CN Lab 3
Wireshark Document
Vishal Puneyani (CSE – A) : 210905037

UDP PACKET ANALYSIS

A.

dns

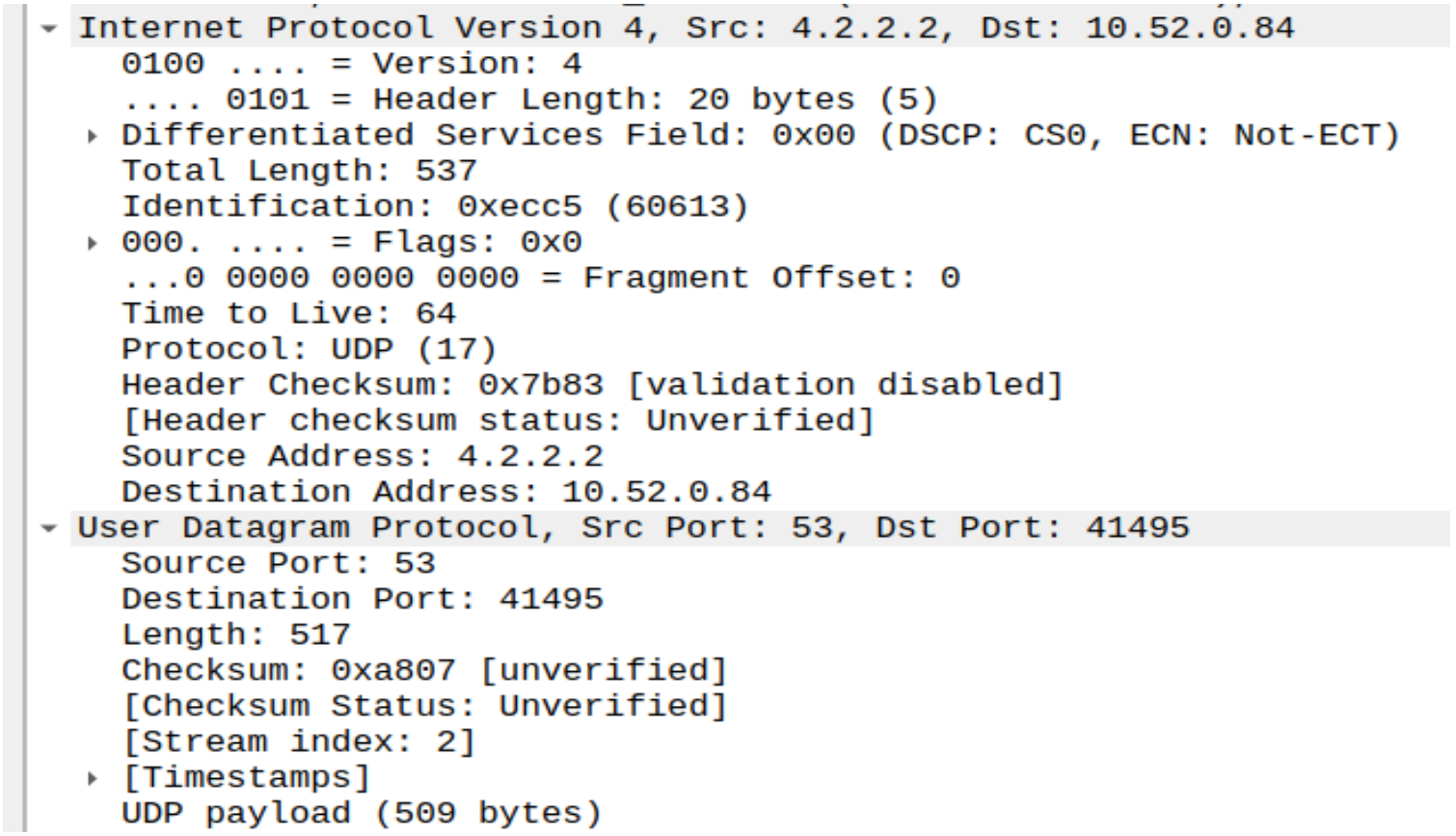
No.	Time	Source	Destination	Protocol	Length	Info
16	2.339363211	10.52.0.84	4.2.2.2	DNS	68	Standard query 0x0e68 A time.com
17	2.339469119	10.52.0.84	4.2.2.2	DNS	68	Standard query 0xcae9 AAAA time.com
18	2.428393699	4.2.2.2	10.52.0.84	DNS	551	Standard query response 0x0e68 A time.com A 52.84.251.128 A 52.84.251.10 A 52.84.251.51 A 52.84.251.121 NS j.root-se…
19	2.440506559	4.2.2.2	10.52.0.84	DNS	487	Standard query response 0xcae9 AAAA time.com NS l.root-servers.net NS d.root-servers.net NS a.root-servers.net NS b.…
23	4.350108436	10.52.0.84	4.2.2.2	DNS	69	Standard query 0x6444 A psyche.co
24	4.350174911	10.52.0.84	4.2.2.2	DNS	69	Standard query 0x5f1e AAAA psyche.co
25	4.435750705	4.2.2.2	10.52.0.84	DNS	488	Standard query response 0x5f1e AAAA psyche.co NS h.root-servers.net NS c.root-servers.net NS k.root-servers.net NS f…
26	4.439286053	4.2.2.2	10.52.0.84	DNS	504	Standard query response 0x6444 A psyche.co A 76.76.21.21 NS c.root-servers.net NS k.root-servers.net NS f.root-serve…

```
▾ Internet Protocol Version 4, Src: 10.52.0.84, Dst: 4.2.2.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 54
    Identification: 0x05a5 (1445)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x6487 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.52.0.84
    Destination Address: 4.2.2.2
▾ User Datagram Protocol, Src Port: 41495, Dst Port: 53
    Source Port: 41495
    Destination Port: 53
    Length: 34
    Checksum: 0x9a12 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  ▸ [Timestamps]
    UDP payload (26 bytes)
```

