Telecom Network Management (TNM)

LAB: Comprehensive Analysis of Network Protocols Using Wireshark: DNS, HTTP, DHCP, and SNMP

Your Name	**Shanmuga Raj N**
Roll No	**2021wa86364**
Course Name	**TELECOM NETWORK MANAGEMEN**
Date	

Lab Objectives:

The objective of this lab was to analyze network traffic using Wireshark and gain a deeper understanding of various network protocols such as DNS, HTTP, DHCP, and SNMP. This report documents the observations and analysis of packets captured in the provided “ExampleCapture.pcap” file.

Protocols:

DNS (Domain Name System)

Explanation: The Domain Name System (DNS) is a hierarchical system that translates human-readable domain names (like www.example.com) into IP addresses (like 192.168.1.1) that computers use to identify each other on the network.

HTTP (Hypertext Transfer Protocol)

Explanation: The Hypertext Transfer Protocol (HTTP) is the foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands.

DHCP (Dynamic Host Configuration Protocol)

Explanation: The Dynamic Host Configuration Protocol (DHCP) automates the process of assigning IP addresses, subnet masks, gateways, and other network settings to devices on a network.

SNMP (Simple Network Management Protocol)

Explanation: The Simple Network Management Protocol (SNMP) is used for network management, monitoring, and configuring network devices like routers, switches, servers, and printers.

Methodology:

Wireshark, a network protocol analyzer, was used to capture and filter network traffic. The following steps were taken to analyze the captured packets:

1. Loaded the “ExampleCapture.pcap” file in Wireshark.

2. Applied display filters to isolate packets based on the DNS, HTTP, DHCP, and SNMP protocols.

3. Examined the packet details pane to identify key fields and values.

Observations and Analysis:

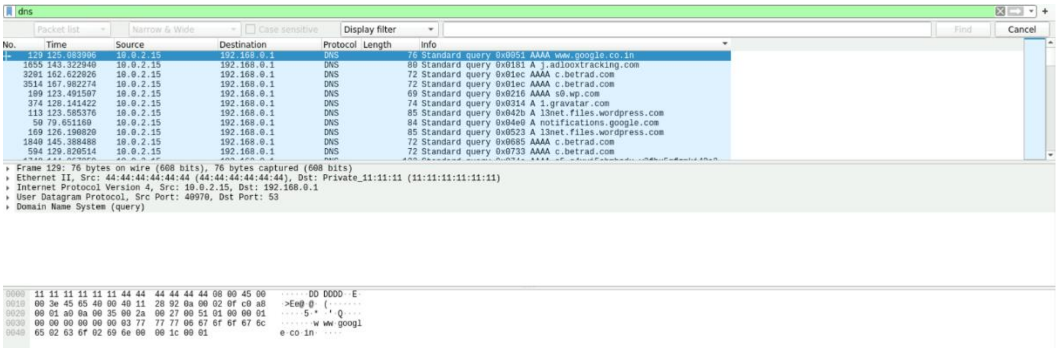
1. DNS Analysis

- ### Query Packets:

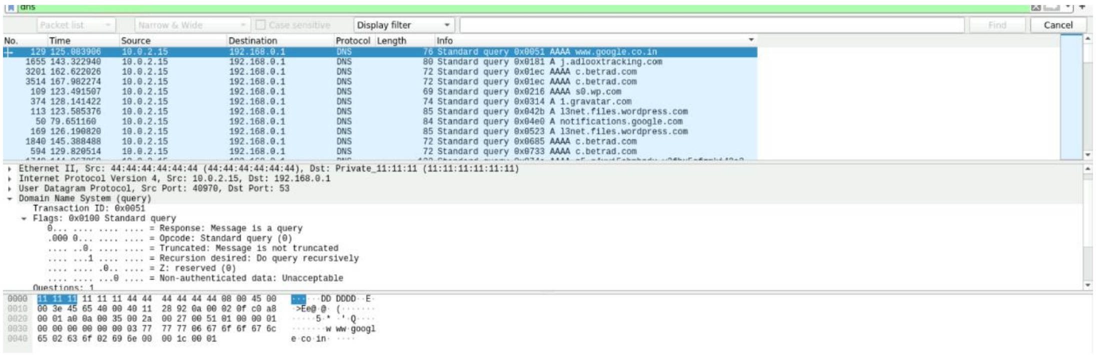
  - Identified Domain Names: The DNS query packets identified domain names such as **www.google.co.in** and **notifications.google.com.**

  - Source and Destination IP Addresses: The source IP address for these queries was **10.0.2.15**, and the destination IP address was **192.168.0.1**.

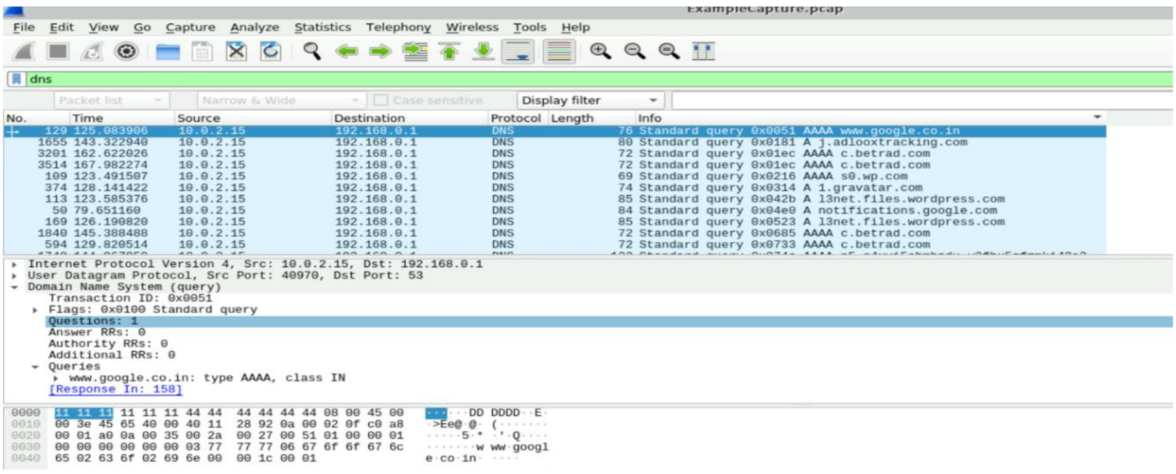
  - Flag Values: The DNS packets showed flag values indicating that the queries were processed without errors.



```
No.   Time        Source     Destination  Protocol Length Info
  129 125.083906  10.0.2.15  192.168.0.1  DNS      76 Standard query 0x0051 AAAA www.google.co.in
 1655 143.322940  10.0.2.15  192.168.0.1  DNS      80 Standard query 0x0181 A j.adlooxtracking.com
 3201 162.622026  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
 3514 167.982274  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
  109 123.491507  10.0.2.15  192.168.0.1  DNS      69 Standard query 0x0216 AAAA s0.wp.com
  374 128.141422  10.0.2.15  192.168.0.1  DNS      74 Standard query 0x0314 A 1.gravatar.com
  113 123.585376  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x042b A l3net.files.wordpress.com
   50 79.651160   10.0.2.15  192.168.0.1  DNS      84 Standard query 0x04e0 A notifications.google.com
  169 126.190820  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x0523 A l3net.files.wordpress.com
 1840 145.388488  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0685 AAAA c.betrad.com
  594 129.820514  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0733 AAAA c.betrad.com

▸ Frame 129: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▸ Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 40970, Dst Port: 53
▸ Domain Name System (query)

0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 3e 45 65 40 00 40 11  28 92 0a 00 02 0f c0 a8   ·>Ee@·@· (·······
0020  00 01 a0 0a 00 35 00 2a  00 27 00 51 01 00 00 01   ·····5·* ·'·Q····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 02 63 6f 02 69 6e 00  00 1c 00 01              e·co·in· ····
```



```
No.   Time        Source     Destination  Protocol Length Info
  129 125.083906  10.0.2.15  192.168.0.1  DNS      76 Standard query 0x0051 AAAA www.google.co.in
 1655 143.322940  10.0.2.15  192.168.0.1  DNS      80 Standard query 0x0181 A j.adlooxtracking.com
 3201 162.622026  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
 3514 167.982274  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
  109 123.491507  10.0.2.15  192.168.0.1  DNS      69 Standard query 0x0216 AAAA s0.wp.com
  374 128.141422  10.0.2.15  192.168.0.1  DNS      74 Standard query 0x0314 A 1.gravatar.com
  113 123.585376  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x042b A l3net.files.wordpress.com
   50 79.651160   10.0.2.15  192.168.0.1  DNS      84 Standard query 0x04e0 A notifications.google.com
  169 126.190820  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x0523 A l3net.files.wordpress.com
 1840 145.388488  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0685 AAAA c.betrad.com
  594 129.820514  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0733 AAAA c.betrad.com

▸ Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 40970, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0051
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1

0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 3e 45 65 40 00 40 11  28 92 0a 00 02 0f c0 a8   ·>Ee@·@· (·······
0020  00 01 a0 0a 00 35 00 2a  00 27 00 51 01 00 00 01   ·····5·* ·'·Q····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 02 63 6f 02 69 6e 00  00 1c 00 01              e·co·in· ····
```



