

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

Лабораторна робота № 1
З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконав:
Студент III курсу
Групи КА-74
Чорний В.В.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи

lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl>-> Чувствительный к регистру букв Дисплейный фильтр

No.	Time	Source	Destination	Protocol	Length	Info
1430	61.156571	192.168.1.149	216.239.32.116	TCP	54	51008 → 443 [FIN, ACK] Seq=652 Ack=793 Win=15616 Len=0
1431	61.156829	192.168.1.149	216.58.209.10	TCP	54	51021 → 443 [FIN, ACK] Seq=582 Ack=8739 Win=16384 Len=0
1432	61.157278	192.168.1.149	216.58.215.78	TCP	54	51024 → 443 [FIN, ACK] Seq=650 Ack=793 Win=15616 Len=0
1433	61.157443	192.168.1.149	172.217.16.33	TCP	54	51010 → 443 [FIN, ACK] Seq=673 Ack=793 Win=15616 Len=0
1434	61.157559	192.168.1.149	172.217.16.46	TCP	54	51020 → 443 [FIN, ACK] Seq=649 Ack=793 Win=15616 Len=0
1435	61.158271	192.168.1.149	192.168.1.1	DNS	79	Standard query 0xb5c7 A clients4.google.com
1436	61.183191	192.168.1.149	192.168.1.1	DNS	79	Standard query 0xb5c7 A clients4.google.com
1437	61.234872	192.168.1.149	149.154.167.50	SSL	143	Continuation Data
1438	61.346786	192.168.1.149	192.168.1.149	TCP	66	[TCP Keep-Alive ACK] 5228 → 50982 [ACK] Seq=1 Ack=2 Win=255 Len=0 SLE=1 SRE=2
1439	61.390585	172.217.16.33	192.168.1.149	TLSv1.3	1484	Continuation Data
1440	61.390721	192.168.1.149	172.217.16.33	TCP	74	[TCP Dup ACK 1427#1] 51009 → 443 [ACK] Seq=2077 Ack=133543 Win=50944 Len=0 SLE=144983 SRE=154993 SLE=134973 SRE=143553
1441	61.390877	18.232.18.11	192.168.1.149	TCP	66	80 → 51025 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
1442	61.391070	192.168.1.149	18.232.18.11	TCP	54	51025 → 80 [ACK] Seq=1 Ack=1 Win=16384 Len=0
1443	61.391578	192.168.1.149	18.232.18.11	TCP	179	51025 → 80 [PSH, ACK] Seq=1 Ack=1 Win=16384 Len=125 [TCP segment of a reassembled PDU]
1444	61.391753	192.168.1.149	18.232.18.11	TCP	1514	51025 → 80 [PSH, ACK] Seq=126 Ack=1 Win=16384 Len=1460 [TCP segment of a reassembled PDU]
1445	61.391756	192.168.1.149	18.232.18.11	HTTP	1153	POST /bulk_safe HTTP/1.1
1446	61.670638	192.168.1.149	149.154.167.50	TCP	143	[TCP Retransmission] 50267 → 443 [PSH, ACK] Seq=615 Ack=2670 Win=533 Len=89

> Frame 1445: 1153 bytes on wire (9224 bits), 1153 bytes captured (9224 bits) on interface Device\NPF{E7910711-2CFD-4CF3-A912-85868977E86D}, id 0
> Ethernet II, Src: AzureWav_87:73:0d (74:c6:3b:87:73:0d), Dst: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b)
> Internet Protocol Version 4, Src: 192.168.1.149, Dst: 18.232.18.11
> Transmission Control Protocol, Src Port: 51025, Dst Port: 80, Seq: 1586, Ack: 1, Len: 1099
> [3 Reassembled TCP Segments (2684 bytes): #1443(125), #1444(1460), #1445(1099)]
▼ Hypertext Transfer Protocol
 > POST /bulk_safe HTTP/1.1\r\n

