

2. С помощью Wireshark или Cisco Packet Tracer отследить трафик, идущий по протоколу HTTP и HTTPS. В чем разница? Попробовать отследить трафик в Wireshark, подключаясь к сервисам Google (например, youtube.com) с помощью браузера Google Chrome. Какой протокол используется для доступа к веб-сервисам?

По протоколу http:

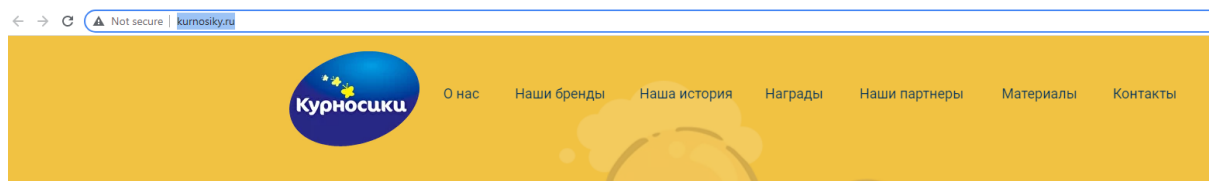


Рис 1. Сайт с незащищенным протоколом

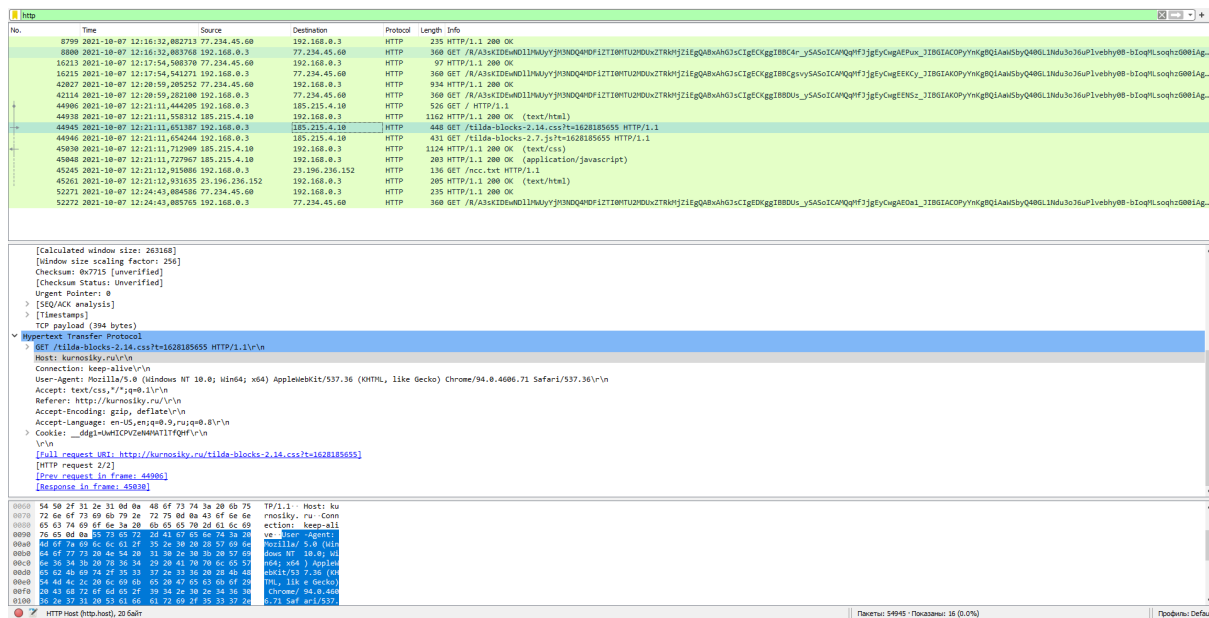


Рис 2. Пример отслеживания трафика сайта с незащищенным протоколом.

