Wire Shark to understand operation of TCP/IP


```
arp                                                                                                      ☒ ➡
No.      Time        Source              Destination       Protocol  Length  Info
5673... 42.735782   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.38? Tell 192.168.31.1
5696... 46.734302   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.37? Tell 192.168.31.1
5709... 48.736116   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.28? Tell 192.168.31.1
5716... 49.734950   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.18? Tell 192.168.31.1
5747... 54.734395   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.38? Tell 192.168.31.1
5793... 61.734111   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.28? Tell 192.168.31.1
5823... 64.735205   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.37? Tell 192.168.31.1
5841... 66.733992   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.38? Tell 192.168.31.1
5853... 68.271803   Micro-St_c2:9d:17   Broadcast         ARP       42  Who has 192.168.0.251? Tell 192.168.31.27
5855... 68.746269   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.18? Tell 192.168.31.1
5857... 69.271744   Micro-St_c2:9d:17   Broadcast         ARP       42  Who has 192.168.0.251? Tell 192.168.31.27
5859... 70.272910   Micro-St_c2:9d:17   Broadcast         ARP       42  Who has 192.168.0.251? Tell 192.168.31.27
5866... 73.066755   Micro-St_e4:eb:d4   Broadcast         ARP       60  Who has 192.168.31.3? Tell 192.168.31.6
5866... 73.066755   Micro-St_e4:eb:d4   Broadcast         ARP       60  Who has 192.168.31.18? Tell 192.168.31.6
5866... 73.066755   Micro-St_e4:eb:d4   Broadcast         ARP       60  Who has 192.168.31.24? Tell 192.168.31.6
5887... 78.734668   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.38? Tell 192.168.31.1
5894... 79.734561   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.37? Tell 192.168.31.1
5900... 80.735218   TP-Link_05:6a:19    Broadcast         ARP       60  Who has 192.168.31.18? Tell 192.168.31.1

> Frame 7701: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: TP-Link_05:6a:19 (9c:53:22:05:6a:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
∨ Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: TP-Link_05:6a:19 (9c:53:22:05:6a:19)
      Sender IP address: 192.168.31.1
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 192.168.31.38
```



```
udp                                                                                                      ☒ ➡
No.      Time        Source              Destination       Protocol  Length  Info
3886 39.960885   192.168.31.27       203.212.24.46     DNS        95  Standard query 0x46a9 A 1D.tlu.dl.delivery.mp.microsoft.com
3887 39.962412   203.212.24.46       192.168.31.27     DNS       317  Standard query response 0x46a9 A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
4001 40.160730   94.29.19.112        192.168.31.27     BT-DHT    159  BitTorrent DHT Protocol
4002 40.160996   192.168.31.27       94.29.19.112      BT-DHT    340  BitTorrent DHT Protocol reply=8 nodes
4725 40.925976   192.168.31.27       203.212.24.46     DNS        95  Standard query 0x084c A 1D.tlu.dl.delivery.mp.microsoft.com
4726 40.927664   203.212.24.46       192.168.31.27     DNS       317  Standard query response 0x084c A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
4782 40.968153   183.21.188.246      192.168.31.27     BT-DHT    143  BitTorrent DHT Protocol
4783 40.968322   192.168.31.27       183.21.188.246    BT-DHT    344  BitTorrent DHT Protocol reply=8 nodes
6250 41.674673   152.89.162.6        192.168.31.27     BT-DHT    297  BitTorrent DHT Protocol
6251 41.674863   192.168.31.27       152.89.162.6      BT-DHT     91  BitTorrent DHT Protocol
7637 43.408337   192.168.31.27       203.212.24.46     DNS        76  Standard query 0x7a45 A pool.minexmr.com
7638 43.409879   203.212.24.46       192.168.31.27     DNS       136  Standard query response 0x7a45 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com

> Frame 7638: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: TP-Link_05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:9d:17 (d8:bb:c1:c2:9d:17)
> Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.27
∨ User Datagram Protocol, Src Port: 53, Dst Port: 58418
      Source Port: 53
      Destination Port: 58418
      Length: 102
      Checksum: 0x79b7 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 7]
   > [Timestamps]
      UDP payload (94 bytes)
> Domain Name System (response)
```

