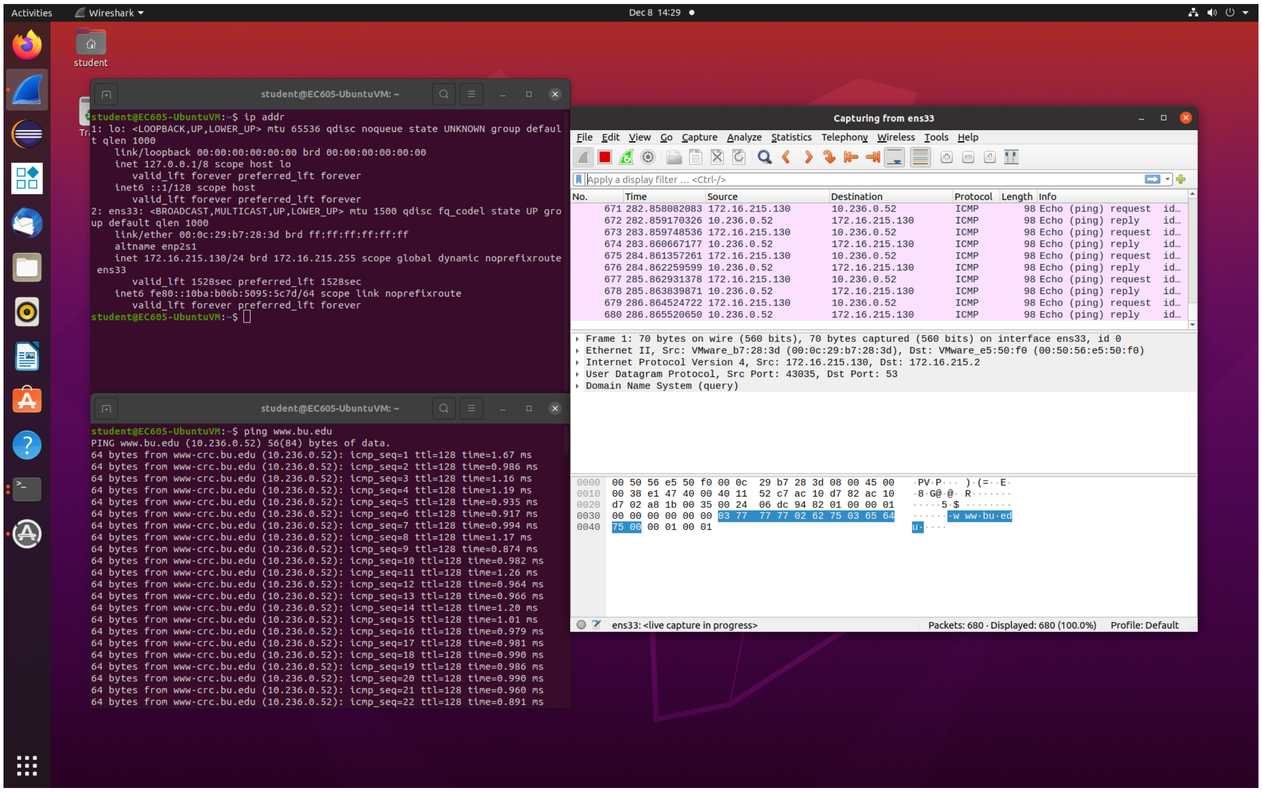
U77561194 Zehao Hui

LAB 7

EC605
December 8, 2021

Task1: Introduction to Wireshark


Activities
Wireshark
Dec 8 14:29
student
student@EC605-UbuntuVM: ~
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
student@EC605-UbuntuVM:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:b7:28:3d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.215.130/24 brd 172.16.215.255 scope global dynamic noprefixroute
 ens33
       valid_lft 1528sec preferred_lft 1528sec
    inet6 fe80::10ba:b06b:5095:5c7d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@EC605-UbuntuVM:~$
```

