**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Московский приборостроительный техникум**

**Лабораторная работа №7**

по учебной практике

УП.01.02 Средства мониторинга и анализа в локальных сетях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование практики*

Профессионального модуля ПМ.01«Выполнение работ по проектированию

сетевой инфраструктуры»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование профессионального модуля*

Специальность 09.02.06 Сетевое и системное администрирование

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*код и наименование специальности*

Студент Карпов Артем Владимирович

*(фамилия, имя, отчество)*

Группа СА50-1-22

Руководитель по практической подготовке от техникума

Кульчинская Нелли Андреевна

*(фамилия, имя, отчество)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 года

1. Зарегистрировался на сайте root-me.org и нашел первую задачу. FTP-аутентификация. (рис. 1 - 5)

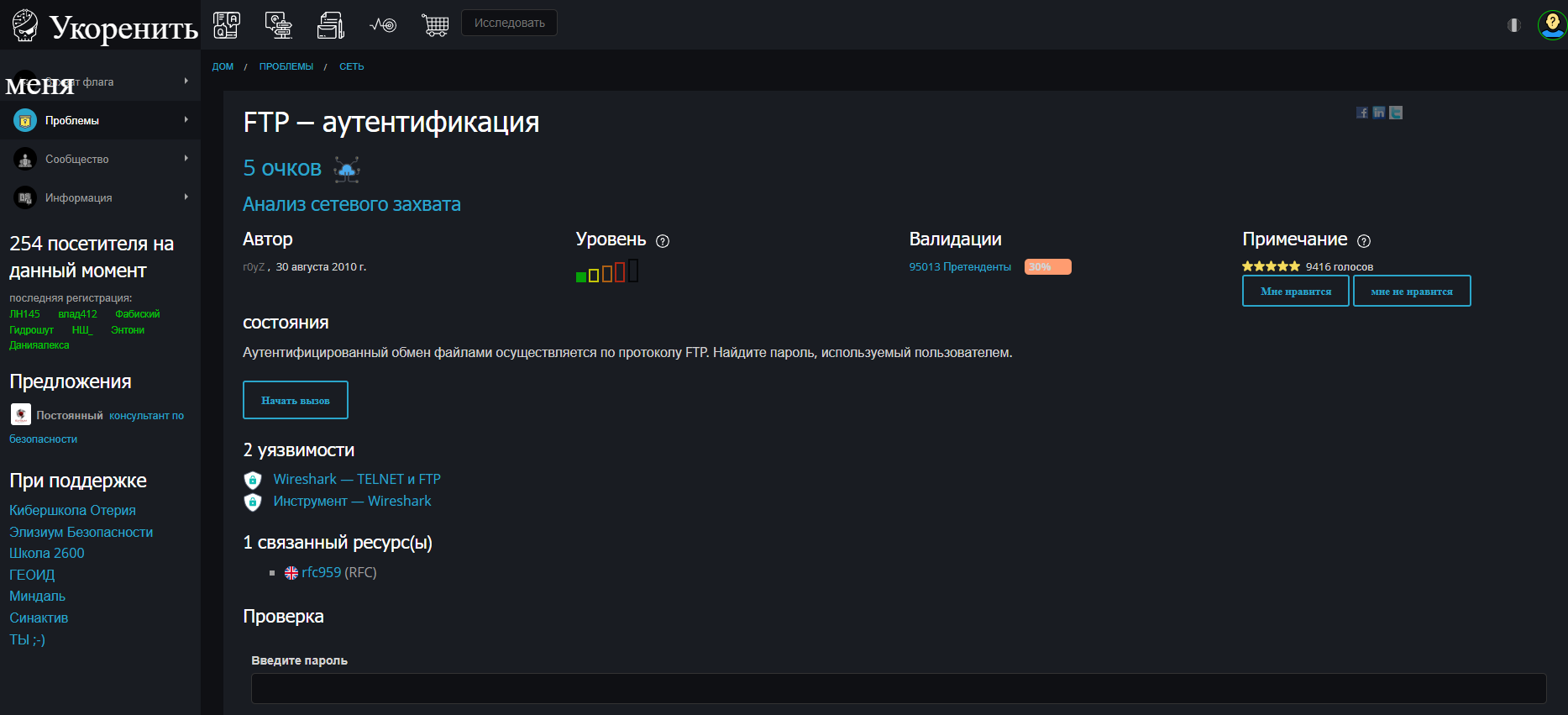


Рис. 1 – FTP-аутентификация

Чтобы скачать от сюда dump трафика надо залезть в код элемента и найти файл .pcap, после отрыть его в wireshark

