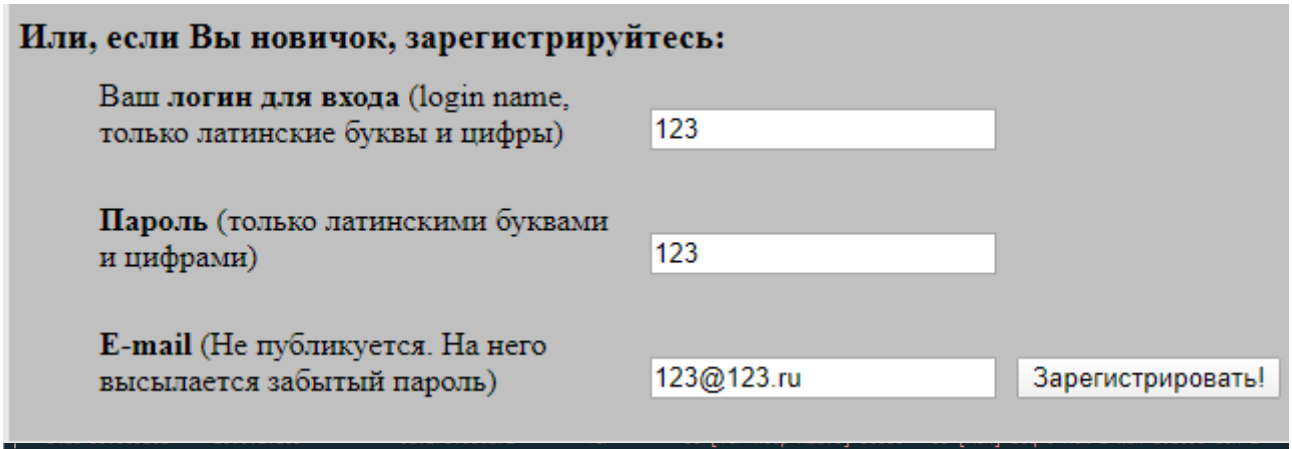
1. Найти нешифрованный http-сайт, где есть регистрация и логин. Отправить фейковые данные. Сможет ли злоумышленник перехватить пароль?

1. Зашел на сайт samlib.ru, перехватил пакеты и нашел свои данные в POST запросе. Пароль соответственно в незашифрованном виде.




```
1430 55.867391   81.176.66.171   10.0.1.165      TCP   60 [TCP Window Update] 80 → 50555 [ACK] Seq=1 Ack=1 Win=65696 Len=0
1472 57.327248   10.0.1.165      81.176.66.171   TCP   55 [TCP Keep-Alive] 50553 → 80 [ACK] Seq=688 Ack=399 Win=1023 Len=1
1473 57.329329   81.176.66.171   10.0.1.165      TCP   60 [TCP Keep-Alive ACK] 80 → 50553 [ACK] Seq=399 Ack=689 Win=8212 Le
1585 61.604228   10.0.1.165      81.176.66.171   TCP   54 50555 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
1588 61.636335   81.176.66.171   10.0.1.165      TCP   60 80 → 50555 [ACK] Seq=1 Ack=2 Win=65696 Len=0
1589 61.636609   81.176.66.171   10.0.1.165      TCP   60 80 → 50555 [FIN, ACK] Seq=1 Ack=2 Win=65696 Len=0
```

```
    Referer: http://samlib.ru/cgi-bin/login\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://samlib.ru/cgi-bin/login]
    [HTTP request 1/1]
    [Response in frame: 285]
    File Data: 75 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "NEW_DATA0" = "123"
  Form item: "NEW_DATA1" = "123"
  Form item: "NEW_EMAIL" = "123@123.ru"
  Form item: "OPERATION" = "add_user"
  Form item: "BACK" = ""
```

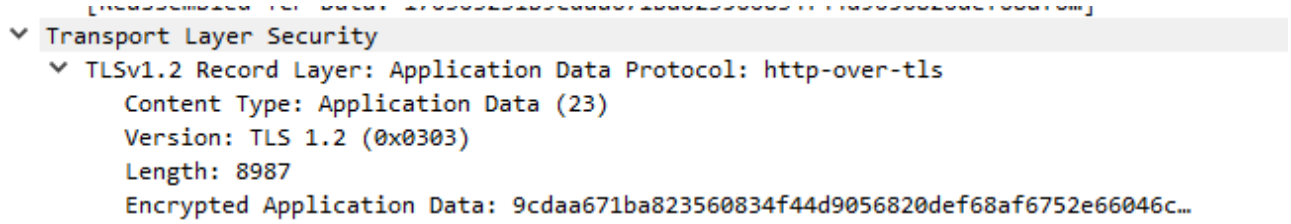
2. Найти нешифрованный http-сайт с множеством картинок. Рекомендуется использовать Google Chrome. Сколько будет открыто tcp-соединений и почему?

```
734 21.271812   10.0.1.165      213.171.51.146   TCP    66 57565 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
735 21.272219   10.0.1.165      213.171.51.146   TCP    66 57566 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
736 21.297152   213.171.51.146  10.0.1.165       TCP    66 80 → 57565 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
737 21.297209   10.0.1.165      213.171.51.146   TCP    54 57565 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
738 21.297431   213.171.51.146  10.0.1.165       TCP    66 80 → 57566 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
739 21.297470   10.0.1.165      213.171.51.146   TCP    54 57566 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
740 21.297823   10.0.1.165      213.171.51.146   HTTP  588 GET / HTTP/1.1
```

```
792 22.035872   10.0.1.165      213.171.51.146   HTTP  588 GET /templates/rt_refraction_j15/css/styles.css HTTP/1.1
793 22.037156   213.171.51.146  10.0.1.165       TCP    66 80 → 57568 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
794 22.037192   10.0.1.165      213.171.51.146   TCP    54 57568 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
795 22.037379   213.171.51.146  10.0.1.165       TCP    66 80 → 57569 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
796 22.037413   10.0.1.165      213.171.51.146   TCP    54 57569 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
797 22.037677   10.0.1.165      213.171.51.146   HTTP  592 GET /templates/rt_refraction_j15/css/typography.css HTTP/1.1
798 22.037871   10.0.1.165      213.171.51.146   HTTP  577 GET /templates/system/css/system.css HTTP/1.1
799 22.038252   213.171.51.146  10.0.1.165       TCP  1514 80 → 57566 [ACK] Seq=1 Ack=521 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
800 22.038452   213.171.51.146  10.0.1.165       TCP  1514 80 → 57566 [ACK] Seq=1461 Ack=521 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
801 22.038483   10.0.1.165      213.171.51.146   TCP    54 57566 → 80 [ACK] Seq=521 Ack=2921 Win=262656 Len=0
802 22.038671   213.171.51.146  10.0.1.165       TCP  1514 80 → 57566 [ACK] Seq=2921 Ack=521 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
803 22.038672   213.171.51.146  10.0.1.165       TCP  1514 80 → 57566 [ACK] Seq=4381 Ack=521 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
804 22.038887   213.171.51.146  10.0.1.165       TCP    66 80 → 57570 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
```

Открыто 5 соединений. Так происходит из-за того что несколько потоков грузят данные параллельно.

3. Повторите п.1 с TLS. Вопрос тот же.



Данные в зашифрованном виде.

4 *Какие интересные протоколы можно обнаружить, если подключиться Google Chrome к YouTube (сработать может не у всех)?

UDP, TCP, TLS