```
student@EC605-UbuntuVM:~$ ping www.bu.edu
PING www.bu.edu (10.236.0.52) 56(84) bytes of data.
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=1 ttl=128 time=1.67 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=2 ttl=128 time=0.986 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=3 ttl=128 time=1.16 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=4 ttl=128 time=1.19 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=5 ttl=128 time=0.935 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=6 ttl=128 time=0.917 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=7 ttl=128 time=0.994 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=8 ttl=128 time=1.17 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=9 ttl=128 time=0.874 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=10 ttl=128 time=0.982 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=11 ttl=128 time=1.26 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=12 ttl=128 time=0.964 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=13 ttl=128 time=0.966 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=14 ttl=128 time=1.20 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=15 ttl=128 time=1.01 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=16 ttl=128 time=0.979 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=17 ttl=128 time=0.981 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=18 ttl=128 time=0.990 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=19 ttl=128 time=0.986 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=20 ttl=128 time=0.990 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=21 ttl=128 time=0.960 ms
64 bytes from www-crc.bu.edu (10.236.0.52): icmp_seq=22 ttl=128 time=0.891 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
671	282.858082083	172.16.215.130	10.236.0.52	ICMP	98	Echo (ping) request id…
672	282.859170326	10.236.0.52	172.16.215.130	ICMP	98	Echo (ping) reply id…
673	283.859748536	172.16.215.130	10.236.0.52	ICMP	98	Echo (ping) request id…
674	283.860667177	10.236.0.52	172.16.215.130	ICMP	98	Echo (ping) reply id…
675	284.861357261	172.16.215.130	10.236.0.52	ICMP	98	Echo (ping) request id…
676	284.862259599	10.236.0.52	172.16.215.130	ICMP	98	Echo (ping) reply id…
677	285.862931378	172.16.215.130	10.236.0.52	ICMP	98	Echo (ping) request id…
678	285.863839871	10.236.0.52	172.16.215.130	ICMP	98	Echo (ping) reply id…
679	286.864524722	172.16.215.130	10.236.0.52	ICMP	98	Echo (ping) request id…
680	286.865520650	10.236.0.52	172.16.215.130	ICMP	98	Echo (ping) reply id…

```
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface ens33, id 0
Ethernet II, Src: VMware_b7:28:3d (00:0c:29:b7:28:3d), Dst: VMware_e5:50:f0 (00:50:56:e5:50:f0)
Internet Protocol Version 4, Src: 172.16.215.130, Dst: 172.16.215.2
User Datagram Protocol, Src Port: 43035, Dst Port: 53
Domain Name System (query)
```

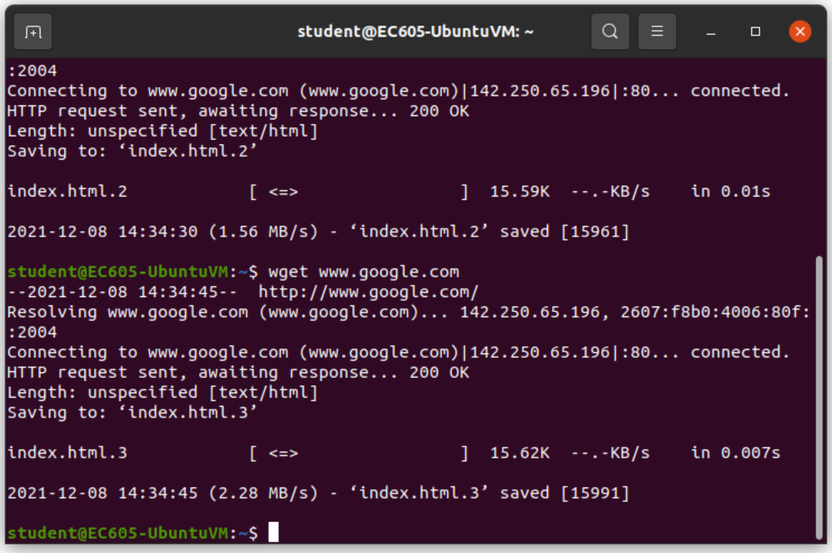
```
0000  00 50 56 e5 50 f0 00 0c  29 b7 28 3d 08 00 45 00   ·PV·P···)·(=··E·
0010  00 38 e1 47 40 00 40 11  52 c7 ac 10 d7 82 ac 10   ·8·G@·@·R·······
0020  d7 02 a8 1b 00 35 00 24  06 dc 94 82 01 00 00 01   ·····5·$········
0030  00 00 00 00 00 00 03 77  77 77 02 62 75 03 65 64   ·······w ww·bu·ed
0040  75 00 00 01 00 01                                  u·····
```

ens33: <live capture in progress>   Packets: 680 · Displayed: 680 (100.0%)   Profile: Default

