گزارشکار آزمایش چهارم ، تحلیل TCP با استفاده از Wireshark

گروه 6 چهارشنبه ساعت 30 : 16 تا 19

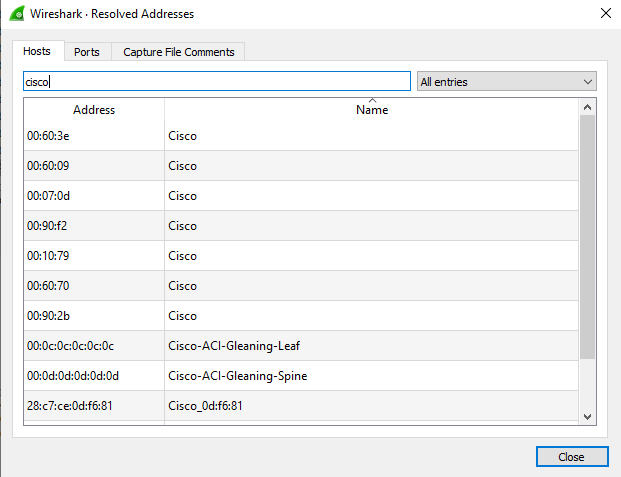
کیوان ایپچی / امیرحسین سرآهنگ

سوال 1 :

پنجره Resolver Addresses شامل 3 قسمت host ، port و ...capture است : که در تب host در بسته هایی که capture کردیم ، آدرس ها به چه اسم هایی map شدند . بعد از آن در تب port ، مشاهده می شود که چه پورت هایی داریم و چه تایپی دارند و به چه اسمی map شدند .

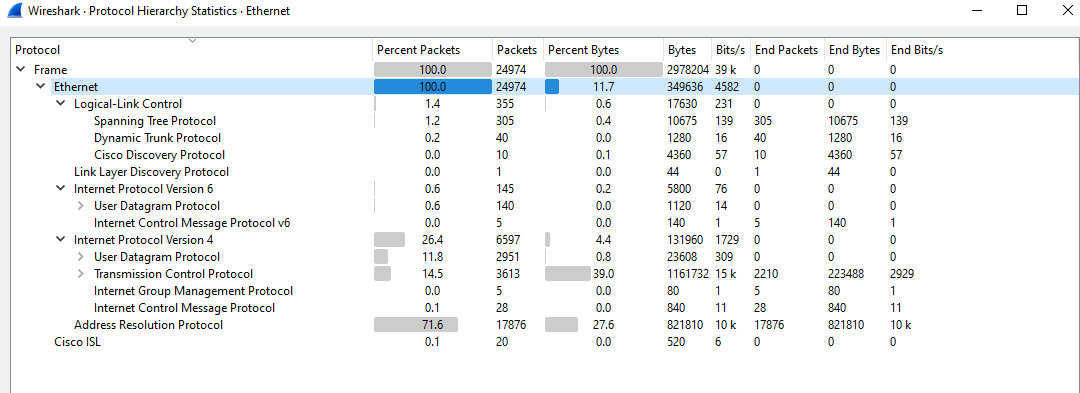
سوال 2 :

در بخش host ، cisco رو سرچ می کنیم و آدرس های فیزیکی مد نظر قابل رویت هستند .



سوال 3 :

در واقع درگاه ها و پروتوکل های مختلف مشاهده می شود و نیز 7 لایه شبکه رو هم به وضوح دیده می شود از جمله internet و transmission و ... برای مثال : 100 % پکت ها از نوع Ethernet هستند .

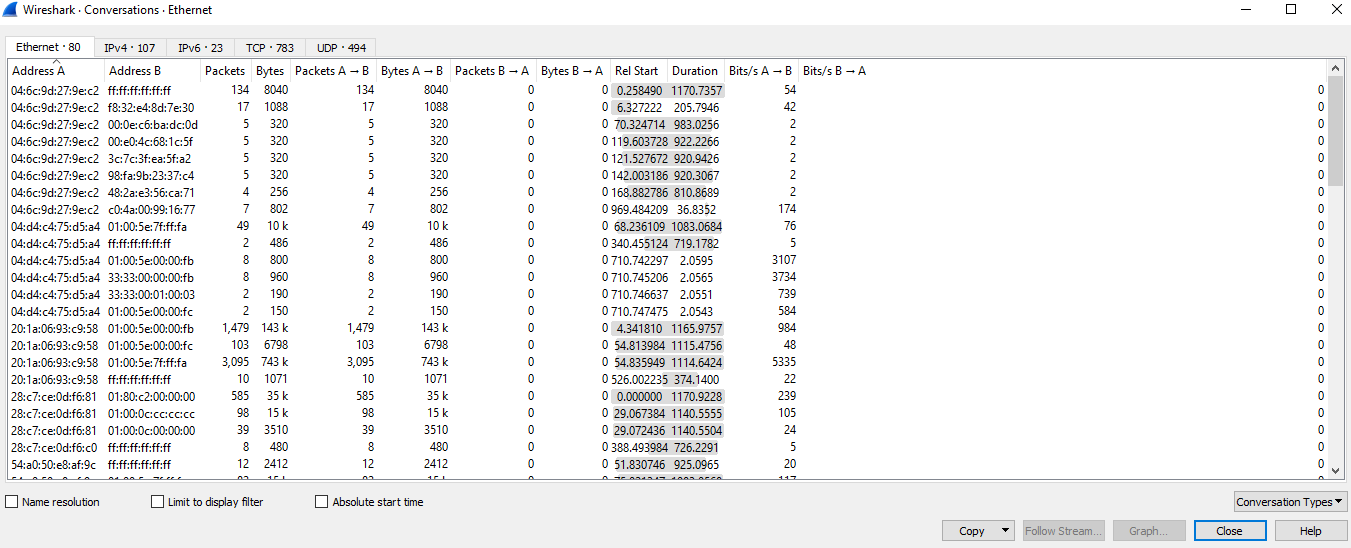


سوال 4 :