http

No.	Time	Source	Destination	Protocol	Length	Info
3210	39.029784	192.168.31.27	209.197.3.8	HTTP	369	GET /filestreamingservice/files/28edaebf-8019-4844-ba32-8ab019bc9391/pieceshash HTTP/1.1
3260	39.096641	209.197.3.8	192.168.31.27	HTTP	291	HTTP/1.1 403 Forbidden
3339	39.182531	209.197.3.8	192.168.31.27	HTTP	252	HTTP/1.1 200 OK
3445	39.302336	192.168.31.27	209.197.3.8	HTTP	498	GET /filestreamingservice/files/28edaebf-8019-4844-ba32-8ab019bc9391?P1=1697170641&P2=404&P3=2&P4=lNrueYOjOuP6mC4Z0qTUs
3513	39.400388	209.197.3.8	192.168.31.27	HTTP	291	HTTP/1.1 403 Forbidden

```
> Internet Protocol Version 4, Src: 175.100.184.168, Dst: 192.168.31.27
> Transmission Control Protocol, Src Port: 80, Dst Port: 8575, Seq: 4296, Ack: 2581, Len: 859
v Hypertext Transfer Protocol
  > HTTP/1.1 206 Partial Content\r\n
    Cache-Control: public, max-age=17280000\r\n
    Content-Type: application/x-chrome-extension\r\n
    Last-Modified: Tue, 17 Oct 2023 06:34:45 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "CGCsOkvfA9w7B2FV8bZcgYSuFgY="\r\n
    X-AspNetMvc-Version: 5.2\r\n
    MS-CorrelationId: e23840bf-45b6-407d-b583-e2667930bc9e\r\n
    MS-RequestId: 8f33fc93-a53b-4f14-9de0-1228964e8f03\r\n
    MS-CV: ORQLzNj/v0mTX2kN.0\r\n
    X-AspNet-Version: 4.0.30319\r\n
    X-Powered-By: ASP.NET\r\n
    X-Powered-By: ARR/3.0\r\n
    X-Powered-By: ASP.NET\r\n
    X-Azure-Ref-OriginShield: Ref A: 7D053F5E115148AD8A4579F7A4849170 Ref B: MNZ221060605007 Ref C: 2023-10-17T06:39:00Z\r\n
    X-MSEdge-Ref: Ref A: F24D50326EB84AE9888E3B9588188061 Ref B: BN3EDGE0917 Ref C: 2023-10-17T06:39:00Z\r\n
    Date: Tue, 17 Oct 2023 09:30:56 GMT\r\n
    Content-Range: bytes 371-387/59434\r\n
  > Content-Length: 17\r\n
    Connection: keep-alive\r\n
    X-CID: 2\r\n
    X-CCC: IN\r\n
    \r\n
    [HTTP response 6/19]
    [Time since request: 0.007530000 seconds]
    [Prev request in frame: 647]
    [Prev response in frame: 648]
    [Request in frame: 7536]
    [Next request in frame: 13030]
    [Next response in frame: 13035]
    [Request URI [truncated]: http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/621a4ceb-00df-4de7-b7ca-42b2435b0a29?P1=1698131432&P2=404&P3=2&P4=ZUOqRGLToLmonsl2WPl…
    File Data: 17 bytes
> Media Type
```

