

## Дементьев Никита Евгеньевич

Сначала заходим в Wireshark и нажимаем кнопку захвата пакетов, после чего нажимаю правой кнопкой мыши по интересующему пакету и выбираю функцию следовать, появится окно с выбором протоколов, в данном случае выбираю протокол HTTP

Time	Source	Destination	Protocol	Length	Info
221 21.932072	192.168.37.244	192.168.9.9	TCP	66	60093 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
222 21.932543	192.168.9.9	192.168.37.244	TCP	66	3128 → 60093 [SYN, ACK] Seq=0 Ack=1 Win=26880 Len=0 MSS=8960 SACK_PERM WS=128
223 21.932645	192.168.37.244	192.168.9.9	TCP	54	60093 → 3128 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
224 21.933254	192.168.37.244	192.168.9.9	HTTP	296	CONNECT ya.ru:443 HTTP/1.1
225 21.935212	192.168.9.9	192.168.37.244	TCP	60	3128 → 60093 [ACK] Seq=1 Ack=243 Win=28032 Len=0
226 21.935212	192.168.9.9	192.168.37.244	TCP	1514	3128 → 60093 [ACK] Seq=1 Ack=243 Win=28032 Len=1460 [TCP segment of a reassembled PDU]
227 21.935213	192.168.9.9	192.168.37.244	TCP	1514	3128 → 60093 [ACK] Seq=1461 Ack=243 Win=28032 Len=1460 [TCP segment of a reassembled PDU]
228 21.935217	192.168.9.9	192.168.37.244	HTTP	1306	HTTP/1.1 407 Proxy Authentication Required (text/html)
229 21.935217	192.168.9.9	192.168.37.244	TCP	60	3128 → 60093 [FIN, ACK] Seq=4173 Ack=243 Win=28032 Len=0
230 21.935353	192.168.37.244	192.168.9.9	TCP	54	60093 → 3128 [ACK] Seq=243 Ack=4173 Win=2102272 Len=0
231 21.935788	192.168.37.244	192.168.9.9	TCP	54	60093 → 3128 [ACK] Seq=243 Ack=4174 Win=2102272 Len=0
232 21.936079	192.168.37.244	192.168.9.9	TCP	54	60093 → 3128 [RST, ACK] Seq=243 Ack=4174 Win=0 Len=0

Рисунок 1. – захват пакетов через Wireshark для обращения на ya.ru

На рис.1 показано обращение к ya.ru по протоколу HTTP. Сначала происходит установление соединения через протокол TCP, он отправляет флаг синхронизации (SYN), после чего уже получает в ответ флаги подтверждения синхронизации (SYN, ACK), затем отправляется флаг ACK, который говорит о том, что процесс установки соединения завершен. Далее видно строку №224, где написано, что соединение по HTTP установлено. Далее видно пакеты передаются по сети, на строках 226 и 227 в скобках написано, что пакет содержит часть более длинного прикладного сообщения или документа, а полное сообщение или документ собирается из нескольких пакетов. Затем остановив анализ появилось сообщение 228 - проху authentication required, оно говорит о том что требуется аутентификация с помощью прокси сервера(делал анализ на работе, поэтому присутствует проху), затем идет сообщение TCP протокола от проху о том, что сессия завершена(FIN), и компьютер посылает подтверждение(ACK), также появляется флаг RST, который говорит о том, что соединение требуется немедленно завершить, появляется из-за остановки захвата трафика.

