زانا مبارکی 401130773

جواب سوال 1) فلگ CIBDG66}} در پکت شماره ی 82 با پروتکل ipv4 بود و برای پیدا کردن ان با استفاده از عبارت ! icmp && ! tcp && ! udp پکت ها را فیلتر کردم و در پکت های ipv4 یک پکت Length ان از بقیه ی پکت ها بیشتر بود به همین دلیل پکت داخل ان بود length بقیه ی پکت ها با پروتکل مختلف یکسان بود.

جواب سوال 2)

بسته های tcp همگی دارای فلگ syn هستند این فلگ نشان می‌دهد که این بسته‌ها اولین بسته‌های یک اتصال TCP هستند. و همگی از پورت 20 به 80 رفته اند. و len انها همگی 0 میباشد که نشان دهنده ی این است که اطلاعاتی داخل انها وجود ندارد.

دستگاه با استفاده از بسته های icmp بسته‌های پینگ به چندین دستگاه مختلف ارسال می‌کند. این نشان می‌دهد که کاربر در حال تلاش است تا وضعیت اتصال به این دستگاه‌ها را بررسی کند که پاسخی از برخی ار انها دریافت نشده.

در بسته های udp با توجه به اطلاعات می توان نتیجه گرفت که ترافیک نشان‌دهنده فعالیت DNS است. و همچنین این بسته ها همگی از پورت 53 به 53 رفته اند و length همه ی انها با هم برابر است.