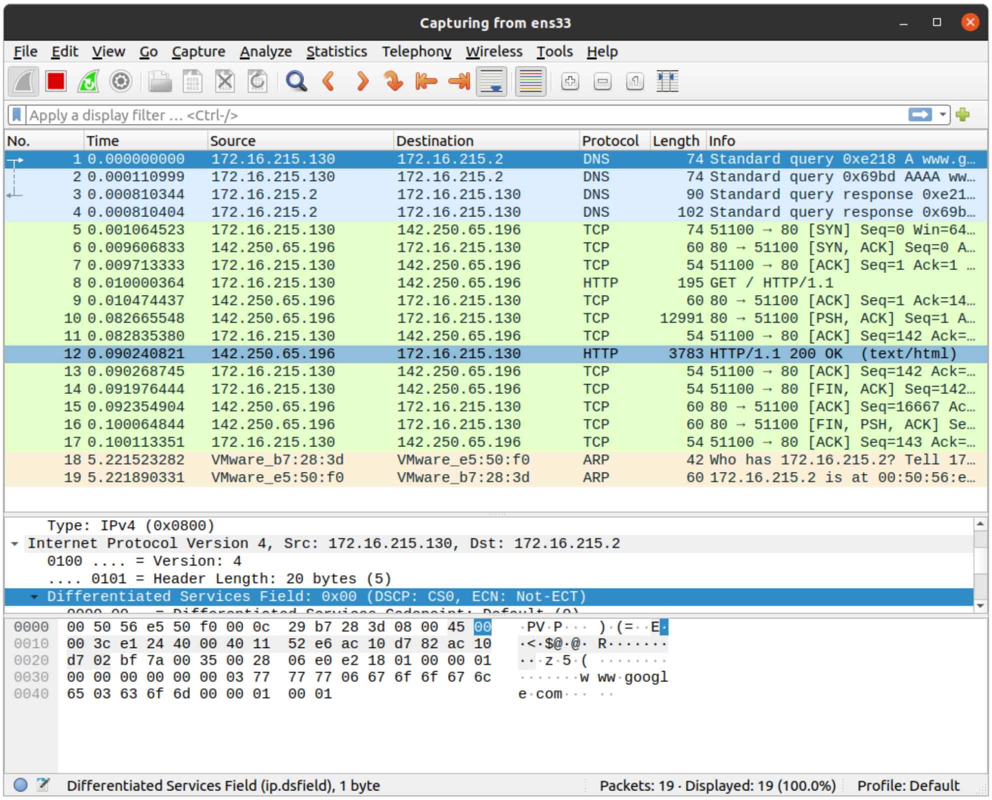
1. The ICMP protocol is used when performing a ping command.

2. The information that if the server is available is transferred in this protocol. It is used to get response on Time to live(TTL).

Task2: Unsecure Packets



```
:2004
Connecting to www.google.com (www.google.com)|142.250.65.196|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.2’

index.html.2            [ <=>                  ]  15.59K  --.-KB/s    in 0.01s

2021-12-08 14:34:30 (1.56 MB/s) - ‘index.html.2’ saved [15961]

student@EC605-UbuntuVM:~$ wget www.google.com
--2021-12-08 14:34:45--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.65.196, 2607:f8b0:4006:80f:
:2004
Connecting to www.google.com (www.google.com)|142.250.65.196|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.3’

index.html.3            [ <=>                  ]  15.62K  --.-KB/s    in 0.007s

2021-12-08 14:34:45 (2.28 MB/s) - ‘index.html.3’ saved [15991]

student@EC605-UbuntuVM:~$ 
```



