

## Задание №1.

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?

Узнал IP хоста <http://samlib.ru>, пропинговав его:

```
$ ping samlib.ru
PING samlib.ru (81.176.66.171): 56 data bytes
64 bytes from 81.176.66.171: icmp_seq=0 ttl=51 time=30.063 ms
64 bytes from 81.176.66.171: icmp_seq=1 ttl=51 time=12.770 ms
64 bytes from 81.176.66.171: icmp_seq=2 ttl=51 time=16.021 ms
64 bytes from 81.176.66.171: icmp_seq=3 ttl=51 time=11.207 ms
64 bytes from 81.176.66.171: icmp_seq=4 ttl=51 time=15.621 ms
64 bytes from 81.176.66.171: icmp_seq=5 ttl=51 time=13.510 ms
```

Через Wireshark проверил фильтр и соединение («тройное рукопожатие») с сервером <http://samlib.ru> (ip 81.176.66.171), после послали GET-запрос и получили ответ в виде HTML-страницы:

229	18.435228	192.168.0.164	81.176.66.171	TCP	78	65019 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=299343
230	18.446223	81.176.66.171	192.168.0.164	TCP	74	80 → 65019 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
231	18.446305	192.168.0.164	81.176.66.171	TCP	66	65019 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=2993439609 TSecr=1388341
234	18.658271	192.168.0.164	81.176.66.171	HTTP	462	GET / HTTP/1.1
243	18.674672	81.176.66.171	192.168.0.164	HTTP	177	HTTP/1.1 304 Not Modified

Минус «незащищенного соединения» в том, что если заполнить поля прим(<http://samlib.ru/cgi-bin/login>) и передать их методом POST на сервер, то эти данные, оказывается так легко перехватить

Wireshark packet capture showing an HTTP POST request to <http://samlib.ru/cgi-bin/login>. The packet list shows a POST request from 192.168.0.164 to 81.176.66.171. The packet details show the request body with form items: OPERATION=login, BACK=, DATA0=qwe, DATA1=123, and a password field with 12 asterisks. The packet bytes pane shows the raw data of the request.

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?

С первой попытки настроить фильтр WireShark на IP Google и YouTube не приводили к успеху как серверы меняли свои IP

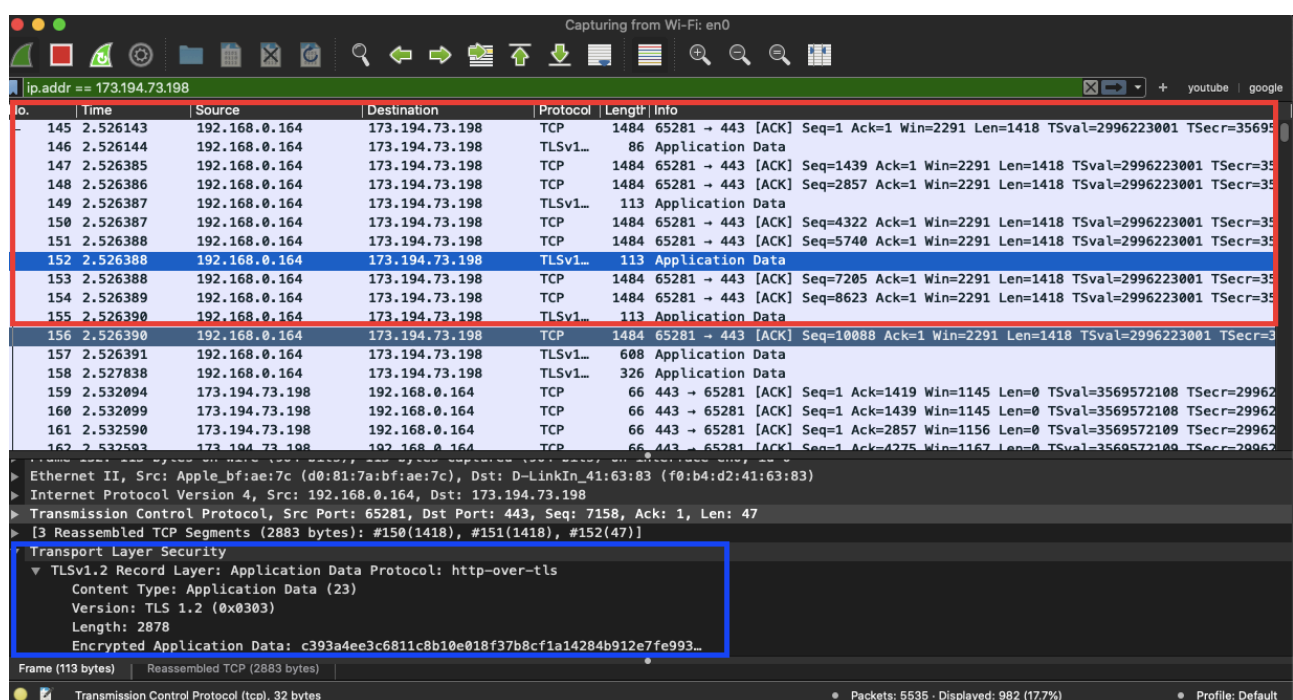
```
$ ping google.com
PING google.com (173.194.73.138): 56 data bytes
64 bytes from 173.194.73.138: icmp_seq=0 ttl=108 time=6.687 ms
64 bytes from 173.194.73.138: icmp_seq=1 ttl=108 time=6.804 ms
64 bytes from 173.194.73.138: icmp_seq=2 ttl=108 time=6.357 ms
64 bytes from 173.194.73.138: icmp_seq=3 ttl=108 time=6.701 ms
64 bytes from 173.194.73.138: icmp_seq=4 ttl=108 time=7.034 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.357/6.717/7.034/0.219 ms

$ ping google.com
PING google.com (173.194.73.101): 56 data bytes
64 bytes from 173.194.73.101: icmp_seq=0 ttl=108 time=6.592 ms
64 bytes from 173.194.73.101: icmp_seq=1 ttl=108 time=6.773 ms
64 bytes from 173.194.73.101: icmp_seq=2 ttl=108 time=6.752 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.592/6.706/6.773/0.081 ms
```

```
PING youtube.com (64.233.162.91): 56 data bytes
64 bytes from 64.233.162.91: icmp_seq=0 ttl=108 time=6.773 ms
64 bytes from 64.233.162.91: icmp_seq=1 ttl=108 time=6.192 ms
64 bytes from 64.233.162.91: icmp_seq=2 ttl=108 time=6.730 ms
64 bytes from 64.233.162.91: icmp_seq=3 ttl=108 time=6.806 ms

PING wide-youtube.l.google.com (173.194.73.198): 56 data bytes
64 bytes from 173.194.73.198: icmp_seq=0 ttl=108 time=6.156 ms
64 bytes from 173.194.73.198: icmp_seq=1 ttl=108 time=6.741 ms
64 bytes from 173.194.73.198: icmp_seq=2 ttl=108 time=6.513 ms
```

