

## Лабораторийн ажил №2

### HTTP, HTTPS протоколууд

МТЭС, МКУТ, Компьютерийн ухаан  
Б.Барсболд, 22B1NUM4397

#### Ажлын зорилго

Энэхүү лабораторийн ажлаар TCP/IP сүлжээний хэрэглээний давхаргын протоколууд болох HTTP, HTTPS протоколууд, түүний ажиллагааны зарчмын талаар судална.

#### Үндсэн ойлголт

HTTP (Hypertext Transfer Protocol) протокол нь вэб сервер болон вэб хөтөч хооронд вэбийн өгөгдөл болох HTML файлуудыг дамжуулахад ашиглагддаг. Харин HTTPS (HTTP over TLS эсвэл HTTP over SSL) нь вэб сервер болон вэб хөтөч хооронд дамжуулж буй өгөгдлийг шифрлэж аюулгүй байдлыг хангадаг протокол юм.

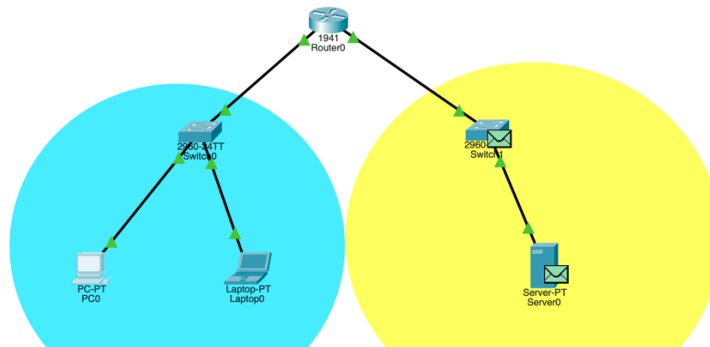
HTTP нь анх 1.1 гэсэн хувилбартай гарч байсан бөгөөд дараа нь HTTP/2 болон HTTP/3 гэсэн хувилбарууд гарсан. HTTP нь хүсэлт-хариу (request-response) гэсэн Client-Server архитектурт ашигладаг протокол юм. Клиент нь HTTP GET хүсэлтийг HTTP сервер рүү илгээдэг бол хүсэлт ирсний дараа HTTP сервер нь хүсэлтийн дагуу HTTP response илгээдэг. Ингэхдээ харгалзан TCP/IP протоколын дагуу хүсэлт болон хариултаа илгээнэ. **TCP 80 портыг** ашигладаг. HTTP нь client төхөөрөмжийн вэб хөтөч болон вэб сервер хоорондын өгөгдөл солилцоход **GET, POST, PUT** мессежүүдийг ашиглана. HTTPS нь HTTP-ийн аюулгүй байдлыг сайжруулж гарч ирсэн хувилбар юм. Баталгаажуулалтыг доод түвшний хөрвүүлэлт хийдэг. **TCP 443 порт** ашигладаг. HTTPS нь HTTP (Hyper Text Transferring Protocol)-г TLS (**Transfer Layer Security**), SSL (**Secure Socket Layer**)-р шифрлэдэг. HTTPS-ийн гол зорилго нь зочилсон вэб хуудас болгон солилцсон мэдээллийн нууцлал, аюулгүй байдал, бүрэн бүтэн байдлыг хадгалах юм. Интернетэд өөрийн байршлаараа, вэб сайт болон холбогдох вэб серверт хэн холбогдож буйг таних ба Man-in-the-middle халдлагаас хамгаалдаг. Үүнээс гадна клиент болон сервер хоёрын хооронд eavesdrop халдлага болон харилцааны агуулгыг хуурамчаар үйлдэх зэргээс хамгаалж, холболтын нууц шифрлэлт үүсгэдэг. HTTP протоколтой холбоотой зайлшгүй хоёр зүйл нь URL болон DNS юм.

- URL (Uniform Resource Locator)- IP хаяг болох 32 биттэй тоон цувааг хэрэглэгчдэд тогтоох болон хэрэглэхэд хялбар байх үүднээс URL-г ашигладаг.
- DNS (Domain Name System)- Web site-н IP хаягийг domain name хэлбэрт шилжүүлснээр хэрэглэгчийн web хандалтыг хялбаршуулна.

