

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.

Лабораторна робота 2

1 Мета роботи

Метою данної лабораторної роботи є аналіз деталей роботи протоколу HTTP.

2. Хід роботи

Під час виконання лабораторної роботи виконано наступні дії:

1. Запущено веб-браузер, очищено кеш браузера.
2. Запущено Wireshark, введено «http» в поле фільтрації, та почато захоплення пакетів.
3. Відкрито за допомогою браузера зазначену нижче адресу:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
4. Зупинено захоплення пакетів.
5. Переглянуто деталі захоплених пакетів. Для цього налаштовано вікно деталей пакету: згорнуто деталі протоколів усіх рівнів крім HTTP
6. Придготовлено відповіді на контрольні запитання 1-7, які надано у розділі 3.
7. Знов розпочато захоплення пакетів.
8. Відкрито у браузері ту ж саму сторінку <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
9. Зупинено захоплення пакетів.
10. Підготовлено відповіді на контрольні запитання 8-11
11. Обрано адрес ресурсу http://awsassets.wwf.ca/img/original/hi_201639.jpg
12. Знов розпочато захоплення пакетів та очищено кеш браузера.
13. Відкрито обраний ресурс браузером.
14. Зупинено захоплення пакетів.
15. Придготовлено відповіді на запитання 12-15, які надано у розділі 3.
16. Знов розпочато захоплення пакетів.
17. Відкрито сторінку за адресою <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
14. Зупинено захоплення пакетів.
19. Підготовлено відповіді на запитання 16, 17.
20. Закрито Wireshark.

3. Відповіді на контрольні питання

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

Яку версію протоколу використовує сервер?

Відповідь: браузер використовує версію HTTP/1.1. Сервер використовує версію HTTP/1.1. Інформацію з Wireshark з версією HTTP браузера та версією HTTP сервера наведено на рисунку 1.