dns

No.	Time	Source	Destination	Protocol	Length	Info
3886	39.960885	192.168.31.27	203.212.24.46	DNS	95	Standard query 0x46a9 A 1D.tlu.dl.delivery.mp.microsoft.com
3887	39.962412	203.212.24.46	192.168.31.27	DNS	317	Standard query response 0x46a9 A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
4725	40.925976	192.168.31.27	203.212.24.46	DNS	95	Standard query 0x084c A 1D.tlu.dl.delivery.mp.microsoft.com
4726	40.927664	203.212.24.46	192.168.31.27	DNS	317	Standard query response 0x084c A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
7637	43.408337	192.168.31.27	203.212.24.46	DNS	76	Standard query 0x7a45 A pool.minexmr.com
7638	43.409879	203.212.24.46	192.168.31.27	DNS	136	Standard query response 0x7a45 No such name A pool.minexmr.com SOA frank.ns.cloudflare.com
7936	44.895941	192.168.31.27	203.212.24.46	DNS	95	Standard query 0xf9df A 1D.tlu.dl.delivery.mp.microsoft.com
7937	44.899030	203.212.24.46	192.168.31.27	DNS	317	Standard query response 0xf9df A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
8507	45.064794	192.168.31.27	203.212.24.46	DNS	95	Standard query 0x10e2 A 1D.tlu.dl.delivery.mp.microsoft.com
8542	45.068274	203.212.24.46	192.168.31.27	DNS	317	Standard query response 0x10e2 A 1D.tlu.dl.delivery.mp.microsoft.com CNAME dcat-tlu-bg-shim.trafficmanager.net CNAME cd
10279	45.932163	192.168.31.27	203.212.24.46	DNS	95	Standard query 0xd230 A 1D.tlu.dl.delivery.mp.microsoft.com

```
> Frame 7637: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:9d:17 (d8:bb:c1:c2:9d:17), Dst: TP-Link_05:6a:19 (9c:53:22:05:6a:19)
> Internet Protocol Version 4, Src: 192.168.31.27, Dst: 203.212.24.46
v User Datagram Protocol, Src Port: 58418, Dst Port: 53
    Source Port: 58418
    Destination Port: 53
    Length: 42
    Checksum: 0xc401 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (34 bytes)
v Domain Name System (query)
    Transaction ID: 0x7a45
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 7638]
```

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7717	43.959047	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [PSH, ACK] Seq=1328674 Ack=855 Win=68096 Len=1428 TSval=2421965003 TSecr=961678702 [TCP segment of a reassem
7718	43.959075	192.168.31.27	209.197.3.8	TCP	66	8629 → 80 [ACK] Seq=855 Ack=1330102 Win=13056 Len=0 TSval=961678788 TSecr=2421965003
7719	43.974390	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [ACK] Seq=1330102 Ack=855 Win=68096 Len=1428 TSval=2421965018 TSecr=961678719 [TCP segment of a reassembled P
7720	43.974415	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [PSH, ACK] Seq=1331530 Ack=855 Win=68096 Len=1428 TSval=2421965018 TSecr=961678719 [TCP segment of a reassembl
7721	43.974430	192.168.31.27	209.197.3.8	TCP	66	8629 → 80 [ACK] Seq=855 Ack=1332958 Win=13056 Len=0 TSval=961678804 TSecr=2421965018
7722	43.988054	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [ACK] Seq=1332958 Ack=855 Win=68096 Len=1428 TSval=2421965032 TSecr=961678732 [TCP segment of a reassembled
7723	43.988174	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [PSH, ACK] Seq=1334386 Ack=855 Win=68096 Len=1428 TSval=2421965032 TSecr=961678732 [TCP segment of a reassembl
7724	43.988191	192.168.31.27	209.197.3.8	TCP	66	8629 → 80 [ACK] Seq=855 Ack=1335814 Win=13056 Len=0 TSval=961678817 TSecr=2421965032
7725	44.027337	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [ACK] Seq=1335814 Ack=855 Win=68096 Len=1428 TSval=2421965069 TSecr=961678772 [TCP segment of a reassembled
7726	44.027404	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [PSH, ACK] Seq=1337242 Ack=855 Win=68096 Len=1428 TSval=2421965069 TSecr=961678772 [TCP segment of a reassem
7727	44.027421	192.168.31.27	209.197.3.8	TCP	66	8629 → 80 [ACK] Seq=855 Ack=1338670 Win=13056 Len=0 TSval=961678857 TSecr=2421965069
7728	44.044027	209.197.3.8	192.168.31.27	TCP	1494	80 → 8629 [ACK] Seq=1338670 Ack=855 Win=68096 Len=1428 TSval=2421965087 TSecr=961678788 [TCP segment of a reassembled P

```
> Frame 7700: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:9d:17 (d8:bb:c1:c2:9d:17), Dst: TP-Link_05:6a:19 (9c:53:22:05:6a:19)
> Internet Protocol Version 4, Src: 192.168.31.27, Dst: 209.197.3.8
v Transmission Control Protocol, Src Port: 8629, Dst Port: 80, Seq: 855, Ack: 1317754, Len: 0
    Source Port: 8629
    Destination Port: 80
    [Stream index: 30]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 855    (relative sequence number)
    Sequence Number (raw): 474013780
    [Next Sequence Number: 855    (relative sequence number)]
    Acknowledgment Number: 1317754    (relative ack number)
    Acknowledgment number (raw): 3619320074
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 46
    [Calculated window size: 11776]
    [Window size scaling factor: 256]
    Checksum: 0xb4b7 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
```