طبق تصویر بالا 26.4 % بسته ها بر روی بستر IPv4 هستند .

سوال 5 :

در واقع مشخصات جفت آدرس هارو مشاهده می کنیم که آدرسA و B و پکت های مبادله شده و حجم آن ها چقدر بوده و همچنین پکت هایی که بهم فرستاده اند بر اساس مبدا و مقصد تفکیک شده به علاوه جفت آدرس ها بر اساس پروتوکل های مختلف نیز تفکیک شده .



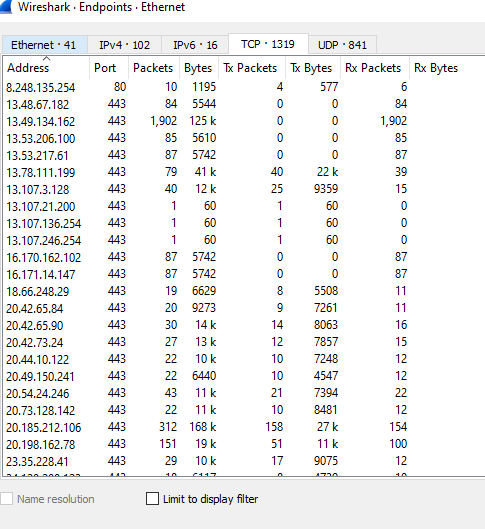
سوال 6 :

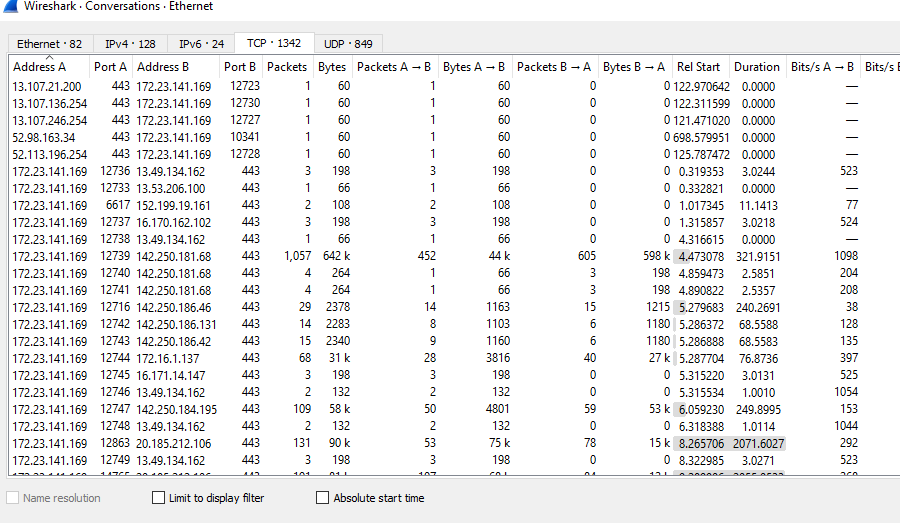
رو پروتکل TCP ، right click کردیم و از قسمت follow ، tcp stream رو انتخاب کردیم و مشاهده کردیم که دیتا به علت https بودن رمزنگاری شده است و قادر به مشاهده دیتای خام آن نیستیم .

سوال 7 :

چون در conversation داریم مبادله اطلاعات می کنیم دو طرفه هست چون هم از A به B هست و بل عکس

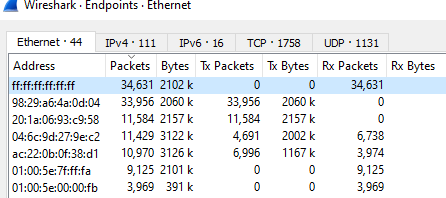
اما در endpoint از دیدگاه گره ای به موضوع نگاه می شود و آدرس ip هایی که در ارتباط tcp با سیستم ما استفاده شده اند قابل رویت هست .





سوال 8 :

لزوما بیشتر پکت رو داشتن دلیل بر defualt gateway بودن نیست اما با میشه با تخمین خوبی گفت که آدرسی که بیشترین تعداد پکت رو داره میتونه defualt gateway باشه !



سوال 9 )

در شرایط ازدحام throughput کاهش پیدا می کنه و RTT افزایش پیدا میکند اما در نقاطی که اردحام کم میشود شرایط عکس اتفاق می افتد !

در Windows scaling نیز زمانی که نشانه ای از ازدحام ظاهر می شود فرستنده مجبود به ارسال مجدد بسته ها می شود و به همین علت به طور ناگهانی کاهش پیدا می کند !