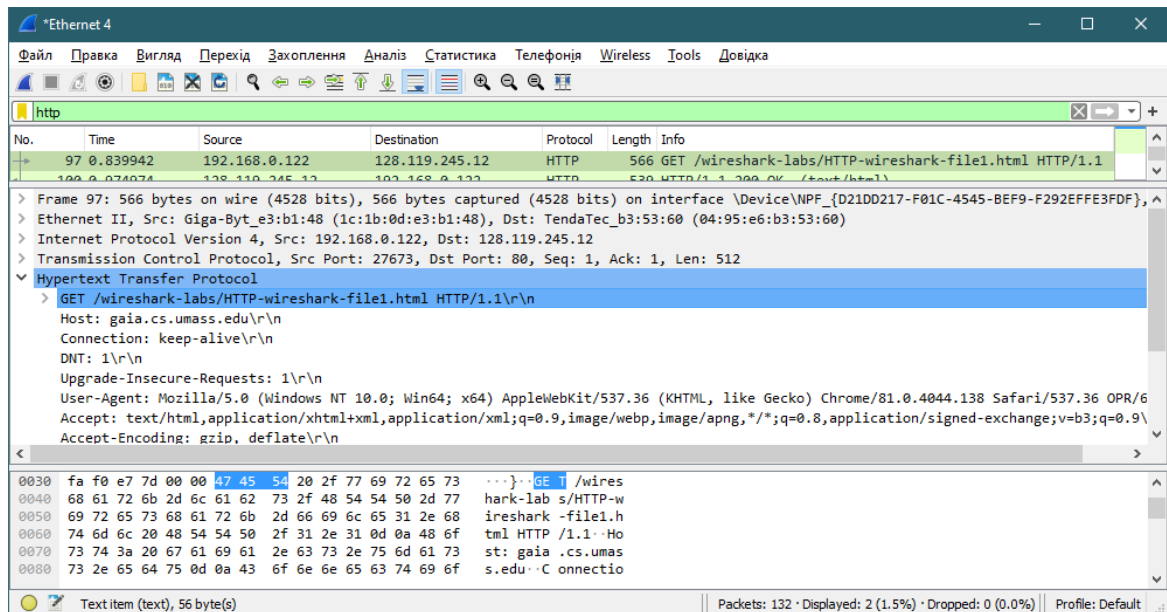
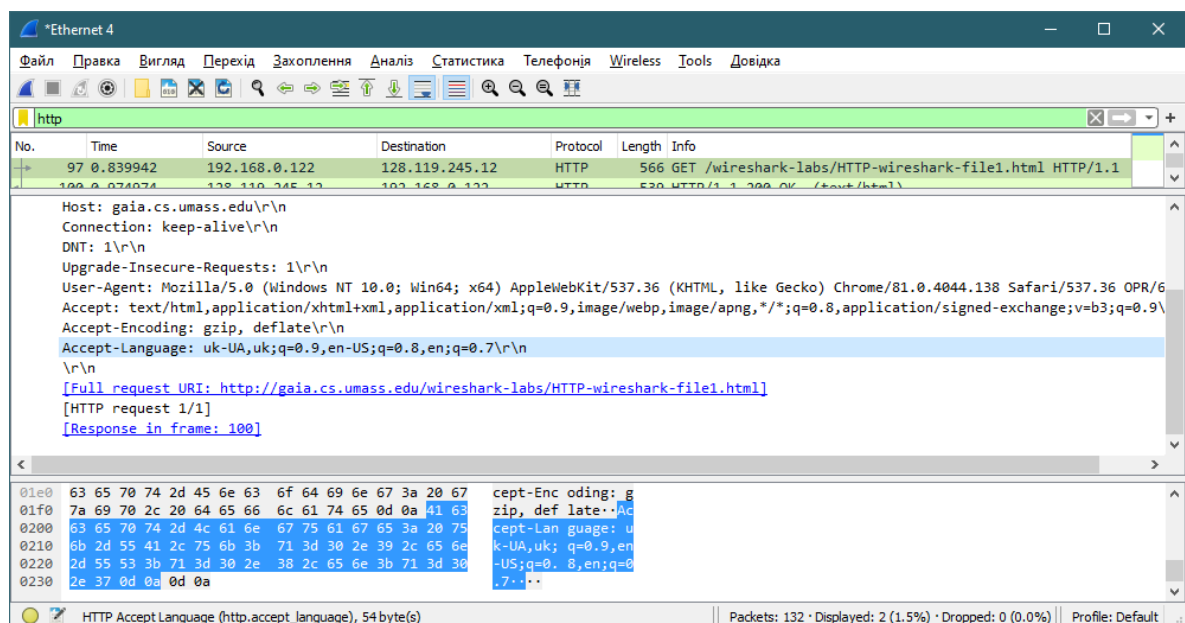


Рис.1 - Інформацію з Wireshark з версією HTTP браузера

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

Відповідь: Браузер вказує, що може прийняти uk-UA,uk;q=0.9,en-US;q=0.8,en;q=0.7 Інформацію з Wireshark з прийнятними мовами для браузера наведено на рисунку 2.



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

Відповідь: Адреса комп'ютера 192.168.0.122, адреса цільового веб-сервера 128.119.245.12 наведено на рисунку 3.