#### Туршилт

Cisco Packet tracer програмыг нээж дараах топологийг байгуулаарай.

1. Веб сервер, 2 компьютер, 2960 свич, 1941 рүтэр ашиглан сүлжээний туршилтын топологийг байгуулж, төхөөрөмжүүдийг хаяглана.



Зураг 1 Туршилтийн тоглогийг Cisco Packet Tracer програм дээр байгуулсан зураг

## 2. Байгуулсан тоглогийн дагуу төхөөрөмжүүдийг дараах хаягаар хаяглана.

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0

Зураг 2 PC0-ийн FastEthernet0 интерфэйсийн тохиргоо

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0

Зураг 3 Laptop0-ийн FastEthernet0 интерфэйсийн тохиргоо

IP Configuration		IP Configuration	
IPv4 Address	192.168.1.1	IPv4 Address	100.100.150.1
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.240

Зураг 4 Router0-ийн GigabitEthernet0/0 GigabitEthernet0/1 интерфэйсүүдийн тохиргоонууд

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	100.100.150.3
Subnet Mask	255.255.255.240

Зураг 5 Server0-ийн FastEthernet0 интерфэйсийн тохиргоо

## Даалгавар



Зураг 6 PC0-ээс Server0 рүү http протокол ашиглан хандсан байдал

Event List		
Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC0
	0.001	--
	0.002	PC0
	0.002	Switch0
	0.003	Switch0
	0.003	Router0
	0.004	Router0
	0.004	Switch1
	0.005	Switch1
	0.005	Server0
	0.006	Server0
	0.006	Switch1
	0.007	Switch1
	0.007	Router0
	0.008	Router0
	0.008	Switch0
Visible	0.009	Switch0

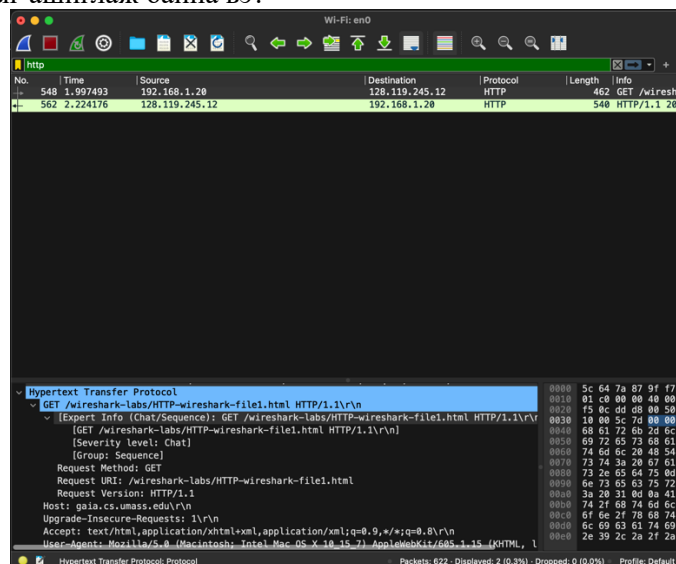
Зураг 7 Simulation горимд холболтыг шалгахад гарсан үр дүн

## Сорих асуулт

### Туриилт 1.

Wireshark програм ажлуулж, холбогдох интерфэйсийн сүлжээний урсгалыг барьж эхлээрэй. Вэб хөтөчийг нээж <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> хаяг руу хандаж энгийн html хуудсыг дуудах ба Wireshark програмыг зогсооно. Хоёр HTTP мессэжийг барих бөгөөд дараах асуултад хариулаарай.

1. Вэб хөтөч HTTP 1.0 эсвэл HTTP 1.1 аль хувилбар дээр ажиллаж байна вэ? Сервер талд HTTP-ийн аль хувилбарыг ашиглаж байна вэ?



Зураг 8 WireShark програмаар gaia.cs.umass.edu website-руу хандсан байдал

Дээрх үр дүнгээс хархад веб хөтөч (Safari 17.2.1) HTTP 1.1 ашиглаж байна. Харин серверээс ирсэн хариунд сервер HTTP 1.1 ашиглаж байна гэж байна. Серверээс ирсэн хариуг доор оруулав.