> Frame 224: 296 bytes on wire (2368 bits), 296 bytes captured (2	0000 90 e2 ba 54 72 f4 24 4b fe 8b 86 a3 08 00 45 00	...Tr...SK...E...
> Ethernet II, Src: ASUSTekC_8b:86:a3 (24:4b:fe:8b:86:a3), Dst: I	0010 01 1a 64 9f 40 00 80 06 00 00 c0 a8 25 f4 c0 a8	...d...%...
> Internet Protocol Version 4, Src: 192.168.37.244, Dst: 192.168.	0020 09 09 ea bd 0c 38 66 52 56 6c 5b eb 32 e5 50 18	...8fr V1[.2.P...
> Transmission Control Protocol, Src Port: 60093, Dst Port: 3128,	0030 20 14 b1 5a 00 00 43 4f 4e 4e 45 43 54 20 79 61	...Z...CO NNECT ya
> Hypertext Transfer Protocol	0040 2e 72 75 3a 34 34 33 20 48 54 54 50 2f 31 2e 31	...ru:443 HTTP/1.1
	0050 0d 0a 48 6f 73 74 3a 20 79 61 2e 72 75 3a 34 34	...Host: ya.ru:44
	0060 33 0d 0a 50 72 6f 78 79 2d 43 6f 6e 6e 65 63 74	3...Proxy -Connect
	0070 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d	ion: kee p-alive
	0080 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a	...User-Agent: Moz
	0090 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77	illa/5.0 (Window
	00a0 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34	s NT 10.0; Win64
	00b0 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b	; x64) A ppleWebK
	00c0 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c	it/537.3 6 (KHTML
	00d0 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68	, like Gecko) Ch
	00e0 72 6f 6d 65 2f 31 31 34 2e 30 2e 30 2e 30 20 59	rome/114.0.0.0 Y
	00f0 61 42 72 6f 77 73 65 72 2f 32 33 2e 37 2e 31 2e	aBrowser /23.7.1.
	0100 31 32 36 36 20 28 63 6f 72 70 29 20 59 6f 77 73	1266 (co rp) Yows
	0110 65 72 2f 32 2e 35 20 53 61 66 61 72 69 2f 35 33	er/2.5 S afari/53
	0120 37 2e 33 36 0d 0a 0d 0a	7.36....

Рисунок 2 – состав кадра протокола HTTP

На рис.2 можно увидеть какие протоколы использовались для подключения, для примера рассмотрим HTTP, так как он находится на прикладном уровне и для его передачи используется TCP, IPv4, Ethernet2, после чего он заворачивается в кадр и уже идет по кабелю. IPv4 содержит в себе ip-адреса source-откуда, destination - куда (3 уровень osi). Ethernet2 содержит в MAC-адреса (2 уровень OSI). Frame состоит из служебной информации и данных. Справа показано как кадр выглядит в общем, он представляется в 16-ой системе счисления и расшифровка. Наводясь на биты можно увидеть из чего состоит сообщение протокола (пр.:контрольная сумма, время жизни(TTL)).

Также в качестве примера рассмотрим sip протокол, на рис.3 показаны все пакеты, которые принимали участие в звонке.

	Time ^	Source	Destination	Protocol	Length	Info
621	13.342134	192.168.64...	192.168.64...	SIP/SDP	1438	Request: INVITE sip:9796@192.168.64.94:5060
622	13.349052	192.168.64...	192.168.64...	SIP	455	Status: 100 Trying
623	13.422103	192.168.64...	192.168.64...	SIP	681	Status: 180 Ringing
730	16.305159	192.168.64...	192.168.64...	SIP/SDP	1134	Status: 200 OK (INVITE)
732	16.313614	192.168.64...	192.168.64...	SIP	477	Request: ACK sip:9796@192.168.64.94:5060
1148	27.269881	192.168.64...	192.168.64...	SIP	523	Request: BYE sip:4011@192.168.64.10:5060
1149	27.273102	192.168.64...	192.168.64...	SIP	557	Status: 200 OK (BYE)

Рисунок 3 – телефонный сеанс по sip протоколу

Сначала идет запрос INVITE для приглашения другого абонента в сессию, затем приходят сообщения 100, 180 и 200, они говорят о том, что соединение

установлено, после чего в АСК происходит разговор, когда разговор заканчивается отправляется запрос BYE на окончание сессии и подтверждение 200.

В Wireshark можно перейти на вкладку телефония – потоки sip, появится окно, в котором можно выбрать данную сессию, нажать Flow Sequence, после чего появится схема, на которой показано откуда и кому идут запросы.