0020 12 0b c7 51 08 50 d3 e2 28 45 5a 4a 4b 07 58 15 -Q-P... (P)NK-P.
0030 00 40 04 86 00 00 65 72 5f 73 68 61 31 5c 22 3a -@....er_shalV.
0040 5c 22 39 44 31 42 37 33 31 46 45 41 33 45 42 45 -\901B73 1FA3EBE
0050 38 38 34 30 43 38 43 36 45 45 43 43 30 42 42 41 -8840C8C6 ECC08BA
0060 46 36 43 45 39 46 37 31 30 30 5c 22 7d 2c 7b 5c -F6CE9F71 00A"),{\n
0070 22 75 6e 69 71 75 65 73 65 72 69 64 5c 22 3a -"uniqueu serid":\n
0080 5c 22 37 34 63 36 33 62 38 37 37 33 30 63 38 37 -\74c63b 87730c87
0090 30 36 5c 22 2c 5c 22 69 6e 73 74 61 6c 6c 65 72 -06"),\n i nstaller
00a0 73 65 73 73 69 6f 6e 69 64 5c 22 3a 5c 22 37 44 -sessioni d":\n7D
00b0 30 30 35 33 36 30 5c 22 2c 5c 22 6f 73 76 65 72 -005360"),\nosver
00c0 73 69 6f 6e 5c 22 3a 5c 22 31 30 2e 30 2e 31 34 -sion":\n "10.0.14
00d0 33 39 33 5c 22 2c 5c 22 6f 73 6c 61 6e 67 5c 22 -393"),\n oslang\n
00e0 3a 5c 22 31 30 34 39 5c 22 2c 5c 22 63 70 75 5c -:\n1049),\n\ncpu\n

Frame (1153 bytes) Reassembled TCP (2684 bytes)
Transmission Control Protocol (tcp), 20 байты

Пакеты: 3482 · Показаны: 3482 (100.0%) Профиль: Default

lab1.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
1445	61.391756	192.168.1.149	18.232.18.11	HTTP	1153	POST /bulk_safe HTTP/1.1
1472	61.807318	18.232.18.11	192.168.1.149	HTTP	304	HTTP/1.1 200 OK (application/json)
3041	88.496871	192.168.1.149	128.119.245.12	HTTP	549	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3044	88.684489	128.119.245.12	192.168.1.149	HTTP	492	HTTP/1.1 200 OK (text/html)
3046	88.991383	192.168.1.149	128.119.245.12	HTTP	481	GET /favicon.ico HTTP/1.1
3048	89.240971	128.119.245.12	192.168.1.149	HTTP	538	HTTP/1.1 404 Not Found (text/html)
3332	140.191152	5.45.62.118	192.168.1.149	HTTP	615	HTTP/1.1 200 OK
3334	140.312533	192.168.1.149	5.45.62.118	HTTP	344	GET /R/A28KIGU2ZTA2NGFhMfHNTmRmGRhMDY4YjE0YTEyEjYyZmFhEgQAEIgcGhK_CgcIBB8D2od6MgoIBB8D2od6GIAK0NmSoJgBQicJrgEdXf5ZNnO3PfdkPzD3Jq...
3404	147.491474	192.168.1.149	149.154.167.50	HTTP	94	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
3405	147.491560	192.168.1.149	149.154.167.51	HTTP	94	POST /api HTTP/1.1 (application/x-www-form-urlencoded)

Checksum: 0x0486 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (1099 bytes)
TCP segment data (1099 bytes)

