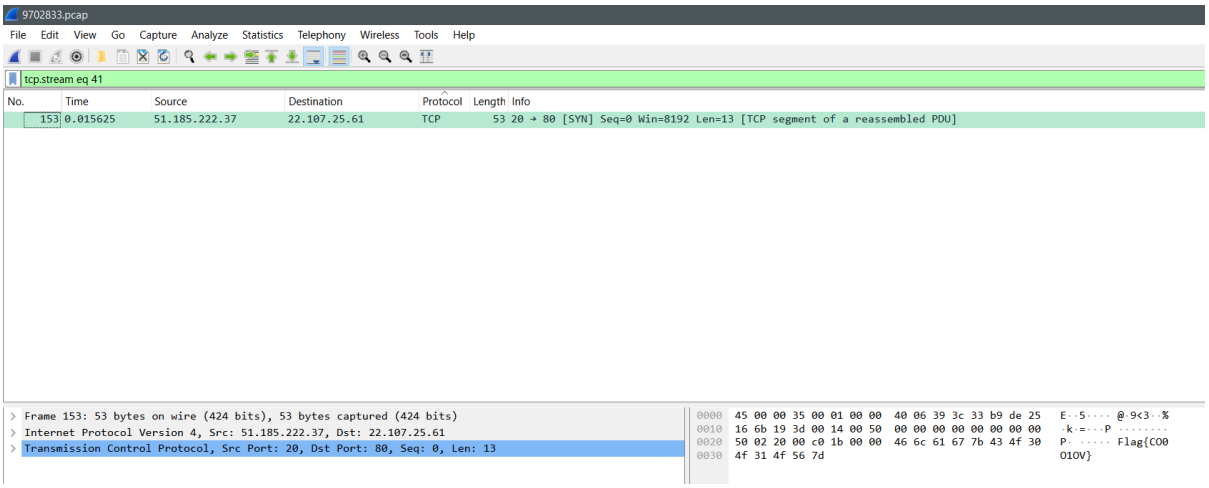
پاسخ تمرین سری چهارم – فاطمه پورالعجل - ۹۷۰۲۸۳۳

۱. ابتدا پکت ها را بر حسب پروتکل مرتب میکنیم. سپس با توجه به اینکه تعداد پکت ها زیاد نیست ان ها را به ترتیب پروتکل چک میکنیم. در پکت های TCP طول بسته اطلاعاتی صفر است و تنها یک پکت وجود دارد که طول بیش از صفر دارد. همان بسته حاوی flag است. CO0O1OV



۲. در این فایل ۴ نوع پروتکل TCP, UDP, IPv4, ICMP وجود دارد:

- بسته های TCP تماما طول صفر دارند. به جز بسته حاوی flag. IP های ارسال و دریافت بسته ها کاملا متفاوت به نظر میرسند.
- بسته های UDP طول صفر دارند. IPهای ارسال و دریافت بسته ها کاملا متفاوت به نظر میرسند.
- بسته های IPv4 به صورت Malformed هستند. محتوای ان ها شامل یک قسمت options با محتوای www.example.com است. قسمت data در این بسته ها خالی است.
- بسته های ICMP بسته های فرمان Ping به صورت multicast یا عادی هستند. موارد عادی با response not found مواجه شده اند. IP های مبدا و مقصد متفاوت هستند.