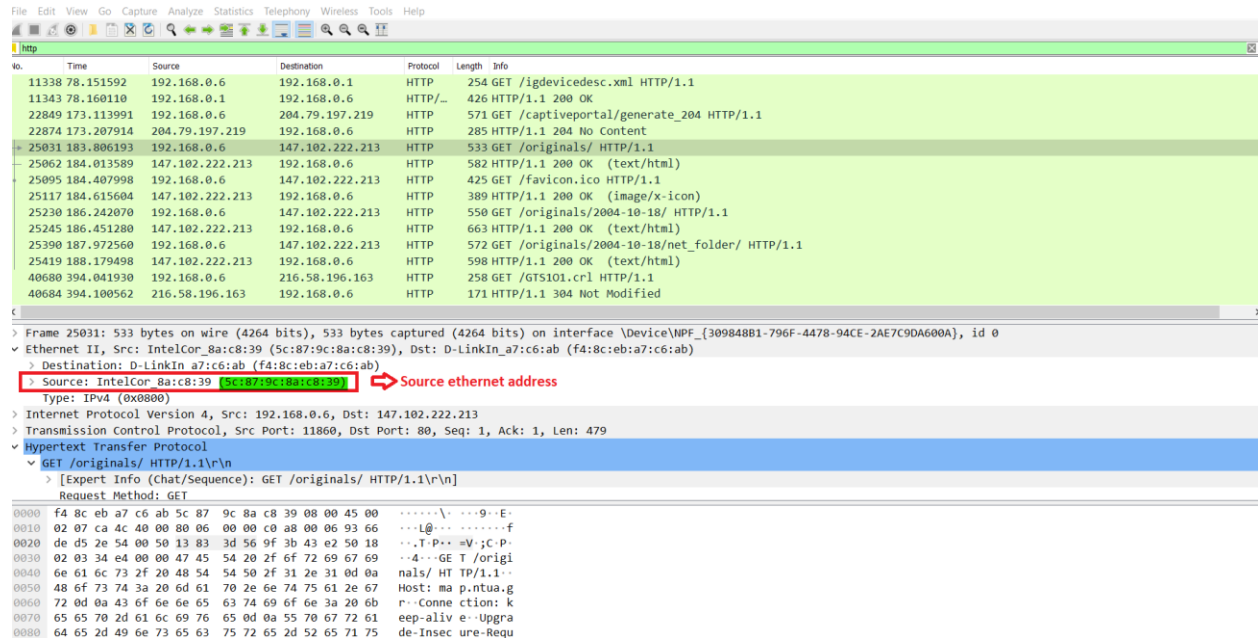


# Lab-7

Do a regular HTTP GET and response

1. What is the 48 bit ethernet address of your computer?



No.	Time	Source	Destination	Protocol	Length	Info
11338	78.151592	192.168.0.6	192.168.0.1	HTTP	254	GET /igdeviceDesc.xml HTTP/1.1
11343	78.160110	192.168.0.1	192.168.0.6	HTTP	426	HTTP/1.1 200 OK
22849	173.113991	192.168.0.6	204.79.197.219	HTTP	571	GET /captiveportal/generate_204 HTTP/1.1
22874	173.207914	204.79.197.219	192.168.0.6	HTTP	285	HTTP/1.1 204 No Content
25031	183.806193	192.168.0.6	147.102.222.213	HTTP	533	GET /originals/ HTTP/1.1
25062	184.013589	147.102.222.213	192.168.0.6	HTTP	582	HTTP/1.1 200 OK (text/html)
25095	184.407998	192.168.0.6	147.102.222.213	HTTP	425	GET /favicon.ico HTTP/1.1
25117	184.615604	147.102.222.213	192.168.0.6	HTTP	389	HTTP/1.1 200 OK (image/x-icon)
25230	186.242070	192.168.0.6	147.102.222.213	HTTP	550	GET /originals/2004-10-18/ HTTP/1.1
25245	186.451280	147.102.222.213	192.168.0.6	HTTP	663	HTTP/1.1 200 OK (text/html)
25390	187.972560	192.168.0.6	147.102.222.213	HTTP	572	GET /originals/2004-10-18/net_folder/ HTTP/1.1
25419	188.179498	147.102.222.213	192.168.0.6	HTTP	598	HTTP/1.1 200 OK (text/html)
40680	394.041930	192.168.0.6	216.58.196.163	HTTP	258	GET /GTS101.crl HTTP/1.1
40684	394.100562	216.58.196.163	192.168.0.6	HTTP	171	HTTP/1.1 304 Not Modified