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Wed, 28 Feb 2024 13:47:33 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 28 Feb 2024 06:59:01 GMT\r\n
    ETag: "80-6126bad80f831"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
  [HTTP response 1/1]
  [Time since request: 0.226683000 seconds]
  [Request in frame: 548]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes

```

Зураг 9 Сервер талаас ирсэн response үр дүн

2. Өөрийн компьютер болон серверийн IP хаяг ямар байна вэ?

Дээрх үр дүнд серверийн IP хаяг 128.119.245.12 харин миний компьютерийн IP хаяг 192.168.1.20 байна.

3. Серверээс ирж байгаа хуудасны төлөвийн код (status code) ямар байна вэ? Бусад төлөвийн кодыг бие дааж судалж, тайланд оруулна уу.

Дээрх үр дүнгээс харвал серверээс 200 ОК гэсэн status code ирж байна.

4. Серверээс ирж байгаа хуудас сервер дээр хамгийн сүүлд хэзээ өөрчлөлт орсон байна вэ?

Дээрх үр дүнгийн Last-Modified field дээр 2024-02-28 гэсэн байна.

5. Вэб хөтөч рүү хэдэн байтын өгөгдөл ирсэн бэ?

128 байт өгөгдөл веб хөтөч рүү ирсэн.

6. Пакетыг хоёрт эсвэл 16-аар харах боломжтой цонхонд харуулж байгаа түүхий өгөгдлийг (raw data) сайтар ажиглаж, уг өгөгдөл дотор пакетын жагсаалтын цонхонд харагдаагүй толгой (headers) хэсэг байгааг ажиглаж, тайланд тусгаж оруулна уу.

```

0000 c8 89 f3 bc d4 1b 5c 64 7a 87 9f f7 08 00 45 00 ..... \d z ..... E
0010 02 0e 66 6f 40 00 27 06 b4 3a 80 77 f5 0c c0 a8 ...fo@'...'w...
0020 01 14 00 50 dd d8 a1 ee a4 29 ba 96 40 eb 50 18 ...P.....)@P
0030 00 ed d5 3f 00 00 48 54 54 50 2f 31 2e 31 20 32 ...?..HT P/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK..D ate: Wed
0050 2c 20 32 38 20 46 65 62 20 32 30 32 34 20 31 33 , 28 Feb 2024 13
0060 3a 34 37 3a 33 33 20 47 4d 54 0d 0a 53 65 72 76 :47:33 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 P/7.4.33 mod_per
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 57 65 64 2c 20 32 38 20 46 65 fied: We d, 28 Fe
00e0 62 20 32 30 32 34 20 30 36 3a 35 39 3a 30 31 20 b 2024 0 6:59:01
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT..ETa g: "80-6
0100 31 32 36 62 61 64 38 30 66 38 33 31 22 0d 0a 41 126bad80 f831"...A
0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes..Con tent-Len
0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 ..Keep-A
0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 ..Connec
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 ..Conten t-Type:
0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; chars
0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8 ....<htm
01a0 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l>..Congr atulatio
01b0 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down
01c0 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 loaded t he file
01d0 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e .http:// gaia.cs.
01e0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 umass.ed u/wiresh
01f0 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 ark-labs /HTTP-wi
0200 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 reshark- file1.ht
0210 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a ml!</ht ml>

