



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

Факультет управления и информатики в технологических системах
Кафедра информационной безопасности
Направление подготовки (специальность) 10.05.03 Информационная
безопасность автоматизированных систем

Отчет **по практической работе №1 «Гипертекстовый протокол HTTP»**

Выполнил студент гр. УБ-11
Юрьев С.В.

Проверил:
Доц. каф. ИБ Денисенко В.В.

Воронеж – 2023

Введение

Цель работы: научиться использовать WireShark.

Условие задачи: установить программу WireShark и научиться ею пользоваться и понимать.

Порядок выполнения:

- 1) Ознакомиться с программным обеспечением WireShark;
- 2) Провести анализ HTTP-трафика;
- 3) Сделать отчёт по проделанной работе.

Программно-аппаратные средства, используемые при выполнении работы: персональный компьютер или ноутбук, Microsoft Word (для создания отчёта), WireShark.

Рассматриваемый ресурс <http://education.vsu.ru>:

The screenshot displays the Wireshark network traffic analysis tool. The main window shows a list of captured packets, with the selected packet (No. 25113) being an HTTP 200 OK response from 10.6.19.242 to 10.6.19.242. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
24260	462.164526	93.88.139.17	10.6.19.242	HTTP	402	HTTP/1.1 200 OK (application/javascript)
24323	462.173523	93.88.139.17	10.6.19.242	HTTP	535	HTTP/1.1 200 OK (application/javascript)
24565	462.202941	93.88.139.17	10.6.19.242	HTTP	299	HTTP/1.1 200 OK (application/javascript)
24789	462.222227	93.88.139.17	10.6.19.242	HTTP	359	HTTP/1.1 404 Not Found (text/html)
24799	462.223277	10.6.19.242	93.88.139.17	HTTP	584	GET /lib/javascript.php/1676016890/lib/requirejs/require.min.js HTTP/1.1
24878	462.228445	93.88.139.17	10.6.19.242	HTTP	287	HTTP/1.1 200 OK (application/javascript)
25013	462.241414	93.88.139.17	10.6.19.242	HTTP	347	HTTP/1.1 200 OK (text/css)
25043	462.299210	10.6.19.242	93.88.139.17	HTTP	96	GET /theme/image.php/classic/core/1676016890/ff/pdf-4a HTTP/1.1
25045	462.299611	10.6.19.242	93.88.139.17	HTTP	102	GET /pluginfile.php/213530/block_html/content/324243.JPG HTTP/1.1
25049	462.300587	10.6.19.242	93.88.139.17	HTTP	96	GET /theme/image.php/classic/forum/1676016890/icon HTTP/1.1
25055	462.301740	10.6.19.242	93.88.139.17	HTTP	94	GET /theme/image.php/classic/url/1676016890/icon HTTP/1.1
25057	462.301897	10.6.19.242	93.88.139.17	HTTP	95	GET /theme/image.php/classic/book/1676016890/icon HTTP/1.1
25071	462.304124	93.88.139.17	10.6.19.242	HTTP	239	HTTP/1.1 200 OK (PNG)
25076	462.305078	93.88.139.17	10.6.19.242	HTTP/X.	425	HTTP/1.1 200 OK
25085	462.306109	93.88.139.17	10.6.19.242	HTTP/X.	235	HTTP/1.1 200 OK
25090	462.306520	10.6.19.242	93.88.139.17	HTTP	109	GET /pluginfile.php/220890/block_html/content/Protiv_pojara.JPG HTTP/1.1
25099	462.307172	93.88.139.17	10.6.19.242	HTTP	79	HTTP/1.1 200 OK
25107	462.310243	10.6.19.242	93.88.139.17	HTTP	109	GET /theme/image.php/classic/core/1676016890/moodlelogo_grayhat HTTP/1.1
25113	462.315813	93.88.139.17	10.6.19.242	HTTP/X.	283	HTTP/1.1 200 OK

Можем получить ссылки на используемые на странице ресурсы

Ethernet

Оайя Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Текущий фильтр: http

No.	Time	Source	Destination	Protocol	Length	Info
24260	462.164526	93.88.139.17	10.6.19.242	HTTP	402	HTTP/1.1 200 OK (application/javascript)
24323	462.173523	93.88.139.17	10.6.19.242	HTTP	535	HTTP/1.1 200 OK (application/javascript)
24565	462.202941	93.88.139.17	10.6.19.242	HTTP	299	HTTP/1.1 200 OK (application/javascript)
24789	462.222227	93.88.139.17	10.6.19.242	HTTP	359	HTTP/1.1 404 Not Found (text/html)
24799	462.223277	10.6.19.242	93.88.139.17	504	GET /lib/jqueryscript.php/1676016890/lib/requirejs/require.min.js HTTP/1.1	
24878	462.228485	93.88.139.17	10.6.19.242	HTTP	287	HTTP/1.1 200 OK (application/javascript)
25013	462.241414	93.88.139.17	10.6.19.242	HTTP	347	HTTP/1.1 200 OK (text/css)
25043	462.299210	10.6.19.242	93.88.139.17	HTTP	99	GET /theme/image.php/classic/core/1676016890/pdf-2a HTTP/1.1
25045	462.299611	10.6.19.242	93.88.139.17	HTTP	102	GET /pluginfile.php/213538/block_html/content/324243.JPG HTTP/1.1
25049	462.300587	10.6.19.242	93.88.139.17	HTTP	96	GET /theme/image.php/classic/forum/1676016890/icon HTTP/1.1
25055	462.301740	10.6.19.242	93.88.139.17	HTTP	94	GET /theme/image.php/classic/url/1676016890/icon HTTP/1.1
25057	462.301897	10.6.19.242	93.88.139.17	HTTP	95	GET /theme/image.php/classic/book/1676016890/icon HTTP/1.1
25071	462.304124	93.88.139.17	10.6.19.242	HTTP	239	HTTP/1.1 200 OK (PNG)
25076	462.305078	93.88.139.17	10.6.19.242	HTTP/X.	425	HTTP/1.1 200 OK
25085	462.306109	93.88.139.17	10.6.19.242	HTTP/X.	235	HTTP/1.1 200 OK
25089	462.306529	10.6.19.242	93.88.139.17	HTTP	109	GET /pluginfile.php/220890/block_html/content/Protiv_pojava.JPG HTTP/1.1
25099	462.307172	93.88.139.17	10.6.19.242	HTTP/X.	79	HTTP/1.1 200 OK
25107	462.310243	10.6.19.242	93.88.139.17	HTTP	109	GET /theme/image.php/classic/core/1676016890/moodlelogo_grayhat HTTP/1.1
25113	462.315813	93.88.139.17	10.6.19.242	HTTP/X.	283	HTTP/1.1 200 OK

