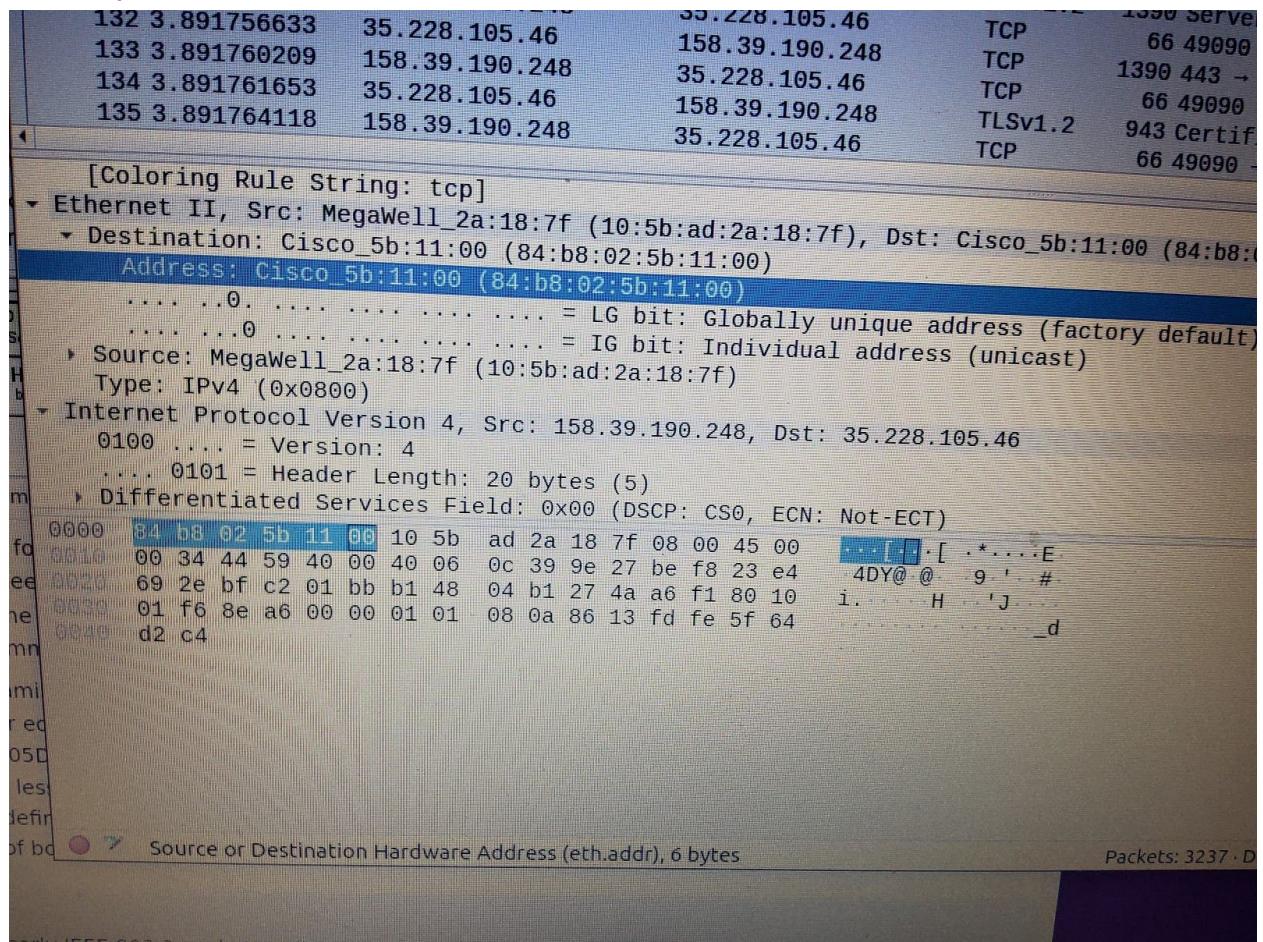


Jobbet i gruppe: Heljar Korbi og Khayam Nami.

Lab 2

Oppgave 1:

Destinasjon MAC-adresse



Denne delen består av destinasjons harware adressen til hvilken enhet pakke skal til. I denne pakken Cisco_5b:11:00 med en mac adresse på 84:b8:02:5b:11:00.