DNS Query Packet 16

a) Source port number : 41495
b) Destination port number : 53
c) Length of user datagram : 34 bytes
d) Length of data : 68 bytes
e) Packet directed from Client to Server as Source IP is of user's laptop and Destination IP is of server.
f) **Application layer protocol** : DNS
g) Checksum status unverified (0x9a12)

B.



DNS response packet 18

Source IP (Query) : 10.52.0.84
Destination IP (Query) : 4.2.2.2

Source IP (Response) : 4.2.2.2
Destination IP (Response) : 10.52.0.84

IP addresses are **reversed** for source and destination in the query and response.

C.

Source Port (Query) : 41495
Destination Port (Query) : 53

Source Port (Response) : 53
Destination Port (Response) : 41495

Port numbers are also **reversed** for source and destination in query and response.

Well-known port number is **53**.

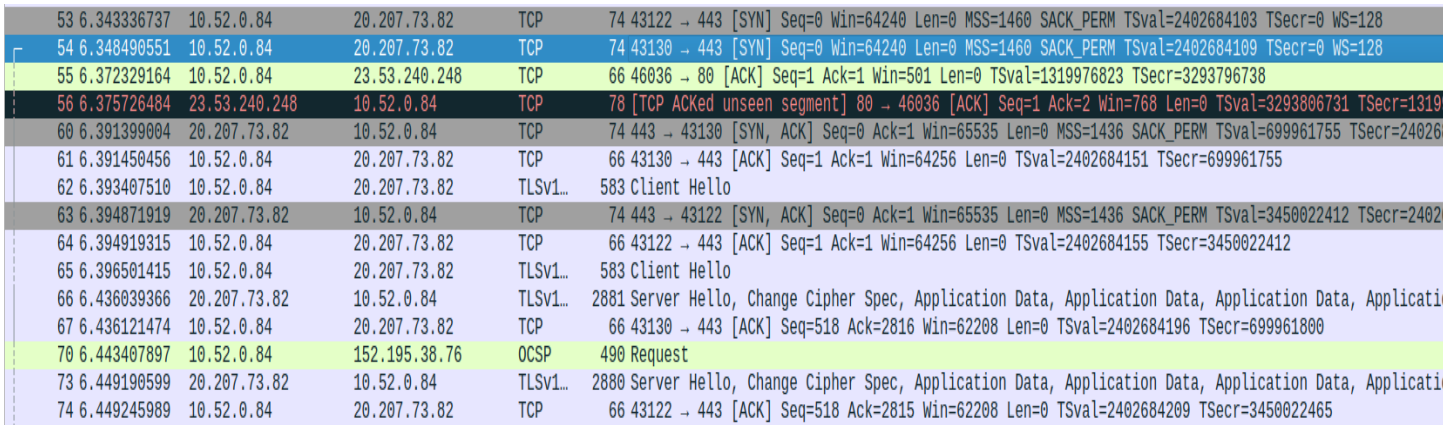
D.