Internet Protocol Version 4, Src: 10.6.19.242, Dst: 93.88.139.17

Transmission Control Protocol, Src Port: 64337, Dst Port: 80, Seq: 1651, Ack: 36229, Len: 55

Reassembled TCP Segments (591 bytes): #25106(536), #25107(55)

Application/javascript

GET /theme/image.php/classic/core/1676016890/moodlelogo_grayhat HTTP/1.1\r\n

Host: education.vsu.ru\r\n

Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/108.0.0.0\r\n

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n

Referer: http://education.vsu.ru/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\r\n

Cookie: ga=GA-2.1013720269.167538268; personal_1; MoodleSession=n9a5bcvflpgeqkatoenrp7n2_id=GA\r\n

Full request URI: http://education.vsu.ru/theme/image.php/classic/core/1676016890/moodlelogo_grayhat

[HTTP request 3/9]

[Prev request in frame: 25049]

[Response in frame: 25113]

[Next request in frame: 25283]

Frame 109 [bytes] Reassembled TCP (591 bytes)

0000 47 45 54 20 2f 7a 68 65 6d 65 2f 69 6d 61 67 65 GET /theme/image

0010 2e 70 68 70 2f 63 6c 61 73 73 69 63 2f 63 6f 72 .php/classic/core

0020 65 2f 31 36 37 36 30 31 36 38 39 30 2f 6d 6f 6f 2 /1676016890/moo

0030 64 6c 65 6c 6f 67 6f 5f 67 62 61 79 68 61 6d dlelogo_grayhat

0040 48 54 50 2f 31 2e 31 6d 0a 48 6f 73 74 3a 20 HTTP/1.1: Host:

0050 65 64 75 63 61 74 69 6f 6e 76 73 65 74 2e education.vsu.ru

0060 72 75 0d 0a 43 6f 6e 65 63 74 69 6e 6a 30 20 -ru: Connection: keep-

0070 65 65 70 2f 63 6c 61 73 73 69 65 0d 0a 55 73 62 keep-alive -User

0080 2d 41 67 65 6e 74 3a 20 4d 6f 74 69 6c 6e 3f -Agent: Mozilla/

0090 65 2e 20 28 5f 69 6e 64 6f 77 20 4e 5a 20 5.0 (Win downs NT

00a0 31 30 2e 3b 30 25 57 69 6e 36 34 3b 20 68 31 2f 10.0; Win 64; x64

00b0 29 20 41 70 70 6c 65 57 65 62 4b 74 2f 35 3f) AppleWebKit/

00c0 37 2e 33 36 20 28 48 54 4d 4c 2c 20 69 6b 6b 7.36 (KHTML, lik

00d0 65 20 47 65 63 6b 6f 29 20 43 68 6f 6d 65 2f /e3636) Chrome/

00e0 31 30 38 2e 30 2e 30 2e 30 2e 53 61 66 61 72 69 108.0.0.0 Safari

00f0 25 33 37 2e 33 36 20 49 4f 50 52 39 34 2e 30 /537.36 OPB/94.0

0100 2e 30 2e 30 0d 0a 41 63 63 65 70 74 30 20 69 6d .0.0 Accept: im

0110 61 67 65 2f 61 76 69 6e 2c 69 6d 61 67 65 2f 77 e/avif,image/w

0120 65 62 70 2c 69 6d 61 67 65 2f 61 6c 6e 67 62 69 ebp,image/apng,i

0130 6d 61 67 65 2f 73 76 6f 70 6d 6c 6e 67 62 61 ebp,image/svg+xml,ima

0140 67 65 2f 2a 2c 2a 2f 2a 3b 71 3d 30 2e 3b 0d 0a ge/*,*/*;q

Скопировал ссылку в браузер и получил данное изображение



Вывод

В данной практической работе я ознакомился с гипертекстовым протоколом HTTP, его историей, различными версиями. Также узнал о базовых понятиях и терминах протокола HTTP, процедурах выполнения над ресурсом. Получил подробную информацию о том, что такое кэш и как он используется. Научился производить анализ HTTP-трафика, с помощью программы Wireshark, изучил её интерфейс, и получил минимальную базу знаний по работе и анализу в данной программе