Подключимся к ютубу

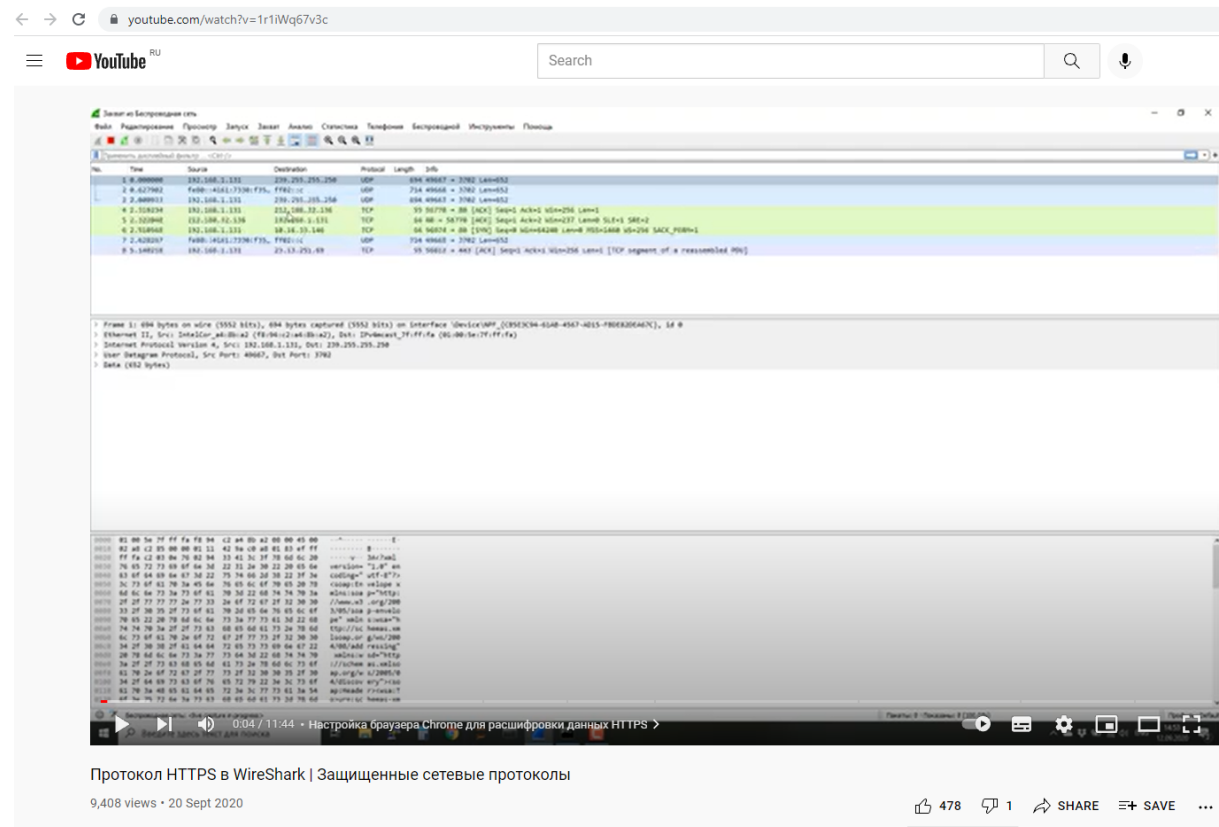


Рис 3. Открытие видео на ютуб.

60	Time	Source	Destination	Protocol	Length	Info
	95 2021-10-07 12:15:43,204716	192.168.0.3	74.125.205.95	QUIC	1392	Initial, DCID=e9a29922d5af34e, PN=1, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO
	96 2021-10-07 12:15:43,205037	192.168.0.3	74.125.205.95	QUIC	118	0-RTT, DCID=e9a29922d5af34e
	97 2021-10-07 12:15:43,205742	192.168.0.3	64.233.162.94	QUIC	108	Initial, DCID=e2190997bde89dc, PN=1, PING, PADDING, PING, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, CRYPTO, PADDING
	98 2021-10-07 12:15:43,206080	192.168.0.3	64.233.162.94	QUIC	115	0-RTT, DCID=e219097bde89dc
	100 2021-10-07 12:15:43,216398	64.233.162.94	192.168.0.3	QUIC	1392	Protected Payload (KWP)
	101 2021-10-07 12:15:43,216400	64.233.162.94	192.168.0.3	QUIC	664	Protected Payload (KWP)
	102 2021-10-07 12:15:43,216401	74.125.205.95	192.168.0.3	QUIC	1392	Protected Payload (KWP)
	103 2021-10-07 12:15:43,216403	74.125.205.95	192.168.0.3	QUIC	664	Protected Payload (KWP)
	104 2021-10-07 12:15:43,218439	192.168.0.3	64.233.162.94	QUIC	1392	Handshake, DCID=e219097bde89dc
	105 2021-10-07 12:15:43,218752	192.168.0.3	64.233.162.94	QUIC	75	Protected Payload (KWP), DCID=e219097bde89dc
	106 2021-10-07 12:15:43,219054	192.168.0.3	74.125.205.95	QUIC	121	Handshake, DCID=e9a29922d5af34e
	107 2021-10-07 12:15:43,219800	192.168.0.3	74.125.205.95	QUIC	75	Protected Payload (KWP), DCID=e9a29922d5af34e
	111 2021-10-07 12:15:43,227287	64.233.162.94	192.168.0.3	QUIC	125	Protected Payload (KWP)
	117 2021-10-07 12:15:43,228075	74.125.205.95	192.168.0.3	QUIC	125	Protected Payload (KWP)
	118 2021-10-07 12:15:43,253183	192.168.0.3	64.233.162.94	QUIC	75	Protected Payload (KWP), DCID=e219097bde89dc
	136 2021-10-07 12:15:43,255267	192.168.0.3	74.125.205.95	QUIC	75	Protected Payload (KWP), DCID=e9a29922d5af34e
	167 2021-10-07 12:15:43,461567	192.168.0.3	173.194.220.119	QUIC	1392	Initial, DCID=e0b06a705460989, PN=1, CRYPTO, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PING, CRYPTO, PADDING, CRYPTO
	168 2021-10-07 12:15:43,461595	192.168.0.3	173.194.220.119	QUIC	118	0-RTT, DCID=e0b06a705460989
	169 2021-10-07 12:15:43,462092	192.168.0.3	173.194.220.119	QUIC	62	0-RTT, DCID=e0b06a705460989

