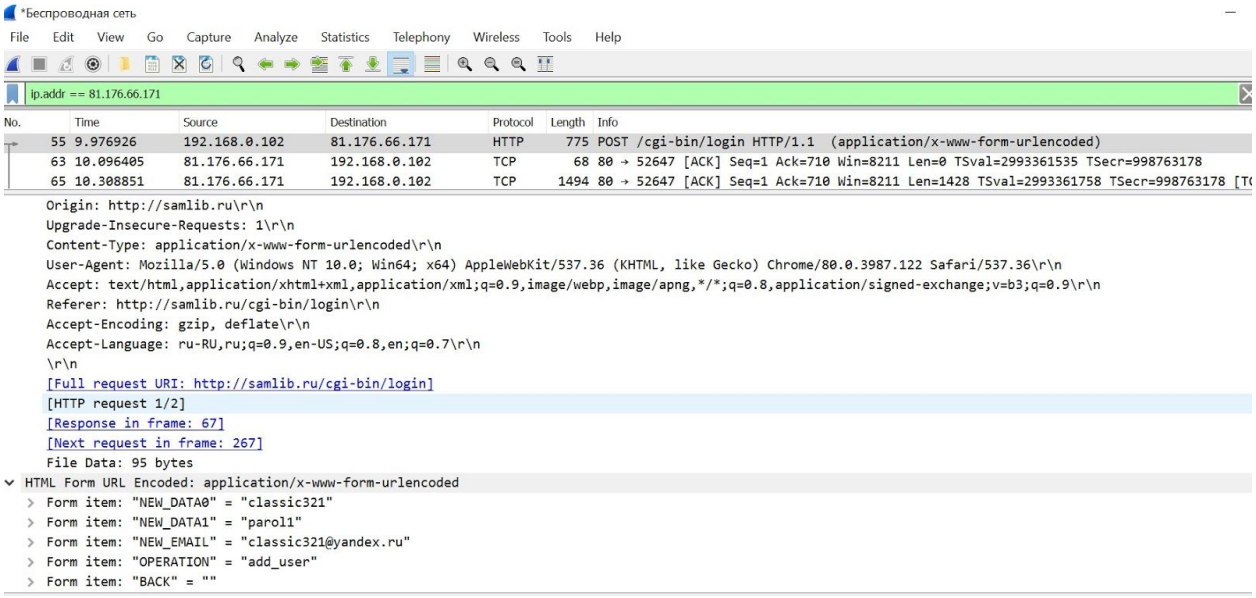
1. Работа в Wireshark.

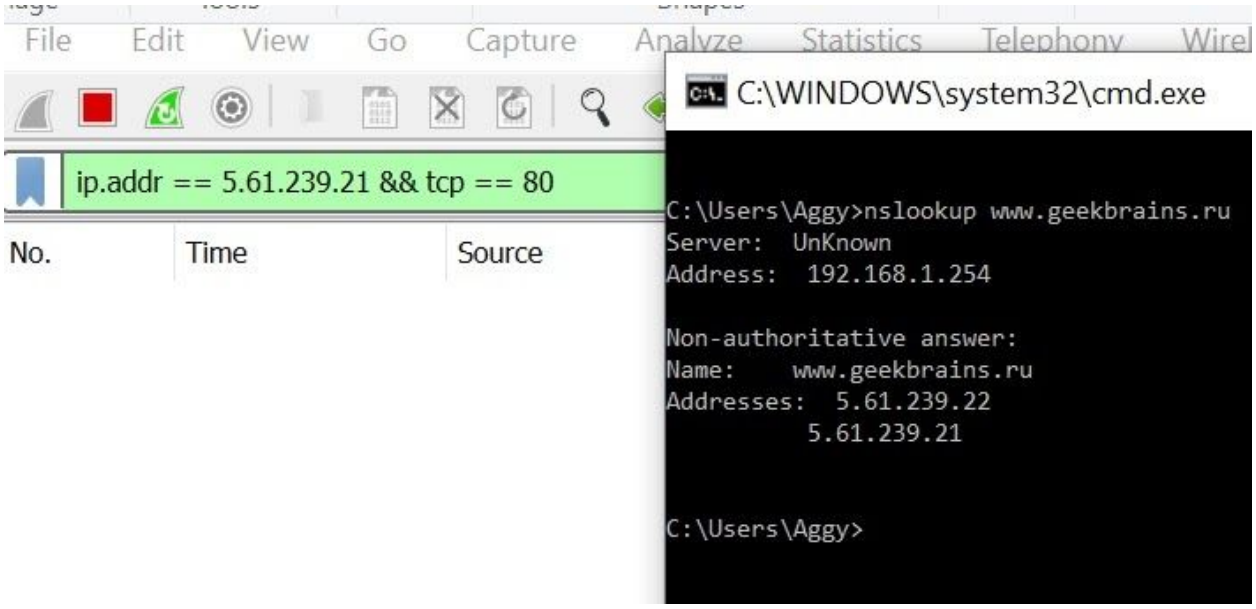
1) Запустить Wireshark, выбрать любой веб-сайт по HTTP, где требуется вход или регистрация по паролю, например зайти на http://samlib.ru (или другой нешифрованный Http), ввести тут http://samlib.ru/cgi-bin/login любой пароль. Какую информацию можно узнать с помощью Wireshark?