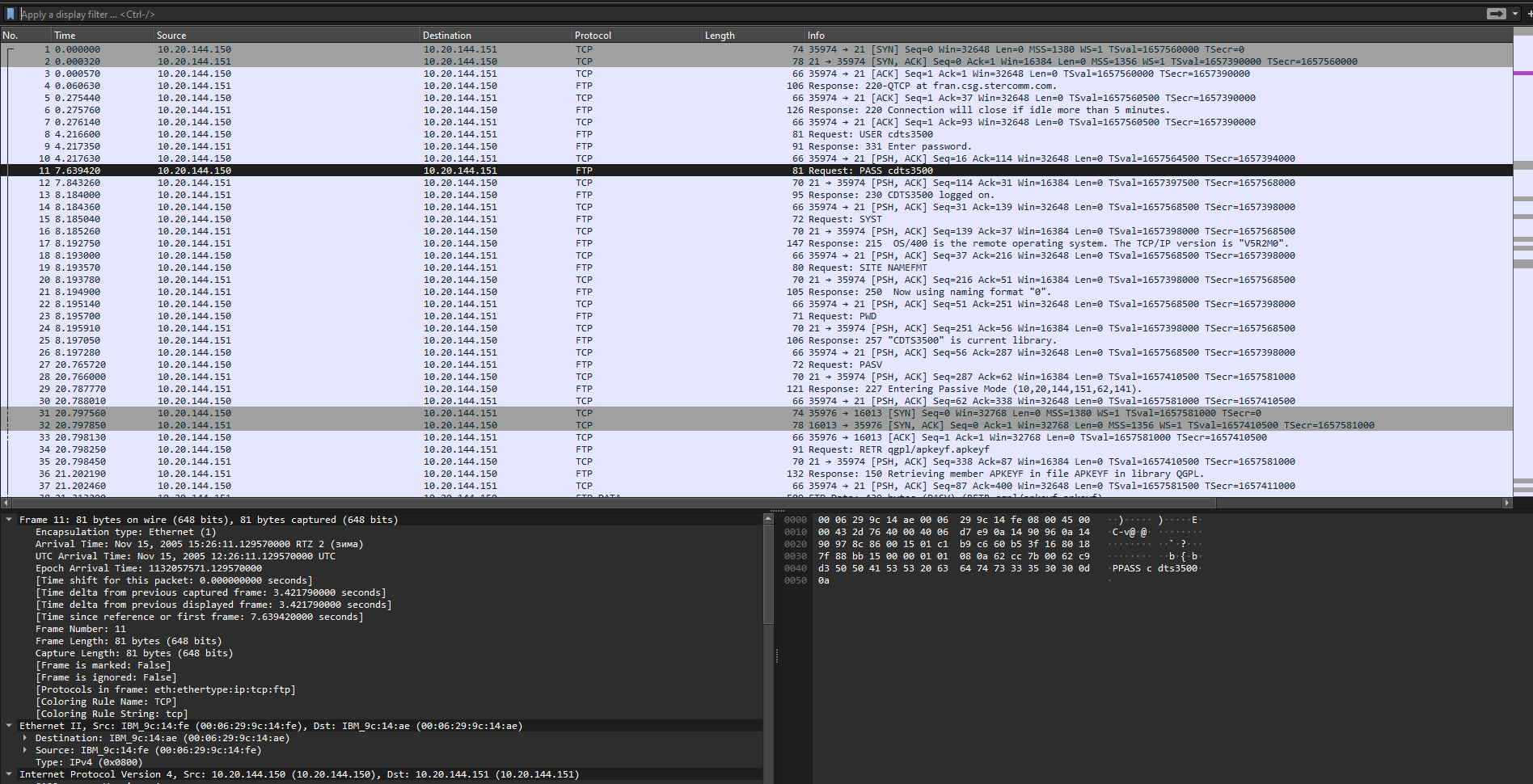


Рис. 2 – dump ftp-auth

После фильтруем запрос и находим информация по аутентификации на сервере по ftp

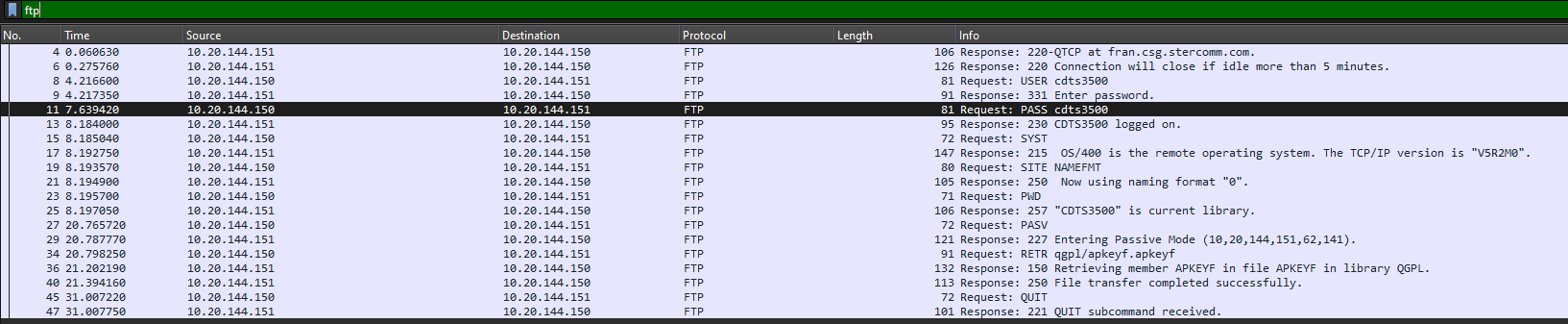


Рис. 3 – фильтрация по ftp

В самих запросах мы видим имя USER и PASS – cdts3500 cdts3500

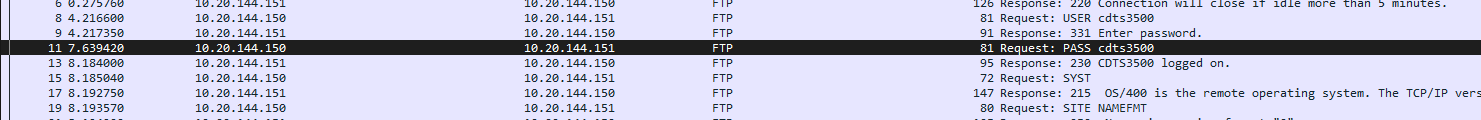


Рис. 4 – PASS ftp-auth

Проверяем наш пароль на сайте

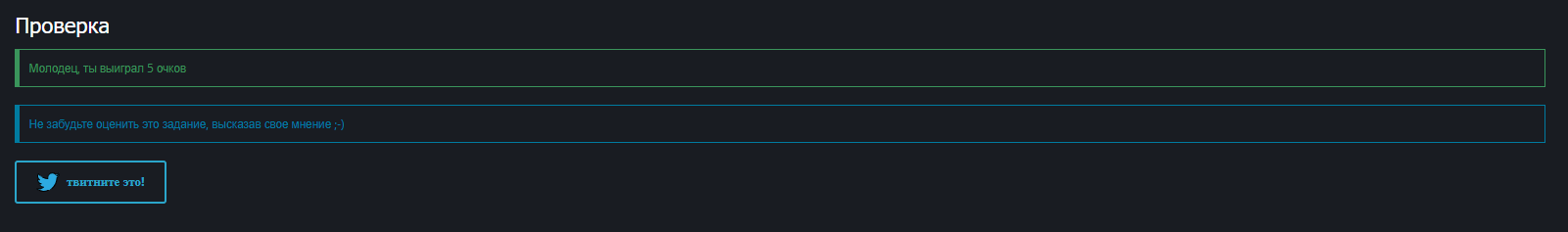


Рис. 5 – проверка пароля

1. Дальше мы находим тест по TELNET – authentication на сайте root-me.org