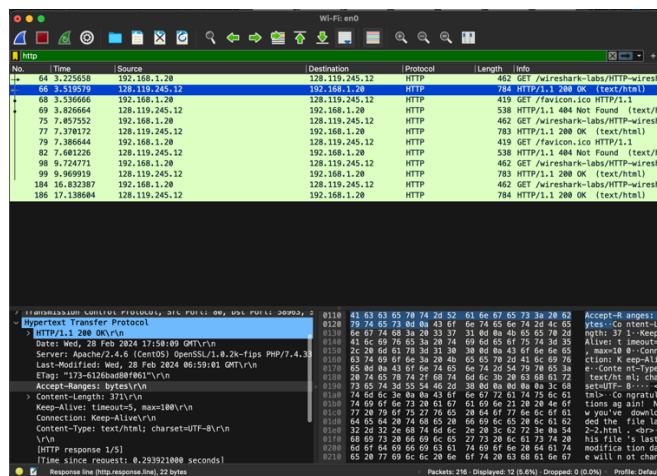
```

Зураг 10 Хариу өгөгдлийн 16-тын тоолол дахь хэлбэр

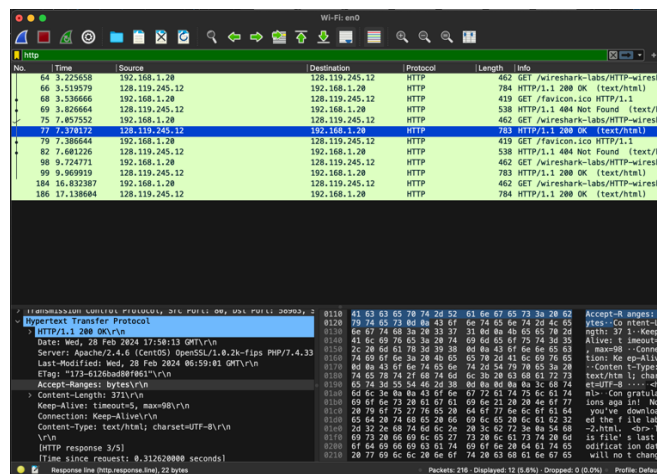
Дээрх өгөгдлөөс харвал header хэсгийн field бүр 0a0d гэсэн 16-ыг өгөгдлөөр харин header body хоёр 2 0a0d гэсэн өгөгдлөөр тусгаарлагдаж байна. 16-ын 2 орон нь 8-бит өгөгдлийг илэрхийлдэг тул бүгдийг 2 оронгоор нь салган харуулж байна. Мөн 0a өгөгдөл нь ASCII стандартад NL (new line) character харин 0d нь CR (carriage return) character байна.

## Туршилт 2.

Эхлээд туршилт хийхээс өмнө веб хөтөчийн кэшийг цэвэрлэх шаардлагатай. Wireshark програм ажлуулж, холбогдох интерфэйсийн сүлжээний урсгалыг барьж эхлээрэй. Веб хөтөчийг нээж <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> хандаж хуудсыг дуудах ба дахин F5 товчийг дарж уг хуудсыг дахин дуудаарай. Wireshark програмыг зогсоож, шүүлтүүр талбарт “http” утгыг оруулах бөгөөд дараах асуултад хариулна уу.



Зураг 11 Өгөгдсөн веб рүү cache-ээ устгаж байгаад хандаж үзсэн байдал



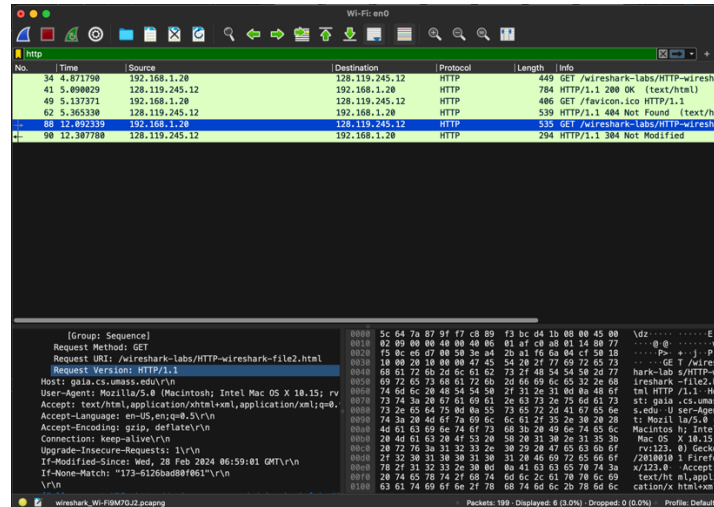
Зураг 12 Дахин ачаалсан байдал

1. Эхний HTTP GET хүсэлт мессэжийн агуулгыг ажиглан, “IF-MODIFIED-SINCE” мөр байна уу?

Байхгүй байна.

2. F5 дарах үеийн HTTP GET хүсэлтийн агуулгыг ажиглаж, “IF-MODIFIED-SINCE” талбар байна уу, байвал ямар утга илэрхийлж байгааг тайлбарлана уу.

Дээрх үр дүнд байхгүй байсан бөгөөд веб хөтөчөө солин Mozilla Firefox-р хүсэлт явуулж үзсэнийг доор оруулав.



Зураг 13 Дээрх туршилтыг Mozilla Firefox веб хөтөчөөр туршсан үр дүн

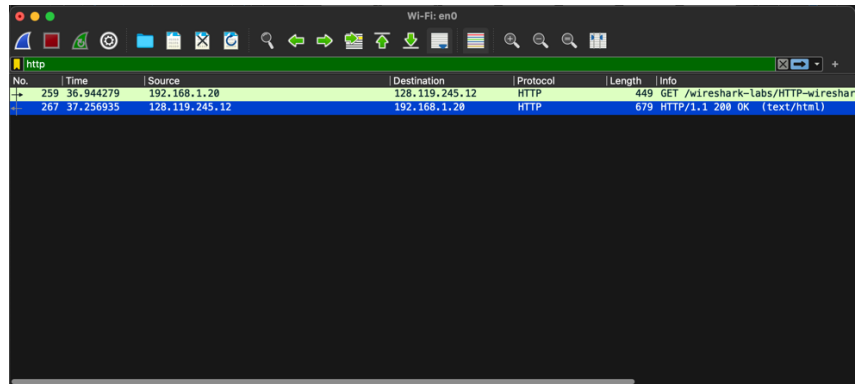
Дээрх үр дүнд “IF-MODIFIED-SINCE” талбар нэмэгдсэн байсан бөгөөд энэ нь эхлээд сервер хүсэлтэд амжилттай буюу 200 кодтой хариу өгөн дахин хүсэлт явуулхад дээрх толгойн талбарыг хэрэглснээр сүүлд өөрчлөгдсөн огноо нь энэ талбарт явуулсан огноогоос өмнө байвал сервер 304 буюу NOT MODIFIED хариуг body-гүйгээр буцаана. Энэ header нь зөвхөн GET болон HEAD хүсэлтүүдэд ашиглагддаг.