Kilde MAC-adresse:

The screenshot shows the Wireshark interface with an Ethernet frame selected. The details pane displays the following information:

- Source: MegaWell_2a:18:7f (10:5b:ad:2a:18:7f)**
- Address: MegaWell_2a:18:7f (10:5b:ad:2a:18:7f)**
-0. = LG bit: Globally unique**
-0. = IG bit: Individual address**
- Type: IPv4 (0x0800)**
- Internet Protocol Version 4, Src: 158.39.190.248, Dst: 35.2...**
- Transmission Control Protocol, Src Port: 49090, Dst Port: 4...**

The bytes pane shows the raw hex and ASCII data of the MAC header:

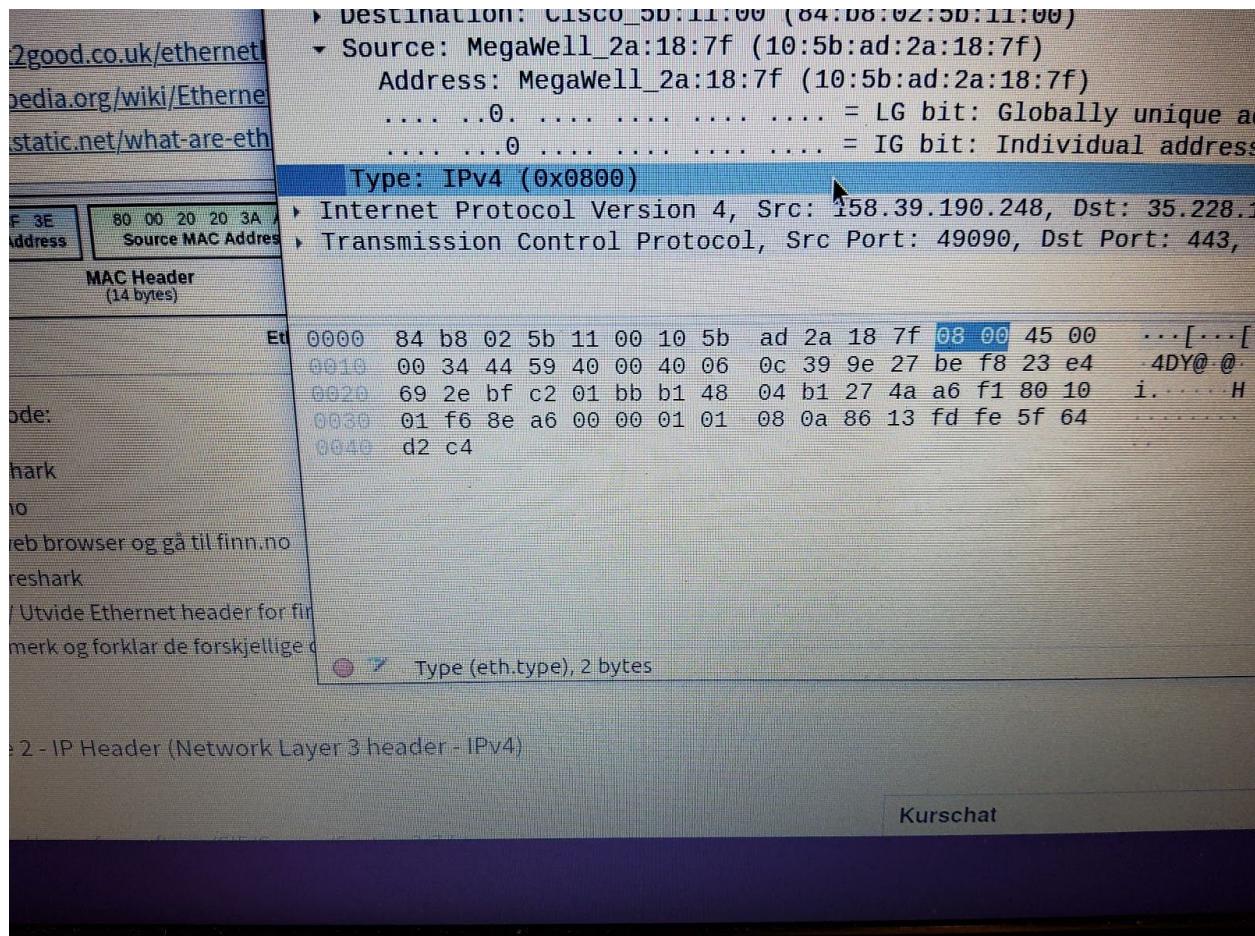
Et	0000	84 b8 02 5b 11 00	10 5b ad 2a 18 7f	08 00 45 00	...[.
0010	00 34 44 59 40 00	40 06	0c 39 9e 27	be f8 23 e4	4DY@
0020	69 2e bf c2 01 bb	b1 48	04 b1 27	4a a6 f1 80 10	i....
0030	01 f6 8e a6 00 00	01 01	08 0a 86 13	fd fe 5f 64
0040	d2 c4				

A tooltip indicates: **Source or Destination Hardware Address (eth.addr), 6 bytes**.