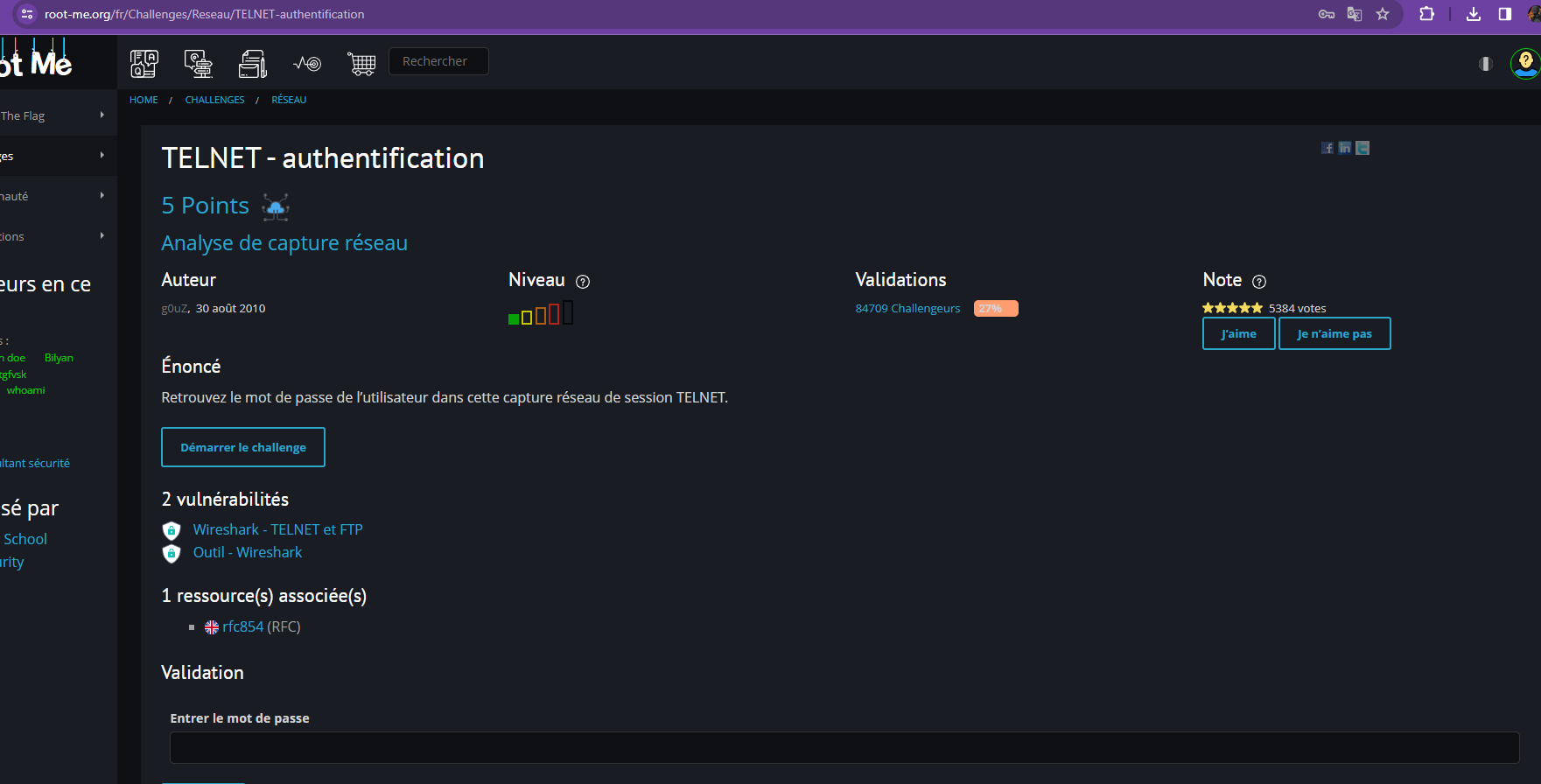


Рис. 5 – telnet-аутентификация

Также скачиваем файл через код элемента и запускаем в wireshark

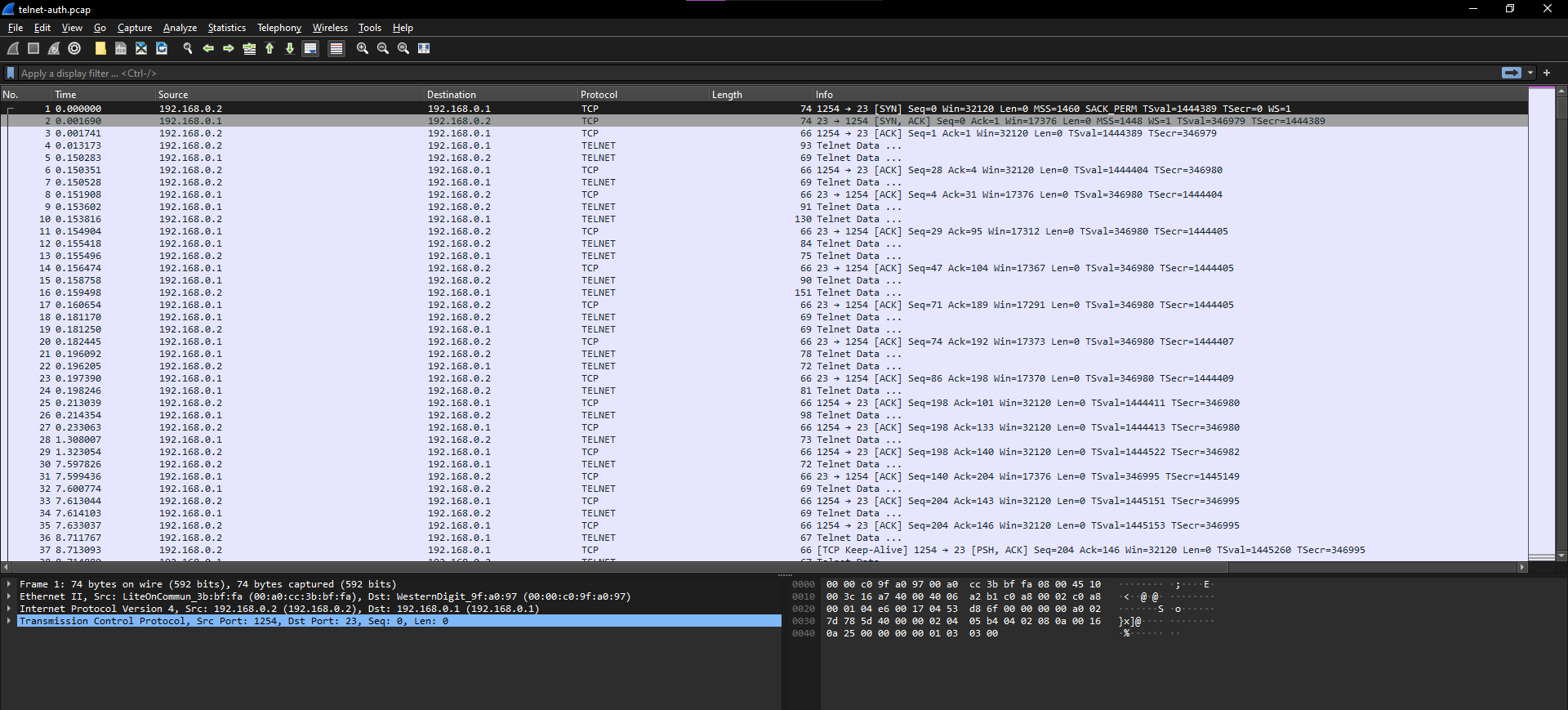


Рис. 6 – telnet-auth

Eсли посмотреть на 56 пункт в dump то можно заметить что сервер требует ввести пароль, и следующий пункт покажет нам пароль, но только последующие 4 пункта показали его, в 58,60,62,64 пункте посивольно указан пароль, если сложить все то мы получим “user”