3. Хоёр дах HTTP GET мессэжийн хариу мессэжид ирсэн төлөвийн код болон нэршил (status code, phrase) ямар байна вэ? Яагаад ийм байгааг тайлбарлана уу.

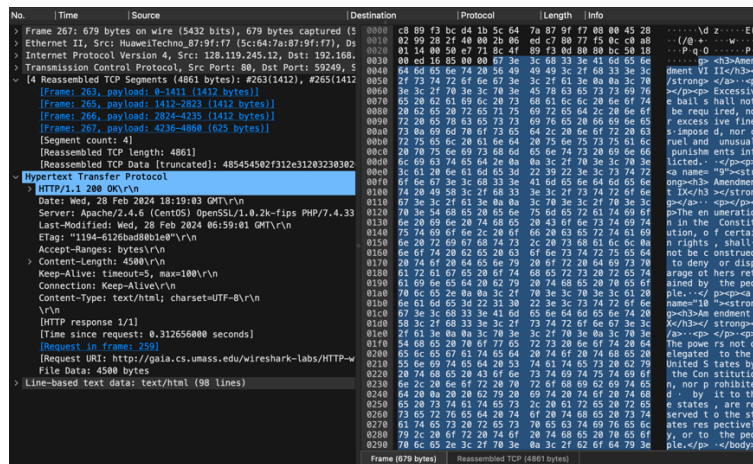
Хоёр дах хүсэлтэд GET мессэжийн хариу 304 буюу NOT MODIFIED байна. Энэ нь веб хөтөч сүүлд энэ хүсэлтийг явуулсанаас хойш өөрчлөгдөөгүй буюу өмнөх хүсэлтийн body-г ашиглаж болно гэсэн үг юм. Ингэснээр сүлжээгээр нэгэнт өөрчлөгдөөгүй том хэмжээний өгөгдлийг дамжуулхын оронд өмнө нь авсан өгөгдлөө ашиглах боломж үүсэх юм.

### Туршилт 3.

Одоо их хэмжээний өгөгдөл татаж авах тухай судална. Wireshark програмыг ажлуулж, холбогдох интерфэйсийн сүлжээний урсгалыг барьж эхлээрэй. Веб хөтөчийг нээж <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> хандаж хуудсыг дуудна. Wireshark програмыг зогсоож, шүүлтүүр талбарт “http” утгыг оруулах бөгөөд дараах асуултад хариулна уу. Энэ өгөгдөл нь 4500 байтын хэмжээтэй тул нэг TCP пакетаар дамжуулах боломжгүй. Тиймээс хэд хэдэн TCP сегментэд хуваагдаж дамжсан байгааг ажиглаж, тайланд хавсаргана уу.



Зураг 14 Туршилт 3-д өгсөн URL руу веб хөтөчөөр хүсэлт илгээн WireShark программаар барьж авсан байдал



Зураг 15 Серверээс ирсэн хариу мессэжийн дэлгэрэнгүй

1. Вэб хөтөчөөс хэдэн HTTP GET мессэж илгээгдэж байна вэ?

Дээрх үр дүнд харуулсанаар веб хөтөчөөс сервер рүү нэг HTTP GET мессэж илгээгдэж байна.

2. Хэд дэх пакетад HTTP GET мессэжийн хариутай холбоотой төлөвийн код, нэршил агуулагдаж байна вэ? Хариуд агуулагдаж байгаа төлөвийн код, нэршил ямар байна вэ?

Эхний пакетад HTTP GET мессэжийн хариутай холбоотой төлөвийн код, нэршил агуулагдаж байна. Хариуд агуулагдаж буй төлөвийн код нь 200 OK байна.