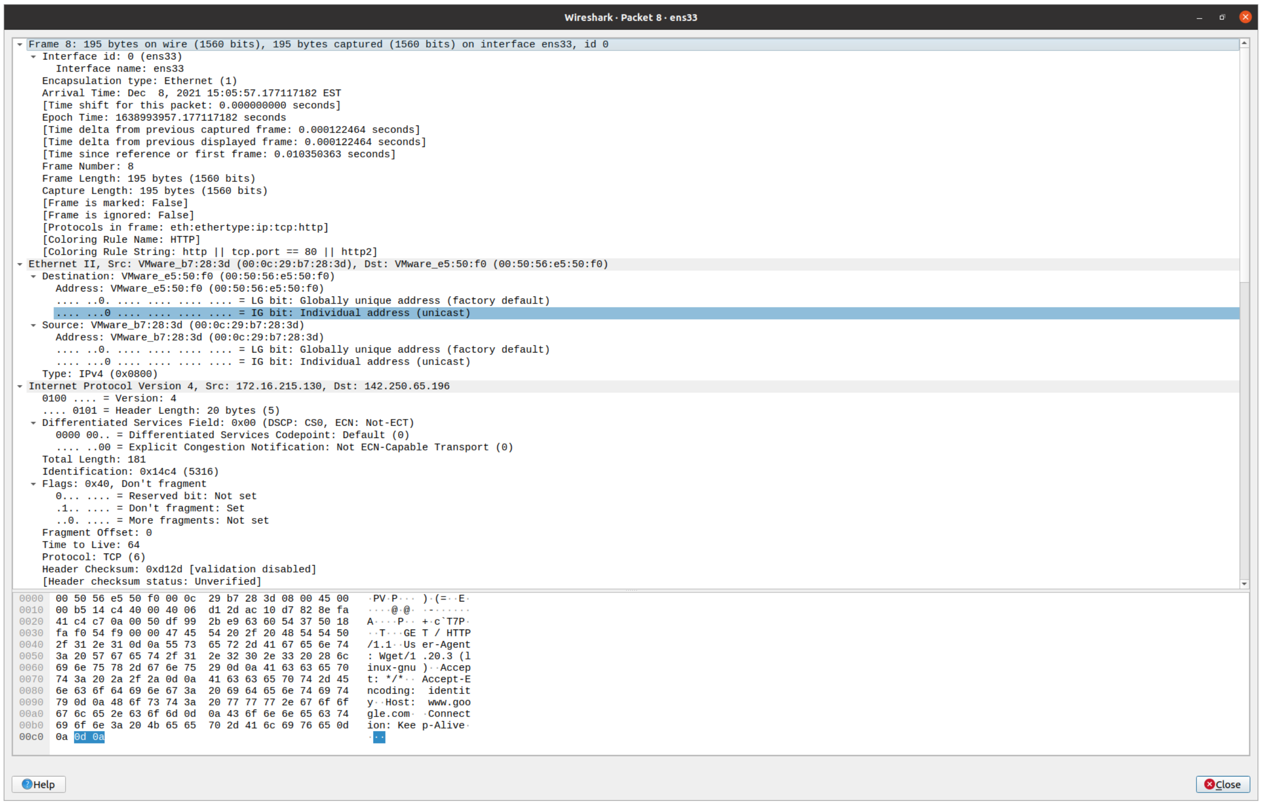
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source            Destination       Protocol Length Info
   1 0.000000000   172.16.215.130    172.16.215.2      DNS        74 Standard query 0xe218 A www.g…
   2 0.000110999   172.16.215.130    172.16.215.2      DNS        74 Standard query 0x69bd AAAA ww…
   3 0.000810344   172.16.215.2      172.16.215.130    DNS        90 Standard query response 0xe21…
   4 0.000810404   172.16.215.2      172.16.215.130    DNS       102 Standard query response 0x69b…
   5 0.001064523   172.16.215.130    142.250.65.196    TCP        74 51100 → 80 [SYN] Seq=0 Win=64…
   6 0.009606833   142.250.65.196    172.16.215.130    TCP        60 80 → 51100 [SYN, ACK] Seq=0 A…
   7 0.009713333   172.16.215.130    142.250.65.196    TCP        54 51100 → 80 [ACK] Seq=1 Ack=1 …
   8 0.010000364   172.16.215.130    142.250.65.196    HTTP      195 GET / HTTP/1.1
   9 0.010474437   142.250.65.196    172.16.215.130    TCP        60 80 → 51100 [ACK] Seq=1 Ack=14…
  10 0.082665548   142.250.65.196    172.16.215.130    TCP     12991 80 → 51100 [PSH, ACK] Seq=1 A…
  11 0.082835380   172.16.215.130    142.250.65.196    TCP        54 51100 → 80 [ACK] Seq=142 Ack=…
  12 0.090240821   142.250.65.196    172.16.215.130    HTTP     3783 HTTP/1.1 200 OK  (text/html)
  13 0.090268745   172.16.215.130    142.250.65.196    TCP        54 51100 → 80 [ACK] Seq=142 Ack=…
  14 0.091976444   172.16.215.130    142.250.65.196    TCP        54 51100 → 80 [FIN, ACK] Seq=142…
  15 0.092354904   142.250.65.196    172.16.215.130    TCP        60 80 → 51100 [ACK] Seq=16667 Ac…
  16 0.100064844   142.250.65.196    172.16.215.130    TCP        60 80 → 51100 [FIN, PSH, ACK] Se…
  17 0.100113351   172.16.215.130    142.250.65.196    TCP        54 51100 → 80 [ACK] Seq=143 Ack=…
  18 5.221523282   VMware_b7:28:3d   VMware_e5:50:f0   ARP        42 Who has 172.16.215.2? Tell 17…
  19 5.221890331   VMware_e5:50:f0   VMware_b7:28:3d   ARP        60 172.16.215.2 is at 00:50:56:e…
```