58 frame



60 frame



62 frame



64 frame



Получился пароль: user

Теперь это надо проверить на сайте

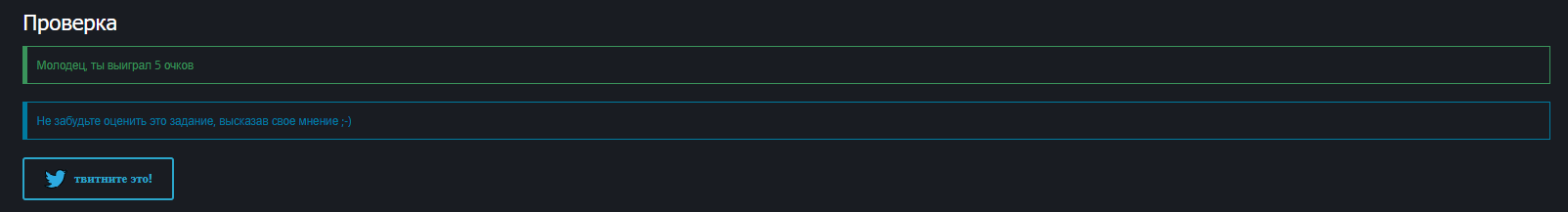


Рис. 7 - проверка

1. Открыл на сайте Ethernet – frame

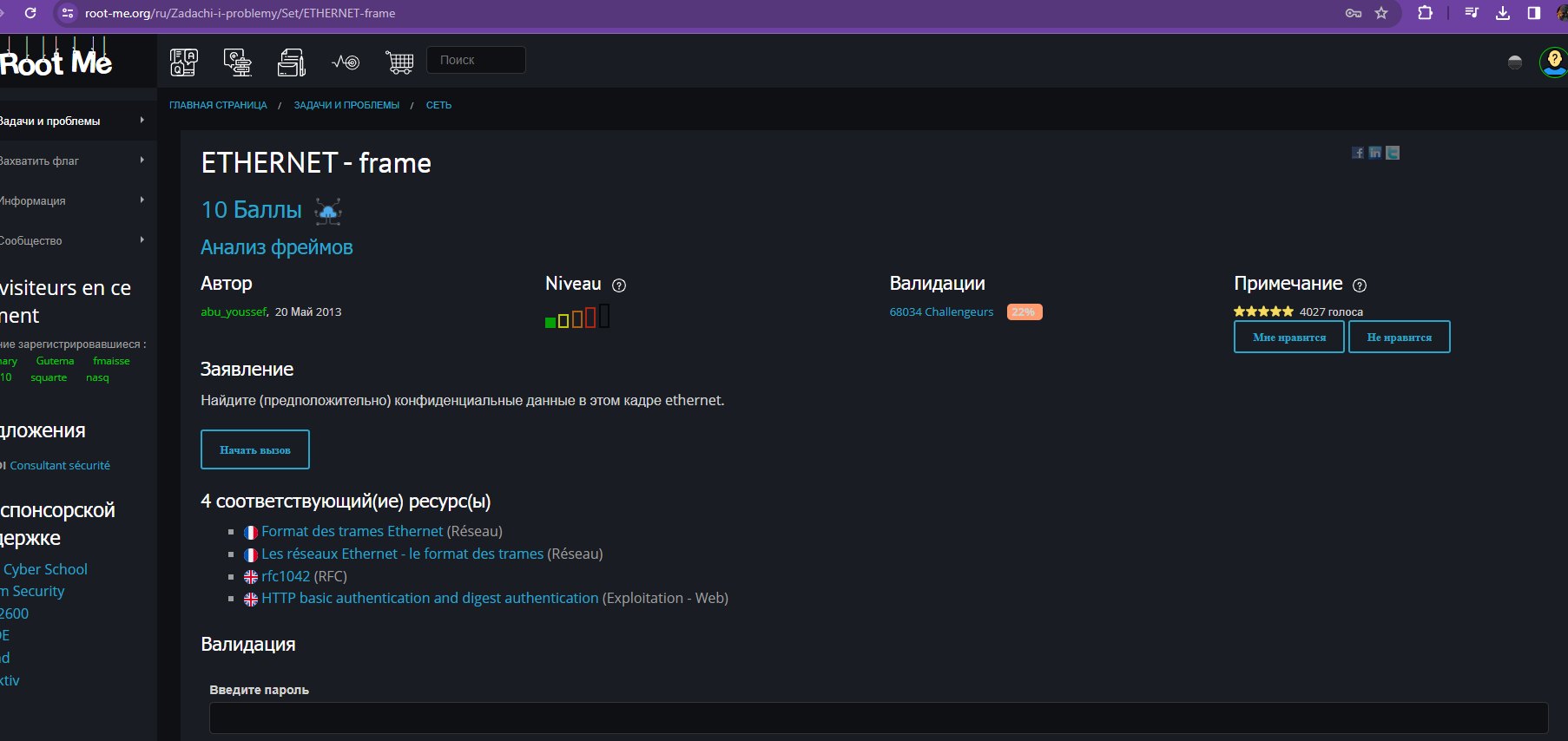


Рис. 8 – ethernet frame

После нажатия кнопки начать вызов мы видим вот такой документ

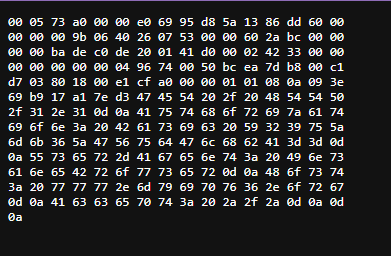