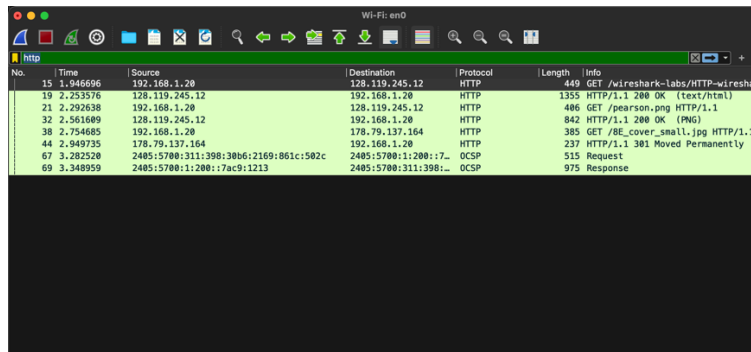
3. Нэг HTTP мессэжийг дамжуулахад хэдэн TCP сегмент ашиглаж байна вэ?

Нэг HTTP мессэжийг дамжуулахад энэ тохиолдолд үр дүнд харуулсанаар 4 TCP сегмент ашиглагдаж байна.

#### Туршилт 4.

Эмбедэд объект татаж авахад юу болох талаар судална. Эхлээд туршилт хийхээс өмнө веб хөтөчийн кэшийг цэвэрлэх шаардлагатай. Wireshark програм ажлуулж, холбогдох интерфэйсийн сүлжээний урсгалыг барьж эхлээрэй. Веб хөтөчийг нээж <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> хандаж хуудсыг дуудна. Wireshark програмыг зогсоож, шүүлтүүр талбарт “http” утгыг оруулах бөгөөд дараах асуултад хариулна уу. Уг хуудсад текст болон 2 зураг агуулагдаж байгаа.





No.	Time	Source	Destination	Protocol	Length	Info
15	1.946696	192.168.1.20	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark
19	2.253576	192.168.1.20	192.168.1.20	HTTP	1355	HTTP/1.1 200 OK (text/html)
21	2.292638	192.168.1.20	128.119.245.12	HTTP	406	GET /pearson.png HTTP/1.1
32	2.561689	128.119.245.12	192.168.1.20	HTTP	842	HTTP/1.1 200 OK (PNG)
38	2.754685	192.168.1.20	178.79.137.164	HTTP	385	GET /BE_cover_small.jpg HTTP/1.1
44	2.949735	178.79.137.164	192.168.1.20	HTTP	237	HTTP/1.1 301 Moved Permanently
67	3.282520	2405:5700:311:398:30b6:2169:861c:582c	2405:5700:1:200::7	OCSP	515	Request
69	3.348959	2405:5700:1:200::7ac9:1213	2405:5700:311:398:...	OCSP	975	Response

Зураг 16 Туршилт 4-д өгсөн URL-ийг веб хөтөчөөр ачаалуулан хүсэлтүүдийг Wireshark програмаар барьж авсан үр дүн

1. Веб хөтөчөөс хэдэн HTTP GET хүсэлт илгээгдэж байна вэ? Эдгээр GET хүсэлтүүд ямар IP хаяг руу илгээгдэж байгааг ажиглаж, тайландаа тусгаарай.

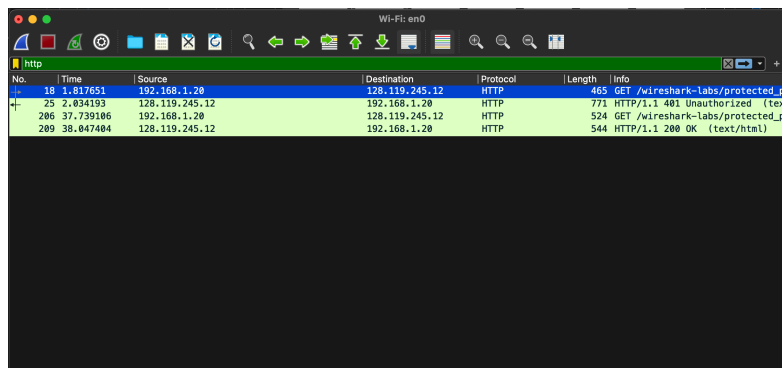
Веб хөтөчөөс гурван HTTP GET хүсэлт илгээгдэж байна.

2. Веб хөтөч хоёр зургийг татахдаа цуваа эсвэл параллелийн аль хэлбэрээр татсан бэ?