Length of packet : 68 bytes

Payload size : 26 bytes

TCP PACKET ANALYSIS

Part 1- Connection Establishment



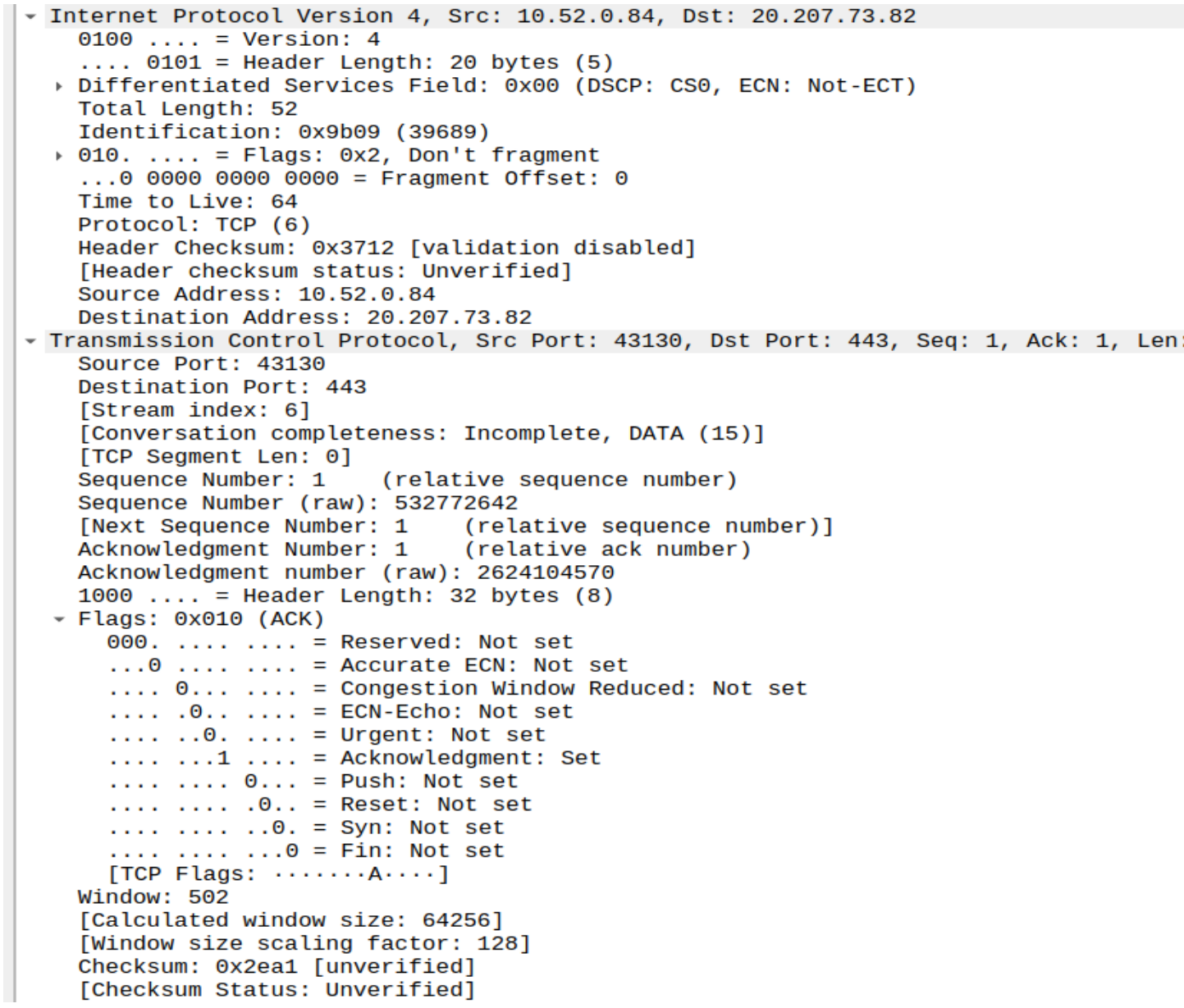
53	6.343336737	10.52.0.84	20.207.73.82	TCP	74 43122 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2402684103 TSecr=0 WS=128
54	6.348490551	10.52.0.84	20.207.73.82	TCP	74 43130 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2402684109 TSecr=0 WS=128
55	6.372329164	10.52.0.84	23.53.240.248	TCP	66 46036 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1319976823 TSecr=3293796738
56	6.375726484	23.53.240.248	10.52.0.84	TCP	78 [TCP ACKed unseen segment] 80 → 46036 [ACK] Seq=1 Ack=2 Win=768 Len=0 TSval=3293806731 TSecr=1319
60	6.391399004	20.207.73.82	10.52.0.84	TCP	74 443 → 43130 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM TSval=699961755 TSecr=24026
61	6.391450456	10.52.0.84	20.207.73.82	TCP	66 43130 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2402684151 TSecr=699961755
62	6.393407510	10.52.0.84	20.207.73.82	TLSv1…	583 Client Hello
63	6.394871919	20.207.73.82	10.52.0.84	TCP	74 443 → 43122 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM TSval=3450022412 TSecr=2402
64	6.394919315	10.52.0.84	20.207.73.82	TCP	66 43122 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2402684155 TSecr=3450022412
65	6.396501415	10.52.0.84	20.207.73.82	TLSv1…	583 Client Hello
66	6.436039366	20.207.73.82	10.52.0.84	TLSv1…	2881 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applicati
67	6.436121474	10.52.0.84	20.207.73.82	TCP	66 43130 → 443 [ACK] Seq=518 Ack=2816 Win=62208 Len=0 TSval=2402684196 TSecr=699961800
70	6.443407897	10.52.0.84	152.195.38.76	OCSP	490 Request
73	6.449190599	20.207.73.82	10.52.0.84	TLSv1…	2880 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applicati
74	6.449245989	10.52.0.84	20.207.73.82	TCP	66 43122 → 443 [ACK] Seq=518 Ack=2815 Win=62208 Len=0 TSval=2402684209 TSecr=3450022465