Рис. 9 – содержимое пакетов

Нам надо достать от сюда пароль, декодируем это из HEX

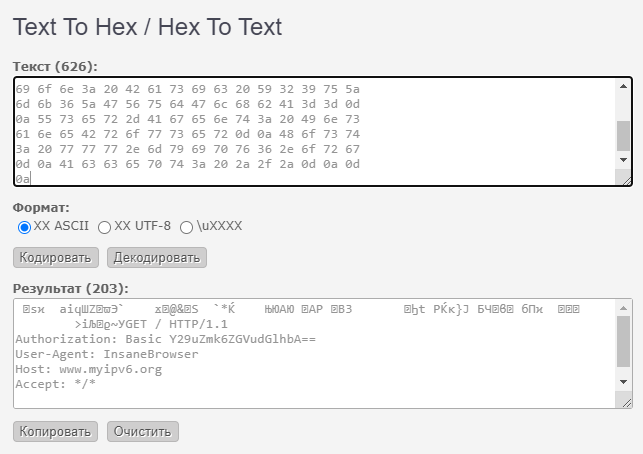


Рис. 10 – декодирование из HEX

Мы видим базовую аутентификацию, следовательно можем узнать пароль

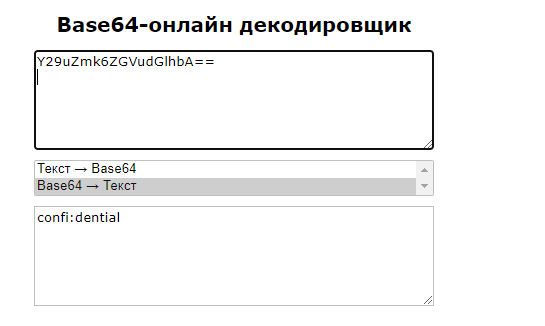


Рис. 11 – декодирование из base64

Пароль confi:dential и это надо проверить

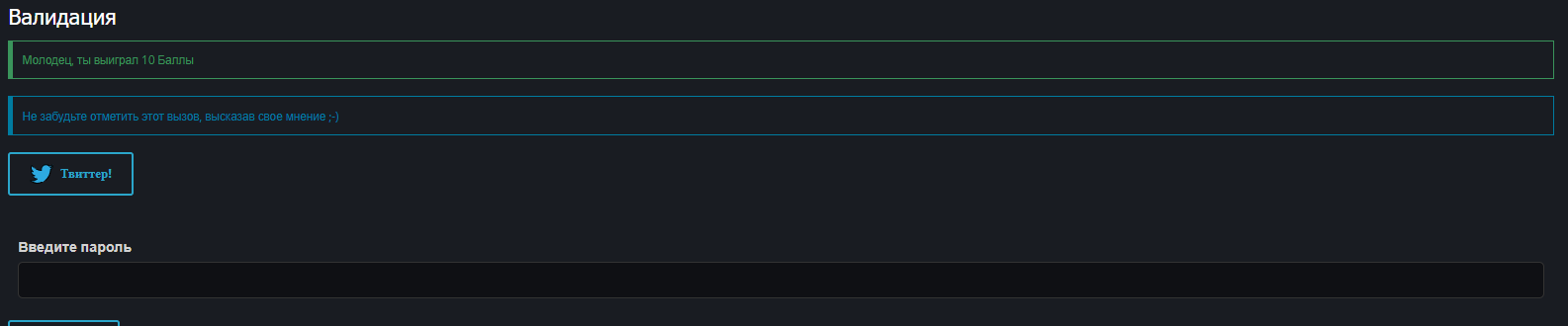