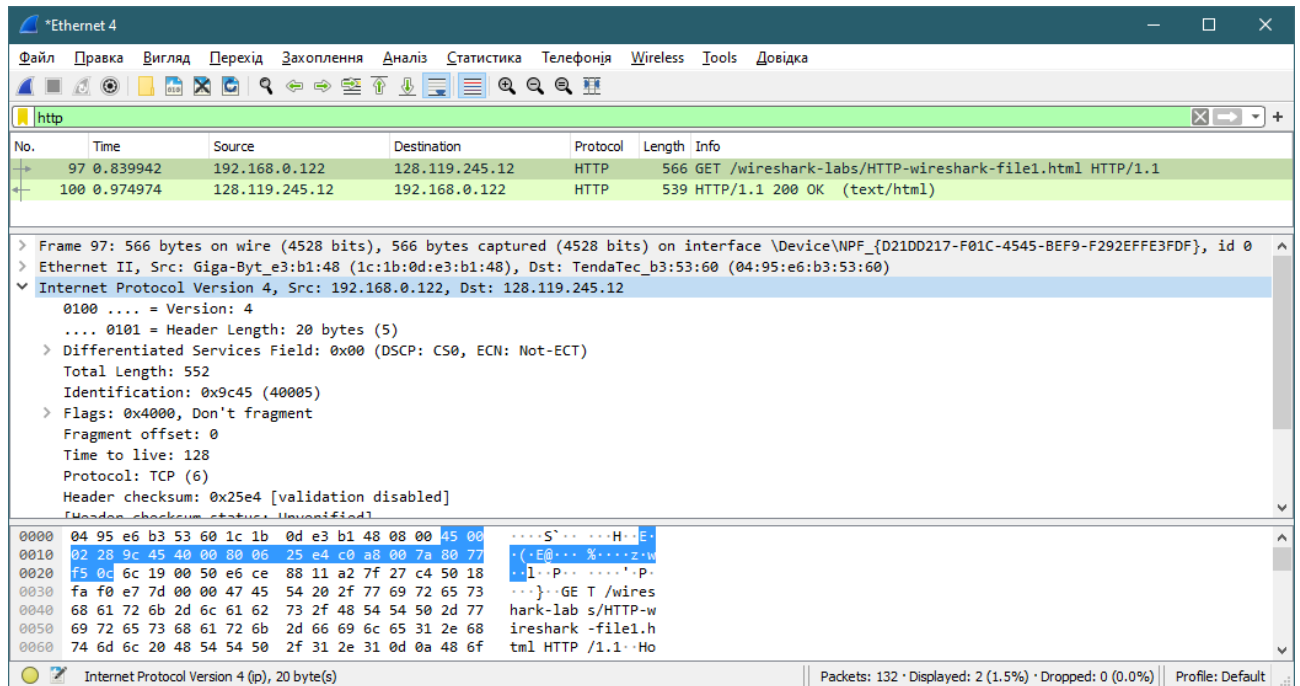


Рис. 3 - Інформацію з Wireshark з IP-адресами

3.4. Який статусний код сервер повернув у відповіді браузеру?

Відповідь: Сервер повернув статусний код 200

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

Відповідь: час останньої модифікації файлу Sun, 31 May 2020 05:59:02 GMT.

3.6. Скільки байт контенту повертається сервером?

Відповідь: Content-Length: 128

3.7. 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.

Відповідь: Ні

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

Відповідь: Ні

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

Відповідь: Так

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

Відповідь: Так, присутній заголовок за параметром If-Modified-Since: If-Modified-Since: Sun, 31 May 2020 05:59:02 GMT Інформацію з Wireshark з заголовком за параметром If-Modified-Since наведено на рисунку 4.