```
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 172.16.215.130, Dst: 172.16.215.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
```

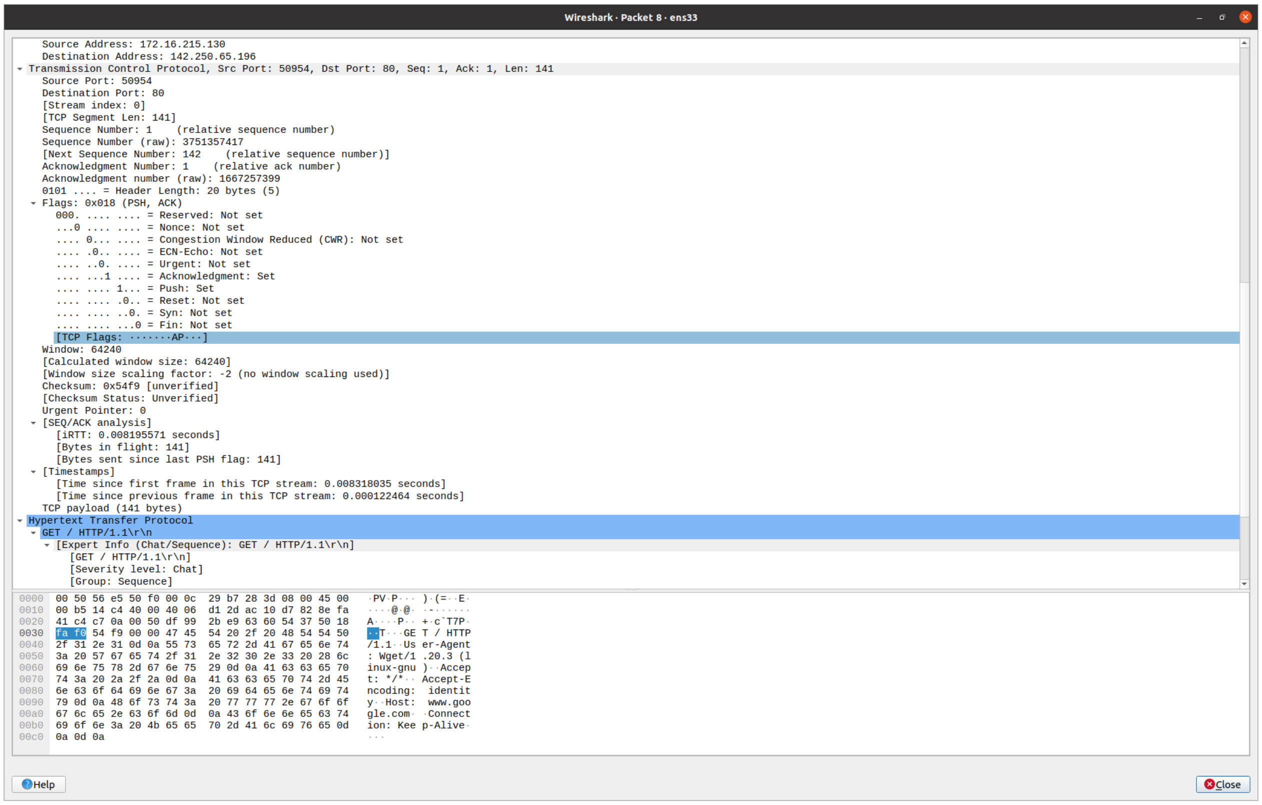
```
0000  00 50 56 e5 50 f0 00 0c  29 b7 28 3d 08 00 45 00   ·PV·P···  )·(=··E·
0010  00 3c e1 24 40 00 40 11  52 e6 ac 10 d7 82 ac 10   ·<·$@·@·  R·······
0020  d7 02 bf 7a 00 35 00 28  06 e0 e2 18 01 00 00 01   ···z·5·(  ········
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w  ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com···  ··
```

Differentiated Services Field (ip.dsfield), 1 byte   Packets: 19 · Displayed: 19 (100.0%)   Profile: Default