Рис. 12 - проверка

1. Заходим на сайт и ищем Twitter authentication

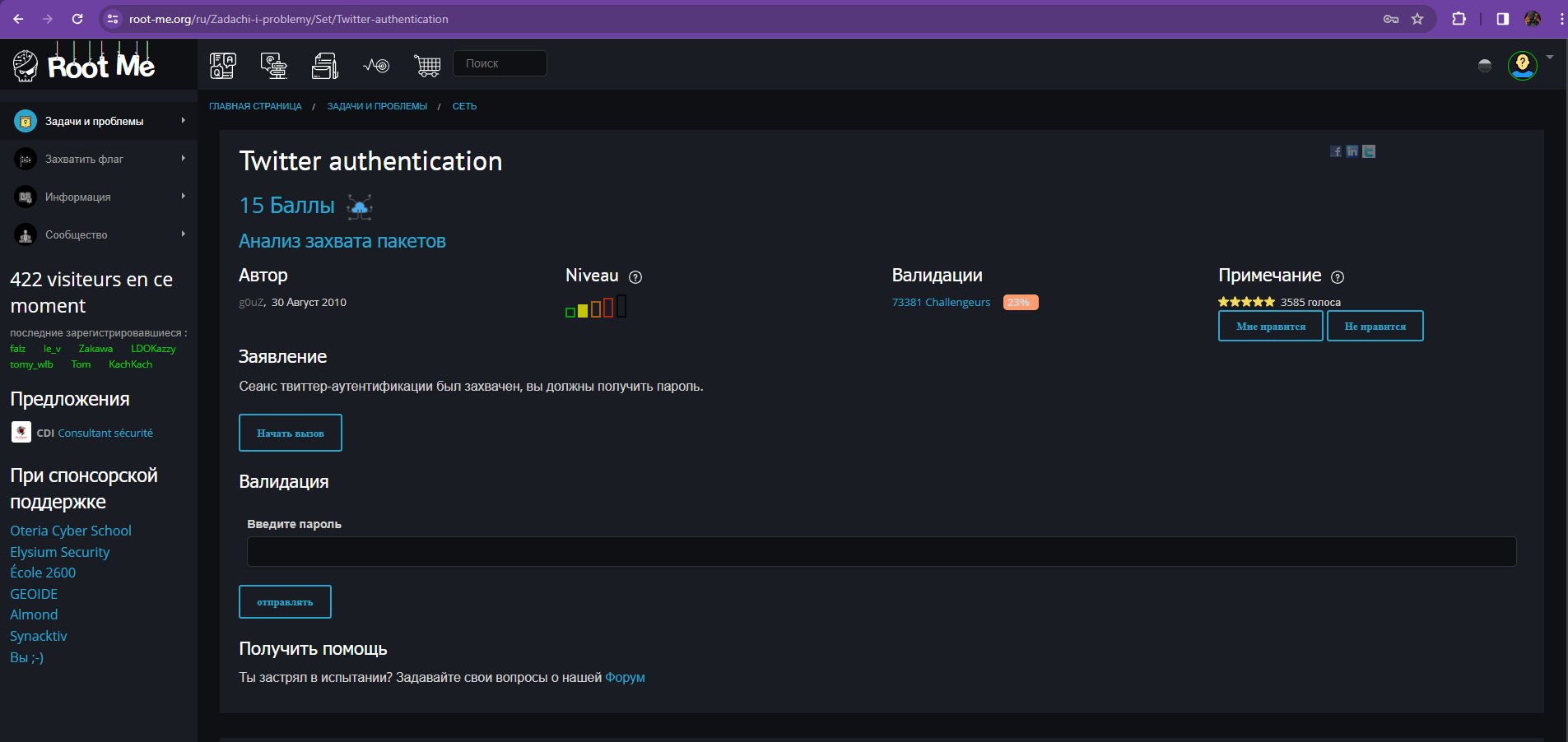


Рис. 13 – twitter authentication

Скачали и открыли файл

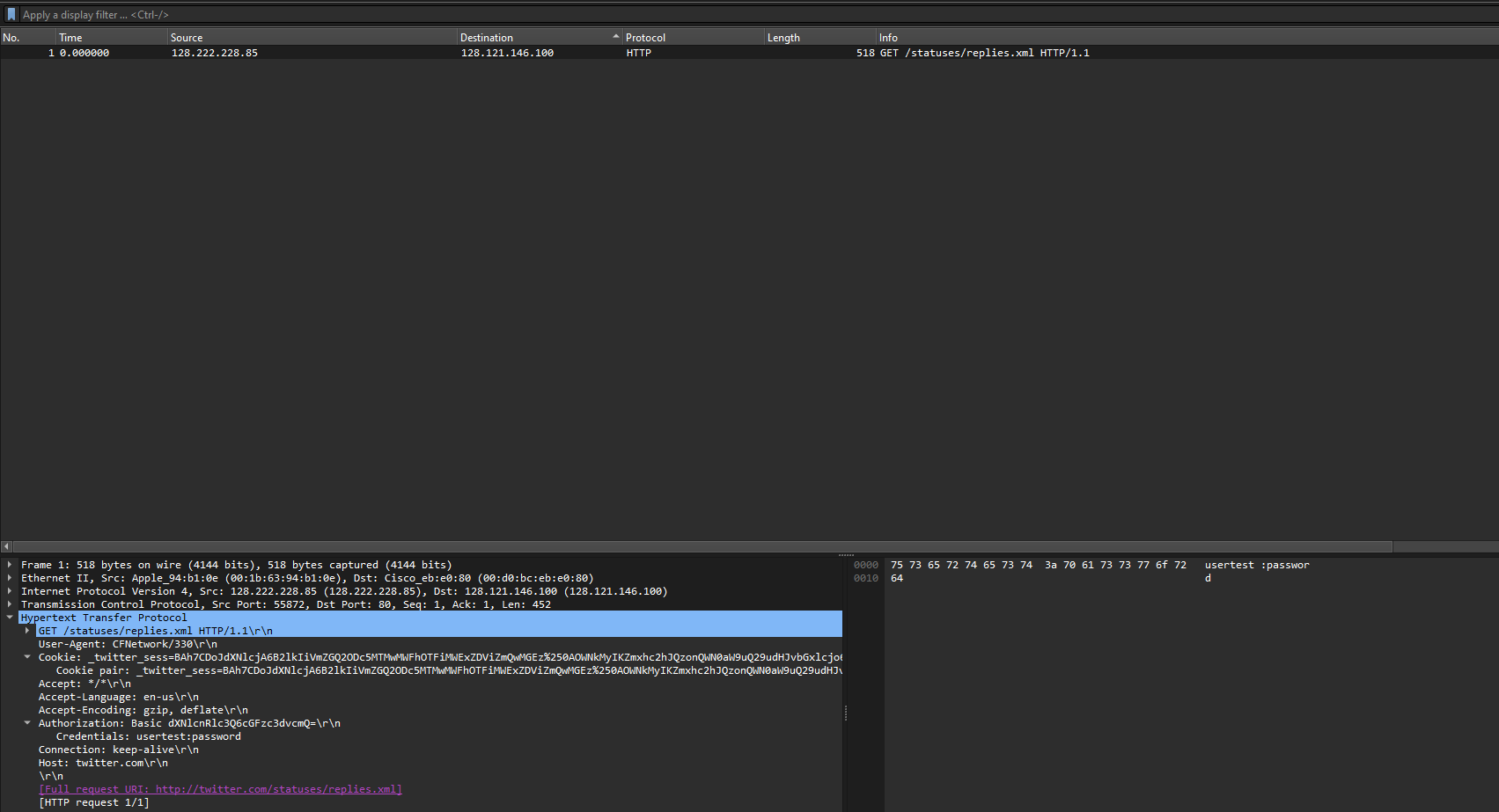


Рис. 14 – twitter auth

В этом дампе нам надо найти пароль от твиттер. Открываем follow TCP stream и видим Basic auth, это значит, что его можно декодировать