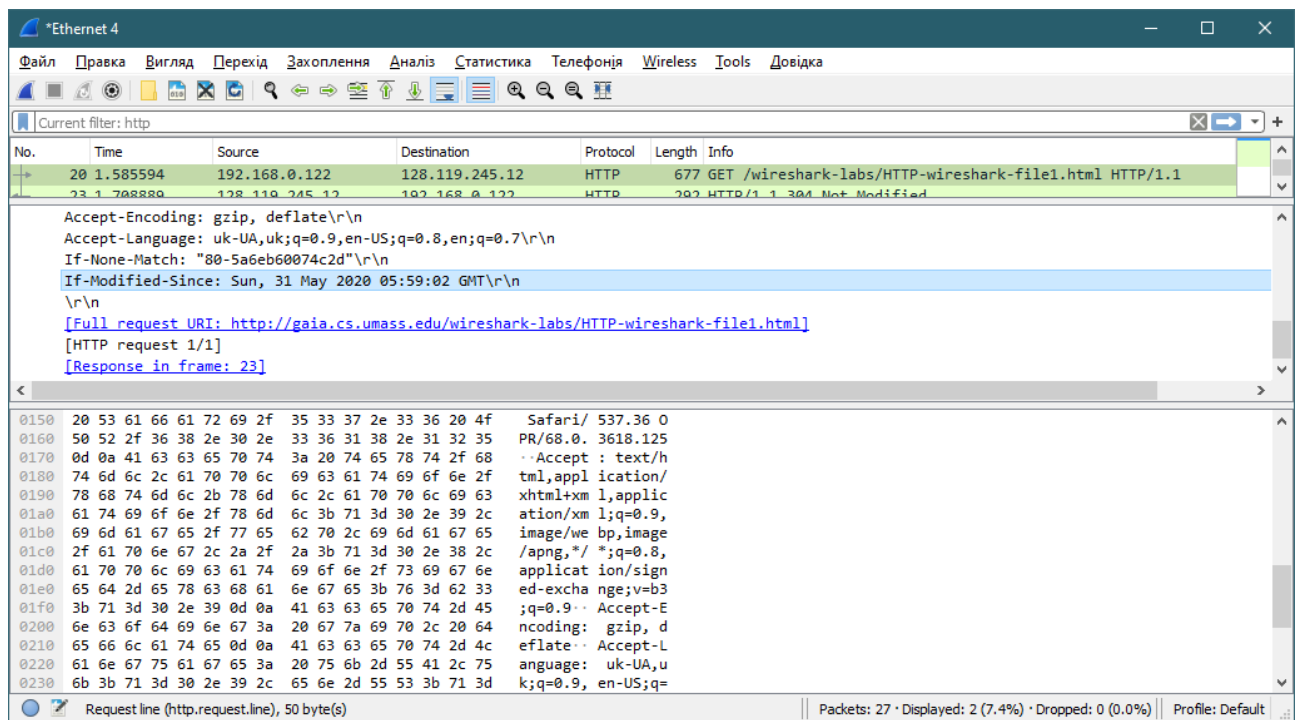


Рис. 4 - Інформацію з Wireshark з заголовком за параметром If-Modified-Since

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

Відповідь: Status Code: 304, безпосередньо файл у відповідь повернутий не був

3.12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

Відповідь: 2. Інформація на рис 5.

