

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра математичних методів системного аналізу

ЗВІТ

про виконання лабораторних робіт
з дисципліни «Комп'ютерні мережі»

Виконав:
студент групи ІС-зп93
Цинковський Д. В.
Прийняв: Кухарєв С.О.

8. Обрано перший пакет HTTP, який відобразився у вікні лістингу, це було

повідомлення GET протоколу HTTP. Також цей пакет вміщував інформацію про інші протоколи нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрито деталі, пов'язані з протоколом HTTP та скрито детальну інформацію про інші протоколи.

Результат деталей заголовку запиту показано на рисунку 2.

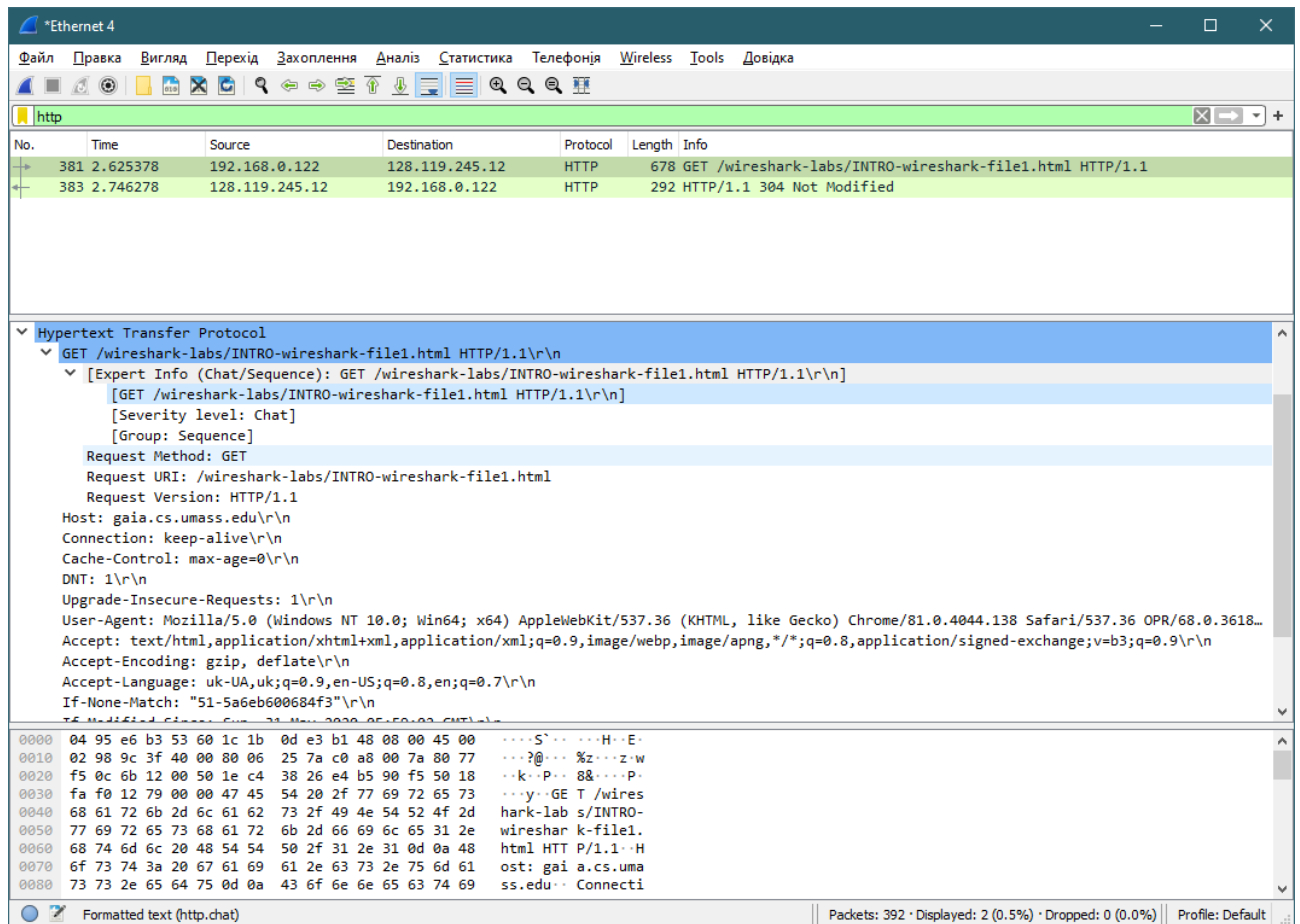


Рис. 2 Деталі заголовку запиту

10. Роздруковано перші пакети запиту та відповіді у відповідні файли.

11. Перевірено, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколи.

12. Закрито Wireshark.