The status bar at the bottom shows: **Frame 2 - IP Header (Network Layer 3 header - IPv4)** and **Kurschat**.

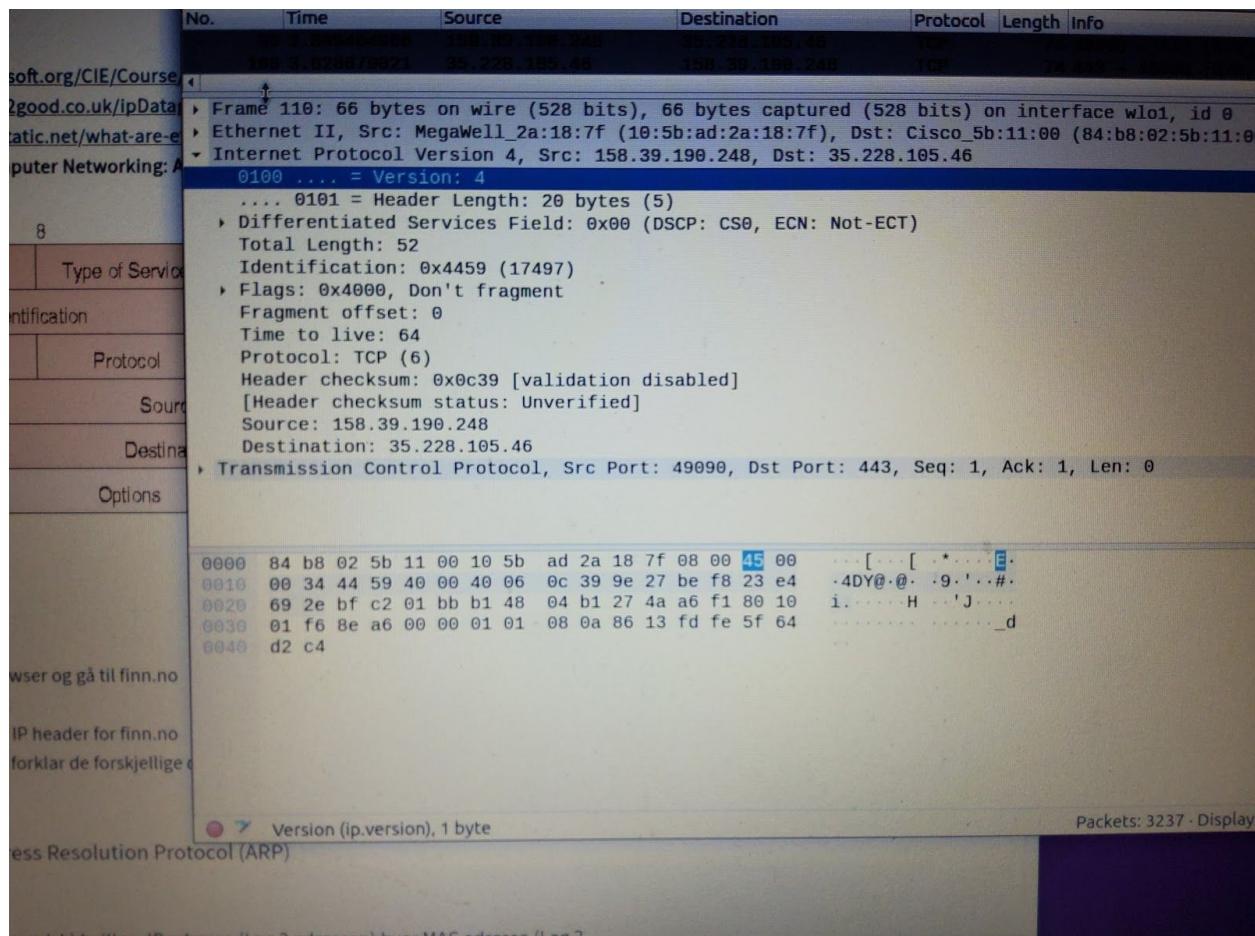
Neste del er mac-adressen til senderen av datapakken som i dette tilfelle er 10:5b:ad:2a:18:7f. Denne delen utgjør den andre delen i MAC headeren i ethernet framen.