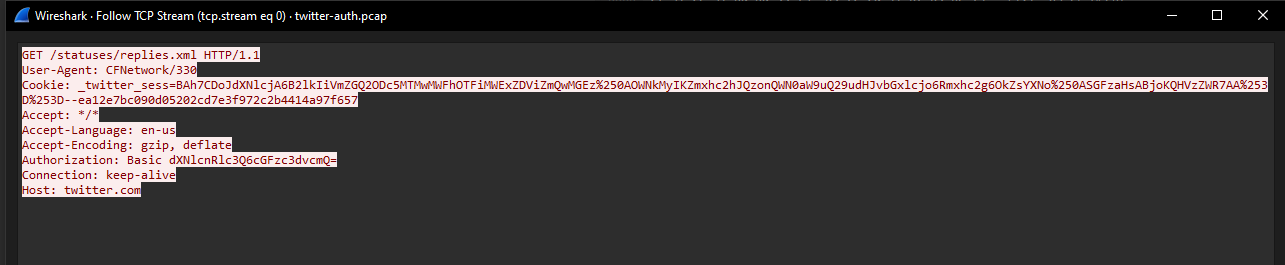


Рис. 15 – follow tcp stream

Находим декодер и декодируем пароль

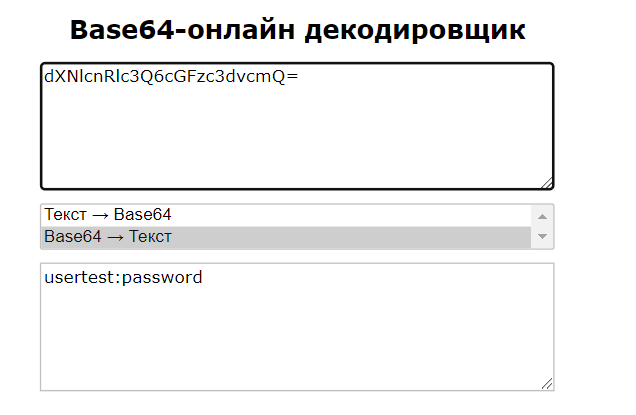


Рис. 16 – онлайн декодер

Пароль password, и теперь это проверяем

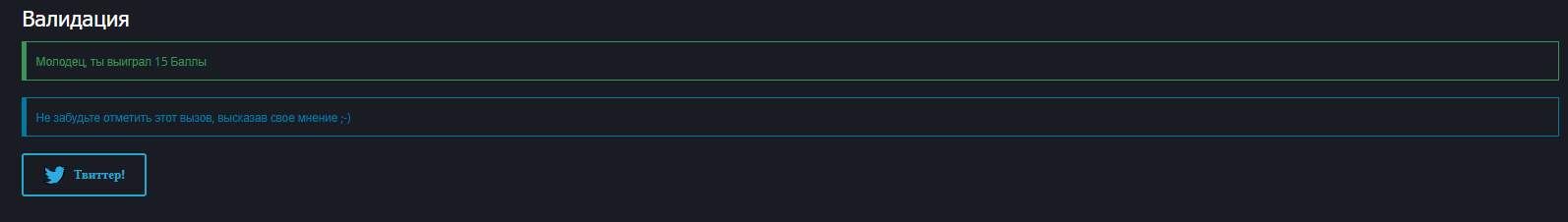


Рис. 17 - проверка

1. Открываем сайт и ищем задачу Bluetooth Unknown file

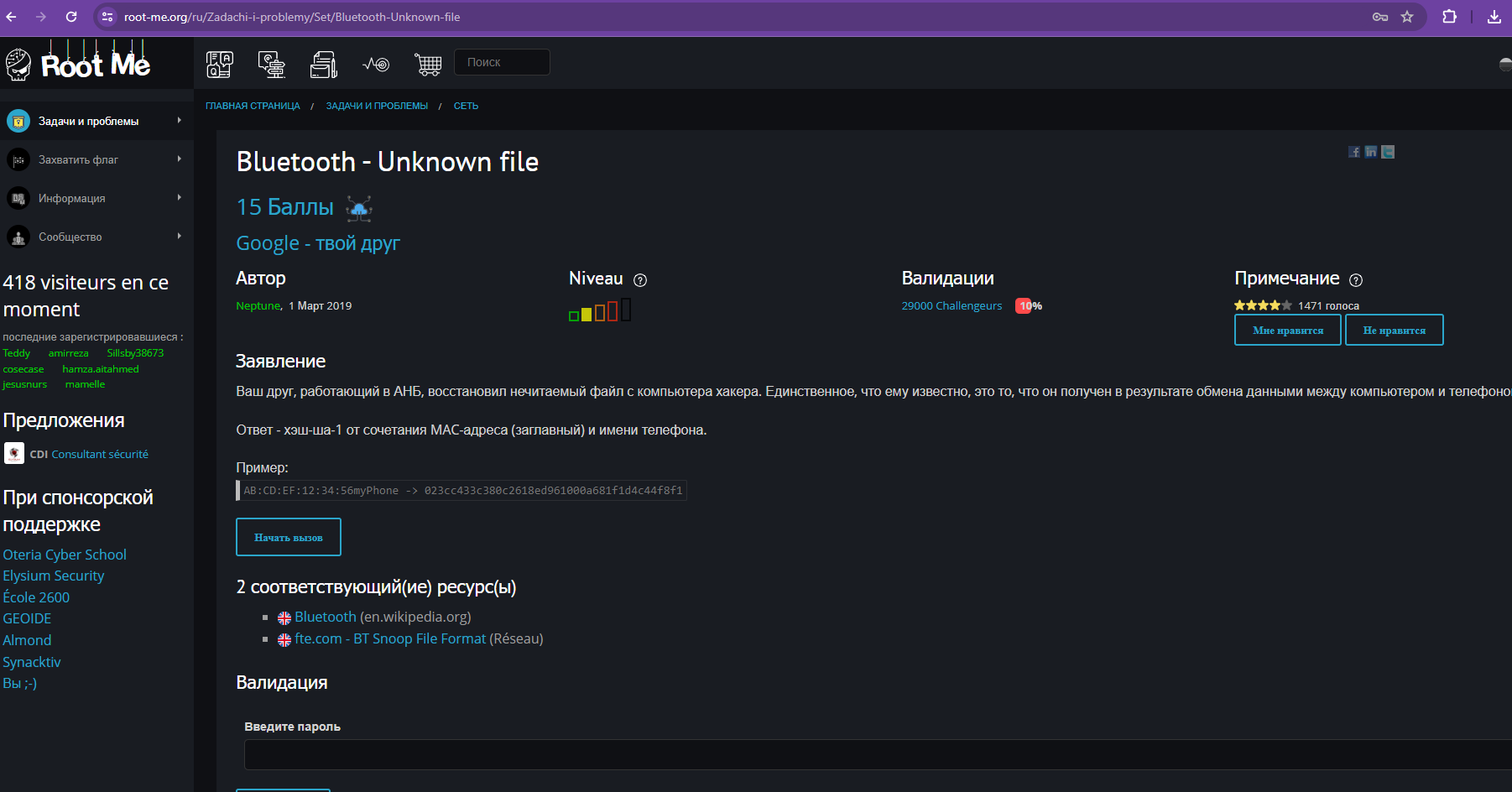


Рис. 18 - Bluetooth Unknown file