```
▾ Frame 8: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface ens33, id 0
  ▾ Interface id: 0 (ens33)
      Interface name: ens33
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  8, 2021 15:05:57.177117182 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1638993957.177117182 seconds
    [Time delta from previous captured frame: 0.000122464 seconds]
    [Time delta from previous displayed frame: 0.000122464 seconds]
    [Time since reference or first frame: 0.010350363 seconds]
    Frame Number: 8
    Frame Length: 195 bytes (1560 bits)
    Capture Length: 195 bytes (1560 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▾ Ethernet II, Src: VMware_b7:28:3d (00:0c:29:b7:28:3d), Dst: VMware_e5:50:f0 (00:50:56:e5:50:f0)
  ▾ Destination: VMware_e5:50:f0 (00:50:56:e5:50:f0)
      Address: VMware_e5:50:f0 (00:50:56:e5:50:f0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: VMware_b7:28:3d (00:0c:29:b7:28:3d)
      Address: VMware_b7:28:3d (00:0c:29:b7:28:3d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 172.16.215.130, Dst: 142.250.65.196
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 181
    Identification: 0x14c4 (5316)
  ▾ Flags: 0x40, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xd12d [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  00 50 56 e5 50 f0 00 0c  29 b7 28 3d 08 00 45 00   ·PV·P··· )·(=··E·
0010  00 b5 14 c4 40 00 40 06  d1 2d ac 10 d7 82 8e fa   ····@·@· ·-······
0020  41 c4 c7 0a 00 50 df 99  2b e9 63 60 54 37 50 18   A····P·· +·c`T7P·
0030  fa f0 54 f9 00 00 47 45  54 20 2f 20 48 54 54 50   ··T···GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 57 67 65 74 2f 31  2e 32 30 2e 33 20 28 6c   : Wget/1 .20.3 (l
0060  69 6e 75 78 2d 67 6e 75  29 0d 0a 41 63 63 65 70   inux-gnu )··Accep
0070  74 3a 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 45   t: */*·· Accept-E
0080  6e 63 6f 64 69 6e 67 3a  20 69 64 65 6e 74 69 74   ncoding:  identit
0090  79 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 67 6f 6f   y··Host:  www.goo
00a0  67 6c 65 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   gle.com· ·Connect
00b0  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
00c0  0a 0d 0a                                           ···
```

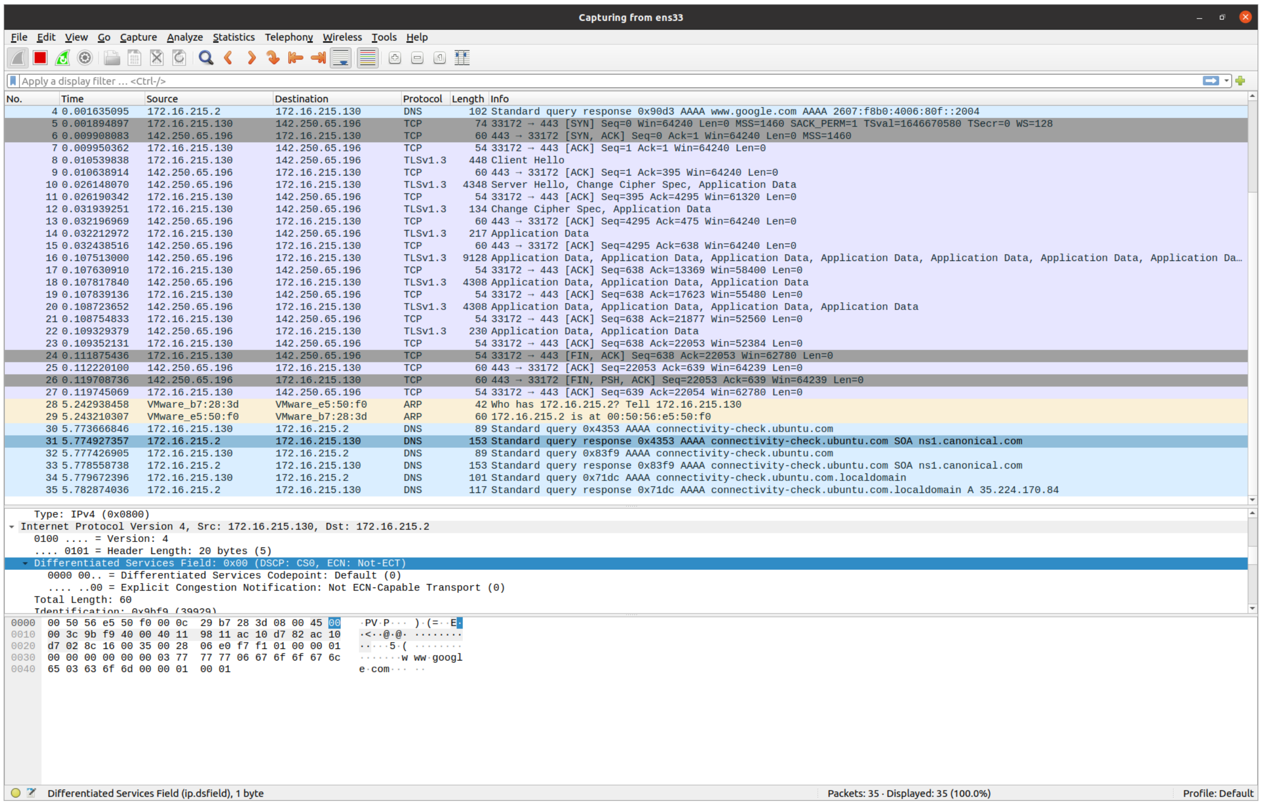