После захвата WireShark-ом IP- YouTube, видно как происходит «общение» между клиентом(порт 65281) и сервером(порт 443) - при первом соединении предполагаю как раз и передается ключ для шифрования, затем кусочки данных передаются в зашифрованном виде, толку от таких данных нет!

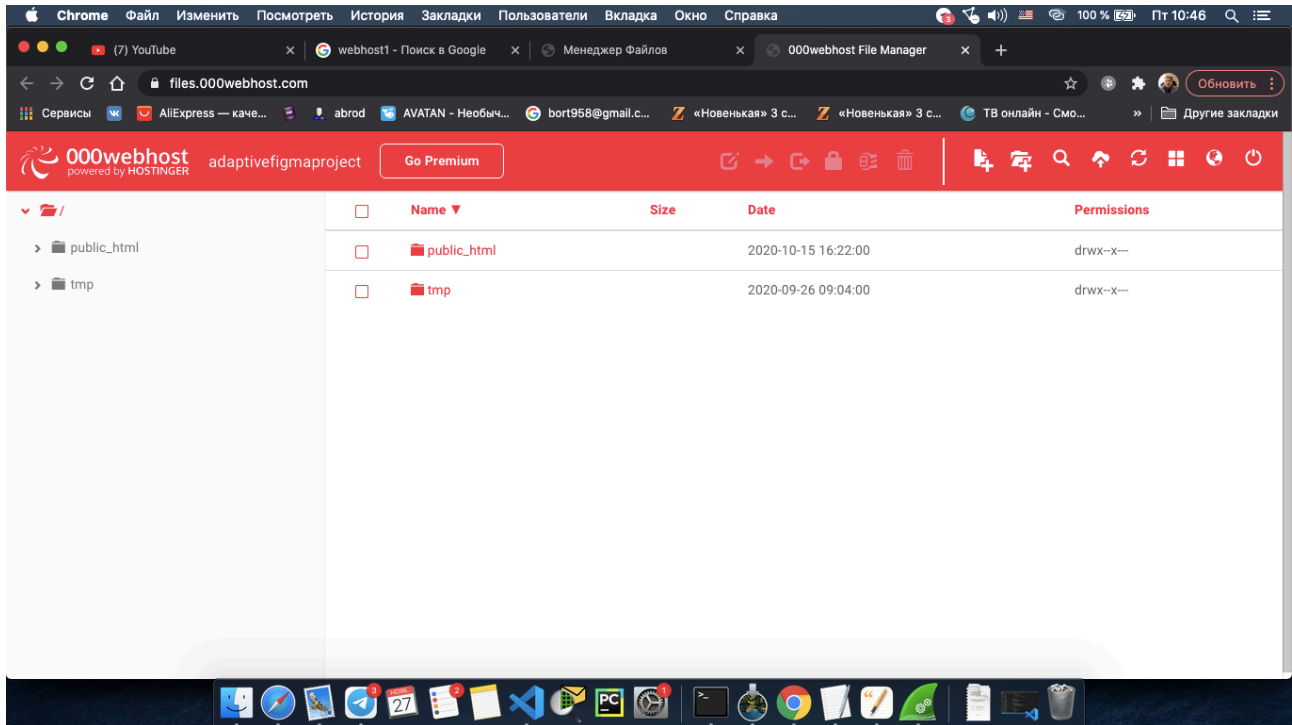


3. С помощью Wireshark отследить трафик при работе с обычным ftp (найти любой ftp-ресурс и подключиться к нему, через браузер). Можно ли через ftp передавать данные на сервер, как предлагают некоторые хостеры?

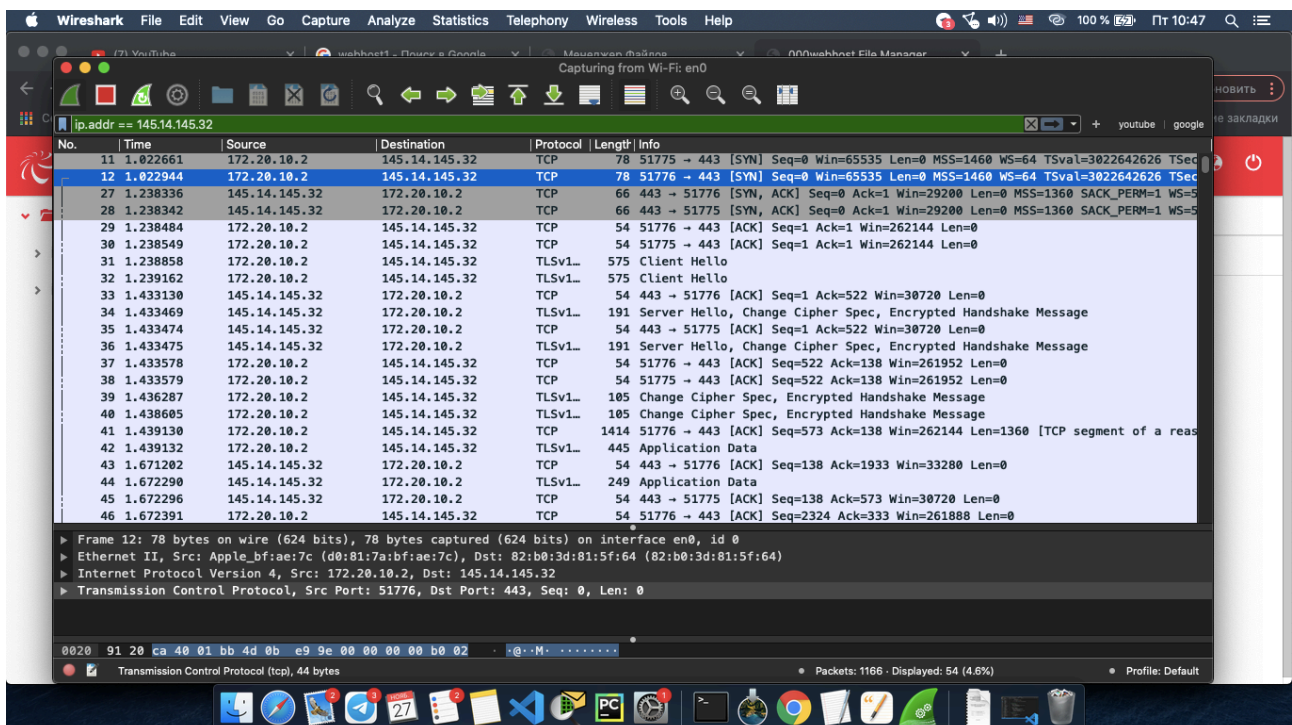
Первые 10 результатов поиска в гугле «online-ftp серверов» разделились следующим образом:

1) Есть ftp -сервера не использующие протокол шифрования HTTPS(соответственно их данные передаются в открытом виде)

2) Есть ftp-сервера использующие протокол HTTPS(пример хостинг <https://ru.000webhost.com>) и его ftp-сервер <https://files.000webhost.com/>



Узнаем IP, фильтруем данные в WireShark и видим, первую передачу по TCP протоколу(передача ключа), затем «тройное рукопожатие» и передача данных(Application Data)



## Задание №2

- 1) Просмотреть А-записи для доменов mail.ru, geekbrains.ru, vk.com. Сколько IP адресов серверов у этих ресурсов? Какой из них отвечает при выполнении команды ping на mail.ru, geekbrains.ru, vk.com соответственно?