EitherType:



Den tredje og siste delen av MAC headeren i ethernet framten forteller hvilken type data det er som kommer. I dette tilfellet så kan vi se at denne pakken har typen data av IPv4.

Oppgave 2:



Version:

Dette feltet indikerer format til internett headeren. I dette tilfellet så er det version 4.

IHL (Internet Header Length):

IHL er lengden på headeren i 32 bit ord, samtidig som den også peker ut på begynnelsen av dataen. En IHL kan ikke være mindre enn 5. Altså <5

Type of Service (ToS)

I denne delen så blir det indikert hva slags prioritet/service det er på dataen. Type tjeneste gir indikasjon på parametre for ønsket kvalitet på tjenesten. Disse parameterne skal brukes til å styre valget av de faktiske tjeneste-parametrene når du overfører et datagram gjennom et bestemt nettverk.

I våres datapaket så ligger parametrene i Default (0). Dette vil si at datapakkene blir mottatt i den rekkefølgen den kommer. De med høyere prioritet vil bli behandlet før denne og de med lavere prioritet vil havne etter pakken.

Total Length:

Total Length i IP-headeren står for totale lengden av hele datagrammet, målt i oktet. Dette inkluderer internet-headeren og dataen. I pakken som vi analyserer så finner vi at den består av 52 oktatter.

Identification:

En tildelt verdig som er satt av senderen for å hjelpe til i sammensetning av fragmentene til et datagram. I denne pakken som blir analysert så er identifikasjon: 0x4459 (17497).

Flags:

Forskjellige flag for å kontrollere ting. I vår pakket så er det 0x4000, Dont fragment. Det vil si at denne pakken ikke er fragmenten av et helt datagram.

Fragment Offset:

Dette feltet indikerer hvor i datagrammet denne fragmenten tilhører. Fragment offsettene er målt i 8 oktetts(64 bit). Første fragment har offsetten 0. Dette er den samme som er i vår datapakket. Noe som er forståelig ettersom at i forrige del (Flags) så ser vi at denne pakken ikke er et fragment av et datagram. Altså 0.

Time to Live (ToT)

Dette feltet indikerer levetiden til et datagram og hvor lenge den har lov til å forbli på nettverket før den blir sendt tilbake. Om dette feltet har verdien 0 så skal datagrammet ikke bli sendt videre, men bli sendt tilbake med info om hvor det stoppet. Tallet i dette feltet tilsier antall sekunder. Vår pakke er på 64 sekunder.

Protocol:

Denne delen indikerer protokollen brukt i det neste laget i data delen av datagrammet. Verdiene til de forskjellige protokollene er spesifisert i "Assigned Numbers". Vår pakke i dette tilfelle har: TCP (6)

Header Checksum:

Denne sjekker summen av headeren bare. Dette er på grunn av at noen deler i headeren endrer på seg. Eksempelvis: Time To Live). Dette blir sjekket og verifisert på hvert punkt av internettet hvor headeren blir prosessert. Vår checksum:0x0c39 (validation disabled)

Source Address:

Adressen til kilden: 32 bits. Vår pakke: 158.39.190.248

Destination Address:

