Домашнее задание урок 6.

1. Найти любой не шифрованный сайт, где требуется форма ввода пароля. Может злоумышленник перехватить этот пароль?

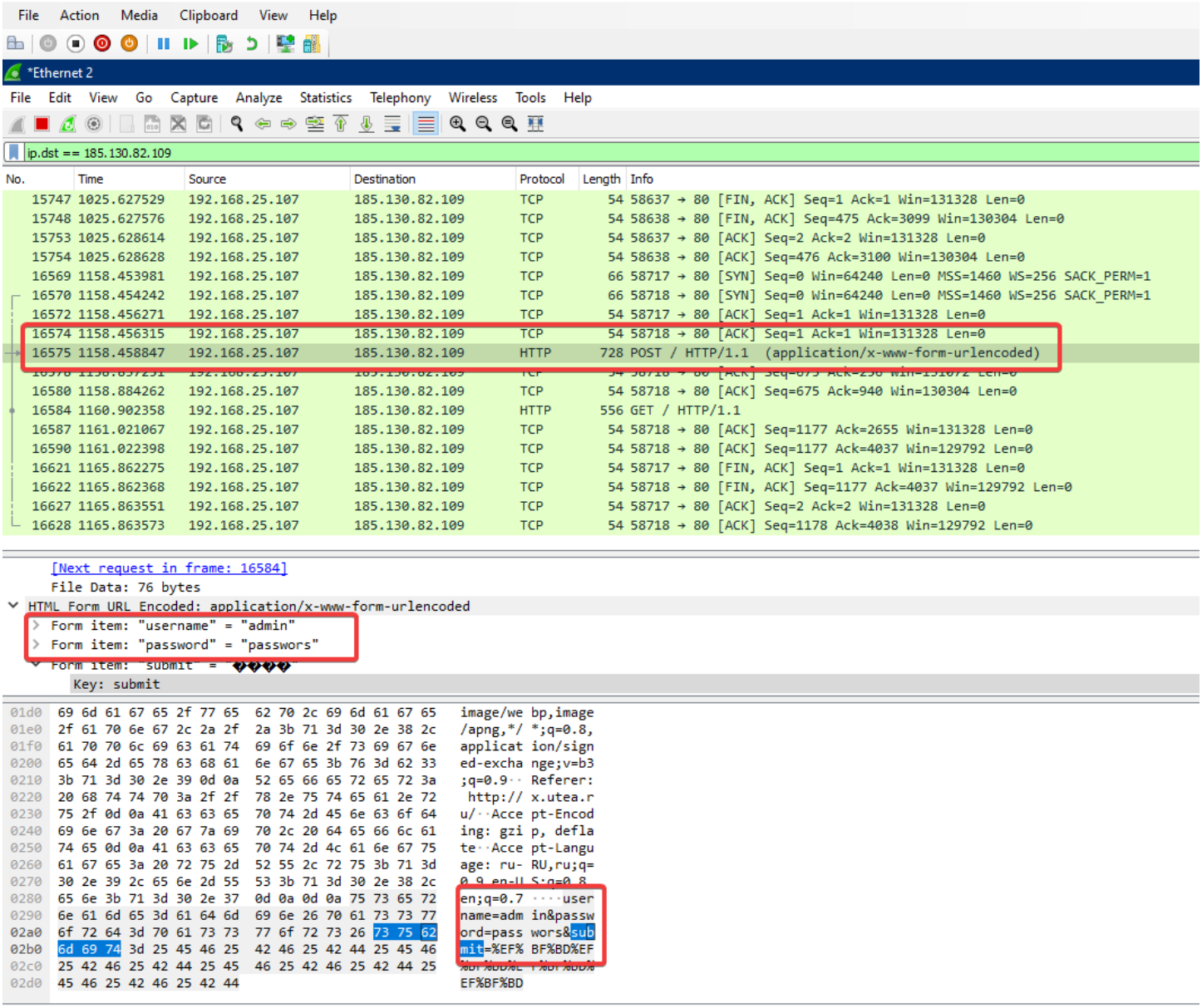
Пришлось воскресить мой старый проект) в который мы рубились одно время: http://x.utea.ru, он весь в кракрозябрах, но думаю это не важно.

Определяем IP: ping x.utea.ru - 185.130.82.109

Ставим фильтр по назначению: ip.dst == 185.130.82.109

Переходим на сайт, вводим логин и пароль, нажимаем «enter».