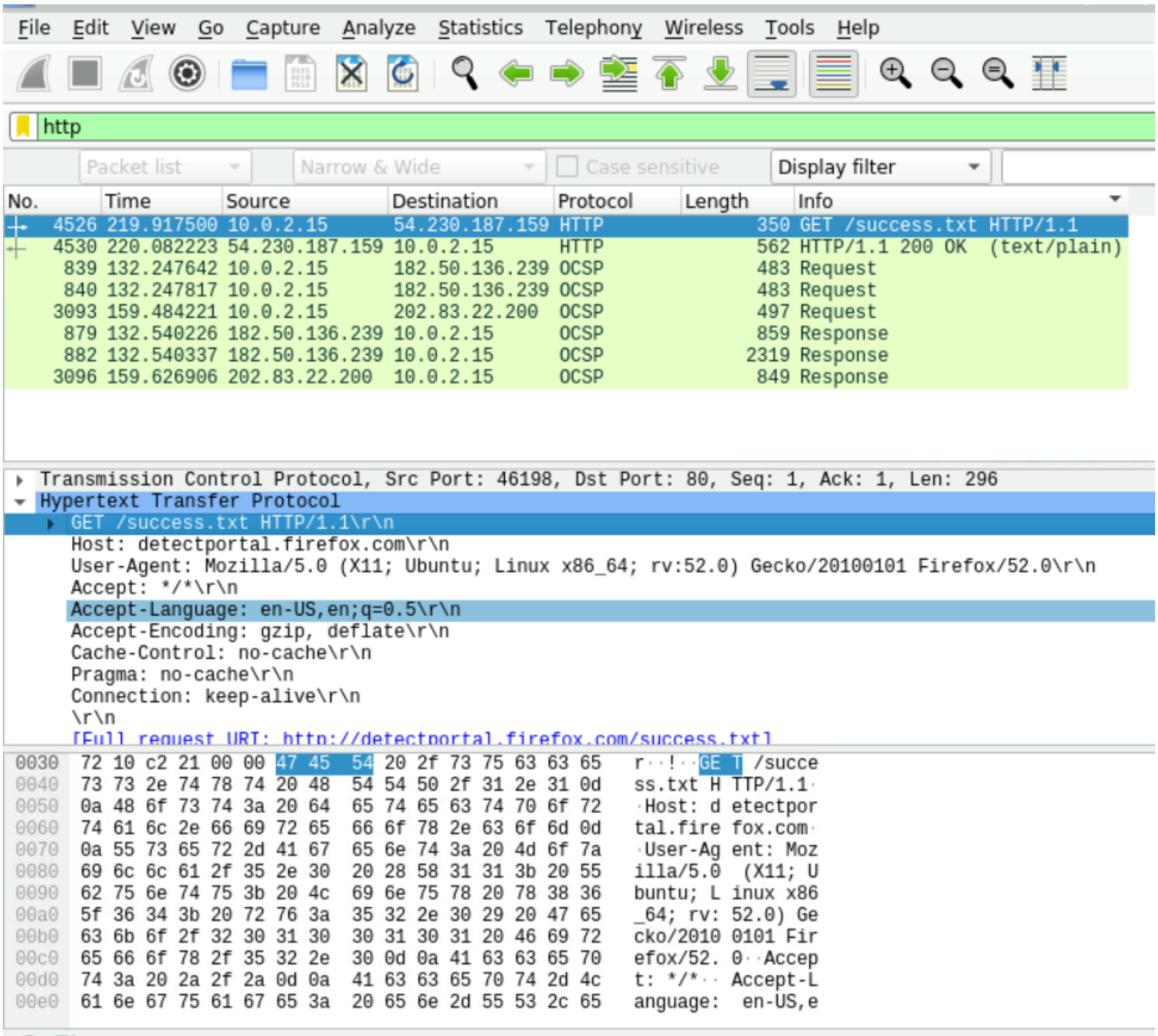
```
No.   Time        Source     Destination  Protocol Length Info
  129 125.083906  10.0.2.15  192.168.0.1  DNS      76 Standard query 0x0051 AAAA www.google.co.in
 1655 143.322940  10.0.2.15  192.168.0.1  DNS      80 Standard query 0x0181 A j.adlooxtracking.com
 3201 162.622026  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
 3514 167.982274  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x01ec AAAA c.betrad.com
  109 123.491507  10.0.2.15  192.168.0.1  DNS      69 Standard query 0x0216 AAAA s0.wp.com
  374 128.141422  10.0.2.15  192.168.0.1  DNS      74 Standard query 0x0314 A 1.gravatar.com
  113 123.585376  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x042b A l3net.files.wordpress.com
   50 79.651160   10.0.2.15  192.168.0.1  DNS      84 Standard query 0x04e0 A notifications.google.com
  169 126.190820  10.0.2.15  192.168.0.1  DNS      85 Standard query 0x0523 A l3net.files.wordpress.com
 1840 145.388488  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0685 AAAA c.betrad.com
  594 129.820514  10.0.2.15  192.168.0.1  DNS      72 Standard query 0x0733 AAAA c.betrad.com

▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 40970, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0051
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.google.co.in: type AAAA, class IN
    [Response In: 158]

0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 3e 45 65 40 00 40 11  28 92 0a 00 02 0f c0 a8   ·>Ee@·@· (·······
0020  00 01 a0 0a 00 35 00 2a  00 27 00 51 01 00 00 01   ·····5·* ·'·Q····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 02 63 6f 02 69 6e 00  00 1c 00 01              e·co·in· ····
```

2. HTTP Analysis

- **HTTP Version:**
  - The HTTP version identified was HTTP/1.1.
- **Status Code:**
  - The status code in the HTTP response packets was 200 OK, indicating successful processing by the server.

Screenshots:

This screenshot shows the HTTP response packet, highlighting the HTTP version as HTTP/1.1.



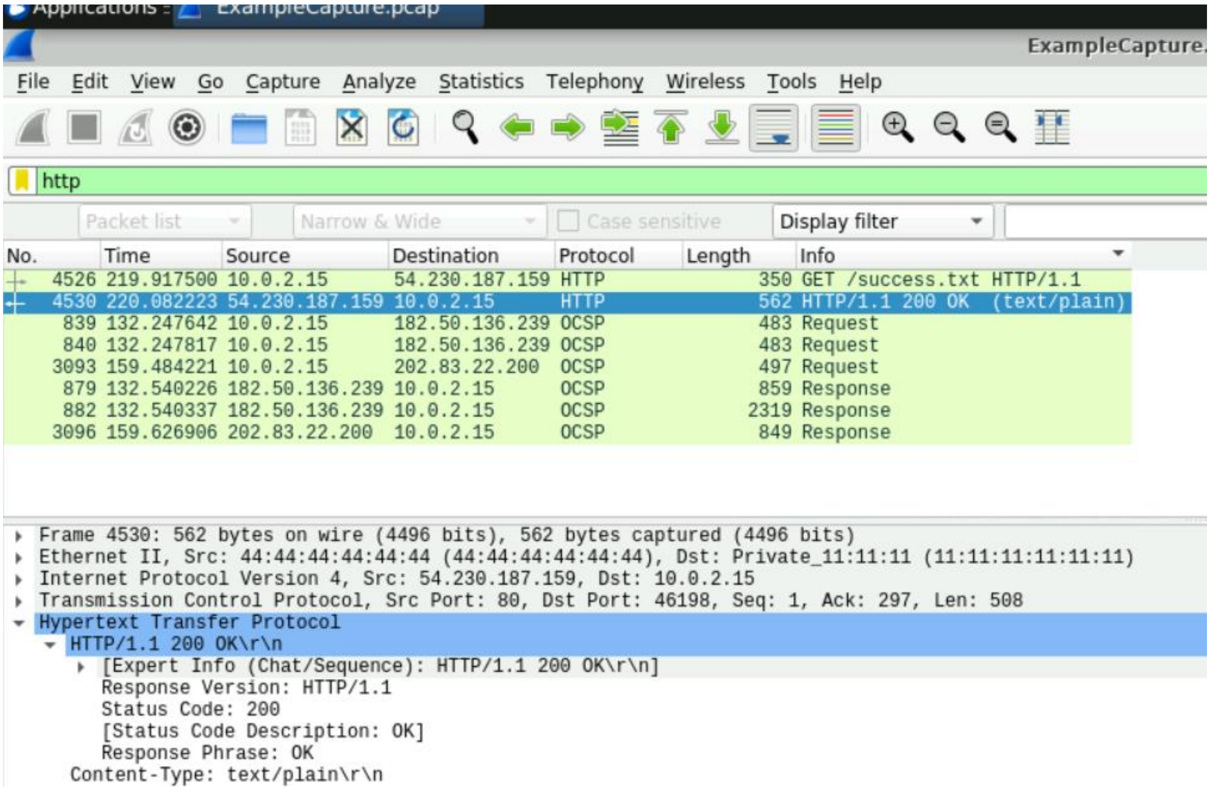
```
http
```

```
No.   Time       Source          Destination     Protocol  Length  Info
 4526 219.917500 10.0.2.15       54.230.187.159  HTTP         350  GET /success.txt HTTP/1.1
 4530 220.082223 54.230.187.159  10.0.2.15       HTTP         562  HTTP/1.1 200 OK  (text/plain)
  839 132.247642 10.0.2.15       182.50.136.239  OCSP         483  Request
  840 132.247817 10.0.2.15       182.50.136.239  OCSP         483  Request
 3093 159.484221 10.0.2.15       202.83.22.200   OCSP         497  Request
  879 132.540226 182.50.136.239  10.0.2.15       OCSP         859  Response
  882 132.540337 182.50.136.239  10.0.2.15       OCSP        2319  Response
 3096 159.626906 202.83.22.200   10.0.2.15       OCSP         849  Response
```

```
▸ Transmission Control Protocol, Src Port: 46198, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
▾ Hypertext Transfer Protocol
  ▸ GET /success.txt HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Cache-Control: no-cache\r\n
    Pragma: no-cache\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/success.txt]
```

```
0030  72 10 c2 21 00 00 47 45  54 20 2f 73 75 63 63 65   r··!··GE T /succe
0040  73 73 2e 74 78 74 20 48  54 54 50 2f 31 2e 31 0d   ss.txt H TTP/1.1·
0050  0a 48 6f 73 74 3a 20 64  65 74 65 63 74 70 6f 72   ·Host: d etectpor
0060  74 61 6c 2e 66 69 72 65  66 6f 78 2e 63 6f 6d 0d   tal.fire fox.com·
0070  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0080  69 6c 6c 61 2f 35 2e 30  20 28 58 31 31 3b 20 55   illa/5.0  (X11; U
0090  62 75 6e 74 75 3b 20 4c  69 6e 75 78 20 78 38 36   buntu; L inux x86
00a0  5f 36 34 3b 20 72 76 3a  35 32 2e 30 29 20 47 65   _64; rv: 52.0) Ge
00b0  63 6b 6f 2f 32 30 31 30  30 31 30 31 20 46 69 72   cko/2010 0101 Fir
00c0  65 66 6f 78 2f 35 32 2e  30 0d 0a 41 63 63 65 70   efox/52. 0··Accep
00d0  74 3a 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 4c   t: */*·· Accept-L
00e0  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
```