SYN Packet 1

SYN,ACK Packet 2

```
▾ Internet Protocol Version 4, Src: 20.207.73.82, Dst: 10.52.0.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0000 (0)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 52
    Protocol: TCP (6)
    Header Checksum: 0xde13 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 20.207.73.82
    Destination Address: 10.52.0.84
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 43130, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 43130
    [Stream index: 6]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2624104569
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 532772642
    1010 .... = Header Length: 40 bytes (10)
  ▾ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A··S·]
    Window: 65535
```

ACK Packet 3



```
▾ Internet Protocol Version 4, Src: 10.52.0.84, Dst: 20.207.73.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x9b09 (39689)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3712 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.52.0.84
    Destination Address: 20.207.73.82
▾ Transmission Control Protocol, Src Port: 43130, Dst Port: 443, Seq: 1, Ack: 1, Len
    Source Port: 43130
    Destination Port: 443
    [Stream index: 6]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 532772642
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2624104570
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: 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: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x2ea1 [unverified]
    [Checksum Status: Unverified]
```

1. Socket addresses for :

Packet 1 : Source IP : 10.52.0.84 | PORT – 43130
Destination IP : 20.207.73.82 | PORT – 433

Packet 2 : Destination IP : 10.52.0.84 | PORT – 43130
Source IP : 20.207.73.82 | PORT – 433

Packet 3 : Source IP : 10.52.0.84 | PORT – 43130
Destination IP : 20.207.73.82 | PORT – 433

2. Flags for each packet

Packet 1 : 0x002 (SYN)
Packet 2 : 0x012 (SYN,ACK)
Packet 3 : 0x010 (ACK)