3. Відповіді на контрольні питання

3.1 Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

Відповідь: в вікні лістингу протоколів до включення фільтрації відображалися наступні протоколи: UDP, SSDP, ARP, TCP, HTTP, IGMPv3

*Ethernet 4						
Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
362	0.412949	192.168.0.122	195.69.84.206	UDP	71	64096 → 443 Len=29
363	0.413043	195.69.84.206	192.168.0.122	UDP	1392	443 → 64096 Len=1350
364	0.413565	195.69.84.206	192.168.0.122	UDP	1392	443 → 64096 Len=1350
365	0.413642	195.69.84.206	192.168.0.122	UDP	822	443 → 64096 Len=780
366	0.414145	192.168.0.122	195.69.84.206	UDP	71	64096 → 443 Len=29
367	0.450626	192.168.0.1	239.255.255.250	SSDP	278	NOTIFY * HTTP/1.1
368	0.450796	192.168.0.1	239.255.255.250	SSDP	350	NOTIFY * HTTP/1.1
369	0.450960	192.168.0.1	239.255.255.250	SSDP	346	NOTIFY * HTTP/1.1
370	0.451126	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
371	0.451294	192.168.0.1	239.255.255.250	SSDP	358	NOTIFY * HTTP/1.1
372	0.451460	192.168.0.1	239.255.255.250	SSDP	340	NOTIFY * HTTP/1.1
373	0.451624	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
374	0.451787	192.168.0.1	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
375	0.960080	TendaTec_b3:53:60	Giga-Byt_e3:b1:48	ARP	60	Who has 192.168.0.122? Tell 192.168.0.1
376	0.960096	Giga-Byt_e3:b1:48	TendaTec_b3:53:60	ARP	42	192.168.0.122 is at 1c:1b:0d:e3:b1:48
377	1.999995	TendaTec_b3:53:60	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/04:95:e6:b3:53:60 Cost = 0 Port = 0x8001
378	2.508931	192.168.0.122	128.119.245.12	TCP	62	27410 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
379	2.625030	128.119.245.12	192.168.0.122	TCP	62	80 → 27410 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_...
380	2.625144	192.168.0.122	128.119.245.12	TCP	54	27410 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
381	2.625378	192.168.0.122	128.119.245.12	HTTP	678	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
382	2.741242	128.119.245.12	192.168.0.122	TCP	60	80 → 27410 [ACK] Seq=1 Ack=625 Win=29952 Len=0
383	2.746278	128.119.245.12	192.168.0.122	HTTP	292	HTTP/1.1 304 Not Modified
384	2.786364	192.168.0.122	128.119.245.12	TCP	54	27410 → 80 [ACK] Seq=625 Ack=239 Win=64002 Len=0
385	3.550208	192.168.0.122	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
386	3.557110	192.168.0.122	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.168.100.1
387	3.907892	192.168.0.122	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any sources
388	3.999963	TendaTec_b3:53:60	Spanning-tree-(for-...	STP	60	Conf. Root = 32768/0/04:95:e6:b3:53:60 Cost = 0 Port = 0x8001
389	4.056479	192.168.0.122	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.168.100.1 for any sources
390	5.985189	172.217.16.46	192.168.0.122	UDP	83	443 → 62735 Len=41
391	5.990135	192.168.0.122	172.217.16.46	UDP	72	62735 → 443 Len=30
> Frame 381: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{D21DD217-F01C-4545-BEF9-F292EFE3FDF}, id 0 > Ethernet II, Src: Giga-Byt_e3:b1:48 (1c:1b:0d:e3:b1:48), Dst: TendaTec_b3:53:60 (04:95:e6:b3:53:60) > Internet Protocol Version 4, Src: 192.168.0.122, Dst: 128.119.245.12 > Transmission Control Protocol, Src Port: 27410, Dst Port: 80, Seq: 1, Ack: 1, Len: 624 > Hypertext Transfer Protocol GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n] [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]						
0000 04 95 e6 b3 53 60 1c 1b 0d e3 b1 48 08 00 45 00 ...S...H..E.						
0010 02 98 9c 3f 40 00 80 06 25 7a c0 a8 00 7a 80 77 ...?@...%z...z.w						
0020 f5 0c 6b 12 00 50 1e c4 38 26 e4 b5 90 f5 50 18 ...k..P..8&...P.						
Formatted text (http.chat)				Packets: 392 · Displayed: 392 (100.0%) · Dropped: 0 (0.0%) Profile: Default		

Рис. 3. Лістинг протоколів

3.2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

Відповідь: у пакеті запиту використовувались eth:ethertype:ip:tcp:http протоколи, у пакеті відповіді eth:ethertype:ip:tcp:http:data-text-lines протоколи. Інформація про пакети з Wireshark зображена на рис. 4