Adressen til destinasjonen: 32 bits. Vår pakke: 35.228.105.46

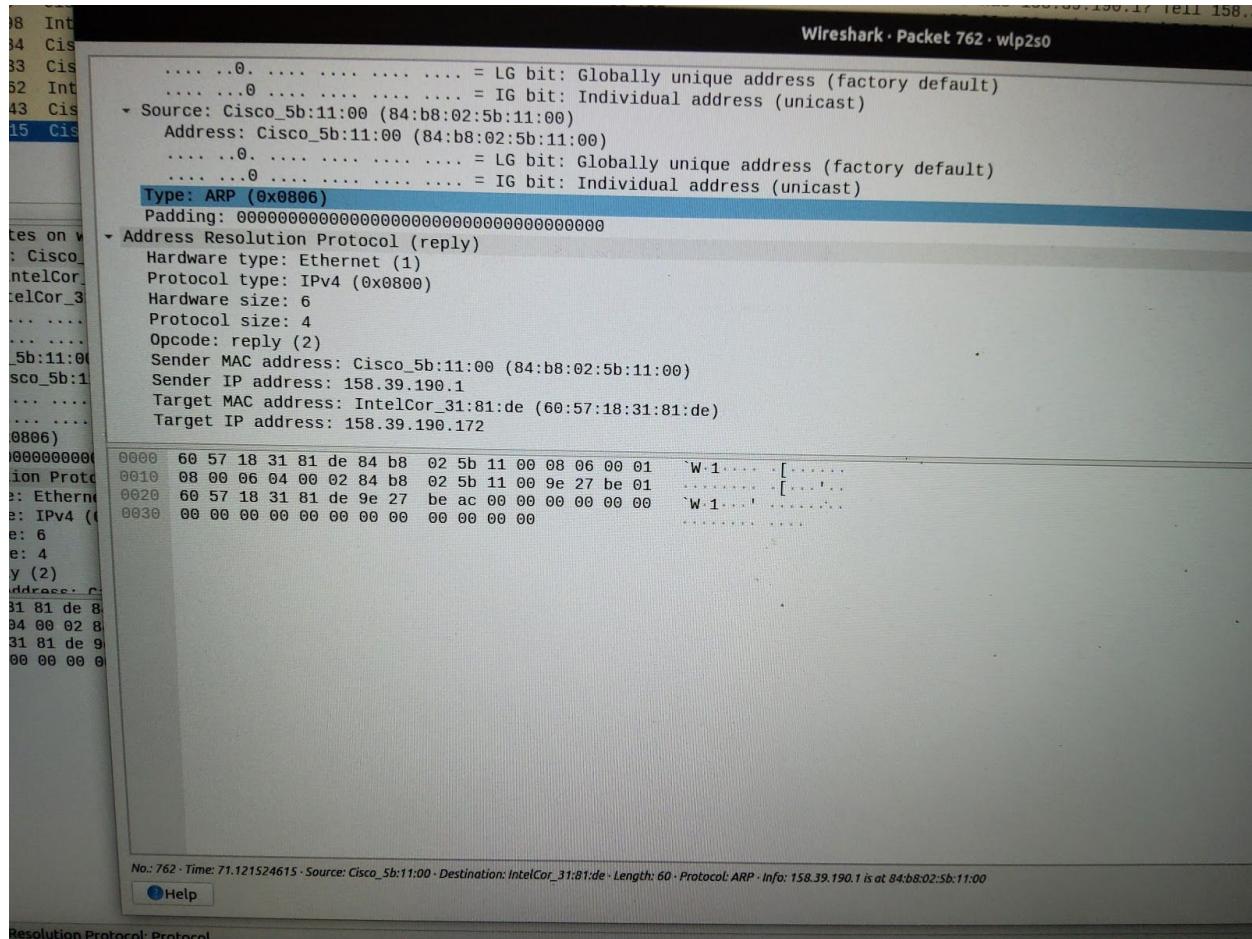
Option variable:

Option variable er en del som kan være med i et datagram, men må nødvendigvis ikke være med. De må være implementert av all IP moduler(hosten og gatewayen), Det som er valgfritt er øverføringen i hvilket som helst datagram, men ikke implementeringen.

Padding:

Paddingen er brukt til å forsikre at internet headeren slutter på en 32 bit grense. Paddingen er 0.

Oppgave 3:



Hardware Type: Denne informerer om hvilken hardware som er brukt lokal nettverksoverføringer.

Protocol Type: Dette feltet komplimenterer "Hardware Type" feltet. Den spesifiserer typen av 3. lag adresser brukt i pakken. F. eks IPv4 adresser bruker 2048(0800 i hex) som er i korrespond med EtherType koden for Internett Protokoll

Hardware Address Length (HAL): Spesifiserer lengden på hardware adresser i denne meldingen. Til Ethernet og andre nettverk som bruker IEEE 802MAC adresser så er verdien 6.

Protocol Adress Length: Igjen et field som komplimenterer den forrige. Denne spesifiserer hvor lang hvor lang tredje lags protokoll adresser er i pakken. Til IPv4 adresser så er denne verdien 4.

Opcode(OP): Dette feltet spesifiserer typen ARP melding som blir sendt. De to første type verdiene(1 og 2) blir brukt til ARP request og ARP reply som.

Sender hardware Address (SHA): Dett er hardware adressen til enheten som sender meldingen. I en IP datagram så er dette source device på en request og/eller "destination reply" i en reply.

Sender Protocol Address(SPA): IP adressen til enheten som sender pakken

Target Hardware Protocol(THA): Hardware adressen(2. lage) til enheten som pakken blir sendt til. I et IP datagram så ville dette være "source device" om det er en request og "destination" om det er en reply.

