

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 2
З дисципліни: Комп'ютерні мережі

Протокол HTTP

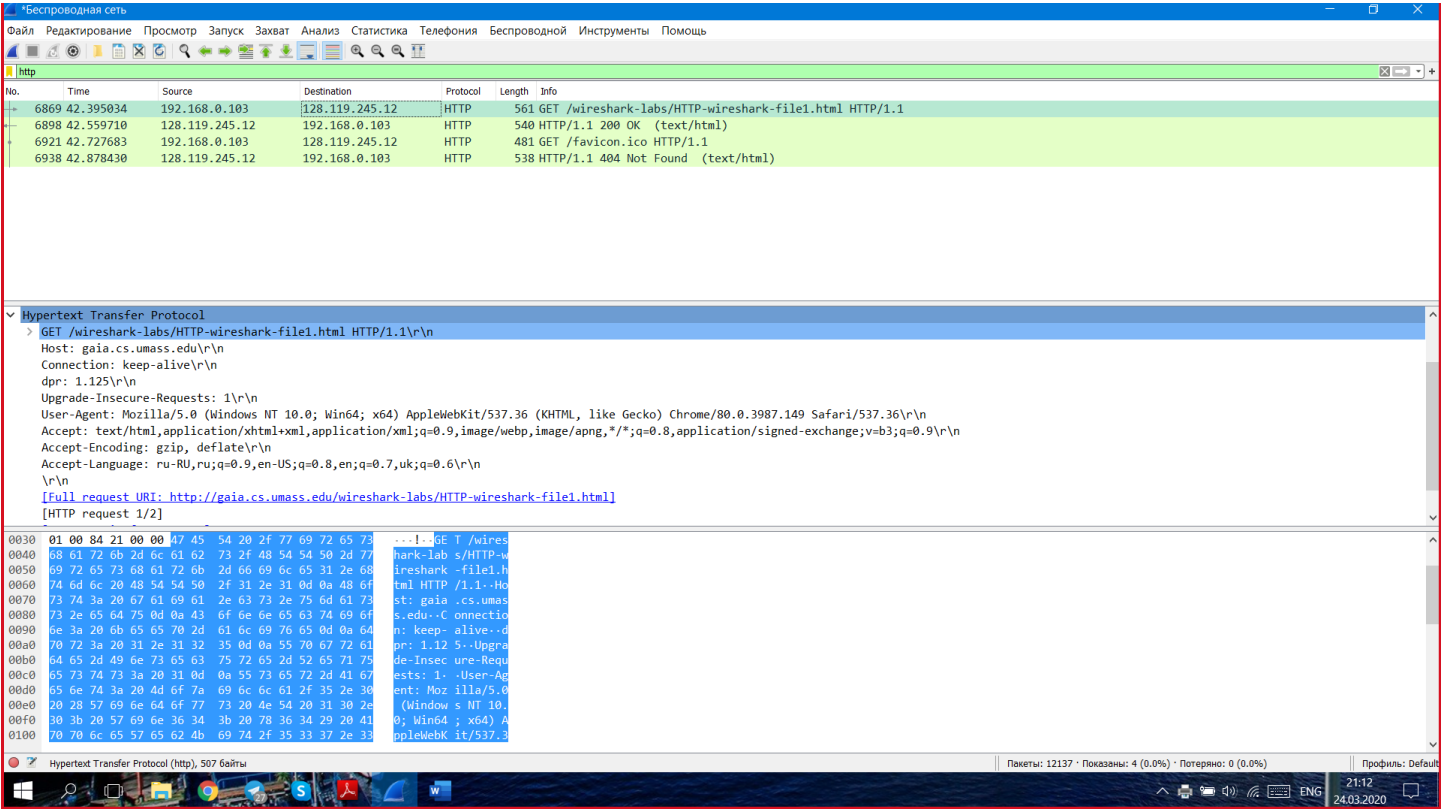
Виконав:
Студент III курсу
Групи КА-72
Третяков М.Ю.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу HTTP.