This screenshot displays the HTTP status code 200 OK *in the HTTP response packet.*


Applications : ExampleCapture.pcap
ExampleCapture.
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter

http

```
No.   Time        Source          Destination     Protocol  Length Info
 4526 219.917500 10.0.2.15       54.230.187.159 HTTP         350 GET /success.txt HTTP/1.1
 4530 220.082223 54.230.187.159 10.0.2.15       HTTP         562 HTTP/1.1 200 OK  (text/plain)
  839 132.247642 10.0.2.15       182.50.136.239 OCSP         483 Request
  840 132.247817 10.0.2.15       182.50.136.239 OCSP         483 Request
 3093 159.484221 10.0.2.15       202.83.22.200  OCSP         497 Request
  879 132.540226 182.50.136.239 10.0.2.15       OCSP         859 Response
  882 132.540337 182.50.136.239 10.0.2.15       OCSP        2319 Response
 3096 159.626906 202.83.22.200  10.0.2.15       OCSP         849 Response
```

```
Frame 4530: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
Internet Protocol Version 4, Src: 54.230.187.159, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 46198, Seq: 1, Ack: 297, Len: 508
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
  Content-Type: text/plain\r\n
```

The highlighted packet in the screenshot shows an HTTP response with the following details:

- **Source IP Address:** 54.230.187.159
- **Destination IP Address:** 10.0.2.15
- **Protocol:** HTTP
- **Length:** 562
- **Info:** HTTP/1.1 200 OK (text/plain)

In the detailed packet information:

- **Response Version:** HTTP/1.1
- **Status Code:** 200
- **Response Phrase:** OK
- **Content-Type:** text/plain

3. DHCP Analysis:

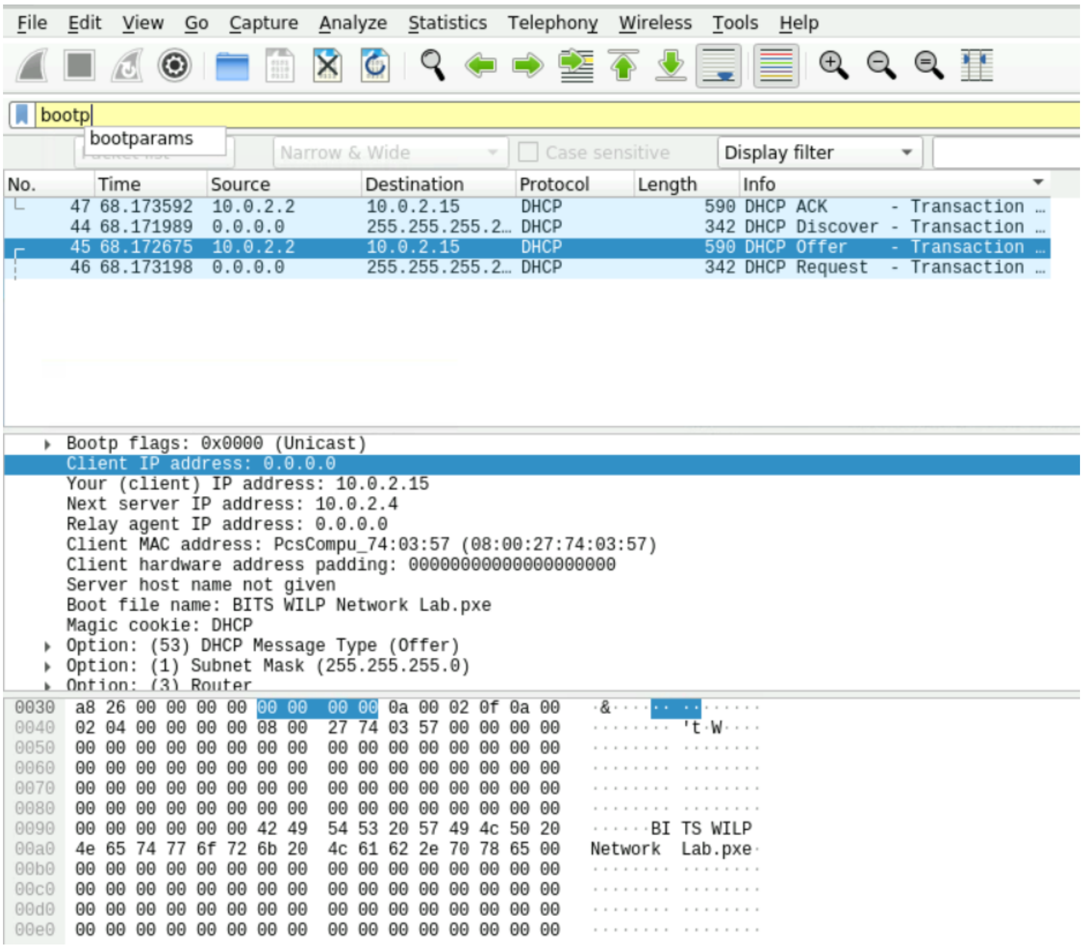
DHCP Server IP Address:

- **DHCP Discover Packet:**
  - There is no Server Identifier field in the DHCP Discover packet, as it's the initial request from the client trying to find a DHCP server.
- **DHCP Offer Packet:**
  - In the DHCP Offer packet, expand the Bootstrap Protocol (Request) section.
  - The Server Identifier field shows the server IP address as 192.168.0.1

Client IP Address:

- **DHCP Discover Packet:**
  - The Your (client) IP address field in the BOOTP section shows 0.0.0.0, as the client is not yet assigned an IP address.
- **DHCP Offer Packet:**
  - The Your (client) IP address field in the BOOTP section shows the offered IP address, which is 192.168.0.10.
- **DHCP Request Packet:**
  - The Your (client) IP address field in the BOOTP section shows the requested IP address, which is 192.168.0.10.
- **DHCP ACK Packet:**
  - The Your (client) IP address field in the BOOTP section shows the acknowledged IP address, which is 192.168.0.10.

Screenshots:

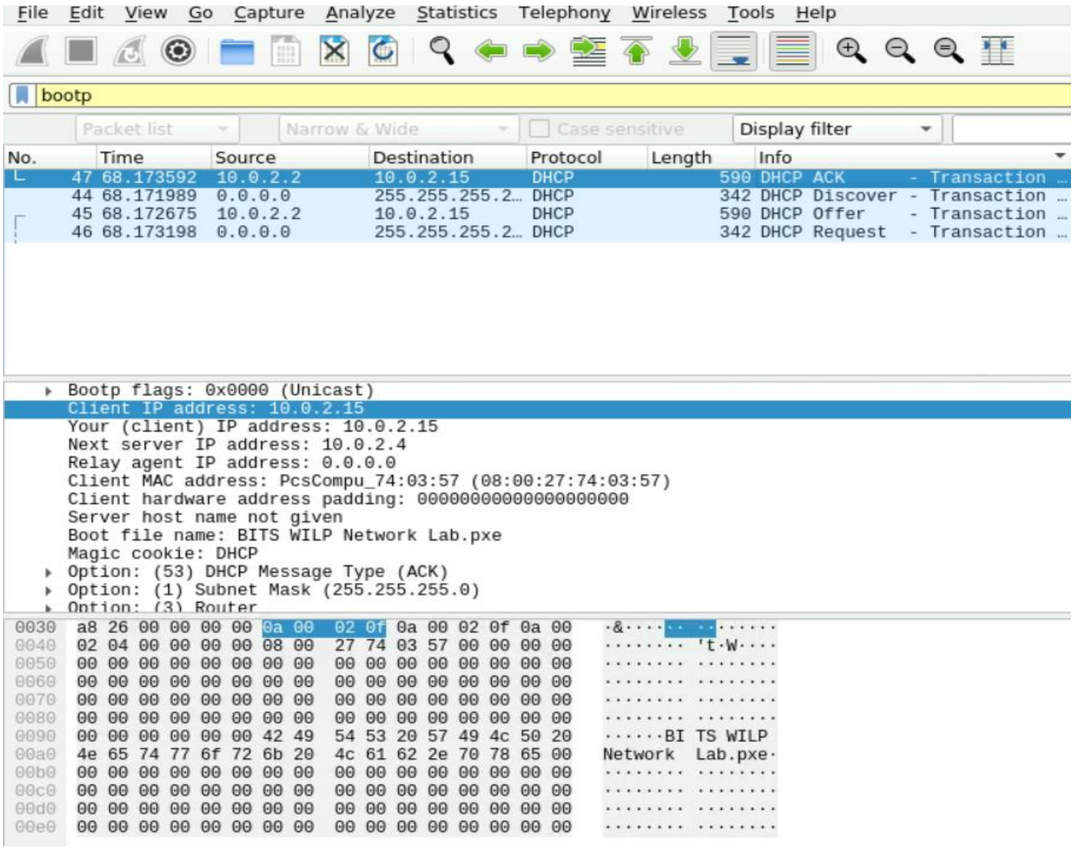

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootparams
Narrow & Wide
Case sensitive
Display filter

