-3522:

- **Packet 3520** (Time: 17.004970): TCP SYN from 10.129.69.152 to 2.23.103.233, port 80
- **Packet 3521** (Time: 17.004753): TCP SYN-ACK from 2.23.103.233 to 10.129.69.152
- **Packet 3539** (Time: 17.035381): TCP ACK completing the handshake

This shows the classic three-step process: SYN → SYN-ACK → ACK establishing a TCP connection.

b. MAC Address of the PC

The MAC address of the client PC is:

28:cd:c4:a4:50:eb

This is shown as the source MAC in the Ethernet II header of Frame 3543.

c. Network Card Manufacturer

Using the MAC address prefix **28:cd:c4**, the network interface card was manufactured by:
CHONGQING FUGUI ELECTRONICS CO.,LTD.

The vendor details show this is a Chinese electronics company based in Chongqing (IEEE Standards Association, 2022).

d. Gateway MAC Address

From the destination MAC addresses visible in the outgoing packets, the gateway device's MAC address appears to be: **86:70:93:61:96:16**

These MAC addresses are visible in the Ethernet frame headers of the captured packets, where the source MAC is your PC's network interface and the destination MAC is typically your router/gateway when communicating with external hosts.

e. PC IP Address

The source IP address in the captured traffic is:

10.129.69.152

This private IP address appears in the IPv4 header of Frame 3543.

f. HTTP Version

The HTTP request shows version:

HTTP/1.1

This appears in the GET request: "GET / HTTP/1.1\r\n"

g. PC Operating System

The User-Agent string reveals the OS platform:

Windows NT 10.0 (Windows 10)

The full string shows: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36..."

h. Browser Language Configuration

The Accept-Language header shows the browser is configured for:

en-US,en;q=0.9,en-CA;q=0.8

This indicates primary preference for US English, then general English, and Canadian English as tertiary preference.

Conclusion

The analysis reveals standard network communication patterns with no immediate red flags. The client is using Windows 10 with a Chinese-manufactured network interface card, communicating over HTTP/1.1. The browser language settings suggest an English-speaking user, possibly in North America. These findings provide a baseline for further network optimization and security hardening (Stallings, 2021).

References

IEEE Standards Association. (2022). IEEE SA - Registration Authority.

Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach. Pearson.

Stallings, W. (2021). Data and Computer Communications. Pearson.

.....