Хід виконання роботи

Перша частина



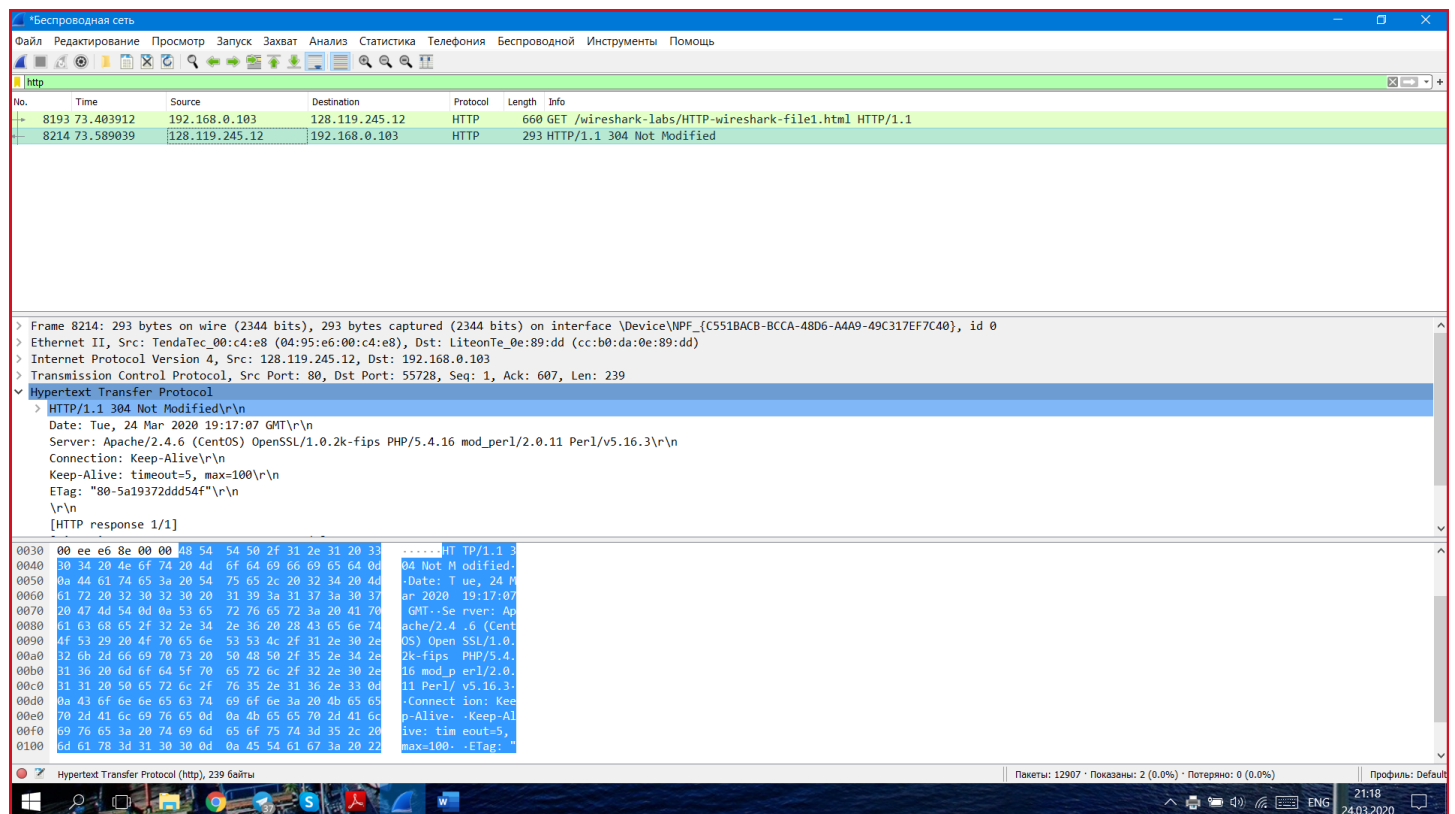
Request:

No. Time Source Destination Protocol Length Info
6869 42.395034 192.168.0.103 128.119.245.12 HTTP 561 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 6869: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55632, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
dpr: 1.125\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 6898]
[Next request in frame: 6921]