> Frame 25031: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF\_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0

> Ethernet II, Src: IntelCor 8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn a7:c6:ab (f4:8c:eb:a7:c6:ab)

> Destination: D-LinkIn a7:c6:ab (f4:8c:eb:a7:c6:ab)

> Source: IntelCor 8a:c8:39 (5c:87:9c:8a:c8:39) **Source ethernet address**

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.6, Dst: 147.102.222.213

> Transmission Control Protocol, Src Port: 11860, Dst Port: 80, Seq: 1, Ack: 1, Len: 479

> Hypertext Transfer Protocol

> GET /originals/ HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /originals/ HTTP/1.1\r\n]

Request Method: GET

0000 f4 8c eb a7 c6 ab 5c 87 9c 8a c8 39 00 00 45 00 ..... \...9...E-

0010 02 07 ca 4c 40 00 80 06 00 00 c0 a8 00 06 93 66 ...L@... ..f

0020 de d5 2e 54 00 50 13 83 3d 56 9f 3b 43 e2 50 18 ...T.P...=V:j:P-

0030 02 03 34 e4 00 00 47 45 54 20 2f 6f 72 69 67 69 ...4...GE T /origi

0040 6e 61 6c 73 2f 20 48 54 54 50 2f 31 2e 31 0d 0a nals/ HT TP/1.1..

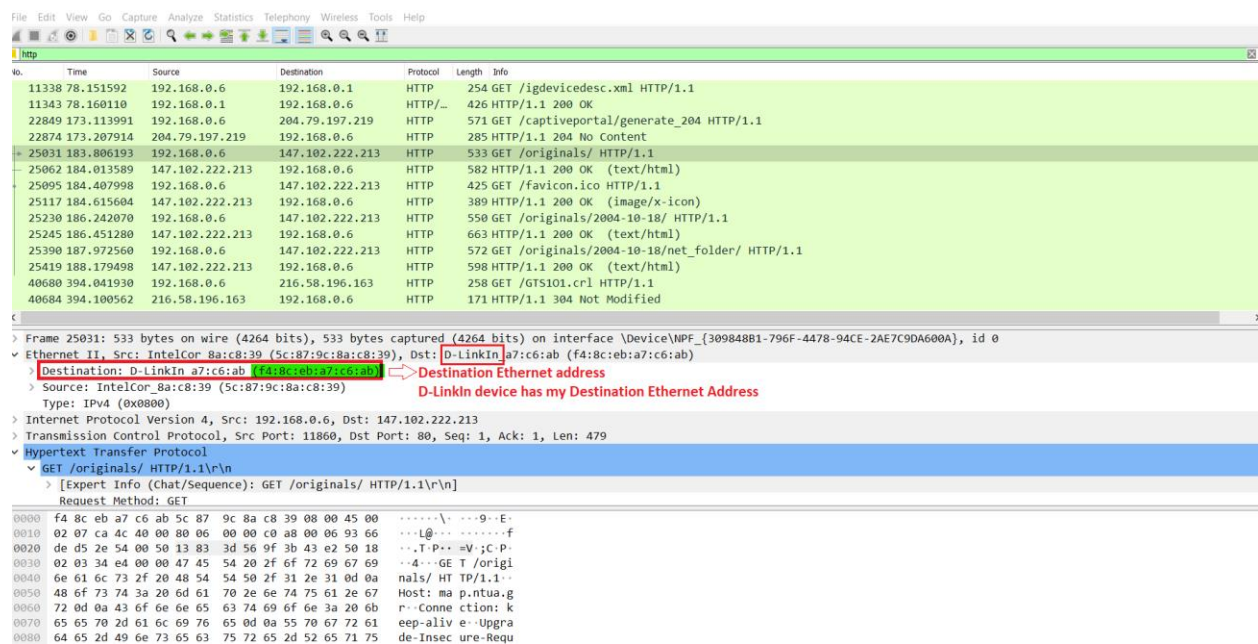
0050 48 6f 73 74 3a 20 6d 61 70 2e 6e 74 75 61 2e 67 Host: ma p.ntua.g