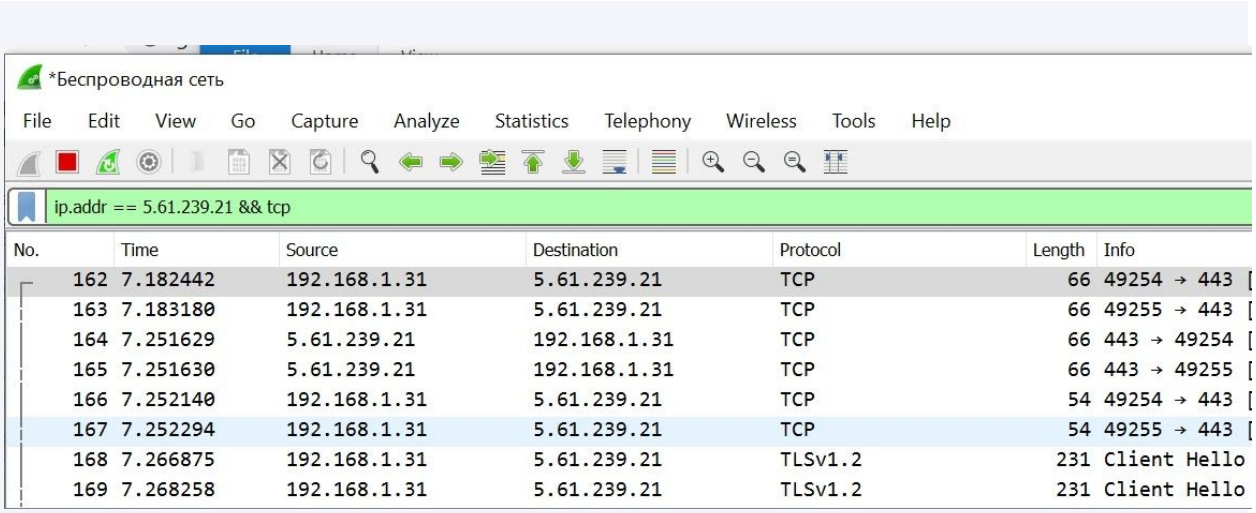


Можно узнать всю передаваемую информацию

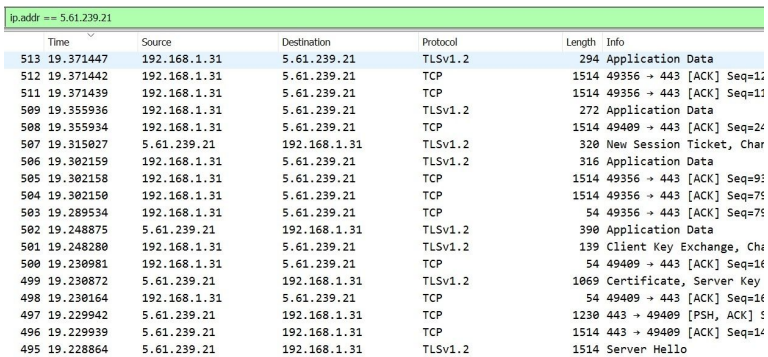
2. С помощью Wireshark или Cisco Packet Tracer отследить трафик, идущий по протоколу HTTP и HTTPS. В чем разница? Попробовать отследить трафик в Wireshark, подключаясь к сервисам Google (например, youtube.com) с помощью браузера Google Chrome. Какой протокол используется для доступа к веб-сервисам?