0030 00 40 04 86 00 00 65 72 5f 73 68 61 31 5c 22 3a -@....er_shalV.
0040 5c 22 39 44 31 42 37 33 31 46 45 41 33 45 42 45 -\901B73 1FA3EBE
0050 38 38 34 30 43 38 43 36 45 45 43 43 30 42 42 41 -8840C8C6 ECC08BA
0060 46 36 43 45 39 46 37 31 30 30 5c 22 7d 2c 7b 5c -F6CE9F71 00A"),{\n
0070 22 75 6e 69 71 75 65 73 65 72 69 64 5c 22 3a -"uniqueu serid":\n
0080 5c 22 37 34 63 36 33 62 38 37 37 33 30 63 38 37 -\74c63b 87730c87
0090 30 36 5c 22 2c 5c 22 69 6e 73 74 61 6c 6c 65 72 -06"),\n i nstaller
00a0 73 65 73 73 69 6f 6e 69 64 5c 22 3a 5c 22 37 44 -sessioni d":\n7D
00b0 30 30 35 33 36 30 5c 22 2c 5c 22 6f 73 76 65 72 -005360"),\nosver
00c0 73 69 6f 6e 5c 22 3a 5c 22 31 30 2e 30 2e 31 34 -sion":\n "10.0.14
00d0 33 39 33 5c 22 2c 5c 22 6f 73 6c 61 6e 67 5c 22 -393"),\n oslang\n
00e0 3a 5c 22 31 30 34 39 5c 22 2c 5c 22 63 70 75 5c -:\n1049),\n\ncpu\n
00f0 22 3a 74 72 75 65 2c 5c 22 76 65 72 73 69 6f 6e -":true,\n"version
0100 5c 22 3a 31 36 38 34 32 37 35 32 2c 5c 22 69 6e -\n":16842.752,\n"in

Frame (1153 bytes) Reassembled TCP (2684 bytes)
Hypertext Transfer Protocol: Protocol

Пакеты: 3482 · Показаны: 10 (0.3%) Профиль: Default

Wireshark - Пакет 1445 - lab1.pcapng

Frame 1445: 1153 bytes on wire (9224 bits), 1153 bytes captured (9224 bits) on interface \Device\NPF_{E7910711-2CFD-4CF3-A912-85B68977E86D}, id 0

Ethernet II, Src: AzureWav_87:73:0d (74:c6:3b:87:73:0d), Dst: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b)

Internet Protocol Version 4, Src: 192.168.1.149, Dst: 18.232.18.11

Transmission Control Protocol, Src Port: 51025, Dst Port: 80, Seq: 1586, Ack: 1, Len: 1099

Source Port: 51025
Destination Port: 80
[Stream index: 34]
[TCP Segment Len: 1099]
Sequence number: 1586 (relative sequence number)
Sequence number (raw): 3550619718
[Next sequence number: 2685 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1582189319
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)

Checksum: 0x0486
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1099 bytes)
TCP segment data (1099 bytes)

0000 b0 48 7a e0 a2 7b 74 c6 3b 87 73 0d 08 00 45 00 -H2--(t; ;s---E-
0010 04 73 3d dc 40 00 80 06 d1 78 c0 a8 01 95 12 e8 -s=@--- -x-----
0020 12 0b c7 51 00 50 d3 a2 28 46 5e 4e 4b 07 50 18 ---Q.P--- (FNMK P-
0030 00 40 04 86 00 00 65 72 5f 73 68 61 31 5c 22 3a -@---er _sha1\":
0040 5c 22 39 44 31 42 37 33 31 46 45 41 33 45 42 45 \\'9D1B73 1FEA3EBE
0050 38 38 34 30 43 38 43 36 45 45 43 41 30 42 42 41 8840C8C6 EEC08BBA
0060 46 36 43 45 39 46 37 31 30 30 5c 22 7d 2c 7b 5c F6CE9F71 00\").{\
0070 22 75 6e 69 71 75 65 75 73 65 72 69 64 5c 22 3a \"unique serid\":
0080 5c 22 37 34 63 36 33 62 38 37 33 30 63 38 37 \\'74c63b 87730c87
0090 30 36 5c 22 2c 5c 22 69 6e 73 74 61 6c 6c 65 72 06\").i nstaller
00a0 73 65 73 73 69 6f 6e 69 64 5c 22 3a 5c 22 37 44 sessioni d\":\"7D
00b0 30 30 35 33 36 30 5c 22 2c 5c 22 6f 73 76 65 72 005360\").\"osver
00c0 73 69 6f 6e 5c 22 3a 5c 22 31 30 2e 30 2e 31 34 sion\":\"10.0.14
00d0 33 39 33 5c 22 2c 5c 22 6f 73 6c 61 6e 67 5c 22 393\").\" oslang\"
00e0 3a 5c 22 31 30 34 39 5c 22 2c 5c 22 63 70 75 5c :\"1049\").\"cpu\
00f0 22 3a 74 72 75 65 2c 5c 22 76 65 72 73 69 6f 6e \":true,\" version
0100 5c 22 3a 31 36 38 34 32 37 35 32 2c 5c 22 69 6e \":16842 752,\"in