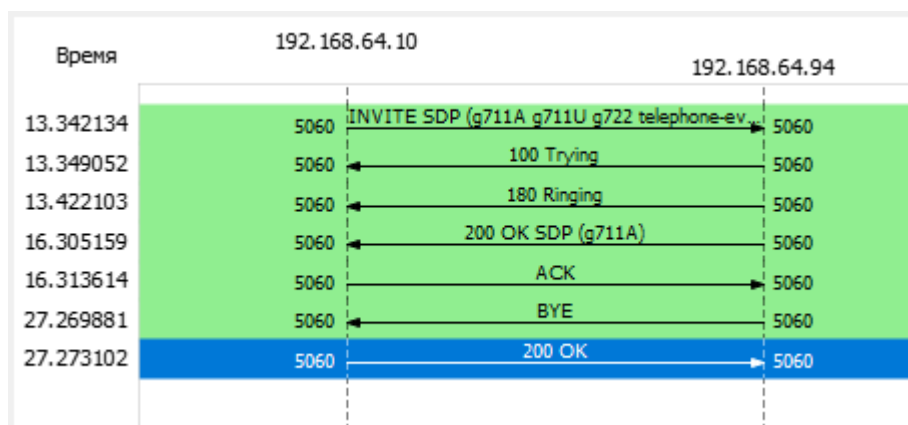


Рисунок 4 – схема запросов

На рис.5 показано какие протоколы используются для sip-телефонии и как выглядит пакет в 16-ом виде, в данном случае в телефонии нам не требуется проверка о том, что сообщение дошло, поэтому здесь используется UDP вместо TCP, далее аналогично протоколу HTTP используется ipv4 и Ethernet2, все эти данные помещаются в кадр после чего отправляются по кабелю

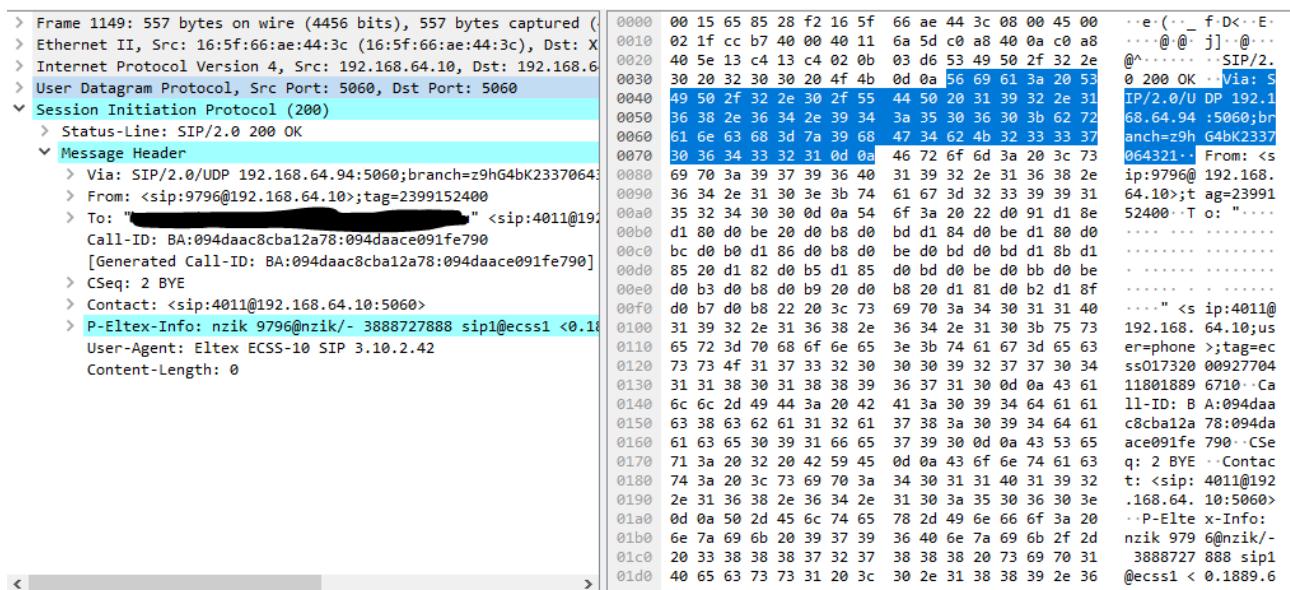


Рисунок 5 – состав кадра протокола http