Дементьев Никита Евгеньевич

Сначала заходим в Wires hark 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. Дальше 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 - proxy authentication required, оно говорит о том что требуется аутентификация с помощью прокси сервера(делал анализ на работе, поэтому присутствует proxy), затем идет сообщение TCP протокола от proxy 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.

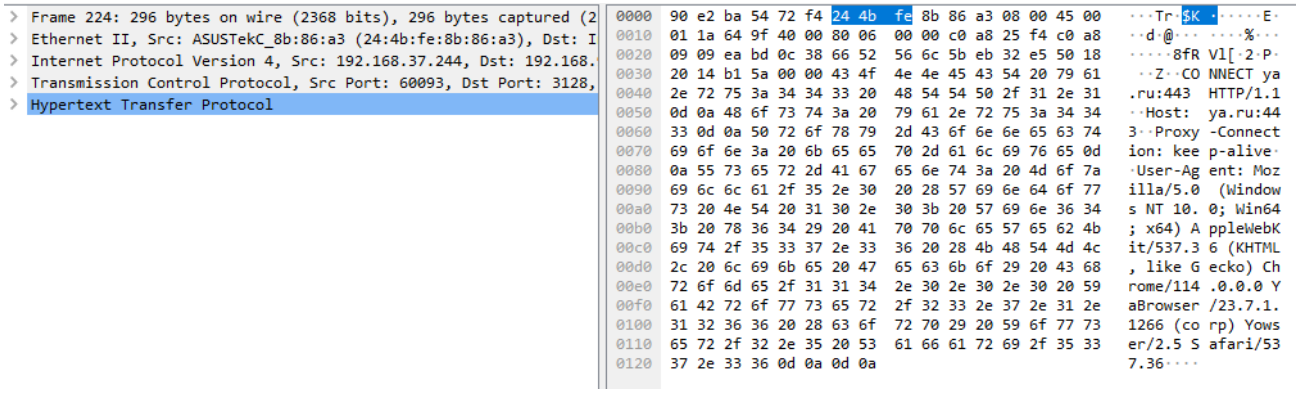

Рисунок 2 – состав кадра протокола HTTP

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 ACK 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.

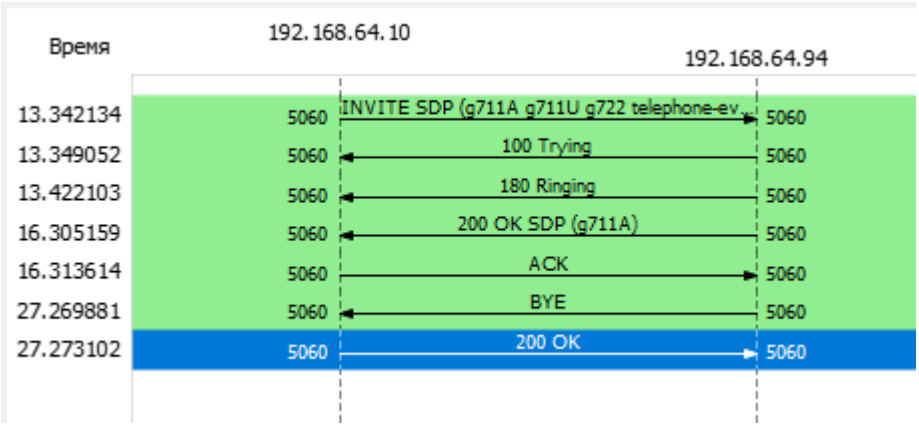

Рисунок 4 – схема запросов

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

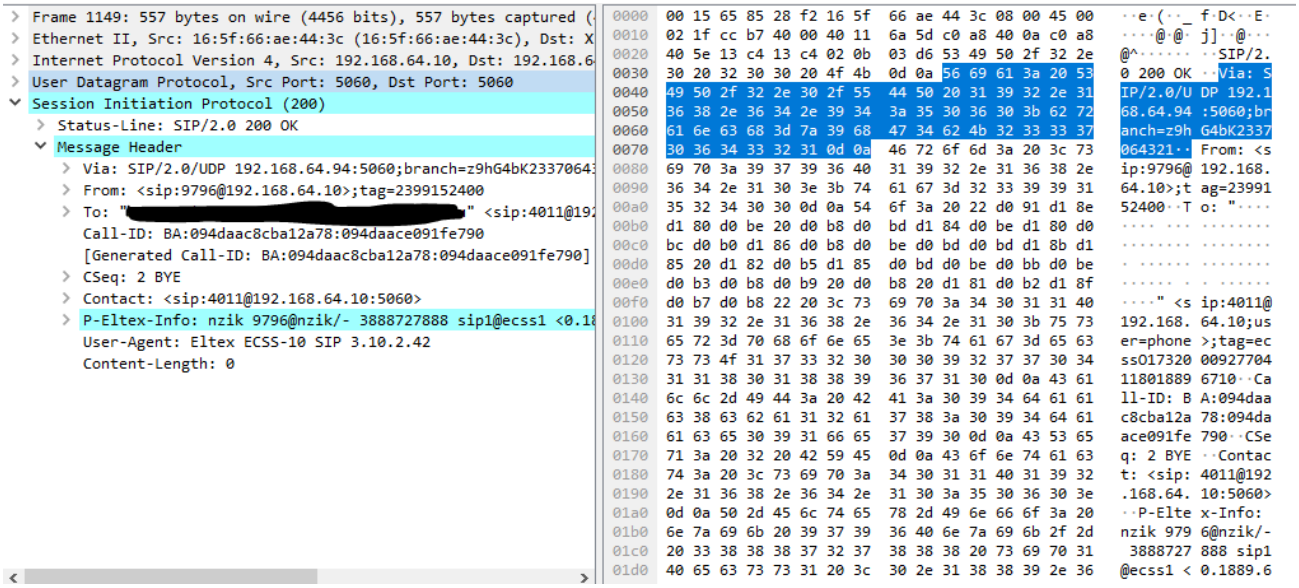

Рисунок 5 – состав кадра протокола http