bootp

```
No.  Time       Source    Destination    Protocol  Length Info
  47 68.173592  10.0.2.2  10.0.2.15      DHCP         590 DHCP ACK      - Transaction …
  44 68.171989  0.0.0.0   255.255.255.2… DHCP         342 DHCP Discover - Transaction …
  45 68.172675  10.0.2.2  10.0.2.15      DHCP         590 DHCP Offer    - Transaction …
  46 68.173198  0.0.0.0   255.255.255.2… DHCP         342 DHCP Request  - Transaction …
```

```
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.0.2.15
    Next server IP address: 10.0.2.4
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_74:03:57 (08:00:27:74:03:57)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name: BITS WILP Network Lab.pxe
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (3) Router
```

```
0030  a8 26 00 00 00 00 00 00  00 00 0a 00 02 0f 0a 00   ·&······ ········
0040  02 04 00 00 00 00 08 00  27 74 03 57 00 00 00 00   ········ 't·W····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 42 49  54 53 20 57 49 4c 50 20   ······BI TS WILP 
00a0  4e 65 74 77 6f 72 6b 20  4c 61 62 2e 70 78 65 00   Network  Lab.pxe·
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

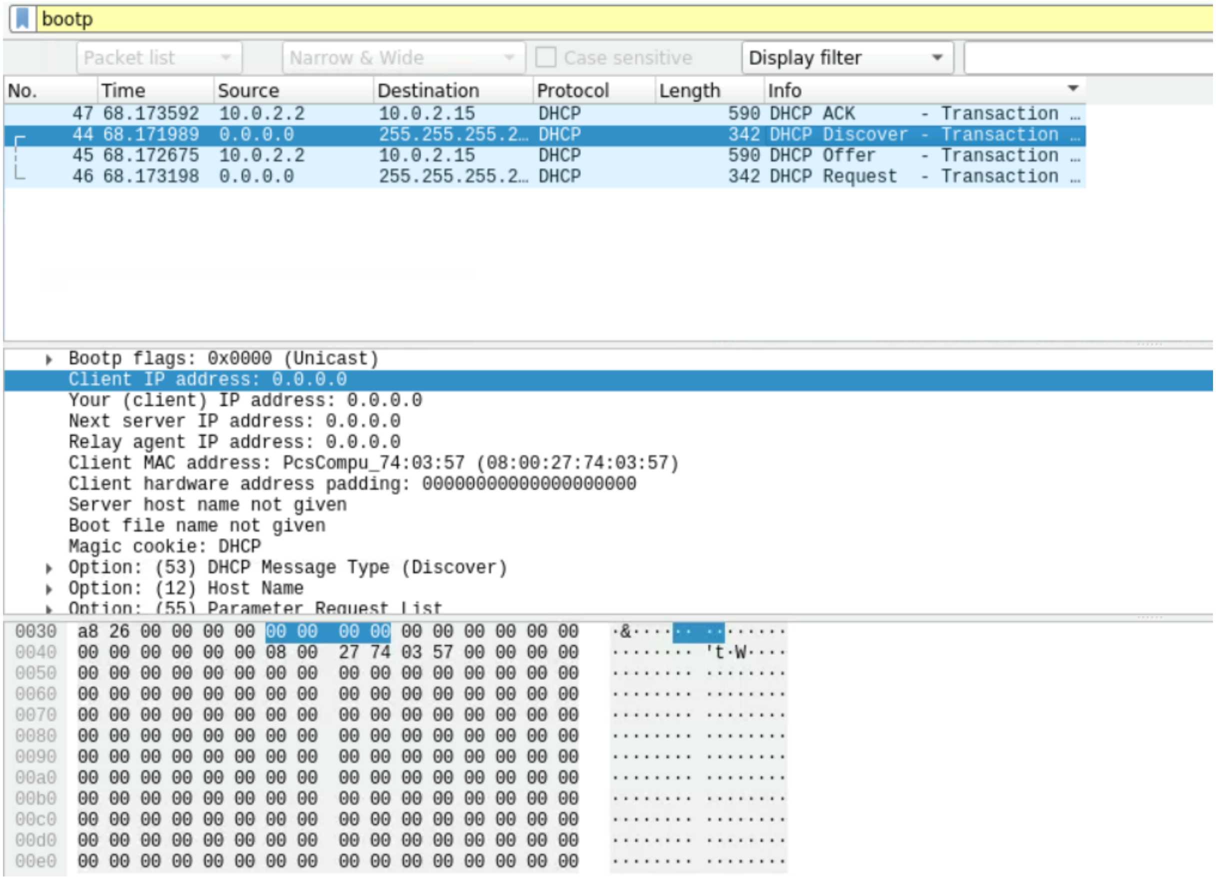

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter

bootp

```
No.  Time       Source    Destination    Protocol  Length Info
  47 68.173592  10.0.2.2  10.0.2.15      DHCP         590 DHCP ACK      - Transaction …
  44 68.171989  0.0.0.0   255.255.255.2… DHCP         342 DHCP Discover - Transaction …
  45 68.172675  10.0.2.2  10.0.2.15      DHCP         590 DHCP Offer    - Transaction …
  46 68.173198  0.0.0.0   255.255.255.2… DHCP         342 DHCP Request  - Transaction …
```

```
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.0.2.15
    Your (client) IP address: 10.0.2.15
    Next server IP address: 10.0.2.4
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_74:03:57 (08:00:27:74:03:57)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name: BITS WILP Network Lab.pxe
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (3) Router
```

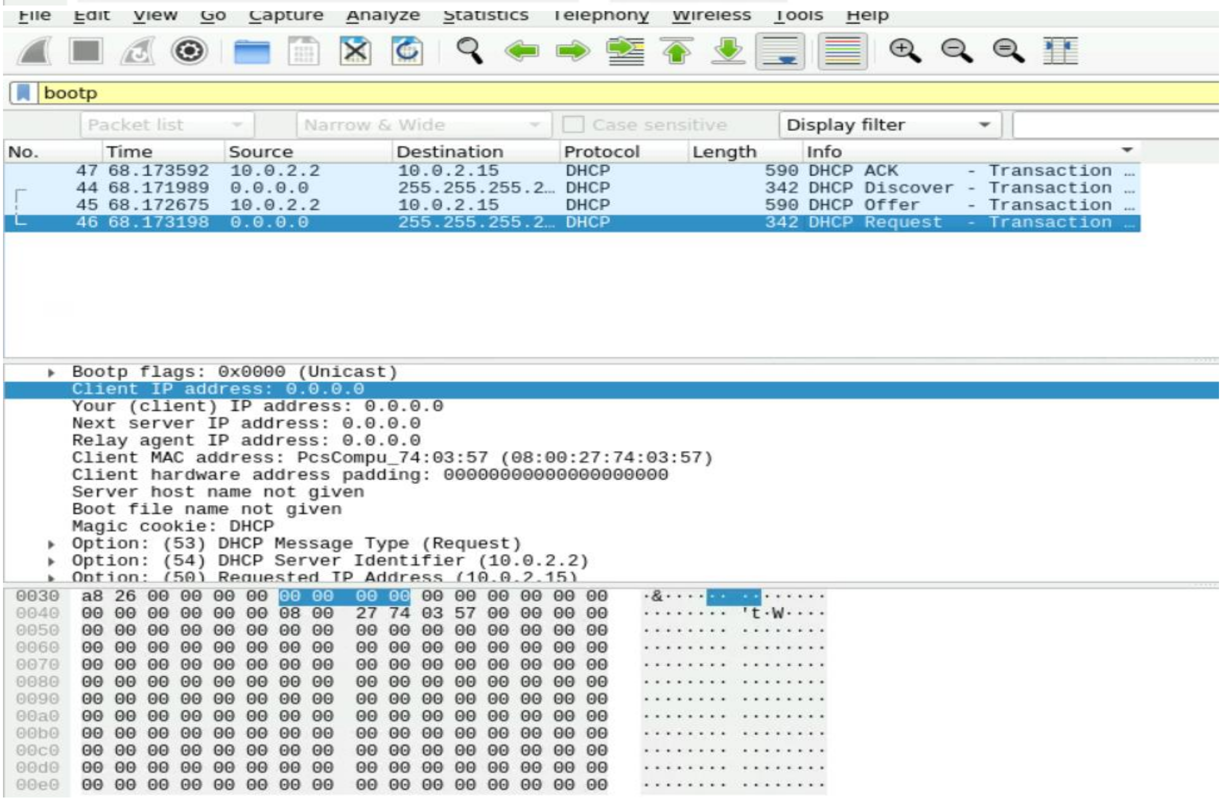
```
0030  a8 26 00 00 00 00 0a 00  02 0f 0a 00 02 0f 0a 00   ·&······ ········
0040  02 04 00 00 00 00 08 00  27 74 03 57 00 00 00 00   ········ 't·W····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 42 49  54 53 20 57 49 4c 50 20   ······BI TS WILP 
00a0  4e 65 74 77 6f 72 6b 20  4c 61 62 2e 70 78 65 00   Network  Lab.pxe·
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```



```
No.   Time       Source     Destination        Protocol  Length Info
   47 68.173592  10.0.2.2   10.0.2.15          DHCP         590 DHCP ACK      - Transaction …
   44 68.171989  0.0.0.0    255.255.255.2…     DHCP         342 DHCP Discover - Transaction …
   45 68.172675  10.0.2.2   10.0.2.15          DHCP         590 DHCP Offer    - Transaction …
   46 68.173198  0.0.0.0    255.255.255.2…     DHCP         342 DHCP Request  - Transaction …
```

```
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_74:03:57 (08:00:27:74:03:57)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Discover)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
```

```
0030  a8 26 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·&······ ········
0040  00 00 00 00 00 00 08 00  27 74 03 57 00 00 00 00   ········ 't·W····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp
Packet list
Narrow & Wide
Case sensitive
Display filter