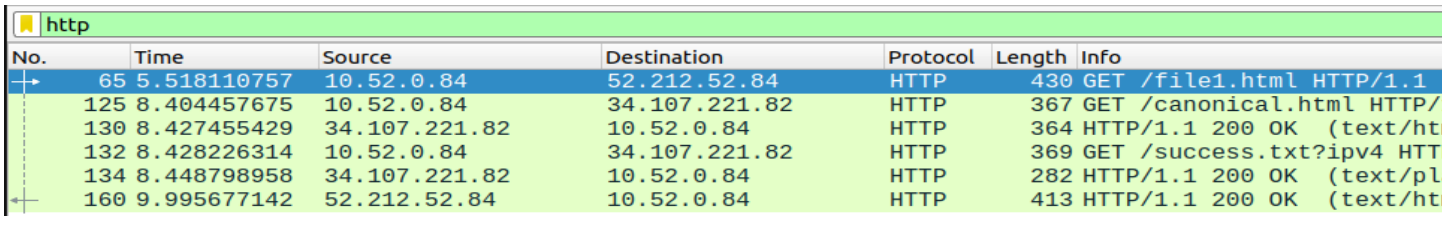
3. Sequence and Acknowledgement number

Packet 1 : 532772641 and 0
Packet 2 : 2624104569 and 532772642
Packet 3 : 532772642 and 2624104570