На примере сайта geekbrains не увидела http трафика, видимо http переадресован на https





При авторизации на сайте включился протокол TLSv1.2



После запуска видео на сайте почему-то ip адрес сайта сменился и выдаче wireshark появилось много адресов в формате ASCII. Не знаю принадлежат ли эти адреса сервисам geekbrains или нет.

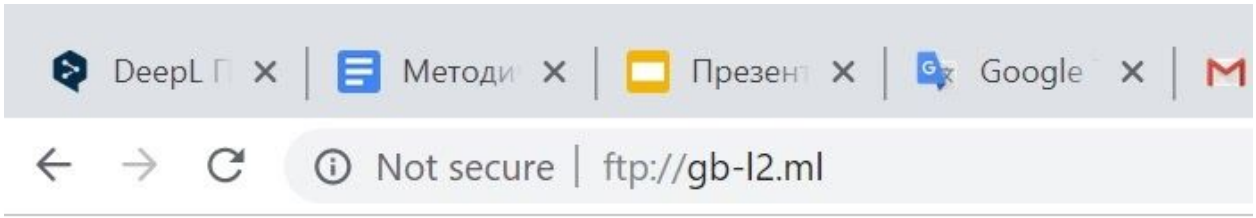
	Time	Source	Destination	Protocol	Length	Info
272…	35.736133	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.736135	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.736328	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
272…	35.737535	5.61.239.22	192.168.1.31	TLSv1.2	1251	Application
272…	35.737537	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737543	5.61.239.22	192.168.1.31	TLSv1.2	1096	Application
272…	35.737544	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737546	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737547	5.61.239.22	192.168.1.31	TLSv1.2	1251	Application
272…	35.737828	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
272…	35.738592	5.61.239.22	192.168.1.31	TLSv1.2	957	Application
274…	35.778282	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
299…	36.385647	5.61.239.22	192.168.1.31	TLSv1.2	225	Application
300…	36.426335	192.168.1.31	5.61.239.22	TCP	54	62419 → 443
382…	38.456744	5.61.239.22	192.168.1.31	TLSv1.2	198	Application
384…	38.497446	192.168.1.31	5.61.239.22	TCP	54	62419 → 443
490…	41.257167	5.61.239.22	192.168.1.31	TLSv1.2	197	Application
491…	41.299196	192.168.1.31	5.61.239.22	TCP	54	62419 → 443

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
2	0.000002	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
3	0.000003	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
4	0.000210	2a01:e34:ed78:8070:1d:16fc:2643:55c2	2600:9000:219c:d40…	TCP	74	53119 → 443 [
5	0.001026	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
6	0.001027	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
7	0.001029	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
8	0.001229	2a01:e34:ed78:8070:1d:16fc:2643:55c2	2600:9000:219c:d40…	TCP	74	53119 → 443 [
9	0.001988	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
10	0.001989	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
11	0.001990	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
12	0.001991	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
13	0.001992	2600:9000:219c:d400:1c:c1dd:3940:21	2a01:e34:ed78:8070…	TCP	1294	[TCP segment
14	0.002235	2a01:e34:ed78:8070:1d:16fc:2643:55c2	2600:9000:219c:d40…	TCP	74	53119 → 443 [