Рис 4. Полученный трафик по протоколу quic.

3. С помощью Wireshark отследить трафик при работе с обычным ftp (найти любой ftp-ресурс и подключиться к нему, через браузер). Можно ли через ftp передавать данные на сервер, как предлагают некоторые хостеры?

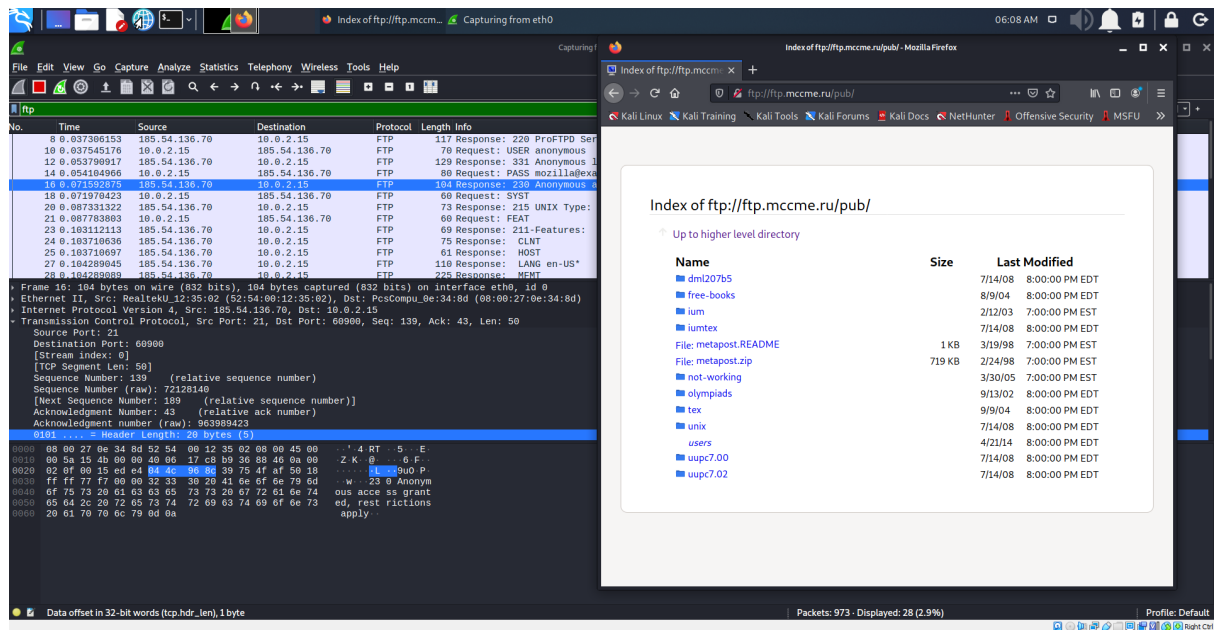


Рис 5. Пример подключения к ftp ресурсу.

Да, данные передавать можно. Но есть одно но. В ftp команды передаются открытым текстом. Что делает его далеко не самым надежным протоколом для аутентификации. Лучше использовать sFTP.