

За допомогою програми Wireshark проаналізували трафік.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Правка', 'Вигляд', 'Перехід', 'Захоплення', 'Аналіз', 'Статистика', 'Телефонія', 'Wireless', 'Tools', and 'Довідка'. Below the menu is a toolbar with various icons. The main display area is divided into three panes. The top pane shows a list of captured packets, with packet 40 selected. The middle pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
40	4.234812	192.168.124.241	128.119.245.12	HTTP	554	GET /wiresh
43	4.370891	128.119.245.12	192.168.124.241	HTTP	294	HTTP/1.1 30
49	4.416111	192.168.124.241	128.119.245.12	HTTP	522	GET /pearso
51	4.550685	128.119.245.12	192.168.124.241	HTTP	293	HTTP/1.1 30
55	4.551435	192.168.124.241	128.119.245.12	HTTP	538	GET /~kuros

Frame 40: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
> Ethernet II, Src: HonHaiPr_56:8c:3f (00:71:cc:56:8c:3f), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)
> Internet Protocol Version 4, Src: 192.168.124.241, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56141, Dst Port: 80, Seq: 1, Ack: 1, Len: 500
> Hypertext Transfer Protocol

0000 00 18 f3 67 19 61 00 71 cc 56 8c 3f 08 00 45 00 ...g·a·q·V·?·E·
0010 02 1c 7d 8d 40 00 80 06 c8 30 c0 a8 7c f1 80 77 ...}·@·...·0·...|·w·
0020 f5 0c db 4d 00 50 10 74 dc 67 2a ee ec 91 50 18 ...M·P·t·g*...P·
0030 00 44 4b 2d 00 00 47 45 54 20 2f 77 69 72 65 73 ...DK...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 55 73 65 72 2d 41 67 65 6e s.edu·U ser-Agen

Зробили запит.

40	4.234812	192.168.124.241	128.119.245.12	HTTP	554 GET /wiresh
----	----------	-----------------	----------------	------	-----------------

В запиті можна виділити наступні складові

The image shows the Wireshark network protocol analyzer interface, specifically the details pane for packet 40. The top menu bar includes options like 'Wireshark', 'Packet 40', 'Беспроводная сеть'. The main display area shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Hypertext Transfer Protocol.

Frame 40: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
> Ethernet II, Src: HonHaiPr_56:8c:3f (00:71:cc:56:8c:3f), Dst: AsustekC_67:19:61 (00:18:f3:67:19:61)
> Internet Protocol Version 4, Src: 192.168.124.241, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56141, Dst Port: 80, Seq: 1, Ack: 1, Len: 500
> Hypertext Transfer Protocol

Для відправки запиту використовується метод GET,

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

Далі ідуть різні типи заголовків в яких описуються потрібні дані, наприклад що виступає в ролі агента, яка мова використовується, версія Windows

```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
```

Можна побачити що сайт зберігається на сервері там де є багато сайтів

```
Connection: keep-alive\r\n
```

Бачимо, що нічого не кешується

```
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
```

Отримуємо відповідь з сервера

```
> HTTP/1.1 200 OK\r\n
Date: Thu, 16 May 2019 16:17:50 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.
Last-Modified: Thu, 16 May 2019 05:59:01 GMT\r\n
ETag: "2ca-588faf66eb82b"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 714\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
```

Також отримуємо картинки які знаходяться на сайті

91 8.765701	128.119.245.12	192.168.124.241	HTTP	746 HTTP/1.1 200 OK (PNG)
240 9.609468	128.119.245.12	192.168.124.241	HTTP	632 HTTP/1.1 200 OK (JPEG JFIF image)

```
> HTTP/1.1 200 OK\r\n
Date: Thu, 16 May 2019 16:17:50 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.
Last-Modified: Tue, 15 Sep 2009 18:23:27 GMT\r\n
ETag: "18a68-473a1e0e6e5c0"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 100968\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: image/jpeg\r\n
```

```
> HTTP/1.1 200 OK\r\n
Date: Thu, 16 May 2019 16:17:50 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.
Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
ETag: "cc3-539645c7f1ee7"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 3267\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: image/png\r\n
```