### А-записи

---

Server: 172.20.10.1  
Address: 172.20.10.1#53

Non-authoritative answer:

Name: mail.ru  
Address: 217.69.139.202  
Name: mail.ru  
Address: 217.69.139.200  
Name: mail.ru  
Address: 94.100.180.201  
Name: mail.ru  
Address: 94.100.180.200

---

Server: 172.20.10.1  
Address: 172.20.10.1#53

Non-authoritative answer:

Name: GEEKBRAINS.ru  
Address: 178.248.232.209

Server: 172.20.10.1  
Address: 172.20.10.1#53

---

Non-authoritative answer:

Name: vk.com  
Address: 87.240.139.194  
Name: vk.com  
Address: 87.240.137.158  
Name: vk.com  
Address: 87.240.190.72  
Name: vk.com  
Address: 93.186.225.208  
Name: vk.com  
Address: 87.240.190.78  
Name: vk.com  
Address: 87.240.190.67

## PING

---

PING mail.ru (94.100.180.201): 56 data bytes

64 bytes from 94.100.180.201: icmp\_seq=0 ttl=48 time=93.182 ms

64 bytes from 94.100.180.201: icmp\_seq=1 ttl=48 time=114.524 ms

64 bytes from 94.100.180.201: icmp\_seq=2 ttl=48 time=117.531 ms

64 bytes from 94.100.180.201: icmp\_seq=3 ttl=48 time=123.652 ms

PING geekbrains.ru (178.248.232.209): 56 data bytes

64 bytes from 178.248.232.209: icmp\_seq=0 ttl=48 time=52.616 ms

64 bytes from 178.248.232.209: icmp\_seq=1 ttl=48 time=51.914 ms

64 bytes from 178.248.232.209: icmp\_seq=2 ttl=48 time=49.243 ms

PING vk.com (87.240.137.158): 56 data bytes

64 bytes from 87.240.137.158: icmp\_seq=0 ttl=53 time=39.245 ms

64 bytes from 87.240.137.158: icmp\_seq=1 ttl=53 time=63.454 ms

2) Просмотреть NS-записи для доменов google.com и youtube.com. Какой можно сделать вывод по результатам вывода этих двух команд?

После просмотра NS записи для доменов google.com и youtube.com., делаем вывод, эти два используют одни сервера, но в зависимости от домена(сервиса) имеют различные IP адреса для соединения

```
nikita_savva@Air-Nikita ~
$ nslookup -q=NS google.com [11:29:32]
Server: 172.20.10.1
Address: 172.20.10.1#53

Non-authoritative answer:
google.com nameserver = ns1.google.com.
google.com nameserver = ns3.google.com.
google.com nameserver = ns4.google.com.
google.com nameserver = ns2.google.com.

Authoritative answers can be found from:

nikita_savva@Air-Nikita ~
$ nslookup -q=NS youtube.com [11:29:45]
Server: 172.20.10.1
Address: 172.20.10.1#53

Non-authoritative answer:
youtube.com nameserver = ns1.google.com.
youtube.com nameserver = ns3.google.com.
youtube.com nameserver = ns4.google.com.
youtube.com nameserver = ns2.google.com.

Authoritative answers can be found from:
```

```
nikita_savva@Air-Nikita ~
$ nslookup -q=A youtube.com ns1.google.com. [11:29:53]
Server: ns1.google.com.
Address: 216.239.32.10#53

Name: youtube.com
Address: 64.233.165.190
Name: youtube.com
Address: 64.233.165.93
Name: youtube.com
Address: 64.233.165.136
Name: youtube.com
Address: 64.233.165.91

nikita_savva@Air-Nikita ~
$ nslookup -q=A google.com ns1.google.com. [11:30:25]
Server: ns1.google.com.
Address: 216.239.32.10#53

Name: google.com
Address: 64.233.161.113
Name: google.com
Address: 64.233.161.139
Name: google.com
Address: 64.233.161.181
Name: google.com
Address: 64.233.161.182
Name: google.com
Address: 64.233.161.138
Name: google.com
Address: 64.233.161.180

nikita_savva@Air-Nikita ~
$ [11:30:41]
```