```
No.   Time       Source     Destination        Protocol  Length Info
   47 68.173592  10.0.2.2   10.0.2.15          DHCP         590 DHCP ACK      - Transaction …
   44 68.171989  0.0.0.0    255.255.255.2…     DHCP         342 DHCP Discover - Transaction …
   45 68.172675  10.0.2.2   10.0.2.15          DHCP         590 DHCP Offer    - Transaction …
   46 68.173198  0.0.0.0    255.255.255.2…     DHCP         342 DHCP Request  - Transaction …
```

```
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_74:03:57 (08:00:27:74:03:57)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▸ Option: (54) DHCP Server Identifier (10.0.2.2)
  ▸ Option: (50) Requested IP Address (10.0.2.15)
```

```
0030  a8 26 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·&······ ········
0040  00 00 00 00 00 00 08 00  27 74 03 57 00 00 00 00   ········ 't·W····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

4. SNMP Analysis

Identify SNMP Version:

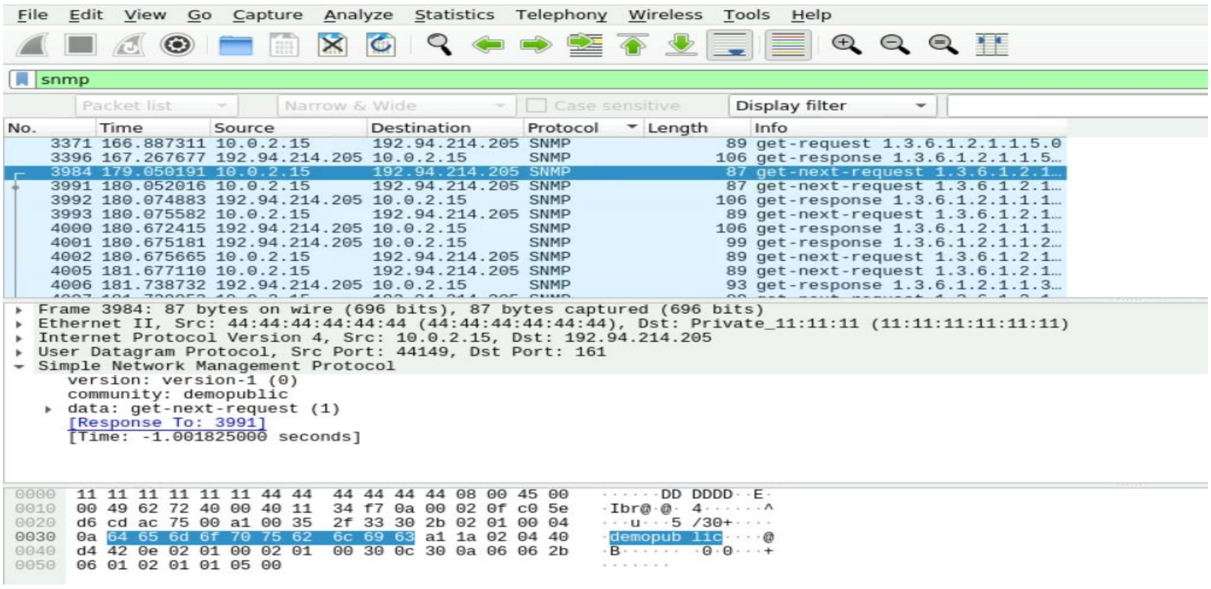
- Selected Packet: The selected packet is an SNMP packet.
- SNMP Version: The packet details show the SNMP version as version-1 (0).

Screenshot :

This screenshot shows the SNMP version as version-1 (0).

SNMP Messages:

1. **Get-Request Message:**
   - **Version:** version-1 (0)
   - **Community:** demopublic
   - **Data Type:** get-request (0)
   - **Request ID:** 1079781443
   - **Error Status:** noError (0)
   - **Error Index:** 0
   - **Variable Bindings:**
     - **Object Name:** 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
     - **Value:** Null



```
No.      Time       Source          Destination     Protocol  Length  Info
   3371 166.887311 10.0.2.15       192.94.214.205 SNMP          89 get-request 1.3.6.1.2.1.1.5.0
   3396 167.267677 192.94.214.205 10.0.2.15       SNMP         106 get-response 1.3.6.1.2.1.1.5…
   3984 179.050191 10.0.2.15       192.94.214.205 SNMP          87 get-next-request 1.3.6.1.2.1…
   3991 180.052016 10.0.2.15       192.94.214.205 SNMP          87 get-next-request 1.3.6.1.2.1…
   3992 180.074883 192.94.214.205 10.0.2.15       SNMP         106 get-response 1.3.6.1.2.1.1.1…
   3993 180.075582 10.0.2.15       192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
   4000 180.672415 192.94.214.205 10.0.2.15       SNMP         106 get-response 1.3.6.1.2.1.1.1…
   4001 180.675181 192.94.214.205 10.0.2.15       SNMP          99 get-response 1.3.6.1.2.1.1.2…
   4002 180.675665 10.0.2.15       192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
   4005 181.677110 10.0.2.15       192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
   4006 181.738732 192.94.214.205 10.0.2.15       SNMP          93 get-response 1.3.6.1.2.1.1.3…
```

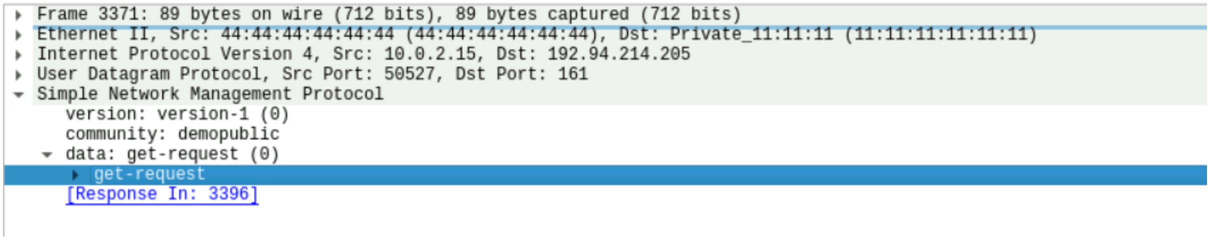
```
▸ Frame 3984: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
▸ Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▸ User Datagram Protocol, Src Port: 44149, Dst Port: 161
▾ Simple Network Management Protocol
     version: version-1 (0)
     community: demopublic
   ▸ data: get-next-request (1)
     [Response To: 3991]
     [Time: -1.001825000 seconds]
```

```
0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 49 62 72 40 00 40 11  34 f7 0a 00 02 0f c0 5e   ·Ibr@·@· 4······^
0020  d6 cd ac 75 00 a1 00 35  2f 33 30 2b 02 01 00 04   ···u···5 /30+····
0030  0a 64 65 6d 6f 70 75 62  6c 69 63 a1 1a 02 04 40   ·demopub lic····@
0040  d4 42 0e 02 01 00 02 01  00 30 0c 30 0a 06 06 2b   ·B······ ·0·0···+
0050  06 01 02 01 01 05 00                               ·······
```

Screenshot 2 :

This screenshot displays the details of an SNMP get-request message, highlighting the object name and value.

2. **Get-Response Message:**
    - **Version:** version-1 (0)
    - **Community:** demopublic
    - **Data Type:** get-response (2)
    - **Request ID:** 1087652366
    - **Error Status:** noError (0)
    - **Error Index:** 0
    - **Variable Bindings:**
        - **Object Name:** 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)
        - **Value (OctetString):** 746573742e6e65742e6f7267