```
    Source Address: 172.16.215.130
    Destination Address: 142.250.65.196
▾ Transmission Control Protocol, Src Port: 50954, Dst Port: 80, Seq: 1, Ack: 1, Len: 141
    Source Port: 50954
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 141]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3751357417
    [Next Sequence Number: 142    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1667257399
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x54f9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ [SEQ/ACK analysis]
      [iRTT: 0.008195571 seconds]
      [Bytes in flight: 141]
      [Bytes sent since last PSH flag: 141]
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.008318035 seconds]
      [Time since previous frame in this TCP stream: 0.000122464 seconds]
    TCP payload (141 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▾ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
```

```
0000  00 50 56 e5 50 f0 00 0c  29 b7 28 3d 08 00 45 00   ·PV·P··· )·(=··E·
0010  00 b5 14 c4 40 00 40 06  d1 2d ac 10 d7 82 8e fa   ····@·@· ·-······
0020  41 c4 c7 0a 00 50 df 99  2b e9 63 60 54 37 50 18   A····P·· +·c`T7P·
0030  fa f0 54 f9 00 00 47 45  54 20 2f 20 48 54 54 50   ··T···GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 57 67 65 74 2f 31  2e 32 30 2e 33 20 28 6c   : Wget/1 .20.3 (l
0060  69 6e 75 78 2d 67 6e 75  29 0d 0a 41 63 63 65 70   inux-gnu )··Accep
0070  74 3a 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 45   t: */*·· Accept-E
0080  6e 63 6f 64 69 6e 67 3a  20 69 64 65 6e 74 69 74   ncoding:  identit
0090  79 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 67 6f 6f   y··Host:  www.goo
00a0  67 6c 65 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   gle.com· ·Connect
00b0  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive·
00c0  0a 0d 0a                                           ···
```

1. The destination IP address is 142.250.65.196.
2. The destination MAC address is 00:50:56:e5:50:f0.
3. The Internet protocol version is 4.
4. Source Port is 50954. Destination Port is 80.
5. The version of wget is 1.20.3.
6. The TCP flags is 0x018.

Task3: Secure vs. Unsecure Packets


Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time        Source          Destination     Protocol Length Info
   4 0.001635095 172.16.215.2    172.16.215.130  DNS       102 Standard query response 0x90d3 AAAA www.google.com AAAA 2607:f8b0:4006:80f::2004
   5 0.001894897 172.16.215.130  142.250.65.196  TCP        74 33172 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1646670580 TSecr=0 WS=128
   6 0.009908083 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   7 0.009950362 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   8 0.010539838 172.16.215.130  142.250.65.196  TLSv1.3   448 Client Hello
   9 0.010638914 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [ACK] Seq=1 Ack=395 Win=64240 Len=0
  10 0.026148070 142.250.65.196  172.16.215.130  TLSv1.3  4348 Server Hello, Change Cipher Spec, Application Data
  11 0.026190342 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=395 Ack=4295 Win=61320 Len=0
  12 0.031939251 172.16.215.130  142.250.65.196  TLSv1.3   134 Change Cipher Spec, Application Data
  13 0.032196969 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [ACK] Seq=4295 Ack=475 Win=64240 Len=0
  14 0.032212972 172.16.215.130  142.250.65.196  TLSv1.3   217 Application Data
  15 0.032438516 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [ACK] Seq=4295 Ack=638 Win=64240 Len=0
  16 0.107513000 142.250.65.196  172.16.215.130  TLSv1.3  9128 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Da…
  17 0.107630910 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=638 Ack=13369 Win=58400 Len=0
  18 0.107817840 142.250.65.196  172.16.215.130  TLSv1.3  4308 Application Data, Application Data, Application Data
  19 0.107839136 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=638 Ack=17623 Win=55480 Len=0
  20 0.108723652 142.250.65.196  172.16.215.130  TLSv1.3  4308 Application Data, Application Data, Application Data, Application Data
  21 0.108754833 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=638 Ack=21877 Win=52560 Len=0
  22 0.109329379 142.250.65.196  172.16.215.130  TLSv1.3   230 Application Data, Application Data
  23 0.109352131 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=638 Ack=22053 Win=52384 Len=0
  24 0.111875436 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [FIN, ACK] Seq=638 Ack=22053 Win=62780 Len=0
  25 0.112220100 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [ACK] Seq=22053 Ack=639 Win=64239 Len=0
  26 0.119708736 142.250.65.196  172.16.215.130  TCP        60 443 → 33172 [FIN, PSH, ACK] Seq=22053 Ack=639 Win=64239 Len=0
  27 0.119745069 172.16.215.130  142.250.65.196  TCP        54 33172 → 443 [ACK] Seq=639 Ack=22054 Win=62780 Len=0
  28 5.242938458 VMware_b7:28:3d VMware_e5:50:f0 ARP        42 Who has 172.16.215.2? Tell 172.16.215.130
  29 5.243210307 VMware_e5:50:f0 VMware_b7:28:3d ARP        60 172.16.215.2 is at 00:50:56:e5:50:f0
  30 5.773666846 172.16.215.130  172.16.215.2    DNS        89 Standard query 0x4353 AAAA connectivity-check.ubuntu.com
  31 5.774927357 172.16.215.2    172.16.215.130  DNS       153 Standard query response 0x4353 AAAA connectivity-check.ubuntu.com SOA ns1.canonical.com
  32 5.777426905 172.16.215.130  172.16.215.2    DNS        89 Standard query 0x83f9 AAAA connectivity-check.ubuntu.com
  33 5.778558738 172.16.215.2    172.16.215.130  DNS       153 Standard query response 0x83f9 AAAA connectivity-check.ubuntu.com SOA ns1.canonical.com
  34 5.779672396 172.16.215.130  172.16.215.2    DNS       101 Standard query 0x71dc AAAA connectivity-check.ubuntu.com.localdomain
  35 5.782874036 172.16.215.2    172.16.215.130  DNS       117 Standard query response 0x71dc AAAA connectivity-check.ubuntu.com.localdomain A 35.224.170.84
```

```
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 172.16.215.130, Dst: 172.16.215.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x9bf9 (39929)
```

```
0000  00 50 56 e5 50 f0 00 0c  29 b7 28 3d 08 00 45 00   ·PV·P··· )·(=··E·
0010  00 3c 9b f9 40 00 40 11  98 11 ac 10 d7 82 ac 10   ·<··@·@· ········
0020  d7 02 8c 16 00 35 00 28  06 e0 f7 f1 01 00 00 01   ·····5·( ········
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com··· ··
```