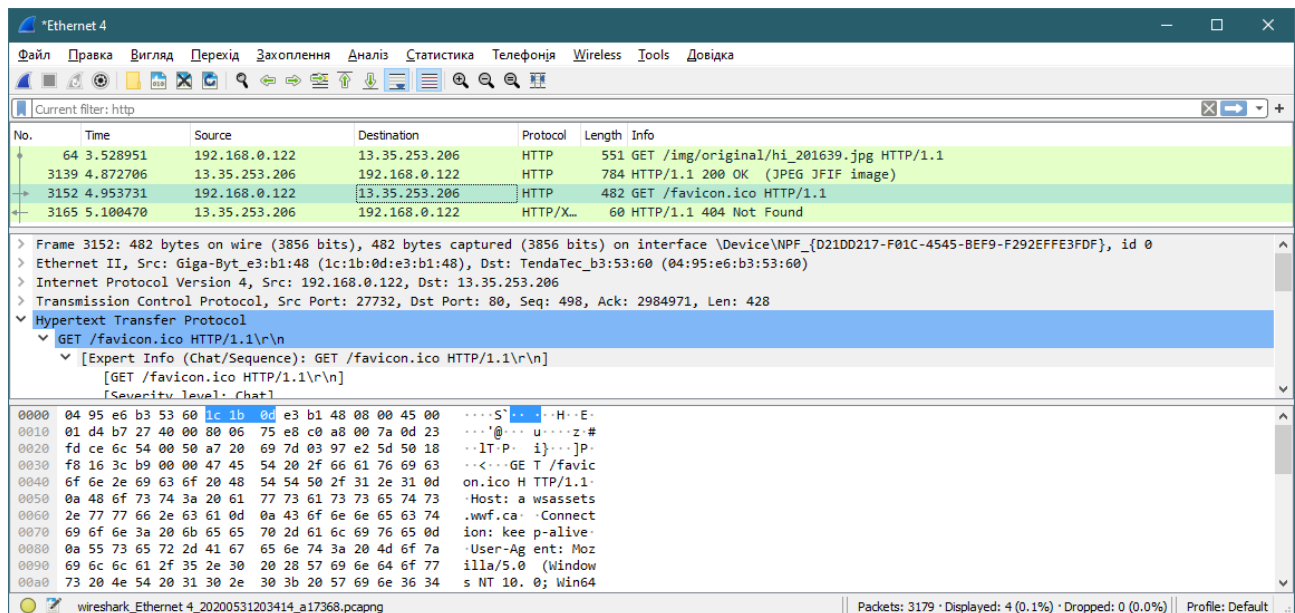


Рис. 5 - Інформацію з Wireshark з заголовком

3.13. Скільки пакетів TCP було необхідно для доставки однієї відповіді HTTP-сервера?

Відповідь: 2045 Reassembled TCP Segments (2984970 bytes).

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

Відповідь: Status Code: 200 OK

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

Відповідь: Зустрічається лише в першому пакеті. Інформація на рис 6.

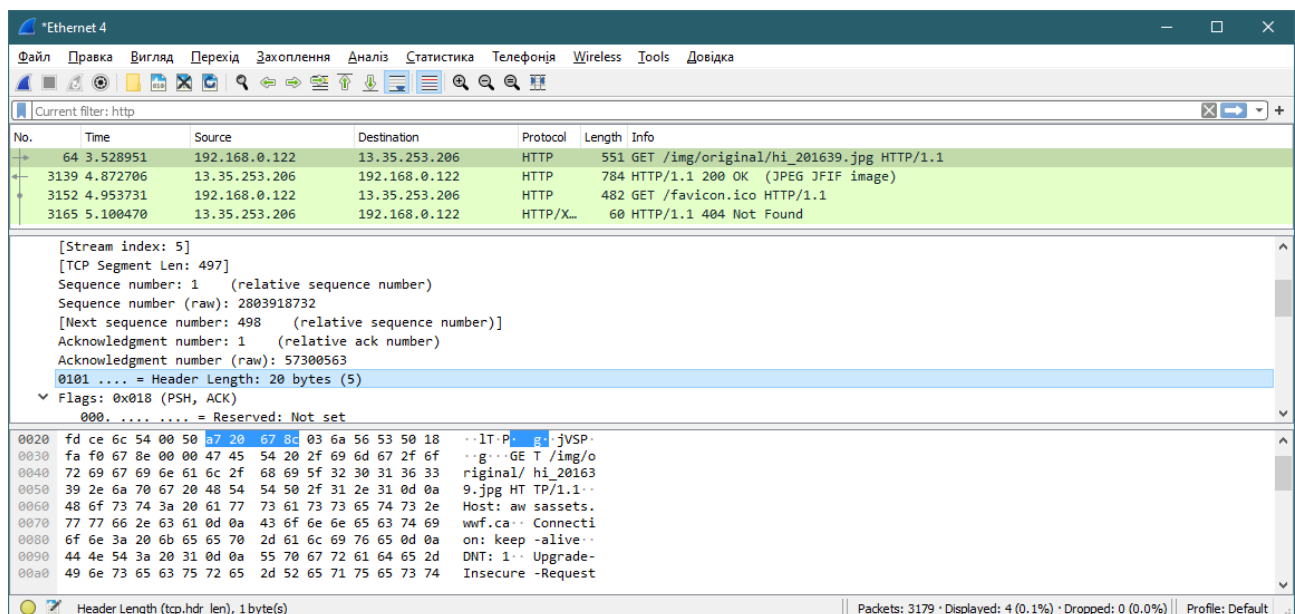


Рис. 6 - Інформацію з Wireshark з заголовком

3.16. Скільки запитів HTTP GET було відправлено вашим браузером?

Якими були цільові IP-адреси запитів?