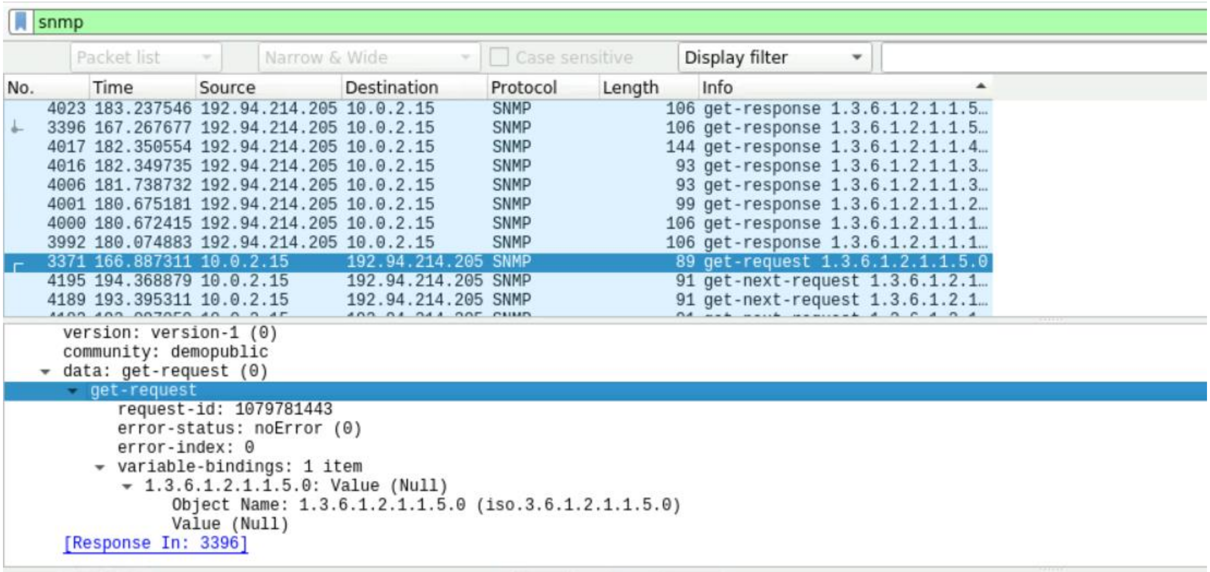
```
▸ Frame 3371: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
▸ Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.94.214.205
▸ User Datagram Protocol, Src Port: 50527, Dst Port: 161
▾ Simple Network Management Protocol
     version: version-1 (0)
     community: demopublic
   ▾ data: get-request (0)
      ▸ get-request
     [Response In: 3396]
```

Screenshot 3 :

This screenshot shows the details of an SNMP get-response message, including the object name and value.

3. **Get-Next-Request Message:**
    - **Version:** version-1 (0)
    - **Community:** demopublic
    - **Data Type:** get-next-request (1)
    - **Request ID:** 1087652388

    - **Error Status:** noError (0)
    - **Error Index:** 0
    - **Variable Bindings:**
        - **Object Name:** 1.3.6.1.2.1.1.9.1.4.5 (iso.3.6.1.2.1.1.9.1.4.5)
        - **Value:** Null



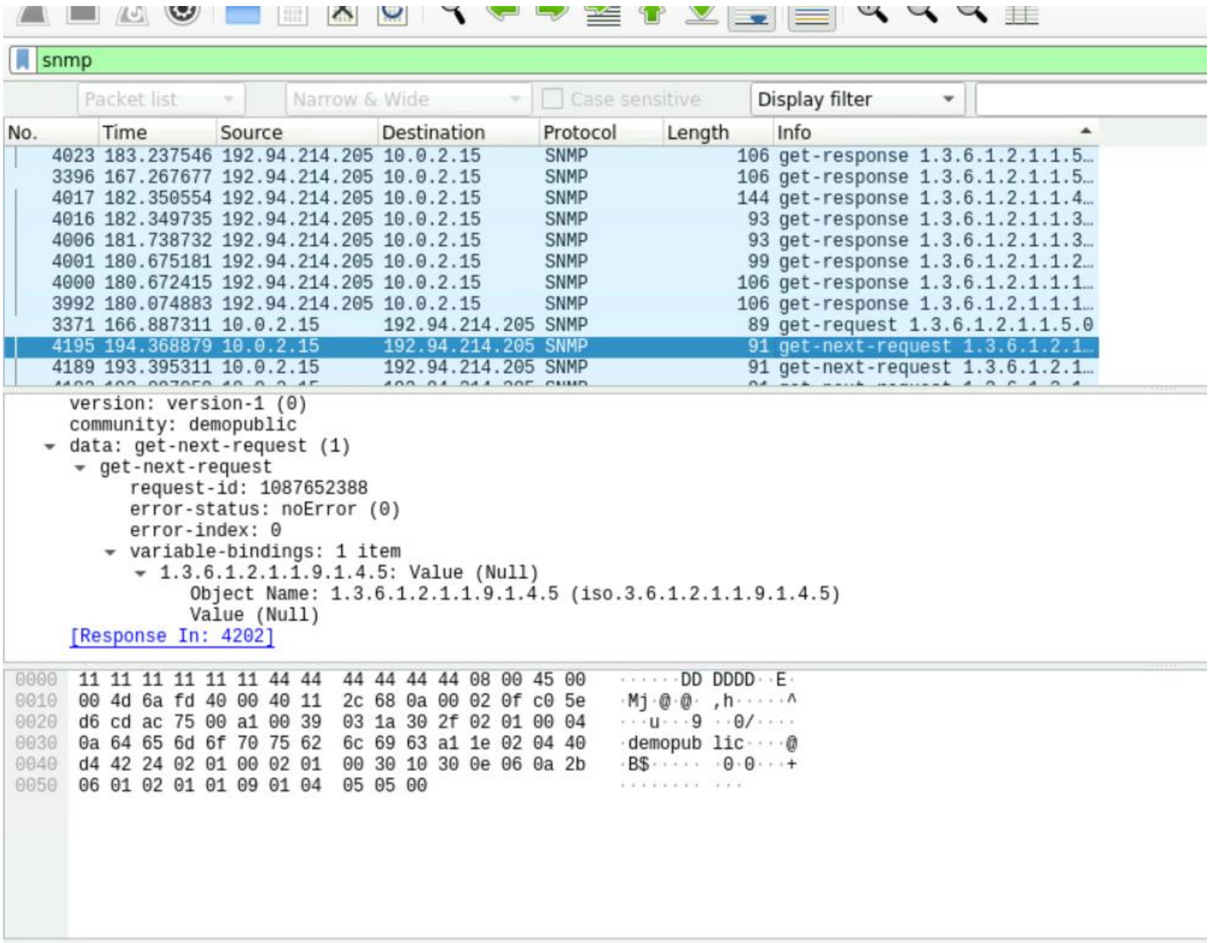
```
No.   Time       Source         Destination    Protocol Length Info
 4023 183.237546 192.94.214.205 10.0.2.15      SNMP     106 get-response 1.3.6.1.2.1.1.5…
 3396 167.267677 192.94.214.205 10.0.2.15      SNMP     106 get-response 1.3.6.1.2.1.1.5…
 4017 182.350554 192.94.214.205 10.0.2.15      SNMP     144 get-response 1.3.6.1.2.1.1.4…
 4016 182.349735 192.94.214.205 10.0.2.15      SNMP      93 get-response 1.3.6.1.2.1.1.3…
 4006 181.738732 192.94.214.205 10.0.2.15      SNMP      93 get-response 1.3.6.1.2.1.1.3…
 4001 180.675181 192.94.214.205 10.0.2.15      SNMP      99 get-response 1.3.6.1.2.1.1.2…
 4000 180.672415 192.94.214.205 10.0.2.15      SNMP     106 get-response 1.3.6.1.2.1.1.1…
 3992 180.074883 192.94.214.205 10.0.2.15      SNMP     106 get-response 1.3.6.1.2.1.1.1…
 3371 166.887311 10.0.2.15      192.94.214.205 SNMP      89 get-request 1.3.6.1.2.1.1.5.0
 4195 194.368879 10.0.2.15      192.94.214.205 SNMP      91 get-next-request 1.3.6.1.2.1…
 4189 193.395311 10.0.2.15      192.94.214.205 SNMP      91 get-next-request 1.3.6.1.2.1…
```

```
    version: version-1 (0)
    community: demopublic
  ▾ data: get-request (0)
    ▾ get-request
        request-id: 1079781443
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 1 item
        ▾ 1.3.6.1.2.1.1.5.0: Value (Null)
            Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
            Value (Null)
    [Response In: 3396]
```

Screenshot 4:

This screenshot displays the details of an SNMP get-next-request message, including the object name and value.

4. **Get-Next-Response Message:**
    - **Version:** version-1 (0)
    - **Community:** demopublic
    - **Data Type:** get-next-response (2)
    - **Request ID:** 1087652390
    - **Error Status:** noError (0)
    - **Error Index:** 0
    - **Variable Bindings:**
        - **Object Name:** 1.3.6.1.2.1.1.9.1.4.6 (iso.3.6.1.2.1.1.9.1.4.6)
        - **Value (OctetString):** 746573742e6e65742e6f7267



