1)

در فایل داده شده از پروتکل های متفاوتی استفاده شده است. اول از tcp شروع میکنم. فیلتر tcp.stream استفاده میکنیم. وقتی که به stream index 13 میرسیم flag رو مشاهده میکنیم

2)

با توجه به پروتکل‌های موجود در فایل pcap که شاملICMP ، TCP، IPv4و UDPاست، می‌توان گفت که این ترافیک شبکه می‌تواند مربوط به فعالیت های زیر باشد:

1. ارتباطات اینترنتی معمولی : TCPو UDP معمولاً برای انتقال داده‌های اپلیکیشن‌های مختلف مانند وب گردش، ایمیل، پخش محتوا و غیره استفاده می‌شوند.
2. پینگ و کنترل ارتباطات: پروتکل ICMP معمولاً برای ارسال پینگ و تشخیص مشکلات شبکه استفاده می‌شود.