Відповідь: Було відправлено 2 HTTP GET запити. Цільові адреси були

Source: 192.168.0.122, Destination: 13.35.253.206. Інформація на рис 7.

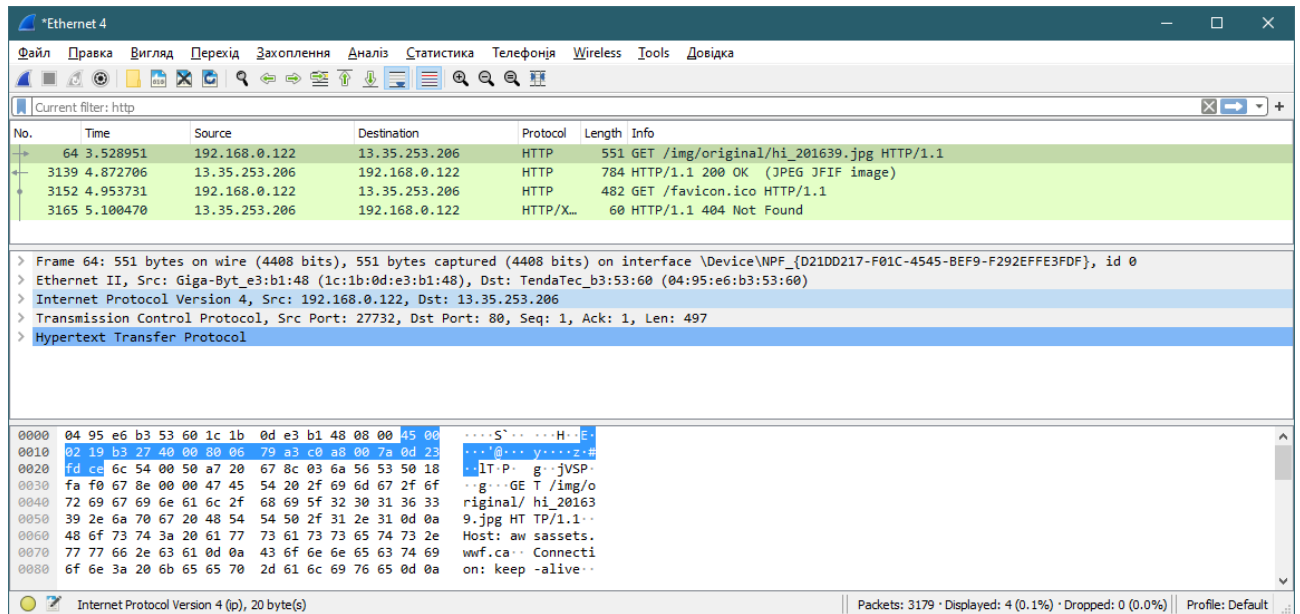


Рис. 7 - Інформацію з Wireshark з заголовком

3.17. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно? Яким чином?

Відповідь: Відповіді запитах надходили послідовно, використовуючи однаковий порт Source Port: 80.

ДОДАТОК 1

No.	Time	Source	Destination	Protocol	Length	Info
20	1.585594	192.168.0.122	128.119.245.12	HTTP	677	GET /wireshark-labs/HTTP-wireshark-file1.html

HTTP/1.1
Frame 20: 677 bytes on wire (5416 bits), 677 bytes captured (5416 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: 27720, Dst Port: 80, Seq: 1, Ack: 1, Len: 623
Source Port: 27720
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 623]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2546402752
[Next sequence number: 624 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1688686004
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xbaea [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (623 bytes)
Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
23	1.708889	128.119.245.12	192.168.0.122	HTTP	292	HTTP/1.1 304 Not Modified

Frame 23: 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: 27720, Seq: 1, Ack: 624, Len: 238
Source Port: 80
Destination Port: 27720
[Stream index: 1]
[TCP Segment Len: 238]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 1688686004
[Next sequence number: 239 (relative sequence number)]
Acknowledgment number: 624 (relative ack number)
Acknowledgment number (raw): 2546403375
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 29904
[Calculated window size: 29904]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xc9ae [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (238 bytes)
Hypertext Transfer Protocol