ip.addr == 192.168.31.27

No.	Time	Source	Destination	Protocol	Length	Info
295	19.091173	192.168.31.27	40.119.249.228	TLSv1.2	268	Client Hello
296	19.154521	40.119.249.228	192.168.31.27	TCP	1494	443 → 8607 [ACK] Seq=1 Ack=215 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
297	19.154632	40.119.249.228	192.168.31.27	TCP	1494	443 → 8607 [ACK] Seq=1441 Ack=215 Win=4194304 Len=1440 [TCP segment of a reassembled PDU]
298	19.154649	40.119.249.228	192.168.31.27	TCP	54	8607 → 443 [ACK] Seq=215 Ack=2881 Win=132352 Len=0
299	19.154671	40.119.249.228	192.168.31.27	TLSv1.2	932	Server Hello, Certificate, Server Key Exchange, Server Hello Done
300	19.156564	192.168.31.27	40.119.249.228	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
301	19.219303	40.119.249.228	192.168.31.27	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
302	19.219303	40.119.249.228	192.168.31.27	TLSv1.2	123	Application Data
303	19.219338	192.168.31.27	40.119.249.228	TCP	54	8607 → 443 [ACK] Seq=373 Ack=3879 Win=131328 Len=0
304	19.225228	192.168.31.27	40.119.249.228	TLSv1.2	141	Application Data
305	19.225251	192.168.31.27	40.119.249.228	TLSv1.2	559	Application Data
306	19.225287	192.168.31.27	40.119.249.228	TLSv1.2	92	Application Data

> Frame 313: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: TP-Link_05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:9d:17 (d8:bb:c1:c2:9d:17)
> Internet Protocol Version 4, Src: 40.119.249.228, Dst: 192.168.31.27
> Transmission Control Protocol, Src Port: 443, Dst Port: 8607, Seq: 4273, Ack: 1004, Len: 42
> Transport Layer Security

```
C:\Users\complab301pc25>ping 192.168.31.37

Pinging 192.168.31.37 with 32 bytes of data:
Reply from 192.168.31.37: bytes=32 time=2ms TTL=128
Reply from 192.168.31.37: bytes=32 time=2ms TTL=128
Reply from 192.168.31.37: bytes=32 time=3ms TTL=128
Reply from 192.168.31.37: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.31.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

igmp

No.	Time	Source	Destination	Protocol	Length	Info
6162...	1109.366846	192.168.31.37	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6162...	1109.388365	192.168.31.27	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
6162...	1109.418736	192.168.31.38	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6162...	1109.457133	192.168.31.28	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6162...	1109.514052	192.168.31.21	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6163...	1109.536113	192.168.31.31	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6163...	1109.546761	192.168.31.11	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6163...	1109.553543	192.168.31.3	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
6163...	1115.053558	192.168.31.1	239.255.255.250	IGMPv3	60	Membership Query, specific for group 239.255.255.250
6163...	1115.082551	192.168.31.18	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
6163...	1115.209549	192.168.31.6	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources

> Frame 613166: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A87B7A28-2BA4-4DA3-B2C3-A3348EBA2A15}, id 0
> Ethernet II, Src: Micro-St_c2:9b:e4 (d8:bb:c1:c2:9b:e4), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 192.168.31.31, Dst: 224.0.0.22
∨ Internet Group Management Protocol
    [IGMP Version: 3]
    Type: Membership Report (0x22)
    Reserved: 00
    Checksum: 0xfb8c [correct]
    [Checksum Status: Good]
    Reserved: 0000
    Num Group Records: 1
  > Group Record : 224.0.0.113 Mode Is Exclude