## سوال اول

Flag ==in packet UDP stream 3

Flag == { 9Y080ZO }

برای پیدا کردن فلگ مورد نظرمان  در شبکه ابتدا باید وارد وایر شارک شده وسپس فایلی که از قبل برایمان تعیین شده برای پیدا کردن فلگ مورد نظر دسترسی پیدا می کنیم. سپس پروتکل های موجود را که مشاهده کرده و همه ی آنها را  بررسی می کنیم.بعد از آن همه ی پروتکل ها را بررسی کرده و در هر پروتکل که الگوی خاصی را مشاهده کردیم و آن ها را به ترتیب بررسی میکنیم و اما این نکته ابسار اهمییت ویژه ای داردکه فلگ ممکن است در هر پروتکلی باشد و ما نباید پروتکل هایی که فیلد شدن را مورد بررسی قرار ندهیم.

مثلا پروتکل هایی که مشاهده میکنیم مثل UDP,TCP,... را با پسوند استریم چک میکنیم از مقادیر 0 و 1 و 2  به بالا سپس به هر مقداری که رسیدیم و معلوم شد در آن فلگ مورد نظر قرار دارد پس آن گزینه درست است و به جواب درست رسیدیم.

## سوال دوم

روش های مؤثر  برای تحلیل فیلترهای مختلف در یک فایل شبکه، استفاده از ابزارهای مانیتورینگ ترافیک شبکه مانند Wireshark یاNetMon  است.

تحلیل و بررسی  پروتکل‌ها: بعد از فیلتر کردن داده‌ها، می‌توانیم پروتکل‌های مختلف را تحلیل  و بررسی کنیم به عنوان مثال، اگر ما با فایل pcap یا داده‌های دیگری که توسط Wireshark ذخیره شده‌اند کار کنیم، می‌توانیم از ویژگی‌های Wireshark برای تحلیل پروتکل‌های TCP، UDP، HTTP، HTTPS، DNS و غیره استفاده کنید.

تحلیل لایه‌های مختلف: فیلترها ممکن است در لایه‌های مختلف شبکه اعمال شوند. برای مثال، فیلترهای مربوط به آدرس IP در لایه شبکه، و فیلترهای مربوط به پورت‌ها در لایه ترانسپورت قرار می‌گیرند. با تحلیل هر لایه می‌توانید فهم بهتری از ترافیک شبکه پیدا کنیم.

نتیجه گیری درمورد شبکه باید نتایج تحلیل خود را گزارش دهیم و این گزارش می‌تواند شامل توضیحات درباره فیلترهای مورد استفاده، تأثیرات آن‌ها بر شبکه، پیشنهادات برای بهبود عملکرد یا امنیت شبکه و ... باشد.