۱) در فایل داده شده از پروتکلهای متفاوتی استفاده شده است. اول از tcp شروع میکنیم.از فیلتر tcp.stream استفاده میکنیم وقتی که به stream index ۱۳ میرسیم flag رو مشاهده میکنیم.

۲) با توجه به پروتکلهای موجود در فایل pcap که شامل IPv4، TCP، ICMP و UDP است میتوان گفت که این ترافیک شبکه میتواند مربوط به فعالیت های زیر باشد:

۱. ارتباطات اینترنتی معمولی : TCP و UDP معمولاً برای انتقال داده های اپلیکیشن های مختلف مانند وب گردش ایمیل پخش محتوا و غیره استفاده می شوند.

۲ پینگ و کنترل ارتباطات پروتکل ICMP معمولاً برای ارسال پینگ و تشخیص مشکلات شبکه استفاده میشود.