0060 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b r...Conne ction: k

0070 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e...Upgra

0080 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

2. What is the 48-bit destination address in the ethernet frame? Which device has this ethernet address?



No.	Time	Source	Destination	Protocol	Length	Info
11338	78.151592	192.168.0.6	192.168.0.1	HTTP	254	GET /igdeviceDesc.xml HTTP/1.1
11343	78.160110	192.168.0.1	192.168.0.6	HTTP	426	HTTP/1.1 200 OK
22849	173.113991	192.168.0.6	204.79.197.219	HTTP	571	GET /captiveportal/generate_204 HTTP/1.1
22874	173.207914	204.79.197.219	192.168.0.6	HTTP	285	HTTP/1.1 204 No Content
25031	183.806193	192.168.0.6	147.102.222.213	HTTP	533	GET /originals/ HTTP/1.1
25062	184.013589	147.102.222.213	192.168.0.6	HTTP	582	HTTP/1.1 200 OK (text/html)
25095	184.407998	192.168.0.6	147.102.222.213	HTTP	425	GET /favicon.ico HTTP/1.1
25117	184.615604	147.102.222.213	192.168.0.6	HTTP	389	HTTP/1.1 200 OK (image/x-icon)
25230	186.242070	192.168.0.6	147.102.222.213	HTTP	550	GET /originals/2004-10-18/ HTTP/1.1
25245	186.451280	147.102.222.213	192.168.0.6	HTTP	663	HTTP/1.1 200 OK (text/html)
25390	187.972560	192.168.0.6	147.102.222.213	HTTP	572	GET /originals/2004-10-18/net_folder/ HTTP/1.1
25419	188.179498	147.102.222.213	192.168.0.6	HTTP	598	HTTP/1.1 200 OK (text/html)
40680	394.041930	192.168.0.6	216.58.196.163	HTTP	258	GET /GTS101.crl HTTP/1.1
40684	394.100562	216.58.196.163	192.168.0.6	HTTP	171	HTTP/1.1 304 Not Modified

> Frame 25031: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF\_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0

> Ethernet II, Src: IntelCor 8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn a7:c6:ab (f4:8c:eb:a7:c6:ab)

> Destination: D-LinkIn a7:c6:ab (f4:8c:eb:a7:c6:ab) **Destination Ethernet address**

> Source: IntelCor 8a:c8:39 (5c:87:9c:8a:c8:39) **D-LinkIn device has my Destination Ethernet Address**

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.6, Dst: 147.102.222.213

> Transmission Control Protocol, Src Port: 11860, Dst Port: 80, Seq: 1, Ack: 1, Len: 479

> Hypertext Transfer Protocol

> GET /originals/ HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /originals/ HTTP/1.1\r\n]

Request Method: GET

0000 f4 8c eb a7 c6 ab 5c 87 9c 8a c8 39 00 00 45 00 ..... \...9...E-

0010 02 07 ca 4c 40 00 80 06 00 00 c0 a8 00 06 93 66 ...L@... ..f

0020 de d5 2e 54 00 50 13 83 3d 56 9f 3b 43 e2 50 18 ...T.P...=V:j:P-

0030 02 03 34 e4 00 00 47 45 54 20 2f 6f 72 69 67 69 ...4...GE T /origi

0040 6e 61 6c 73 2f 20 48 54 54 50 2f 31 2e 31 0d 0a nals/ HT TP/1.1..

0050 48 6f 73 74 3a 20 6d 61 70 2e 6e 74 75 61 2e 67 Host: ma p.ntua.g

0060 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b r...Conne ction: k

0070 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e...Upgra

0080 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

**D-LinkIn** device (my router) has my destination ethernet address

3. What is the content of frame type field? Which upper layer protocol does this correspond to?

Content of frame type field: **0x0800**

It corresponds to **IPv4** upper layer protocol

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets, with packet 25031 selected. The middle pane shows the details of this packet, expanded to show the 'Hypertext Transfer Protocol' section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet 25031: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF\_{309848B1-796F-4478-94CE-2AE7C9DA600A}, id 0

Ethernet II, Src: IntelCor\_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn\_a7:c6:ab (f4:8c:eb:a7:c6:ab)

Destination: D-LinkIn\_a7:c6:ab (f4:8c:eb:a7:c6:ab)

Source: IntelCor\_8a:c8:39 (5c:87:9c:8a:c8:39)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.6, Dst: 147.102.222.213

Transmission Control Protocol, Src Port: 11860, Dst Port: 80, Seq: 1, Ack: 1, Len: 479

Hypertext Transfer Protocol

GET /originals/ HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /originals/ HTTP/1.1\r\n]

Request Method: GET

0000 f4 8c eb a7 c6 ab 5c 87 9c 8a c8 39 08 00 45 00 ..... \ . . . 9 . . E -

0010 02 07 ca 4c 40 00 80 06 00 00 c0 a8 00 06 93 66 ... L @ . . . . . . . . f

0020 de d5 2e 54 00 50 13 83 3d 56 9f 3b 43 e2 50 18 ... T . P . . = V ; C . P

0030 02 03 34 e4 00 00 47 45 54 20 2f 6f 72 69 67 69 .. 4 . . . G E T /origi

0040 6e 61 6c 73 2f 20 48 54 54 50 2f 31 2e 31 0d 0a nals/ HT TP/1.1 .