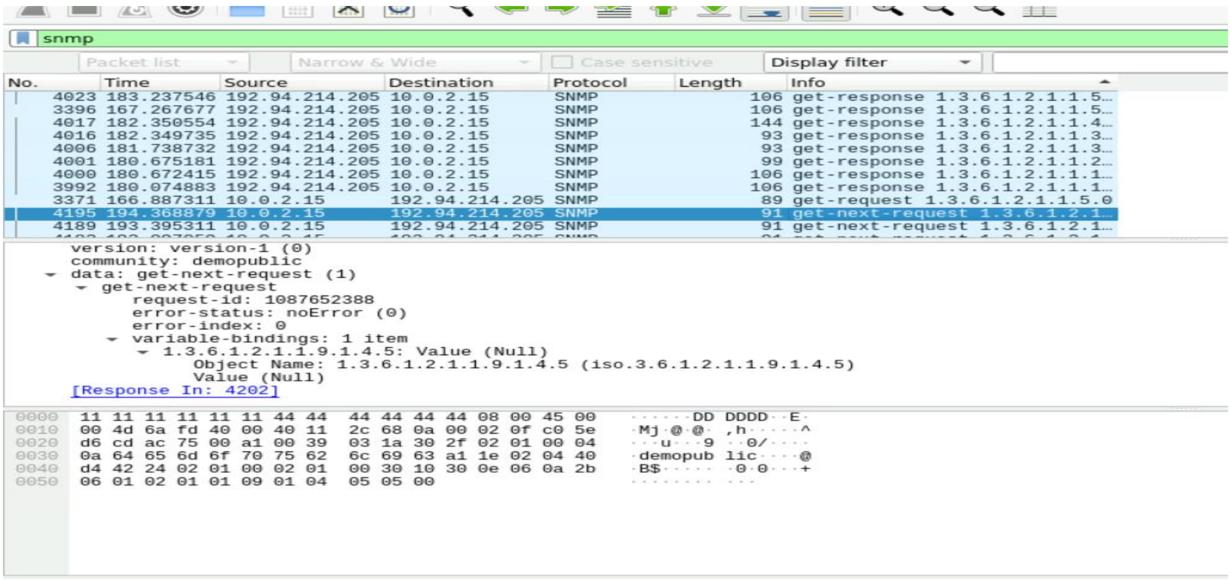
```
No.    Time        Source          Destination     Protocol  Length  Info
  4023 183.237546 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.5…
  3396 167.267677 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.5…
  4017 182.350554 192.94.214.205 10.0.2.15       SNMP       144 get-response 1.3.6.1.2.1.1.4…
  4016 182.349735 192.94.214.205 10.0.2.15       SNMP        93 get-response 1.3.6.1.2.1.1.3…
  4006 181.738732 192.94.214.205 10.0.2.15       SNMP        93 get-response 1.3.6.1.2.1.1.3…
  4001 180.675181 192.94.214.205 10.0.2.15       SNMP        99 get-response 1.3.6.1.2.1.1.2…
  4000 180.672415 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.1…
  3992 180.074883 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.1…
  3371 166.887311 10.0.2.15       192.94.214.205 SNMP        89 get-request 1.3.6.1.2.1.1.5.0
  4195 194.368879 10.0.2.15       192.94.214.205 SNMP        91 get-next-request 1.3.6.1.2.1…
  4189 193.395311 10.0.2.15       192.94.214.205 SNMP        91 get-next-request 1.3.6.1.2.1…
```

```
    version: version-1 (0)
    community: demopublic
  ▾ data: get-next-request (1)
    ▾ get-next-request
        request-id: 1087652388
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 1 item
        ▾ 1.3.6.1.2.1.1.9.1.4.5: Value (Null)
            Object Name: 1.3.6.1.2.1.1.9.1.4.5 (iso.3.6.1.2.1.1.9.1.4.5)
            Value (Null)
    [Response In: 4202]
```

```
0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 4d 6a fd 40 00 40 11  2c 68 0a 00 02 0f c0 5e   ·Mj·@·@· ,h·····^
0020  d6 cd ac 75 00 a1 00 39  03 1a 30 2f 02 01 00 04   ···u···9 ··0/····
0030  0a 64 65 6d 6f 70 75 62  6c 69 63 a1 1e 02 04 40   ·demopub lic····@
0040  d4 42 24 02 01 00 02 01  00 30 10 30 0e 06 0a 2b   ·B$····· ·0·0···+
0050  06 01 02 01 01 09 01 04  05 05 00                  ········ ···
```

Screenshot 5:

This screenshot shows the details of an SNMP get-next-response message, highlighting the object name and value.



snmp
Packet list
Narrow & Wide
Case sensitive
Display filter

```
No.    Time        Source          Destination     Protocol  Length  Info
  4023 183.237546 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.5…
  3396 167.267677 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.5…
  4017 182.350554 192.94.214.205 10.0.2.15       SNMP       144 get-response 1.3.6.1.2.1.1.4…
  4016 182.349735 192.94.214.205 10.0.2.15       SNMP        93 get-response 1.3.6.1.2.1.1.3…
  4006 181.738732 192.94.214.205 10.0.2.15       SNMP        93 get-response 1.3.6.1.2.1.1.3…
  4001 180.675181 192.94.214.205 10.0.2.15       SNMP        99 get-response 1.3.6.1.2.1.1.2…
  4000 180.672415 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.1…
  3992 180.074883 192.94.214.205 10.0.2.15       SNMP       106 get-response 1.3.6.1.2.1.1.1…
  3371 166.887311 10.0.2.15       192.94.214.205 SNMP        89 get-request 1.3.6.1.2.1.1.5.0
  4195 194.368879 10.0.2.15       192.94.214.205 SNMP        91 get-next-request 1.3.6.1.2.1…
  4189 193.395311 10.0.2.15       192.94.214.205 SNMP        91 get-next-request 1.3.6.1.2.1…
```

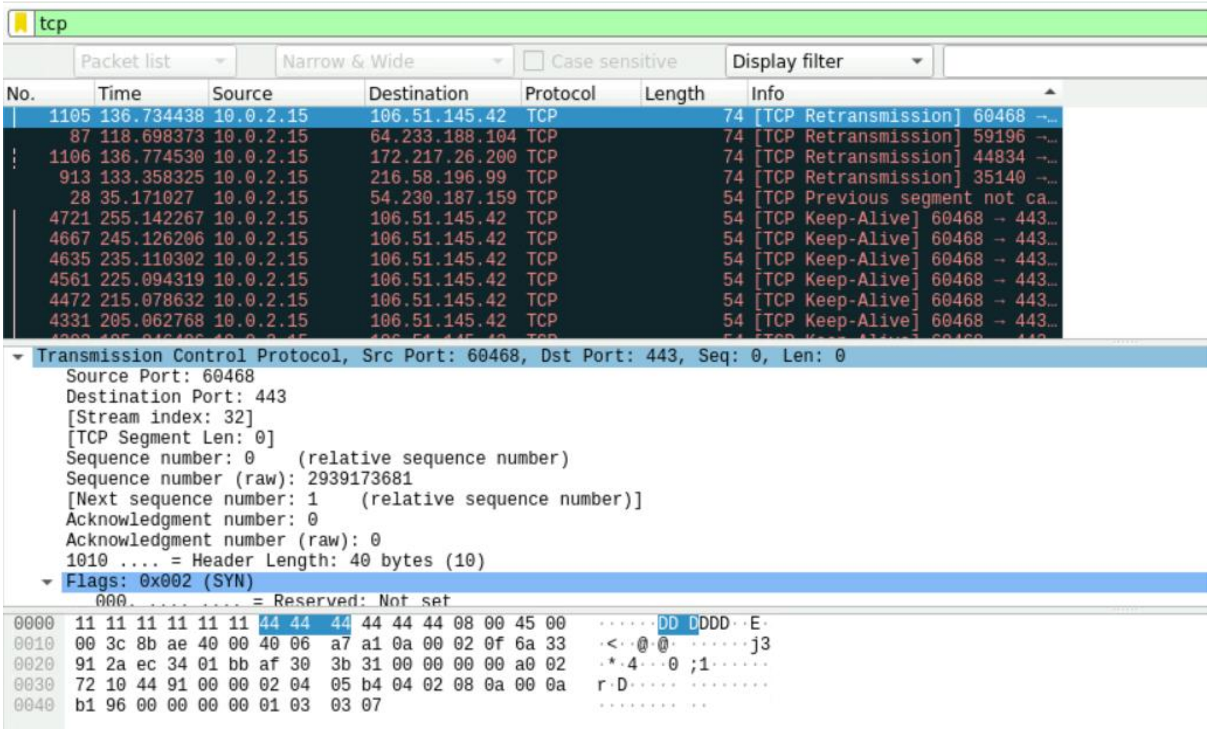
```
    version: version-1 (0)
    community: demopublic
  ▾ data: get-next-request (1)
    ▾ get-next-request
        request-id: 1087652388
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 1 item
        ▾ 1.3.6.1.2.1.1.9.1.4.5: Value (Null)
            Object Name: 1.3.6.1.2.1.1.9.1.4.5 (iso.3.6.1.2.1.1.9.1.4.5)
            Value (Null)
    [Response In: 4202]
```

```
0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 4d 6a fd 40 00 40 11  2c 68 0a 00 02 0f c0 5e   ·Mj·@·@· ,h·····^
0020  d6 cd ac 75 00 a1 00 39  03 1a 30 2f 02 01 00 04   ···u···9 ··0/····
0030  0a 64 65 6d 6f 70 75 62  6c 69 63 a1 1e 02 04 40   ·demopub lic····@
0040  d4 42 24 02 01 00 02 01  00 30 10 30 0e 06 0a 2b   ·B$····· ·0·0···+
0050  06 01 02 01 01 09 01 04  05 05 00                  ········ ···
```

5. Transport Layer (e.g., TCP, UDP)

For TCP packets, you can view the following details in Wireshark:

- **Source Port: The port number of the sender (e.g., 60468).**
- **Destination Port: The port number of the receiver (e.g., 443).**
- **Sequence Number: A number used to ensure packets are reassembled in the correct order.**
- **Acknowledgment Number: Used for acknowledging receipt of packets.**
- **Flags: Various control flags (e.g., SYN, ACK).**
- **Window Size: Flow control.**
- **Checksum: Error-checking.**
- **Options: Any options.**



```
No.   Time       Source      Destination     Protocol Length Info
 1105 136.734438 10.0.2.15   106.51.145.42   TCP          74 [TCP Retransmission] 60468 →…
   87 118.698373 10.0.2.15   64.233.188.104  TCP          74 [TCP Retransmission] 59196 →…
 1106 136.774530 10.0.2.15   172.217.26.200  TCP          74 [TCP Retransmission] 44834 →…
  913 133.358325 10.0.2.15   216.58.196.99   TCP          74 [TCP Retransmission] 35140 →…
   28 35.171027  10.0.2.15   54.230.187.159  TCP          54 [TCP Previous segment not ca…
 4721 255.142267 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
 4667 245.126206 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
 4635 235.110302 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
 4561 225.094319 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
 4472 215.078632 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
 4331 205.062768 10.0.2.15   106.51.145.42   TCP          54 [TCP Keep-Alive] 60468 → 443…
```

```
▾ Transmission Control Protocol, Src Port: 60468, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 60468
    Destination Port: 443
    [Stream index: 32]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2939173681
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▾ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
```

