**Задание:** С помощью Wireshark или Cisco Packet Tracer отследить трафик, идущий по протоколу HTTP и HTTPS. В чем разница?

**Ответ:**

Основные различия между HTTP и HTTPS (скриншот **EX.2\_1**):

* Протокол HTTP не является безопасным, т.к. передает данные в открытом виде, в то время, как HTTPS для шифрования данных использует SSL или TLS;
* По умолчанию HTTP работает по 80му порту, а HTTPS по 443;
* HTTP работает на уровне приложения, а HTTPS на транспортном уровне.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Задание:** 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?

**Ответ:**

Изначально стоит оговориться, что подключение к сервисам производилось в браузере Firefox. Как видно на скриншоте **EX.2\_2**, при подключении к youtube.com Wireshark сразу не отловил никаких пакетов по фильтру "**http**". Однако, через некоторое время начали появляться пакеты протокола HTTP, но, как видно на скриншоте **EX.2\_3**, обмен пакетами происходил в одной подсети (**192.168.43.0/24**).

На скриншоте **EX.2\_4** видно, что при изменении фильтра на "**tls && ip.addr == 172.217.17.238"** и попытке подключиться к сервису docs.google.com Wireshark начал отлавлить пакеты HTTPS (**TLSv1.3**). Исходя из вышесказанного можно сделать вывод, что для подключения к сервисам google.com используется протокол **HTTPS**.