Response:

```
No.      Time      Source      Destination      Protocol Length Info
 6898 42.559710    128.119.245.12  192.168.0.103    HTTP      540      HTTP/1.1 200 OK (text/html)
Frame 6898: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103
Transmission Control Protocol, Src Port: 80, Dst Port: 55632, Seq: 1, Ack: 508, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 24 Mar 2020 19:10:16 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Tue, 24 Mar 2020 05:59:02 GMT\r\n
  ETag: "80-5a19372ddd54f"\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 1/2]
[Time since request: 0.164676000 seconds]
[Request in frame: 6869]
[Next request in frame: 6921]
[Next response in frame: 6938]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
  File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

Друга частина



Request:

```
No.      Time      Source      Destination      Protocol Length Info
 8193 73.403912    192.168.0.103 128.119.245.12   HTTP      660      GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 8193: 660 bytes on wire (5280 bits), 660 bytes captured (5280 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55728, Dst Port: 80, Seq: 1, Ack: 1, Len: 606
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
  If-None-Match: "80-5a19372ddd54f"\r\n
  If-Modified-Since: Tue, 24 Mar 2020 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 8214]
```

Response:

```
No.      Time      Source      Destination      Protocol Length Info
 8214 73.589039    128.119.245.12  192.168.0.103    HTTP      293      HTTP/1.1 304 Not Modified
Frame 8214: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-A4A9-49C317EF7C40}, id 0
Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103
Transmission Control Protocol, Src Port: 80, Dst Port: 55728, Seq: 1, Ack: 607, Len: 239
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Tue, 24 Mar 2020 19:17:07 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "80-5a19372ddd54f"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.185127000 seconds]
[Request in frame: 8193]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

Третья часть

Скриншот интерфейса Wireshark, отображающего сетевые пакеты в беспроводной сети. В верхней панели меню и панели инструментов. Основная панель отображает список пакетов с колонками: No., Time, Source, Destination, Protocol, Length, Info. Выбран пакет 7093 (HTTP 1.1 200 OK (JPEG JFIF image)). В нижней панели отображается детальный просмотр пакета, включающий Ethernet II, Internet Protocol Version 4, Transmission Control Protocol и Hypertext Transfer Protocol. В нижней панели также отображается HEX-код и ASCII-код пакета.

No.	Time	Source	Destination	Protocol	Length	Info
6718	50.083032	192.168.0.103	195.201.43.30	HTTP	851	GET /kartinki/lambo/22235-lamborghini-huracan-lp-580-2.html HTTP/1.1
6760	50.233532	195.201.43.30	192.168.0.103	HTTP	60	HTTP/1.1 200 OK (text/html)
6811	50.637183	192.168.0.103	195.201.43.30	HTTP	826	GET /uploads/gallery/thumb/32/kartinki24_ru_serials_269.jpg HTTP/1.1
6825	50.677367	192.168.0.103	81.19.89.18	HTTP	467	GET /top100.jcn?3048816 HTTP/1.1
6846	50.742409	192.168.0.103	195.201.43.30	HTTP	830	GET /uploads/gallery/thumb/447/kartinki24_ru_skyscrapers_51.jpg HTTP/1.1
6862	50.748080	192.168.0.103	195.201.43.30	HTTP	833	GET /uploads/gallery/thumb/526/kartinki24_ru_spring_flowers_83.jpg HTTP/1.1
6863	50.748823	192.168.0.103	195.201.43.30	HTTP	826	GET /uploads/gallery/thumb/50/kartinki24_ru_kangaroo_12.jpg HTTP/1.1
6864	50.748850	192.168.0.103	195.201.43.30	HTTP	839	GET /uploads/gallery/thumb/268/kartinki24_ru_bougquets_of_flowers_201.jpg HTTP/1.1
6865	50.749246	192.168.0.103	195.201.43.30	HTTP	827	GET /uploads/gallery/thumb/322/kartinki24_ru_roosters_19.jpg HTTP/1.1
7026	50.889210	81.19.89.18	192.168.0.103	HTTP	1514	[TCP Previous segment not captured] Continuation[Malformed Packet]
7028	50.890703	81.19.89.18	192.168.0.103	HTTP	1514	Continuation[Malformed Packet]
7093	50.930527	195.201.43.30	192.168.0.103	HTTP	1477	HTTP/1.1 200 OK (JPEG JFIF image)
7172	50.987643	81.19.89.18	192.168.0.103	HTTP	1514	Continuation
7173	50.987644	81.19.89.18	192.168.0.103	HTTP	1514	Continuation
7179	50.992815	81.19.89.18	192.168.0.103	HTTP	1514	Continuation
7181	50.994291	81.19.89.18	192.168.0.103	HTTP	1514	Continuation
7182	50.994295	81.19.89.18	192.168.0.103	HTTP	1514	Continuation