ДОДАТОК 2

```
No.      Time      Source      Destination      Protocol Length Info
64 3.528951 192.168.0.122 13.35.253.206 HTTP 551 GET /img/original/hi_201639.jpg HTTP/1.1
Frame 64: 551 bytes on wire (4408 bits), 551 bytes captured (4408 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: 13.35.253.206
Transmission Control Protocol, Src Port: 27732, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
  Source Port: 27732
  Destination Port: 80
  [Stream index: 5]
  [TCP Segment Len: 497]
  Sequence number: 1 (relative sequence number)
  Sequence number (raw): 2803918732
  [Next sequence number: 498 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Acknowledgment number (raw): 57300563
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 64240
  [Calculated window size: 64240]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x678e [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (497 bytes)
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
3139 4.872706 13.35.253.206 192.168.0.122 HTTP 784 HTTP/1.1 200 OK (JPEG JFIF image)
Frame 3139: 784 bytes on wire (6272 bits), 784 bytes captured (6272 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: 13.35.253.206, Dst: 192.168.0.122
Transmission Control Protocol, Src Port: 80, Dst Port: 27732, Seq: 2984241, Ack: 498, Len: 730
  Source Port: 80
  Destination Port: 27732
  [Stream index: 5]
  [TCP Segment Len: 730]
  Sequence number: 2984241 (relative sequence number)
  Sequence number (raw): 60284803
  [Next sequence number: 2984971 (relative sequence number)]
  Acknowledgment number: 498 (relative ack number)
  Acknowledgment number (raw): 2803919229
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 30016
  [Calculated window size: 30016]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x8e92 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (730 bytes)
  TCP segment data (730 bytes)
[2045 Reassembled TCP Segments (2984970 bytes): #66(1460), #67(1460), #69(1460), #70(1460), #72(1460), #73(1460), #75(1460), #76(1460), #78(1460), #79(1460), #81(1460), #82(1460), #84(1460), #85(1460), #87(1460), #88(1460), #90(1460), #91(1)]
Hypertext Transfer Protocol
JPEG File Interchange Format
No.      Time      Source      Destination      Protocol Length Info
3152 4.953731 192.168.0.122 13.35.253.206 HTTP 482 GET /favicon.ico HTTP/1.1
Frame 3152: 482 bytes on wire (3856 bits), 482 bytes captured (3856 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: 13.35.253.206
Transmission Control Protocol, Src Port: 27732, Dst Port: 80, Seq: 498, Ack: 2984971, Len: 428
  Source Port: 27732
  Destination Port: 80
  [Stream index: 5]
  [TCP Segment Len: 428]
  Sequence number: 498 (relative sequence number)
  Sequence number (raw): 2803919229
  [Next sequence number: 926 (relative sequence number)]
  Acknowledgment number: 2984971 (relative ack number)
  Acknowledgment number (raw): 60285533
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 63510
  [Calculated window size: 63510]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x3cb9 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
```

```

[Timestamps]
TCP payload (428 bytes)
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
  3165  5.100470    13.35.253.206    192.168.0.122    HTTP/XML 60    HTTP/1.1 404 Not Found
Frame 3165: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 13.35.253.206, Dst: 192.168.0.122
Transmission Control Protocol, Src Port: 80, Dst Port: 27732, Seq: 2985621, Ack: 926, Len: 5
  Source Port: 80
  Destination Port: 27732
  [Stream index: 5]
  [TCP Segment Len: 5]
  Sequence number: 2985621 (relative sequence number)
  Sequence number (raw): 60286183
  [Next sequence number: 2985626 (relative sequence number)]
  Acknowledgment number: 926 (relative ack number)
  Acknowledgment number (raw): 2803919657
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 31088
  [Calculated window size: 31088]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xbebb [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (5 bytes)
  TCP segment data (5 bytes)
[2 Reassembled TCP Segments (655 bytes): #3164(650), #3165(5)]
Hypertext Transfer Protocol
eXtensible Markup Language

```