فرهاد امان 9931006

1- Wireshark یک نرم افزار متن‌باز بر روی سیستم‌عامل‌های ویندوز و لینوکس است که با استفاده از آن می‌توانیم کار شنود و تحلیل پروتکل‌های شبکه را انجام دهیم. در واقع کار این نرم‌افزار تحلیل ترافیک شبکه است. این پروژه در چارچوب Qt و با استفاده از زبان C/Cpp توسعه داده شده است.

2- در سیستم‌عامل ویندوز برنامه Wireshark با استفاده از کتابخانه Winpcap طراحی شده و اقدام به شنود بسته‌ها می‌کند. Winpcap از بخش‌های مختلفی تشکیل شده است. در ابتدا فیلترهای توسط کاربر مشخص می‌شوند این فیلترها توسط NPF ترجمه شده و روی بسته‌ها اعمال می‌شوند (همان Capture Filter) سپس Winpcap دارای یک بافر در سطح کرنل می‌باشد. سپس packet.dll و wpcap.dll قرار دارند که اینترفیس این برنامه هستند و همچنین یک بافردر سطر کاربر نیز وجود دارد.

3- دو نوع روش برای فیلتر کردن بسته‌ها در Wireshark وجود دارد.
روش اول Capture Filter است. این فیلتر توسط NPF روی بسته‌ها اعمال می‌شود پس در واقع این فیلتر برروی دریافت بسته‌ها تاثیرگذار است. این فیلتر قبل از شروع به شنود بسته‌ها اعمال و مقداردهی می‌شود.
روش دوم Display Filter است. در این روش فیلتر بر روی بسته‌های دریافت شده تاثیر می‌گذارد. در واقع ابتدا تمام بسته‌ها جمع‌آوری می‌شوند و سپس با استفاده از این فیلتر انتخاب می‌کنیم که کدام بسته‌ها نمایش داده شوند.