Скачиваем файл и открываем в wireshark

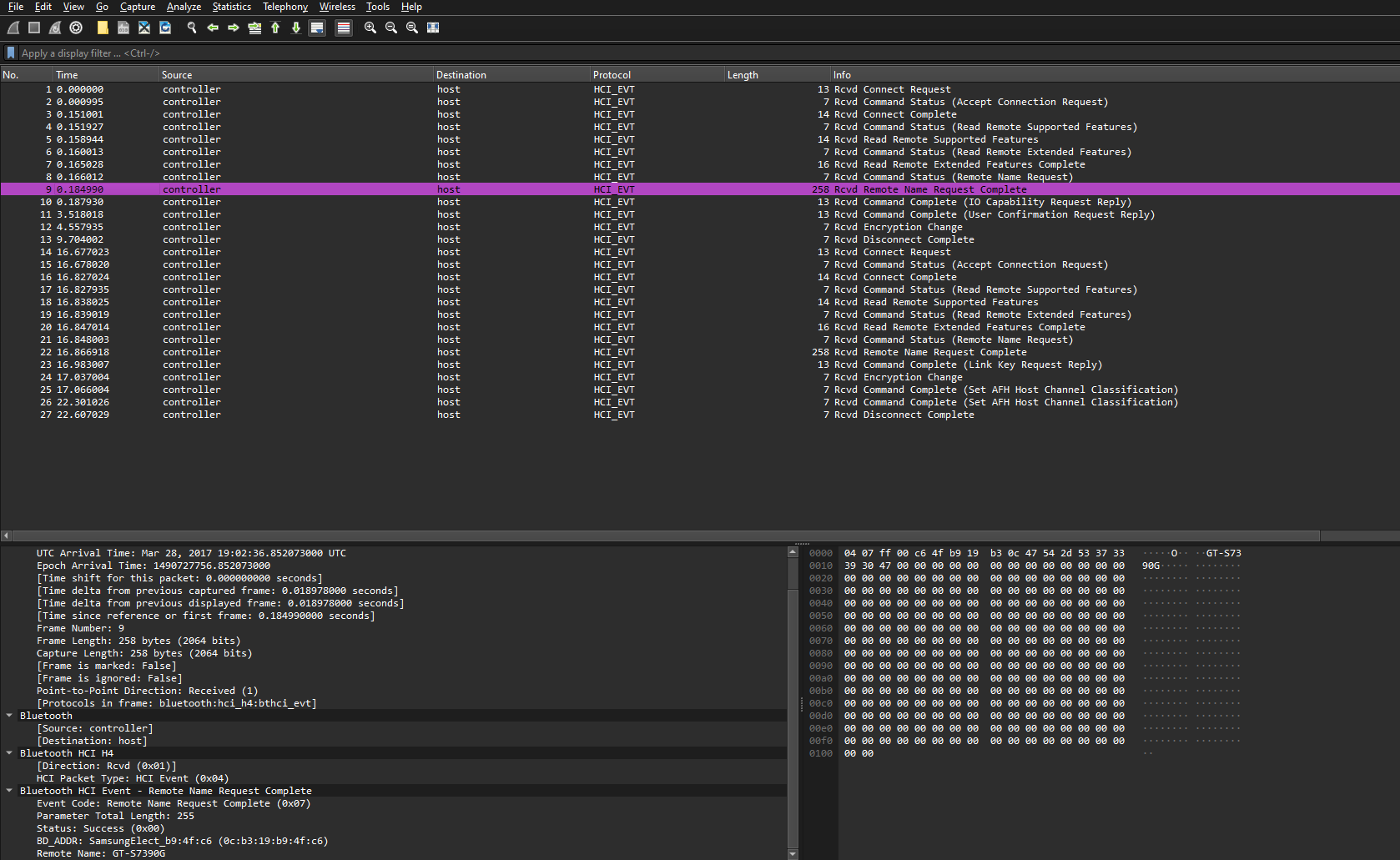


Рис. 19 – файл bluetooth

Теперь надо найти хэш чтобы его декодировать



Рис. 20 - хэш

После этого декодируем sha1

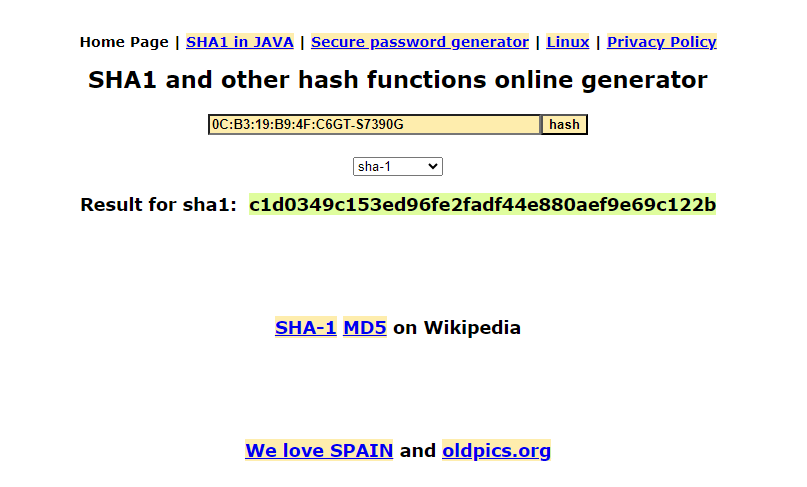


Рис. 21 - декодирование

Проверяем пароль

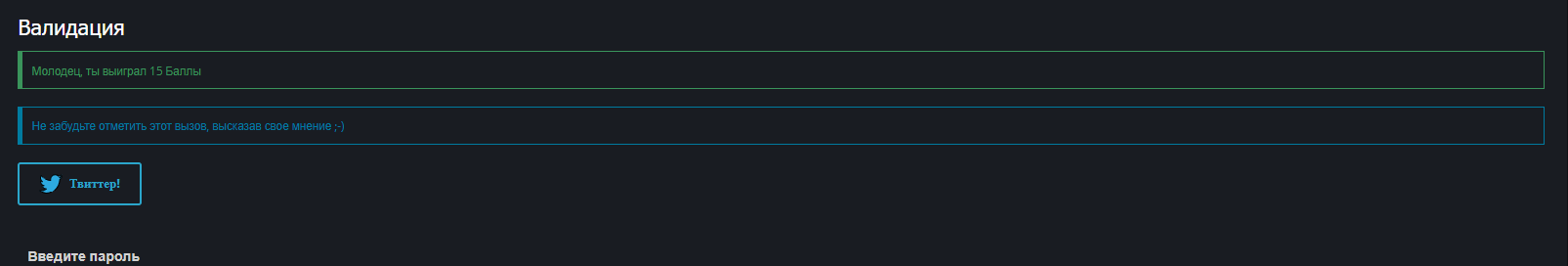


Рис. 22 - проверка

Решенные задачи:

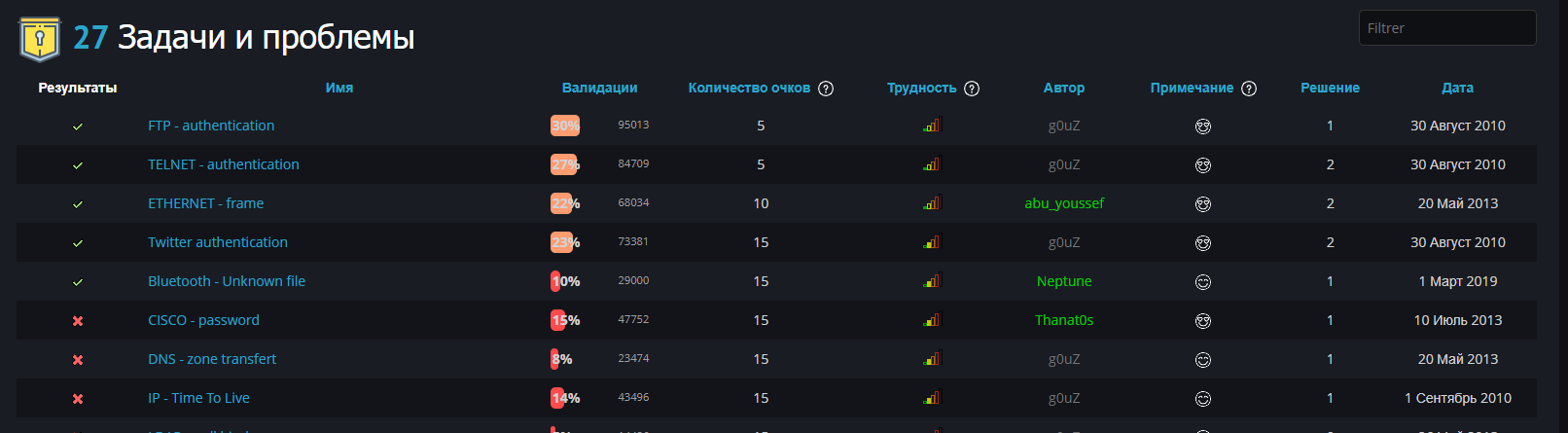


Рис. 23 – решенные задачи