Target Protocol Address: IP adressen til enheten som denne pakken blir sendt til.

Oppgave 4:

DHCP (Dynamic Host Configuration Protocol) er en kommunikasjonsprotokoll som brukes med hjelp av en DHCP-server til å tildele IP-adresser og andre nettverks parametre til tilkoblede enheter(PC'er,

mobilier, printere, sikkerhetssystemer, etc). Fordelen med DHCP er at man slipper å sette opp manuelle IP-adresser når man skifter fra ett nettverk til et annet et. Selvet DHCP er delt opp i fire

hovedpunkter, disse er: DHCP Discovery, DHCP Offers, DHCP Request og DHCP Acknowledgement.

DHCP Discovery:

Når man kobler en enhet til et nettverk med en aktivert DHCP så vil den sende ut en kringkasting i form av en UDP(Datagram) pakke som holder en DHCPDISCOVER melding. Dette kan kalles en forespørsel av enheten til DHCP-serveren. Om enheten ikke mottar så vil den tilordne seg selv en egen adresse i form av APIPA(Automatic Private Ipv4 address). Man skal være oppmerksom at dette avhenger av enhet til enhet ettersom at det er som oftest «bakt inn» i operativsystemet. Eks:

Windows. Selv APIPA adressen vil være mellom 169.254.0.1-169.254.255.254 med subnet maske på 255.255.0.0.

Videre i DHCP Discover pakken så finner vi også en liste med forespørsel av flere typer informasjon. Som blant annet, subnet masken, router, domene navn, osv...

DHCP Offers:

Etter første del av DHCP har blitt gjennomført så vil enheten motta et «lease-tilbud» fra DHCP-serveren. I denne «avtalen» så ligger det hvor lenge klienten kommer kan bruke IP-informasjonen den blir tildelt. Infoen den får tildelt er: IP-adresse, nettverksmaske, adressen til DHCP serveren og klientens MAC-adresse.

The screenshot shows a network traffic capture in Wireshark. A single DHCP Offer message is selected. The message details are as follows:

- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
 - Length: 1
 - DHCP: Offer (2)
- Option: (1) Subnet Mask (255.255.254.0)
 - Length: 4
 - Subnet Mask: 255.255.254.0
- Option: (58) Renewal Time Value
 - Length: 4
 - Renewal Time Value: (600s) 10 minutes
- Option: (59) Rebinding Time Value
 - Length: 4
 - Rebinding Time Value: (1050s) 17 minutes, 30 seconds
- Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (1200s) 20 minutes
- Option: (54) DHCP Server Identifier (1.1.1.1)
 - Length: 4
 - DHCP Server Identifier: 1.1.1.1
- Option: (3) Router
 - Length: 4
 - Router: 158.39.190.1
- Option: (15) Domain Name
 - Length: 6 bytes
 - Domain Name: c Sc5 : X; .6 hiof. no] <

The raw hex dump of the message shows the following structure:

Hex	Dec	Text
0000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0110	00 00 00 00 00 63 82 53 63 35 01 02 01 04 ff	c Sc5
0120	ff fe 00 3a 04 00 00 02 58 3b 04 00 00 04 1a 33	: X; .6
0130	04 00 00 04 b0 36 04 01 01 01 01 03 04 9e 27 be	hiof. no
0140	01 0f 08 68 69 6f 66 2e 6e 6f 00 06 10 9e 27 a8	
0150	21 9e 27 a8 20 9e 27 b0 5d 9e 27 b0 3c ff 00 00	! ' '] ' <
0160	00 00	

Detailed description: The screenshot shows a network traffic capture in Wireshark. A single DHCP Offer message is selected. The message details are as follows:

- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
 - Length: 1
 - DHCP: Offer (2)
- Option: (1) Subnet Mask (255.255.254.0)
 - Length: 4
 - Subnet Mask: 255.255.254.0
- Option: (58) Renewal Time Value
 - Length: 4
 - Renewal Time Value: (600s) 10 minutes
- Option: (59) Rebinding Time Value
 - Length: 4
 - Rebinding Time Value: (1050s) 17 minutes, 30 seconds
- Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (1200s) 20 minutes
- Option: (54) DHCP Server Identifier (1.1.1.1)
 - Length: 4
 - DHCP Server Identifier: 1.1.1.1
- Option: (3) Router
 - Length: 4
 - Router: 158.39.190.1
- Option: (15) Domain Name
 - Length: 6 bytes
 - Domain Name: c Sc5 : X; .6 hiof. no] <