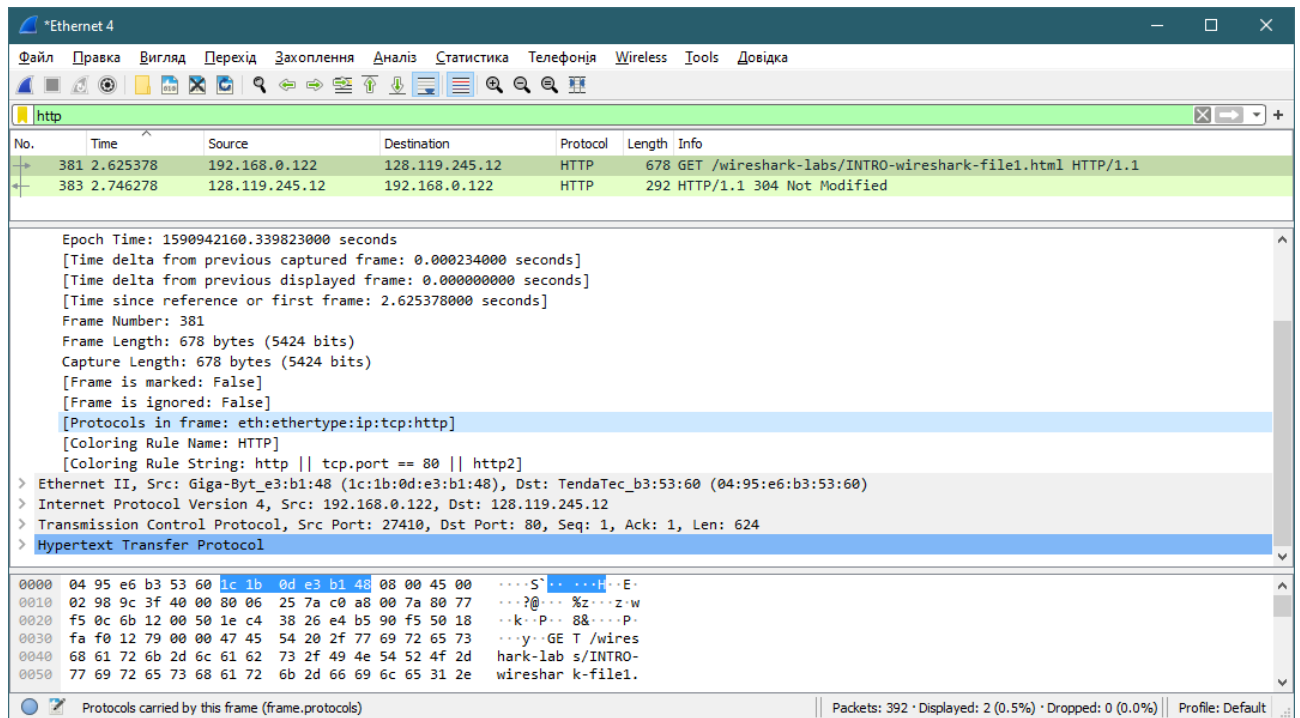


Рис. 4 Протоколи, які використовувались у пакеті запиту

3.3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Відповідь: час відправки пакету запиту May 31, 2020 19:22:40.339823000 Фінляндія (літо), отримання пакету відповіді May 31, 2020 19:22:40.460723000 Фінляндія (літо), період часу між пакетом запиту та відповіді склав [Time delta from previous displayed frame: 0.120900000 seconds].

3.4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Відповідь: для пакету запиту Source 192.168.0.122, Destination 128.119.245.12 для пакету відповіді Source 128.119.245.12, Destination 192.168.0.105 Інформації з Wireshark про вихідні та цільові адреси пакетів із запитом та відповіддю зображено на рисунку 5.