	Time	Source	Destination	Protocol	Length	Info
272…	35.736133	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.736135	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.736328	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
272…	35.737535	5.61.239.22	192.168.1.31	TLSv1.2	1251	Application
272…	35.737537	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737543	5.61.239.22	192.168.1.31	TLSv1.2	1096	Application
272…	35.737544	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737546	5.61.239.22	192.168.1.31	TCP	1514	443 → 62368
272…	35.737547	5.61.239.22	192.168.1.31	TLSv1.2	1251	Application
272…	35.737828	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
272…	35.738592	5.61.239.22	192.168.1.31	TLSv1.2	957	Application
274…	35.778282	192.168.1.31	5.61.239.22	TCP	54	62368 → 443
299…	36.385647	5.61.239.22	192.168.1.31	TLSv1.2	225	Application
300…	36.426335	192.168.1.31	5.61.239.22	TCP	54	62419 → 443
382…	38.456744	5.61.239.22	192.168.1.31	TLSv1.2	198	Application
384…	38.497446	192.168.1.31	5.61.239.22	TCP	54	62419 → 443
490…	41.257167	5.61.239.22	192.168.1.31	TLSv1.2	197	Application
491…	41.299196	192.168.1.31	5.61.239.22	TCP	54	62419 → 443

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?

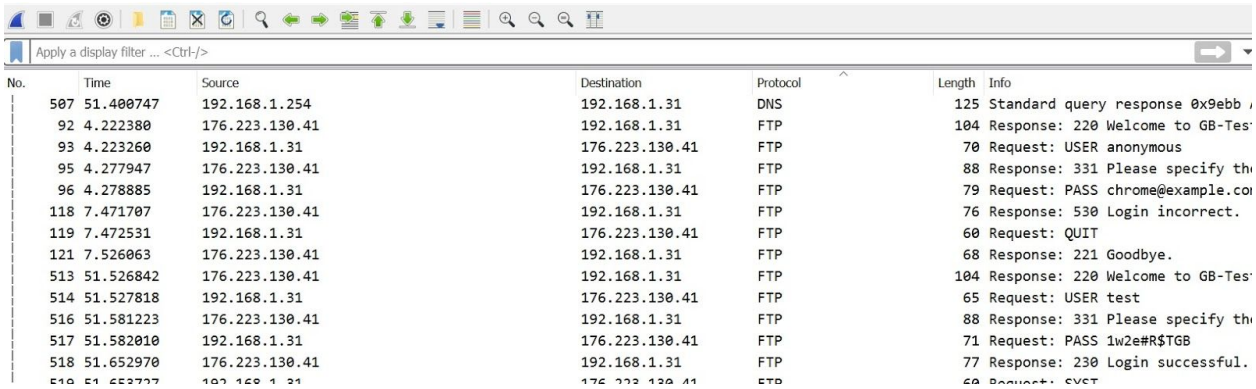
Зашла по адресу ftp:// gb-l2.ml с паролем и логином
User: test
Pass: 1w2e#R$TGB



Index of /

Name Size Date Modified

И проследила трафик в wireshark



No.	Time	Source	Destination	Protocol	Length	Info
507	51.400747	192.168.1.254	192.168.1.31	DNS	125	Standard query response 0x9ebb
92	4.222380	176.223.130.41	192.168.1.31	FTP	104	Response: 220 Welcome to GB-Tes
93	4.223260	192.168.1.31	176.223.130.41	FTP	70	Request: USER anonymous
95	4.277947	176.223.130.41	192.168.1.31	FTP	88	Response: 331 Please specify th
96	4.278885	192.168.1.31	176.223.130.41	FTP	79	Request: PASS chrome@example.co
118	7.471707	176.223.130.41	192.168.1.31	FTP	76	Response: 530 Login incorrect.
119	7.472531	192.168.1.31	176.223.130.41	FTP	60	Request: QUIT
121	7.526063	176.223.130.41	192.168.1.31	FTP	68	Response: 221 Goodbye.
513	51.526842	176.223.130.41	192.168.1.31	FTP	104	Response: 220 Welcome to GB-Tes
514	51.527818	192.168.1.31	176.223.130.41	FTP	65	Request: USER test
516	51.581223	176.223.130.41	192.168.1.31	FTP	88	Response: 331 Please specify th
517	51.582010	192.168.1.31	176.223.130.41	FTP	71	Request: PASS 1w2e#R$TGB
518	51.652970	176.223.130.41	192.168.1.31	FTP	77	Response: 230 Login successful.

Как видно в таблице, пароль и логин без всякого шифрования видны в выдаче.
Соответственно, протокол ftp является небезопасным и пользоваться им не стоит.

2. Работа с nslookup.

К сожалению не успеваю доделать дз. Недостающее дошлю к следующему уроку.