The raw hex dump of the message shows the following structure:

Hex	Dec	Text
0000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0110	00 00 00 00 00 63 82 53 63 35 01 02 01 04 ff	c Sc5
0120	ff fe 00 3a 04 00 00 02 58 3b 04 00 00 04 1a 33	: X; .6
0130	04 00 00 04 b0 36 04 01 01 01 01 03 04 9e 27 be	hiof. no
0140	01 0f 08 68 69 6f 66 2e 6e 6f 00 06 10 9e 27 a8	
0150	21 9e 27 a8 20 9e 27 b0 5d 9e 27 b0 3c ff 00 00	! ' '] ' <
0160	00 00	

For eksempel i vår DHCP Offer pakke så ser vi de forskjellige vilkårene i den tilbyddet "leieavtalen" fra DHCP-serveren. Blant annet Subnet mask (255.255.254.0), ruteradressen (158.39.190.1), osv.

DHCP Requests:

I denne delen så vil enheten(klienten) fortelle DHCP-serveren om den har godtatt eller ikke godtatt «kontrakten/avtalen» fra serveren. Om klienten skulle sende melding til serveren at den aksepterer avtalen så vil DHCP-serveren kringkaste bli gitt ut av serveren til andre DHCP-servere at den nylig koblete klienten skal ikke bli tildelt andre «tilbud».

Wireshark · Packet 3400 · wlo1

```
Relay agent IP address: 0.0.0.0
Client MAC address: MegaWell_2a:18:7f (10:5b:ad:2a:18:7f)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
- Option: (53) DHCP Message Type (Request)
  Length: 1
  DHCP: Request (3)
- Option: (54) DHCP Server Identifier (1.1.1.1)
  Length: 4
  DHCP Server Identifier: 1.1.1.1
- Option: (50) Requested IP Address (158.39.190.248)
  Length: 4
  Requested IP Address: 158.39.190.248
- Option: (12) Host Name
  Length: 8
  Host Name: heljarp
- Option: (55) Parameter Request List
  Length: 13
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (28) Broadcast Address
  Parameter Request List Item: (2) Time Offset
  Parameter Request List Item: (3) Router
  Parameter Request List Item: (15) Domain Name
  Parameter Request List Item: (6) Domain Name Server
  Parameter Request List Item: (119) Domain Search
  Parameter Request List Item: (12) Host Name
  Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
  Parameter Request List Item: (47) NetPTOS over TCP/IP Secopt
```

DHCP Acknowledgement:

Dene siste delen består av at det annerkjennes avtalen mellom klient og DHCP-server. I denne fasen så blir den avtalte informasjonen tildelt av serveren til klienten. Denne blir sendt i form av en DHCPACK pakke til klienten hvor den inneholder konfigurasjonsinformasjonen klienten har sendt forespørsel om.

Hops: 0
Transaction ID: 0xb611c35f
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
0... = Broadcast flag: Unicast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 158.39.190.248
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: MegaWell_2a:18:7f (10:5b:ad:2a:18:7f)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Length: 1
DHCP: ACK (5)
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (600s) 10 minutes
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (1050s) 17 minutes, 30 seconds
0010 01 54 00 00 00 00 ff 11 5b 77 01 01 01 01 9e 27 .T..... [W....
0020 be f8 00 43 00 44 01 40 be 4a 02 01 06 00 b6 11 .. C D @ J ,
0030 c3 5f 00 00 00 00 00 00 00 00 9e 27 be f8 00 00 [*
0040 00 00 00 00 00 00 10 5b ad 2a 18 7f 00 00 00 00
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
Header checksum (ip.checksum), 2 bytes

Her kan du se at IP-adressen 158.39.190.248 har blitt gitt til klienten og at dette har blitt delt med nettverket med Unicast.

Spørsmål a:

DHCP bruker UDP protokollen. Dette kan man se i pakkene under "Protocol:" i Wireshark

Spørsmål b:

DHCP serveren bruker port 67

Spørsmål c:

DHCP klient bruker port 68 vanligvis, men kan bruke hvilken som helst UDP port.