Frame (1153 bytes) Reassembled TCP (2684 bytes)

No.: 1445 - Time: 61.391756 - Source: 192.168.1.149 - Destination: 18.232.18.11 - Protocol: HTTP - Length: 1153 - Info: POST /bulk_safe HTTP/1.1

Frame (1153 bytes) Reassembled TCP (2684 bytes)

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1 099 байты

Пакеты: 3482 - Показаны: 10 (0,3%)

Профиль: Default

Wireshark - Печать

Формат Пакета

☒ Строка итогов

☒ Включить заголовки столбцов

☒ Подробности:

☐ Все свернуто

☒ Как отображено

☐ Все развёрнуто

☐ Байты

☐ Печатайте каждый пакет на новой странице

Диапазон Пакетов

☒ Все пакеты 3482 10

☐ Только выбранные пакеты 1 1

☐ Только помеченные пакеты 0 0

☐ От первого к последнему помеченному 0 0

☐ Диапазон: 0 0

☐ Удалить пропущенные пакеты 0 0

Page Setup... Print... Cancel Help

Checksum: 0x0486 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1099 bytes)
TCP segment data (1099 bytes)

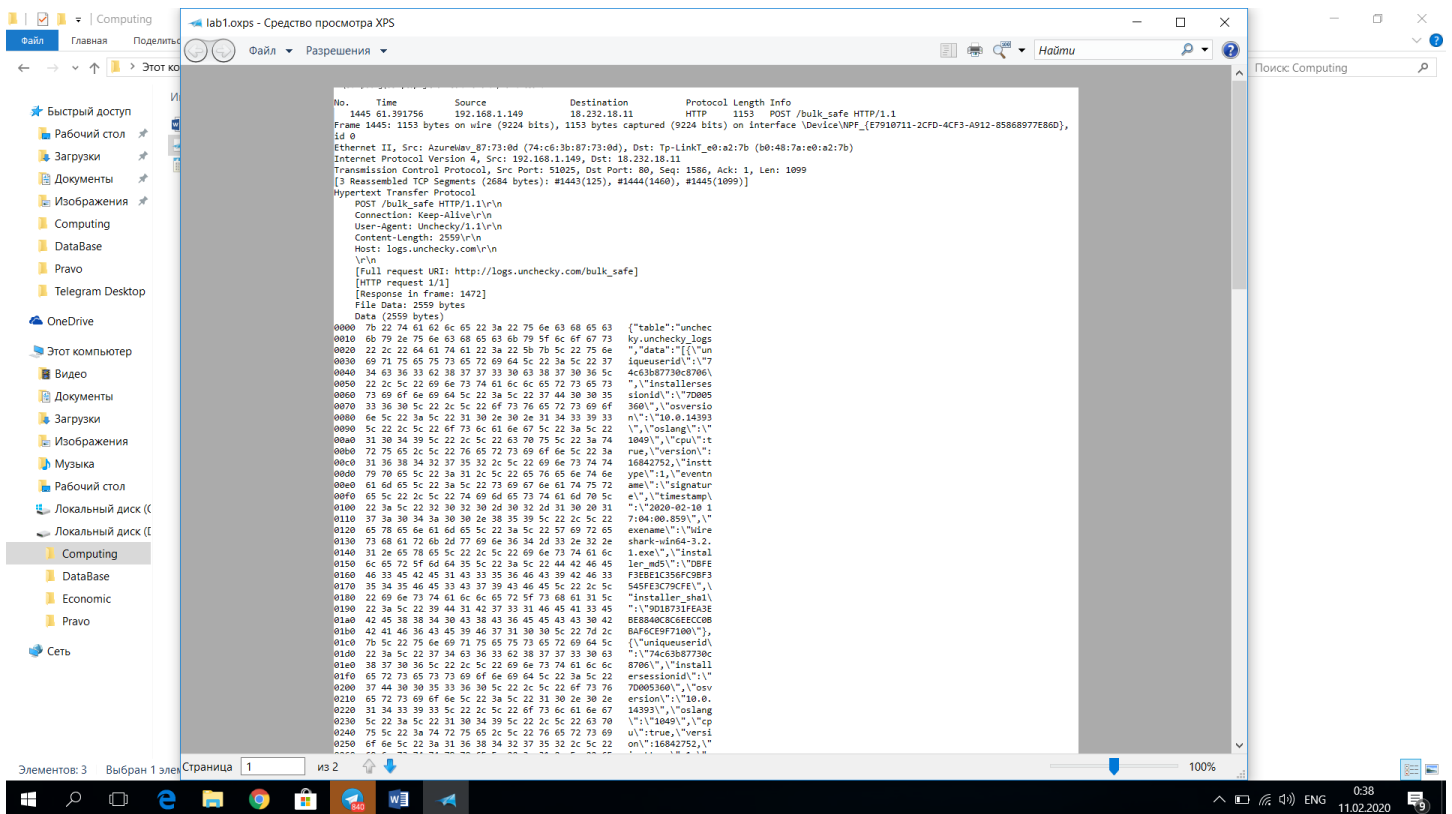
0030 00 40 04 86 00 00 65 72 5f 73 68 61 31 5c 22 3a -@---er _sha1\":
0040 5c 22 39 44 31 42 37 33 31 46 45 41 33 45 42 45 \\'9D1B73 1FEA3EBE
0050 38 38 34 30 43 38 43 36 45 45 43 41 30 42 42 41 8840C8C6 EEC08BBA
0060 46 36 43 45 39 46 37 31 30 30 5c 22 7d 2c 7b 5c F6CE9F71 00\").{\
0070 22 75 6e 69 71 75 65 75 73 65 72 69 64 5c 22 3a \"unique serid\":
0080 5c 22 37 34 63 36 33 62 38 37 33 30 63 38 37 \\'74c63b 87730c87