Веб хөтөч хоёр зургийг цуваа байдлаар татсан. Эхний хүсэлтийн хариу ирсний дараагаар хоёр дахь зургийг авах хүсэлт явж байна.

#### Туршилт 5.

Вэб хуудас руу хэрэглэгчийн эрхээр нэвтэрч орох үед юу болдог талаар судална. Wireshark програм ажлуулж, холбогдох интерфэйсийн сүлжээний урсгалыг барьж эхлээрэй. Веб хөтөчийг нээж [http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html) хандаж, хэрэглэгчийн нэр: “wireshark-students”, нууц үг: “network” байна. Wireshark програмыг зогсоож, шүүлтүүр талбарт “http” утгыг оруулах бөгөөд дараах асуултад хариулна уу.



No.	Time	Source	Destination	Protocol	Length	Info
18	1.817651	192.168.1.20	128.119.245.12	HTTP	465	GET /wireshark-labs/protected_pages
25	2.034193	128.119.245.12	192.168.1.20	HTTP	771	HTTP/1.1 401 Unauthorized (text/
286	37.739186	192.168.1.20	128.119.245.12	HTTP	524	GET /wireshark-labs/protected_page
289	38.047404	128.119.245.12	192.168.1.20	HTTP	544	HTTP/1.1 200 OK (text/html)

Зураг 17 Туршилт 5-ын зааварт өгсний дагуу ажилуулсан үр дүн

1. Эхний HTTP GET мессэжийн хариу мессэжийн төлөвийн код болон нэршил ямар байна вэ?

Эхний HTTP GET мессэжийн хариу мессэжийн төлөвийн код нь 401 Unauthorized байна.

2. Хоёр дах удаа HTTP GET мессэж илгээхэд, HTTP GET мессэжид ямар шинэ талбар агуулагдсан байна вэ?



Хоёр дах HTTP GET хүсэлтэд Authorization талбар шинээр үүссэн байна.

## Дүгнэлт

Энэхүү лабораторийн хүрээнд Cisco Packet Tracer програм ашиглан жижиг веб сервер болон клиентуудтай топологи үүсгэн сүлжээний тохиргоо хийн веб сервисийг тестелж үзлээ. Мөн WireShark програм ашиглан төрөл бүрийн HTTP GET хүсэлт явуулах хэрхэн серверийн cache ажилладаг, том хэмжээний өгөгдөл хэрхэн дамждаг болон эмбеддэд өгөгдлүүд хэрхэн зөөвөрлөгддөг талаар судлан туршиж үзлээ.