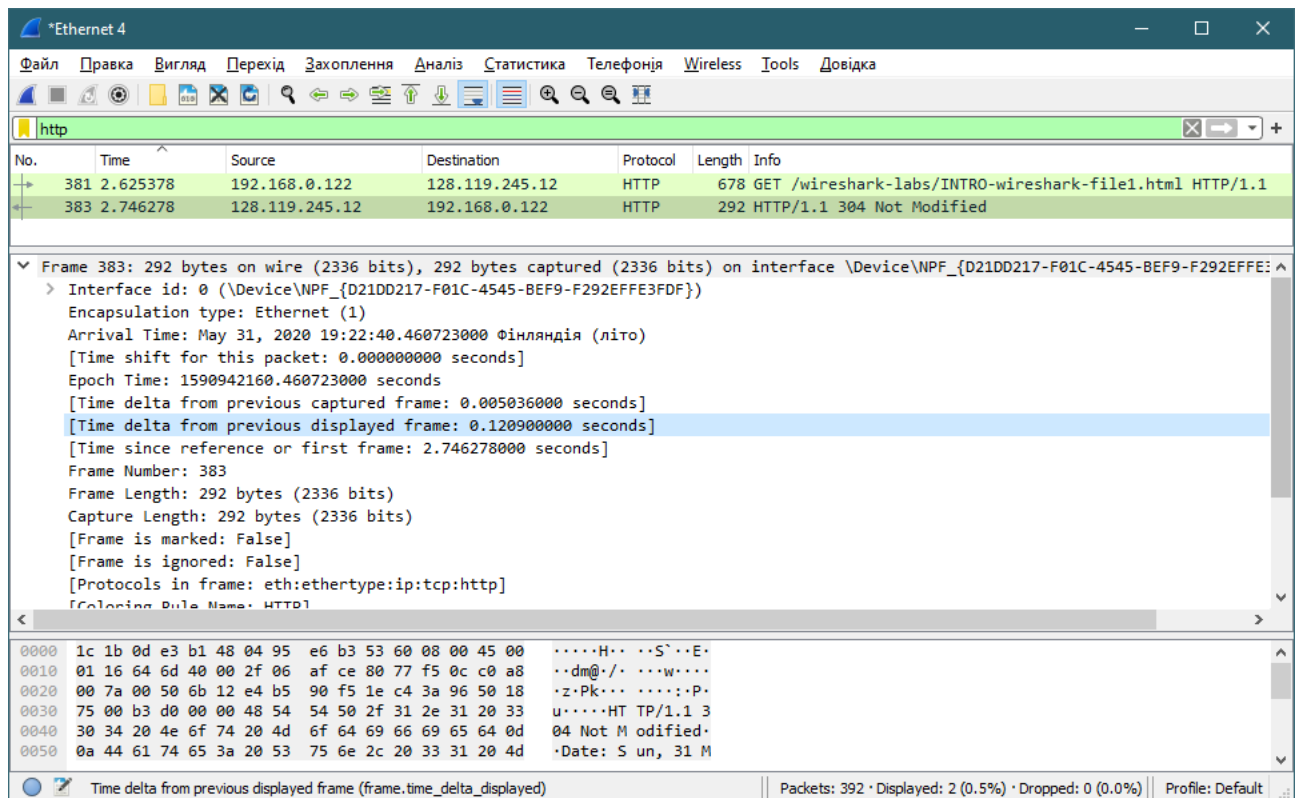


Рис. 5. Інформація з Wireshark про вихідні та цільові адреси пакетів із Запитом

3.5. Яким був перший рядок запиту на рівні протоколу HTTP?

Відповідь: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

3.6. Яким був перший рядок відповіді на рівні протоколу HTTP?

Відповідь: HTTP/1.1 304 Not Modified\r\n

ДОДАТОК 1

```
No.      Time      Source      Destination      Protocol Length Info
381 2.625378    192.168.0.122    128.119.245.12    HTTP      678      GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 381: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits) on interface \Device\NPF_{D21DD217-F01C-4545-BEF9-F292EFE3FDF}, id 0
Ethernet II, Src: Giga-Byt_e3:b1:48 (1c:1b:0d:e3:b1:48), Dst: TendaTec_b3:53:60 (04:95:e6:b3:53:60)
Internet Protocol Version 4, Src: 192.168.0.122, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 27410, Dst Port: 80, Seq: 1, Ack: 1, Len: 624
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Request Method: GET
  Request URI: /wireshark-labs/INTRO-wireshark-file1.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  DNT: 1\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/81.0.4044.138 Safari/537.36 OPR/68.0.3618.125\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: uk-UA,uk;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  If-None-Match: "51-5a6eb600684f3"\r\n
  If-Modified-Since: Sun, 31 May 2020 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 383]
No.      Time      Source      Destination      Protocol Length Info
383 2.746278    128.119.245.12    192.168.0.122    HTTP      292      HTTP/1.1 304 Not Modified
Frame 383: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface \Device\NPF_{D21DD217-F01C-4545-BEF9-F292EFE3FDF}, id 0
Ethernet II, Src: TendaTec_b3:53:60 (04:95:e6:b3:53:60), Dst: Giga-Byt_e3:b1:48 (1c:1b:0d:e3:b1:48)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.122
Transmission Control Protocol, Src Port: 80, Dst Port: 27410, Seq: 1, Ack: 625, Len: 238
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    [HTTP/1.1 304 Not Modified\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
  Date: Sun, 31 May 2020 16:22:41 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.6 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: "51-5a6eb600684f3"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.120900000 seconds]
[Request in frame: 381]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```