Oppgave 5:

HTTP Request:

The screenshot shows a NetworkMiner capture of an HTTP POST request. The request details are as follows:

- [Expert Info (Chat/Sequence): POST / HTTP/1.1\r\n]
- [POST / HTTP/1.1\r\n]
- [Severity level: Chat]
- [Group: Sequence]
- Request Method: POST**
- Request URI: /
- Request Version: HTTP/1.1
- Host: ocsp.digicert.com\r\n
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
- Accept: */*\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Content-Type: application/ocsp-request\r\n
- Content-Length: 83\r\n

The raw hex dump of the request body shows the OCSP request message. The dump starts with:

```
00 84 b8 02 5b 11 00 10 5b ad 2a 18 7f 08 00 45 00 ... [ * . E
01 01 af fa a6 40 00 40 06 a7 ac 9e 27 be f8 5d b8 ... @ @ ' ]
02 dc 1d b6 a2 00 50 e6 ff 77 d0 ce 08 3c 31 80 18 ... P w <1 ...
03 01 f5 5c b3 00 00 01 01 08 0a 16 64 af 37 5f 45 \ ..... d 7_E
04 49 39 50 4f 53 54 20 2f 20 48 54 54 50 2f 31 2e I9POST / HTTP/1.
05 31 0d 0a 48 6f 73 74 3a 20 6f 63 73 70 2e 64 69 1 Host: ocsp.di
06 67 69 63 65 72 74 2e 63 6f 6d 0d 0a 55 73 65 72 gicert.c om User
07 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
08 35 2e 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 5.0 (X11 ; Ubuntu
09 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 ; Linux x86_64;
0a 72 76 3a 38 30 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:80.0) Gecko/2
0b 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
0c 38 30 2e 30 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 80.0 Ac cept: */
0d 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 * Accep t-Langua
0e 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 ge: en-U S,en;q=0
0f 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 .5 Acce pt-Encod
```

No.: 18608 · Time: 154.132523101 · Source: 158.39.190.248 · Destination: 93.184.220.29 · Protocol: OCSP · Length: 445 · Info: Request

User-agent: Informasjon om nettleser og system software klienten bruker.

Accept language: Hvilket språk innholdet er på

Accept-Encoding: Compression algoritmer som klienten kan bruke.

Connection: Vilkår/parametere på f. eks hvor lenge klienten kan være på denne siden eller hvor mange requests som kan bli sendt til serveren.

HTTP Respons:

Wireshark - Packet 18609 · wlo1

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Accept-Ranges: bytes\r\n

Age: 2302\r\n

Cache-Control: max-age=150343\r\n

Content-Type: application/ocsp-response\r\n

Date: Fri, 18 Sep 2020 19:13:40 GMT\r\n

Etag: "5f64a62d-13a"\r\n

Expires: Sun, 20 Sep 2020 12:59:23 GMT\r\n

Last-Modified: Fri, 18 Sep 2020 12:21:01 GMT\r\n

Server: FCS (sts/DB4D)\r\n

Hex	Dec	Text
0010	02 b6 31 cd 00 00 38 06	b7 7f 5d b8 dc 1d 9e 27
0020	be f8 00 50 b6 a2 ce 08	3c 31 e6 ff 79 4b 80 18
0030	00 8d 88 b0 00 00 01 01	08 0a 5f 45 4c d1 16 64
0040	af 37 48 54 54 50 2f 31	2e 31 20 32 30 30 20 4f
0050	4b 0d 0a 41 63 63 65 70	74 2d 52 61 6e 67 65 73
0060	3a 20 62 79 74 65 73 0d	0a 41 67 65 3a 20 32 33
0070	30 32 0d 0a 43 61 63 68	65 2d 43 6f 6e 74 72 6f
0080	6c 3a 20 6d 61 78 2d 61	67 65 3d 31 35 30 33 34
0090	33 0d 0a 43 6f 6e 74 65	6e 74 2d 54 79 70 65 3a
00a0	20 61 70 70 6c 69 63 61	74 69 6f 6e 2f 6f 63 73
00b0	70 2d 72 65 73 70 6f 6e	73 65 0d 0a 44 61 74 65
00c0	3a 20 46 72 69 2c 20 31	38 20 53 65 70 20 32 30
00d0	32 30 20 31 39 3a 31 33	3a 34 30 20 47 4d 54 0d
00e0	0a 45 74 61 67 3a 20 22	35 66 36 34 61 36 32 64
00f0	2d 31 33 61 22 0d 0a 45	78 70 69 72 65 73 3a 20
0100	53 75 6e 2c 20 32 30 20	53 65 70 20 32 30 32 30

Help

Respons versjon: Forteller versjonen av HTTP

Status Code: Forteller statusen webserveren

Response Phrase: Et ord som sier hvordan statusen er.