> Frame 7093: 1477 bytes on wire (11816 bits), 1477 bytes captured (11816 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-AA9-49C317EF7C40}, id 0
> Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
> Internet Protocol Version 4, Src: 195.201.43.30, Dst: 192.168.0.103
> Transmission Control Protocol, Src Port: 80, Dst Port: 55977, Seq: 91271, Ack: 1570, Len: 1423
> [58 Reassembled TCP Segments (83426 bytes): #6835(243), #6837(1460), #6841(1460), #6844(1460), #6847(1460), #6848(1460), #6849(1460), #6850(1460), #6851(1460), #6852(1460), #6897(1460), #6898(1460), #6900(1460)]
> Hypertext Transfer Protocol
> JPEG File Interchange Format

Frame (1477 bytes) Reassembled TCP (83426 bytes)

Wireshark: Беспроводная сеть_20200324212348_03016.pcapng

Пакеты: 9856 - Показаны: 34 (0.3%) - Потеряно: 0 (0.0%)

Профиль: Default

21:28 24.03.2020

No. Time Source Destination Protocol Length Info
7093 50.930527 195.201.43.30 192.168.0.103 HTTP 1477 HTTP/1.1 200 OK (JPEG JFIF image)
Frame 7093: 1477 bytes on wire (11816 bits), 1477 bytes captured (11816 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-AA9-49C317EF7C40}, id 0
Ethernet II, Src: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8), Dst: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd)
Internet Protocol Version 4, Src: 195.201.43.30, Dst: 192.168.0.103
Transmission Control Protocol, Src Port: 80, Dst Port: 55977, Seq: 91271, Ack: 1570, Len: 1423
[58 Reassembled TCP Segments (83426 bytes): #6835(243), #6837(1460), #6841(1460), #6844(1460), #6847(1460), #6848(1460), #6849(1460), #6850(1460), #6851(1460), #6852(1460), #6897(1460), #6898(1460), #6900(1460), #6902(1460), #6904(1460), #6]
Hypertext Transfer Protocol
JPEG File Interchange Format

Четверта частина

Захват из Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
1059	8.251699	192.168.0.103	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1080	8.397635	128.119.245.12	192.168.0.103	HTTP	1127	HTTP/1.1 200 OK (text/html)
1094	8.521406	192.168.0.103	128.119.245.12	HTTP	481	GET /pearson.png HTTP/1.1
1118	8.680345	128.119.245.12	192.168.0.103	HTTP	745	HTTP/1.1 200 OK (PNG)
1171	9.026504	192.168.0.103	128.119.245.12	HTTP	495	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
1362	9.563632	128.119.245.12	192.168.0.103	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 1059: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{C551BACB-BCCA-48D6-AA9C-317EF7C40}, id 0
> Ethernet II, Src: LiteonTe_0e:89:dd (cc:b0:da:0e:89:dd), Dst: TendaTec_00:c4:e8 (04:95:e6:00:c4:e8)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56039, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
> Hypertext Transfer Protocol

0030 01 00 c8 65 00 00 47 45 54 20 2f 77 69 72 65 73 ...e-GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 ireshark -file4.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1- Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu- C connectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 64 n: keep- alive- 0
00a0 70 72 3a 20 31 2e 31 32 35 0d 0a 55 70 67 72 61 pr: 1.12.5.0 Upgra
00b0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
00c0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1- -User-Ag
00d0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00e0 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.