Ну и собственно особо и искать не пришлось, сразу и видно, в запросе POST все передается в открытом виде:



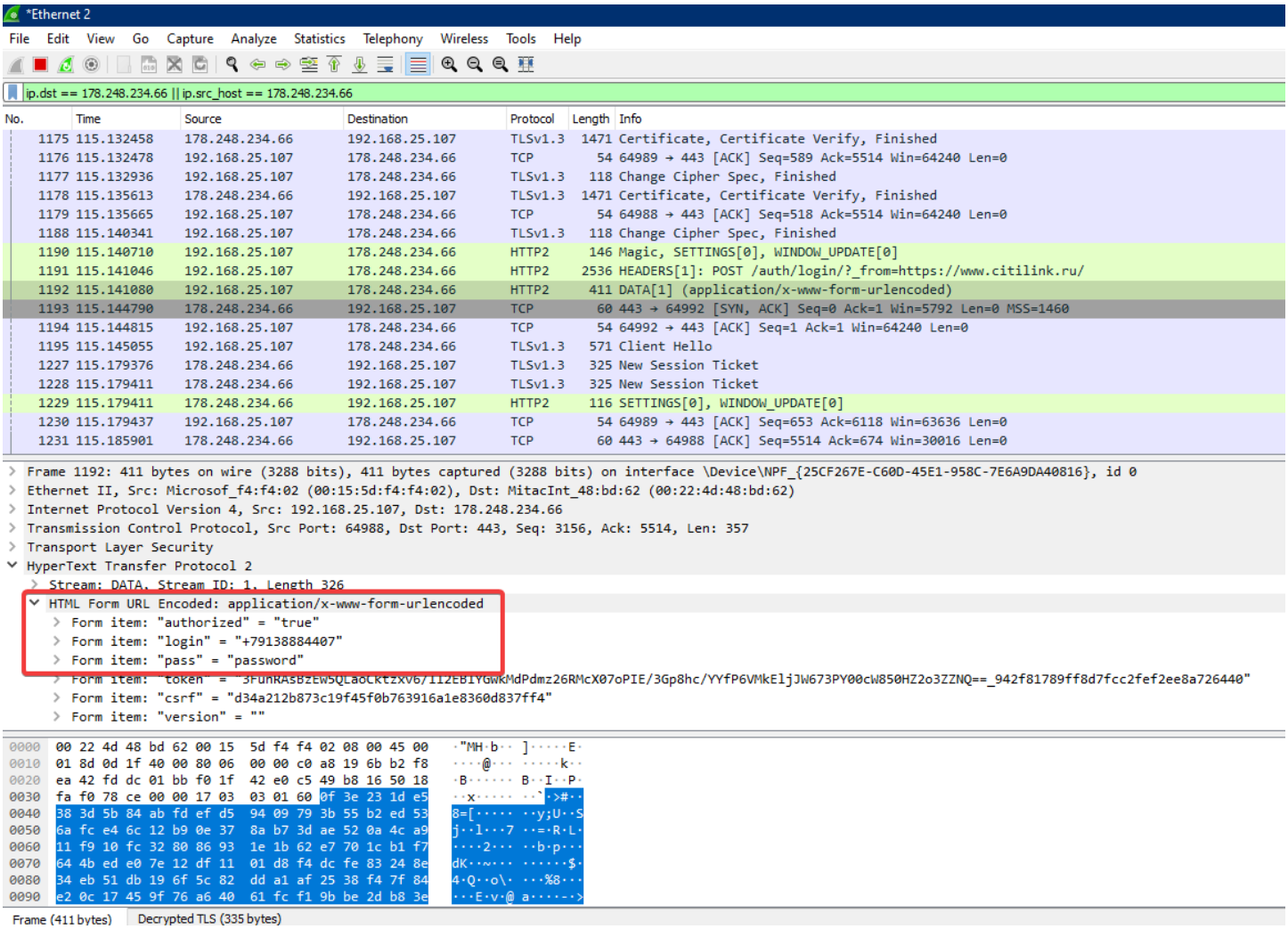
Выводы: если у злоумышленника будет доступ к каналу передачи, он сможет получить пароль.

2. Использовать гугл хром. Нужно найти сайт с картинками не шифрованный. Сколько открыто TCP-сессий и зачем.

Ответа нет, как я ни силися я не понял, что от меня требуется. Буду ждать разбора ДЗ

3. Повторить задание 1 с https. Вопрос аналогичный.

При использовании https трафик шифруется и в wireshark мы видим кракрозябры) Но! имея некоторые представления о шифровании я понимаю, что оба субъекта должны обменятся ключами для шифрования, следовательно, делаю предположение, что их можно перехватить. Немного углубившись в эту тему, я понял, что так и есть, если очень упрощенно, клиент используя открытый ключ сервера добавляя некоторую случайную информацию, обменивается с сервером сеансовыми ключами наверное теоретически и их тоже можно перехватить. В случае если есть доступ к локальной машине, то можно попросить браузер их сохранять и даже настроить wireshark для расшифровки трафика, на скрине обращение к сайту “citilink.ru” (178.248.234.66), форма авторизации там мы видим расшифрованный трафик, ну а раз смог wireshark смогут и другие:



Вывод: На самом деле все конечно же сложнее, но не мне вам это объяснять) Если трафик слушается на локальной машине, то https полагаю не спасет). А вот если вклинится в сеть передачи, то задача сильно усложняется.