4. Window size of packets

Packet 1 : 62420
Packet 2 : 65535
Packet 3 : 502

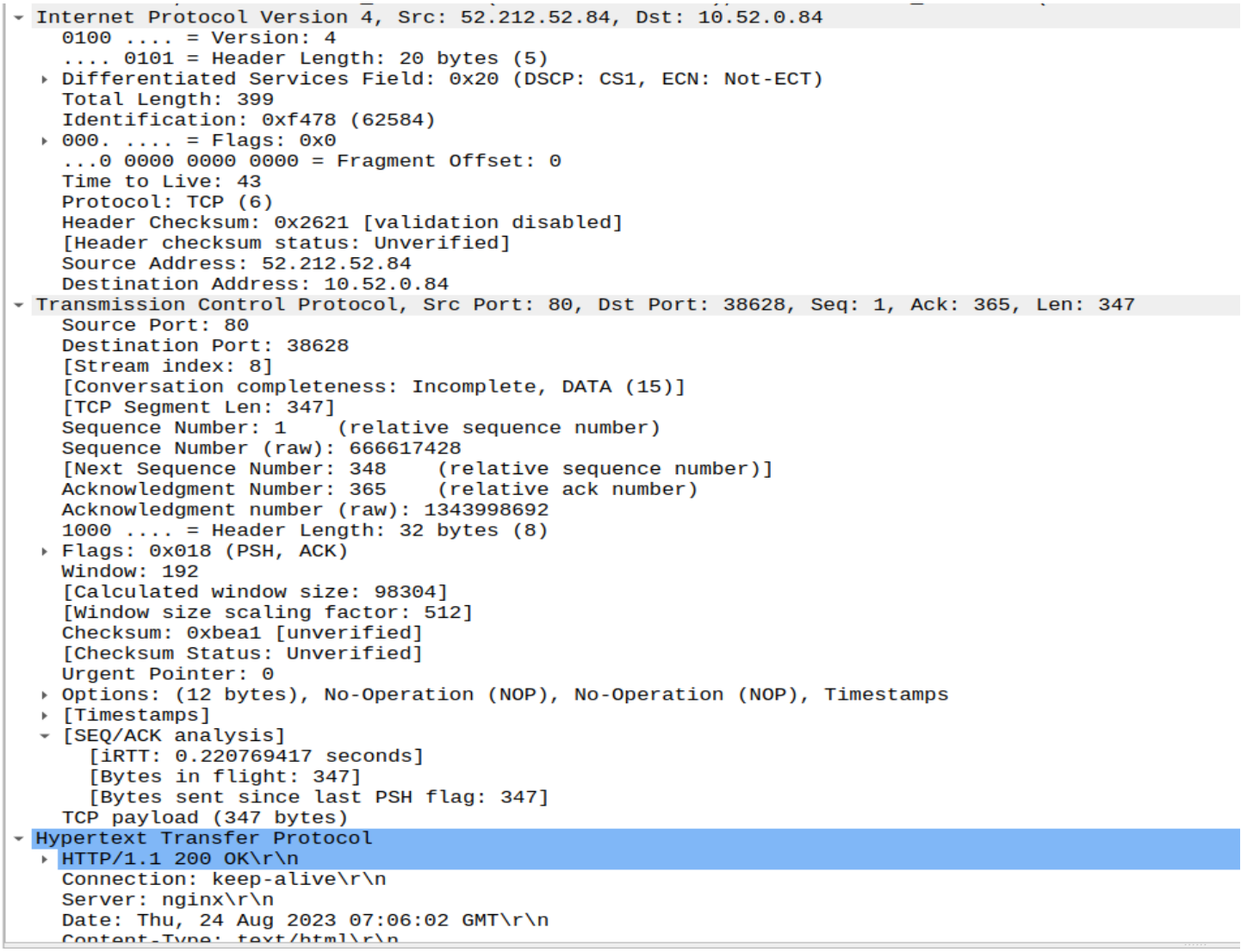
Part 2 – Data Transfer



HTTP GET Request Packet

```
Internet Protocol Version 4, Src: 10.52.0.84, Dst: 52.212.52.84
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 416
  Identification: 0xa856 (43094)
▸ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x1d52 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.52.0.84
  Destination Address: 52.212.52.84
Transmission Control Protocol, Src Port: 38628, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
  Source Port: 38628
  Destination Port: 80
  [Stream index: 8]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 364]
  Sequence Number: 1    (relative sequence number)
  Sequence Number (raw): 1343998328
  [Next Sequence Number: 365    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 666617428
  1000 .... = Header Length: 32 bytes (8)
▸ Flags: 0x018 (PSH, ACK)
```

HTTP OK Packet



1. Flags for GET : 0x018 (PSH,ACK)
2. 416 bytes transmitted
3. 4.477568365 seconds
4. 4
5. 5
6. 6
7. 7

Part 3 – Connection Termination

```
211 10.529170457 10.52.0.84      52.212.52.84     TCP    66 38616 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1199798666 TSecr=2677139111
213 10.599541387 10.52.0.84      172.217.166.35   TCP    66 [TCP Dup ACK 9#1] 45156 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=368263611 TSecr=
214 10.638839184 172.217.166.35  10.52.0.84       TCP    66 [TCP Dup ACK 10#1] 80 → 45156 [ACK] Seq=1 Ack=2 Win=277 Len=0 TSval=4276447191 TSec
216 10.752862579 52.212.52.84    10.52.0.84       TCP    66 80 → 38616 [FIN, ACK] Seq=1 Ack=2 Win=35840 Len=0 TSval=2677144342 TSecr=1199798666
217 10.752916969 10.52.0.84      52.212.52.84     TCP    66 38616 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0 TSval=1199798890 TSecr=2677144342
```

Packet 1 for termination

```
▾ Internet Protocol Version 4, Src: 10.52.0.84, Dst: 52.212.52.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x4127 (16679)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x85ed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.52.0.84
    Destination Address: 52.212.52.84
▾ Transmission Control Protocol, Src Port: 38616, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 38616
    Destination Port: 80
    [Stream index: 7]
    [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1263299105
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4172361807
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x011 (FIN, ACK)
```

Packet 2 for termination

```
Internet Protocol Version 4, Src: 52.212.52.84, Dst: 10.52.0.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xacb8 (44216)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 45
    Protocol: TCP (6)
    Header Checksum: 0x2d3c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 52.212.52.84
    Destination Address: 10.52.0.84
Transmission Control Protocol, Src Port: 80, Dst Port: 38616, Seq: 1, Ack: 2, Le
    Source Port: 80
    Destination Port: 38616
    [Stream index: 7]
    [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4172361807
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 1263299106
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x011 (FIN, ACK)
    Window: 70
    [Calculated window size: 35840]
    [Window size scaling factor: 512]
    Checksum: 0x3178 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

Packet 3 for termination

```
Internet Protocol Version 4, Src: 10.52.0.84, Dst: 52.212.52.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x4128 (16680)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x85ec [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.52.0.84
    Destination Address: 52.212.52.84
Transmission Control Protocol, Src Port: 38616, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
    Source Port: 38616
    Destination Port: 80
    [Stream index: 7]
    [Conversation completeness: Complete, NO_DATA (23)]
    [TCP Segment Len: 0]
    Sequence Number: 2    (relative sequence number)
    Sequence Number (raw): 1263299106
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 2    (relative ack number)
    Acknowledgment number (raw): 4172361808
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
```