Hypertext Transfer Protocol (http), 507 байта

Пакеты: 6762 - Показаны: 6 (0.1%)

Профиль: Default

21:31
24.03.2020

4.pcapng

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
244	20.330451	192.168.1.102	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
245	20.333653	192.168.1.102	128.119.245.12	TCP	66	53842 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
246	20.348742	172.217.16.46	192.168.1.102	TCP	54	443 → 53841 [ACK] Seq=824 Ack=2610 Win=67584 Len=0
247	20.450924	128.119.245.12	192.168.1.102	TCP	1514	80 → 53839 [ACK] Seq=1074 Ack=889 Win=31360 Len=1460 [TCP segment of a reassembled PDU]
248	20.451492	128.119.245.12	192.168.1.102	TCP	1514	80 → 53839 [ACK] Seq=2534 Ack=889 Win=31360 Len=1460 [TCP segment of a reassembled PDU]
249	20.451528	192.168.1.102	128.119.245.12	TCP	54	53839 → 80 [ACK] Seq=889 Ack=3994 Win=17520 Len=0
250	20.453832	128.119.245.12	192.168.1.102	HTTP	745	HTTP/1.1 200 OK (PNG)
251	20.453952	128.119.245.12	192.168.1.102	TCP	66	80 → 53842 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
252	20.454011	192.168.1.102	128.119.245.12	TCP	54	53842 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
253	20.455511	192.168.1.102	128.119.245.12	HTTP	478	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

> Frame 250: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404865AB4DF}, id 0
> Ethernet II, Src: Tp-LinkT_71:2a:bb (e8:94:f6:71:2a:bb), Dst: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 53839, Seq: 3994, Ack: 889, Len: 691
[3 Reassembled TCP Segments (3611 bytes): #247(1460), #248(1460), #250(691)]
[Frame: 247, payload: 0-1459 (1460 bytes)]
[Frame: 248, payload: 1460-2919 (1460 bytes)]
[Frame: 250, payload: 2920-3610 (691 bytes)]
[Segment count: 3]
[Reassembled TCP length: 3611]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a204d...]
> Hypertext Transfer Protocol

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
0010 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 30 32 20 4d Date: Mon, 02 M
0020 61 72 20 32 30 32 30 20 30 30 3a 31 35 3a 31 31 ar 2020 00:15:11
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT-Se rver: Ap
0040 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent
0050 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.
0060 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e 2k-fips PHP/5.4.
0070 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_p erl/2.0.
0080 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3
0090 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 Last-Mod ified:
00a0 53 61 74 2c 20 30 36 20 41 75 67 20 32 30 31 36 Sat, 06 Aug 2016

Frame (745 bytes) Reassembled TCP (3611 bytes)

TCP Segment (tcp.segment), 1,460 bytes

Пакеты: 410 - Displayed: 410 (100.0%)

Профиль: Default

EN

17:21
24.03.2020

Відповіді на контрольні запитання:

1. Яку версію протоколу HTTP використовує ваш браузер (1.0 чи 1.1)? Яку версію протоколу використовує сервер?

І браузер, і сервер використовують версію протоколу HTML 1.1. (HTTP200)

2. Які мови (якщо вказано) браузер може прийняти від сервера?

Мови: en, ru, uk. (Accept Lang)

3. Які IP-адреси вашого комп'ютера та цільового веб-сервера?

IP адреса мого комп'ютера: 192.168.0.103; сервера: 128.119.245.12

4. Який статусний код сервер повернув у відповіді вашому браузеру?

200 OK

5. Коли на сервері в останній раз був модифікований файл, який запитується браузером?

Sun, 16 Feb 2020 06:59:03 GMT

6. Скільки байт контенту повертається сервером?

81 bytes

7. Переглядаючи нерозібраний байтовий потік пакету, чи бачите ви деякі заголовки в потоці, які не відображаються у вікні деталей пакету? Якщо так, назвіть один з них.

Ні.

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в ньому заголовок IF-MODIFIED-SINCE?

Ні.

9. Перевірте вміст першої відповіді сервера. Чи повернув сервер вміст файлу безпосередньо у відповіді?

Так

10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIED-SINCE? Якщо так, яке значення йому відповідає?

Так

11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді?

304 Not modified

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Одне.

13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?

58 TCP Fragments.

14. Який код та опис статусу був у відповіді сервера?

200 OK.

15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та описом статусу відповіді, або ж якісь заголовки протоколу HTTP?

Ні

16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були цільові IP-адреси запитів?

Три. Усі 128.119.245.12

17. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно?

Яким чином?

Послідовно, бо GET запит відправлявся лише після отримання відповіді на попередній.

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення та аналізу пакетів. Було розглянуто інформацію, що містить в собі протокол HTTP.