تمرین شماره ۰۴، علیرضا صابریان، ۴۰۰۱۳۰۳۳۳

۱. Flag{I5ZA7VV}

NO.	Time	Source	Source Port	Destination	Protocol	Lenght	TD	Info
37	0.014045	123.51.212.84		67.116.213.198	DNS	41	0.000000000	Unknown operation (12) 0x466c[Malformed Packet]

نحوه ی یافتن flag به این صورت بود که متوجه شدم پروتکل های udp قابلیت flag داشتن را دارند پس فیلتر udp زدم و پس از آن متوجه شدم همه ی نتایج فیلتر شده، Stream index از ایندکس ۰ تا ۳۱ دارند بنابراین تک تک آنها را چک کردم و packet بالا دارای یک flag بود.

۲.

۱. **پروتکل‌ها**: با استفاده از فیلترهای مختلف می‌توان پروتکل‌های مورد استفاده در ترافیک را شناسایی کرد مانند TCP، UDP، ICMP، و DNS
۲. **پورت‌ها**: تعیین سرویس‌هایی که بر روی پورت‌های مشخصی در حال ارتباط هستند؛ به عنوان مثال، سرویس TCP (پورت ۲۰)
۳. **آدرس‌های IP**: با استفاده از فیلترهای مختلف می‌توان آدرس‌های IP مبدا و مقصد مرتبط با ترافیک را شناسایی کرد.
۴. **شناسایی بسته‌های ناقص یا خراب**: با جستجوی بسته‌هایی که دارای فیلد Malformed Packetهستند، می‌توان بسته‌هایی که به درستی ساختاردهی نشده‌اند را شناسایی کرد.
۵. **تحلیل محتوا:** در صورتی که ترافیک شامل پیام‌های مشخصی باشد مثل پروتکلDNS ، می‌توان با استفاده از فیلترهای مربوط به محتوا، جزئیات بیشتری را مشاهده کرد.