0090 30 36 5c 22 2c 5c 22 69 6e 73 74 61 6c 6c 65 72 06\").i nstaller
00a0 73 65 73 73 69 6f 6e 69 64 5c 22 3a 5c 22 37 44 sessioni d\":\"7D
00b0 30 30 35 33 36 30 5c 22 2c 5c 22 6f 73 76 65 72 005360\").\"osver
00c0 73 69 6f 6e 5c 22 3a 5c 22 31 30 2e 30 2e 31 34 sion\":\"10.0.14
00d0 33 39 33 5c 22 2c 5c 22 6f 73 6c 61 6e 67 5c 22 393\").\" oslang\"
00e0 3a 5c 22 31 30 34 39 5c 22 2c 5c 22 63 70 75 5c :\"1049\").\"cpu\
00f0 22 3a 74 72 75 65 2c 5c 22 76 65 72 73 69 6f 6e \":true,\" version
0100 5c 22 3a 31 36 38 34 32 37 35 32 2c 5c 22 69 6e \":16842 752,\"in

Frame (1153 bytes) Reassembled TCP (2684 bytes)

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1 099 байты

Пакеты: 3482 - Показаны: 10 (0,3%)

Профиль: Default



Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
TCP, HTTP, DNS, SSL, TLSv1.3, ICMPv6, UDP

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
ICP, Ethernet II, HTTP, TCP.

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

Пройшло 0,002954 с.

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

Запит:

Вихідна:192.168.1.149

Цільова:18.232.18.11

Відповідь:

Вихідний:18.232.18.11

Цільовий:192.168.1.149

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

```
POST /bulk_safe HTTP/1.1
```

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

```
HTTP/1.1 200 OK (application/json)
```

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.