0050 48 6f 73 74 3a 20 6d 61 70 2e 6e 74 75 61 2e 67 Host: ma p.ntua.g

0060 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b r . . Conne ction: k

0070 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e . . Upgra

0080 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

4. How many bytes from the beginning does the GET appear in the ethernet frame?

After **54** bytes, GET appear in ethernet frame.

http						
No.	Time	Source	Destination	Protocol	Length	Info
11338	78.151592	192.168.0.6	192.168.0.1	HTTP	254	GET /igdevice-desc.xml HTTP/1.1
11343	78.160110	192.168.0.1	192.168.0.6	HTTP/...	426	HTTP/1.1 200 OK
22849	173.113991	192.168.0.6	204.79.197.219	HTTP	571	GET /captiveportal/generate_204 HTTP/1.1
22874	173.207914	204.79.197.219	192.168.0.6	HTTP	285	HTTP/1.1 204 No Content
25031	183.806193	192.168.0.6	147.102.222.213	HTTP	533	GET /originals/ HTTP/1.1
25062	184.013589	147.102.222.213	192.168.0.6	HTTP	582	HTTP/1.1 200 OK (text/html)
25095	184.407998	192.168.0.6	147.102.222.213	HTTP	425	GET /favicon.ico HTTP/1.1
25117	184.615604	147.102.222.213	192.168.0.6	HTTP	389	HTTP/1.1 200 OK (image/x-icon)
25230	186.242070	192.168.0.6	147.102.222.213	HTTP	550	GET /originals/2004-10-18/ HTTP/1.1
25245	186.451280	147.102.222.213	192.168.0.6	HTTP	663	HTTP/1.1 200 OK (text/html)
25390	187.972560	192.168.0.6	147.102.222.213	HTTP	572	GET /originals/2004-10-18/net_folder/ HTTP/1.1
25419	188.179498	147.102.222.213	192.168.0.6	HTTP	598	HTTP/1.1 200 OK (text/html)
40680	394.041930	192.168.0.6	216.58.196.163	HTTP	258	GET /GTS101.crl HTTP/1.1
40684	394.100562	216.58.196.163	192.168.0.6	HTTP	171	HTTP/1.1 304 Not Modified

<

▼ Ethernet II, Src: IntelCor\_8a:c8:39 (5c:87:9c:8a:c8:39), Dst: D-LinkIn\_a7:c6:ab (f4:8c:eb:a7:c6:ab)

- > Destination: D-LinkIn\_a7:c6:ab (f4:8c:eb:a7:c6:ab)
- > Source: IntelCor\_8a:c8:39 (5c:87:9c:8a:c8:39)
- Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 192.168.0.6, Dst: 147.102.222.213
- > Transmission Control Protocol, Src Port: 11860, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
- ▼ Hypertext Transfer Protocol
  - ▼ GET /originals/ HTTP/1.1\r\n
    - > [Expert Info (Chat/Sequence): GET /originals/ HTTP/1.1\r\n]
    - Request Method: GET
    - Request URI: /originals/

0000 f4 8c eb a7 c6 ab 5c 87 9c 8a c8 39 08 00 45 00 .....\r\n...9..E.

0010 02 07 ca 4c 40 00 00 06 00 00 c0 a8 00 06 93 66 ...L@... .....

0020 de d5 2e 54 00 50 13 83 3d 56 9f 3b 43 e2 50 18 ...T.P... =V.;C.P.

0030 02 03 34 e4 00 00 47 45 54 20 2f 6f 72 69 67 69 ...4...GE T /origi

0040 6e 61 6c 73 2f 20 48 54 54 50 2f 31 2e 31 0d 0a nals/ HT IP/1.1..

0050 48 6f 73 74 3a 20 6d 61 70 2e 6e 74 75 61 2e 67 Host: ma p.ntua.g

0060 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b r..Conne ction: k

0070 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e..Upgra

0080 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