Differentiated Services Field (ip.dsfield), 1 byte

Packets: 35 · Displayed: 35 (100.0%)

Profile: Default

Compare to task2, when we use https connection, there has TLS in the communication and the port is 443 rather than 80. During the communication, the data will not be sent until the client and server both sent Hello. It will be safer.

Packets:

1. Client Hello: the client send the confirmation to server in order to know that the server is right.

2. Server Hello: the server send the confirmation to client in order to tell the client that it is the right server. And it can be used to create the key, generates the session ID and the way to encrypt the data.

3. Certificate: Verify if the server is the correct one.

4. Certificate Key Exchange: When use TLS, this is used to provide parameters for encryption.

5. Change Cipher Spec: It tells the server that the message will be encrypted before sending.

6. New Session Ticket: Used to restore the communication between client and server.

7. Application Data: Encrypted data.

Task4: Find an Image File in the Trace

1.

(1) 192.168.1.17, 216.58.219.238, 128.197.26.34, 74.125.29.189 are in the trace.

(2) 192.168.1.17 is the client.

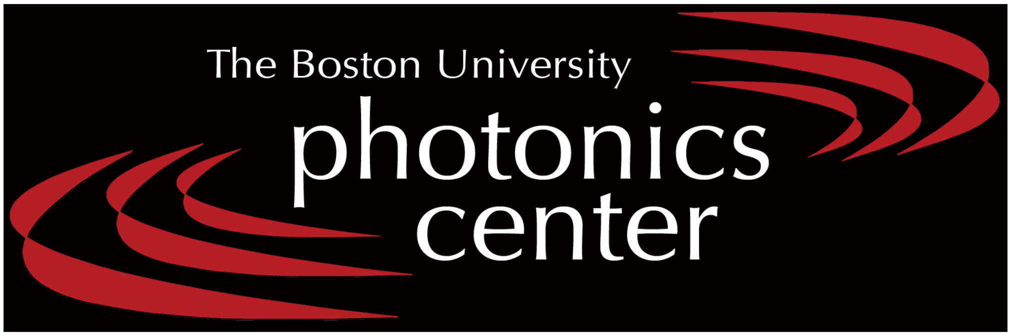
(3) 192.168.1.17 is Internet Assigned Numbers Authority (IANA).

216.58.219.238 is Google LLC.

128.197.26.34 is Boston University.

74.125.29.189 is Google LLC.

2.


The Boston University
photonics
center