

(۱)

Flag{2GNU1Q7}

با فیلتر کردن پروتکل های مختلف و استریم کردن آنها ، Flag به راحتی قابل تشخیص است، البته ابتدا ترافیک را با tcp.stream که ۲۸ شماره یا Index داشت را بررسی کردم و سپس UDP و DNS که Flag ما در DNS و در خط ۱۰ وجود داشت.

(۲)

TCP

در این پروتکل ما 28 = tcp.stream داریم ، Port مبدا ما ۲۰ و Port مقصد ما ۸۰ است

UDP

با فیلتر کردن با این پروتکل udp.stream=12 و در Port 53 قابل مشاهده است

DNS

با فیلتر کردن با این پروتکل یک مورد دیده میشود که در Port 53 قابل مشاهده است که Flag ما هم در این پروتکل است