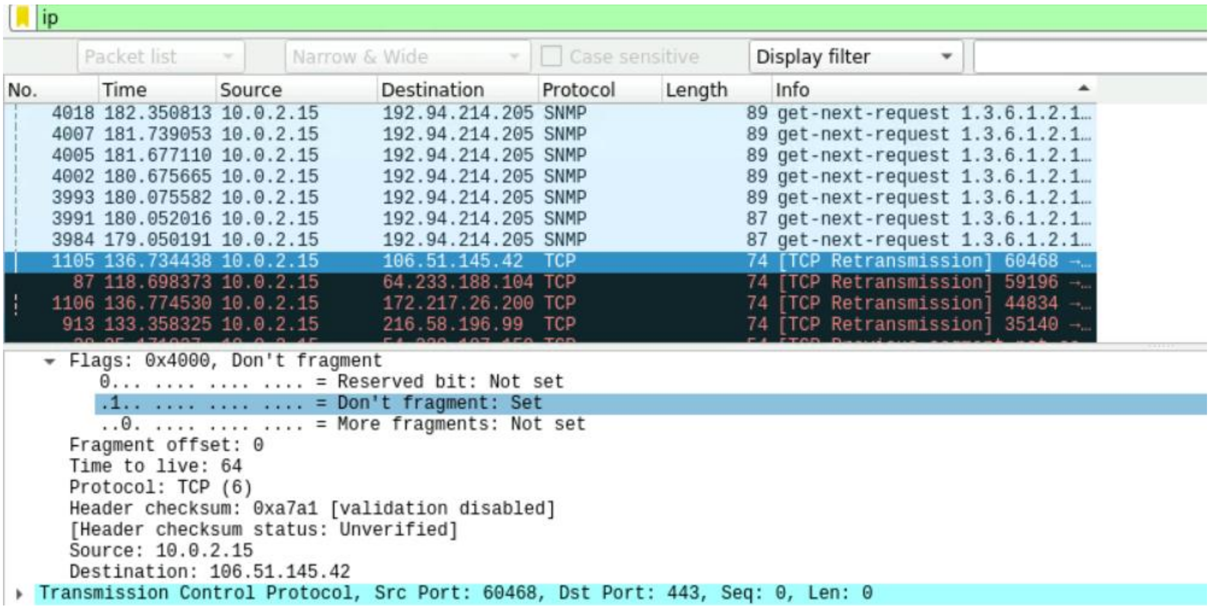
```
0000  11 11 11 11 11 11 44 44  44 44 44 44 08 00 45 00   ······DD DDDD··E·
0010  00 3c 8b ae 40 00 40 06  a7 a1 0a 00 02 0f 6a 33   ·<··@·@· ······j3
0020  91 2a ec 34 01 bb af 30  3b 31 00 00 00 00 a0 02   ·*·4···0 ;1······
0030  72 10 44 91 00 00 02 04  05 b4 04 02 08 0a 00 0a   r·D····· ········
0040  b1 96 00 00 00 00 01 03  03 07                     ········ ··
```

2. Network Layer (e.g., IP)

In the IP section, you can see:

- **Source IP Address: The IP address of the sender (e.g., 10.0.2.15).**
- **Destination IP Address: The IP address of the receiver (e.g., 106.51.145.42).**

- **Time to Live (TTL): How many hops the packet can traverse before being discarded (e.g., 64).**
- **Protocol: Indicates the protocol used in the data portion (e.g., TCP).**
- **Header Checksum: Used for error-checking of the header.**



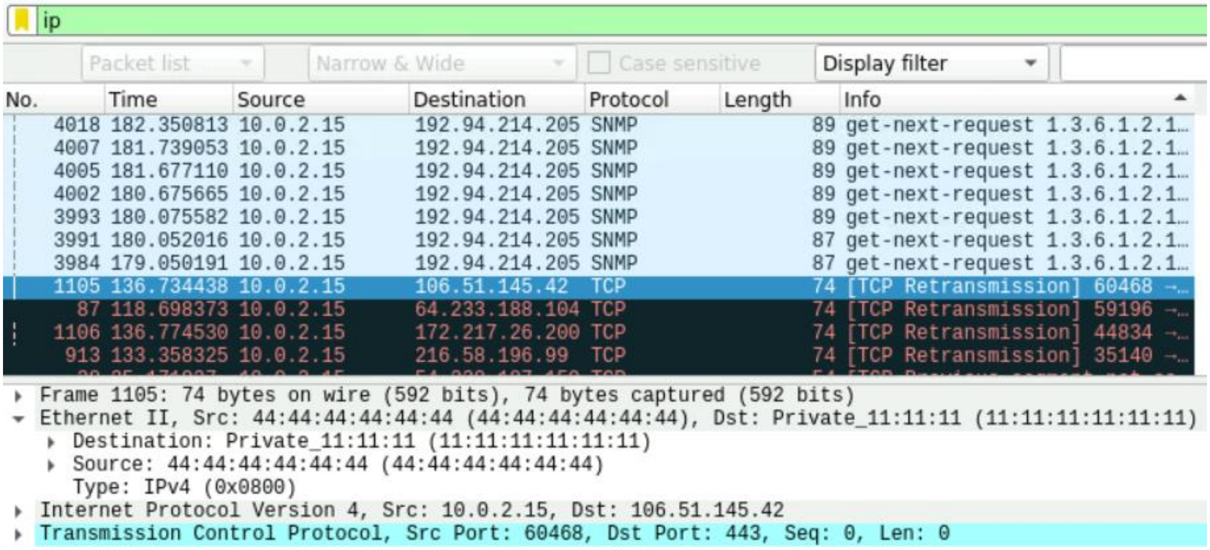
```
No.    Time       Source      Destination     Protocol   Length   Info
  4018 182.350813 10.0.2.15   192.94.214.205 SNMP      89 get-next-request 1.3.6.1.2.1…
  4007 181.739053 10.0.2.15   192.94.214.205 SNMP      89 get-next-request 1.3.6.1.2.1…
  4005 181.677110 10.0.2.15   192.94.214.205 SNMP      89 get-next-request 1.3.6.1.2.1…
  4002 180.675665 10.0.2.15   192.94.214.205 SNMP      89 get-next-request 1.3.6.1.2.1…
  3993 180.075582 10.0.2.15   192.94.214.205 SNMP      89 get-next-request 1.3.6.1.2.1…
  3991 180.052016 10.0.2.15   192.94.214.205 SNMP      87 get-next-request 1.3.6.1.2.1…
  3984 179.050191 10.0.2.15   192.94.214.205 SNMP      87 get-next-request 1.3.6.1.2.1…
  1105 136.734438 10.0.2.15   106.51.145.42  TCP       74 [TCP Retransmission] 60468 →…
    87 118.698373 10.0.2.15   64.233.188.104 TCP       74 [TCP Retransmission] 59196 →…
  1106 136.774530 10.0.2.15   172.217.26.200 TCP       74 [TCP Retransmission] 44834 →…
   913 133.358325 10.0.2.15   216.58.196.99  TCP       74 [TCP Retransmission] 35140 →…
```

```
  ▾ Flags: 0x4000, 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: 0xa7a1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 106.51.145.42
▸ Transmission Control Protocol, Src Port: 60468, Dst Port: 443, Seq: 0, Len: 0
```

3. Link Layer (e.g., Ethernet)

In the Ethernet section, you can see:

- **Source MAC Address: The MAC address of the sender.**
- **Destination MAC Address: The MAC address of the receiver.**
- **Type: Indicates the protocol encapsulated in the payload of the frame (e.g., IP).**



```
No.    Time       Source      Destination     Protocol  Length  Info
  4018 182.350813 10.0.2.15   192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
  4007 181.739053 10.0.2.15   192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
  4005 181.677110 10.0.2.15   192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
  4002 180.675665 10.0.2.15   192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
  3993 180.075582 10.0.2.15   192.94.214.205 SNMP          89 get-next-request 1.3.6.1.2.1…
  3991 180.052016 10.0.2.15   192.94.214.205 SNMP          87 get-next-request 1.3.6.1.2.1…
  3984 179.050191 10.0.2.15   192.94.214.205 SNMP          87 get-next-request 1.3.6.1.2.1…
  1105 136.734438 10.0.2.15   106.51.145.42  TCP           74 [TCP Retransmission] 60468 →…
    87 118.698373 10.0.2.15   64.233.188.104 TCP           74 [TCP Retransmission] 59196 →…
  1106 136.774530 10.0.2.15   172.217.26.200 TCP           74 [TCP Retransmission] 44834 →…
   913 133.358325 10.0.2.15   216.58.196.99  TCP           74 [TCP Retransmission] 35140 →…
```

```
▸ Frame 1105: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▾ Ethernet II, Src: 44:44:44:44:44:44 (44:44:44:44:44:44), Dst: Private_11:11:11 (11:11:11:11:11:11)
   ▸ Destination: Private_11:11:11 (11:11:11:11:11:11)
   ▸ Source: 44:44:44:44:44:44 (44:44:44:44:44:44)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 106.51.145.42
▸ Transmission Control Protocol, Src Port: 60468, Dst Port: 443, Seq: 0, Len: 0
```