پروژه دوم شبکه

مریم خدایاری

۴۰۱۱۳۰۲۹۳

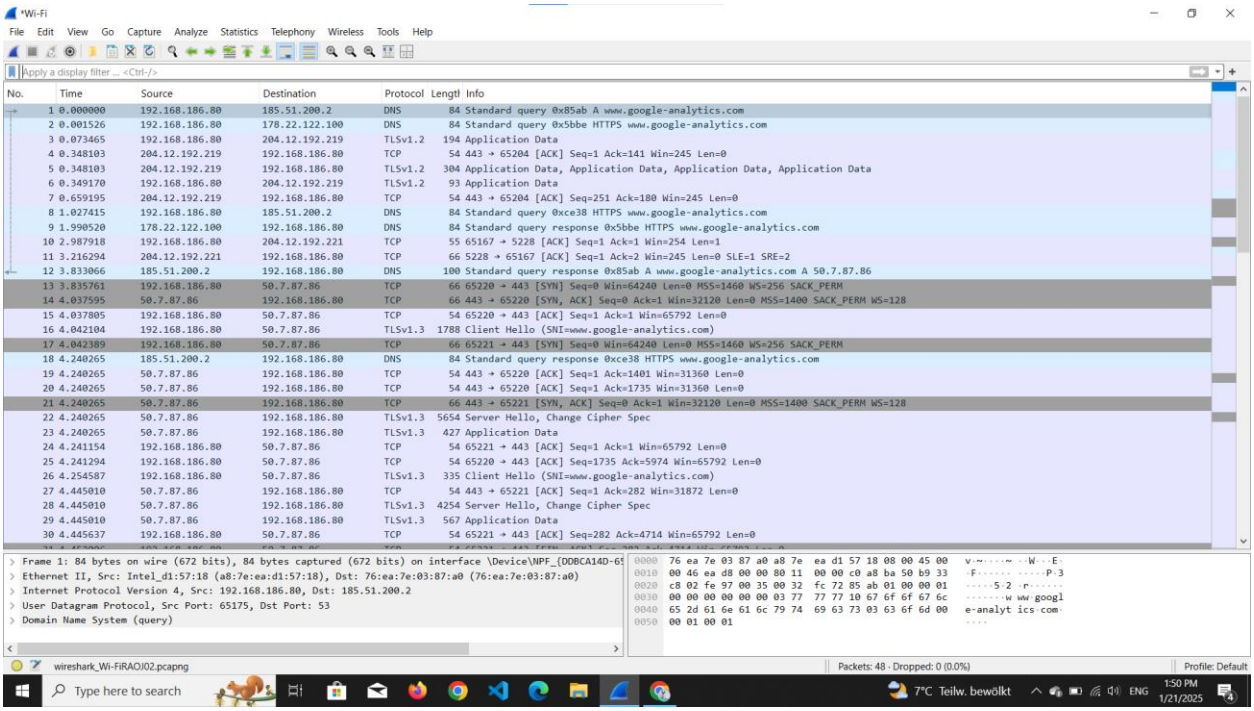
پاسخ سوال یک:

HTTP : پروتکل انتقال داده‌ها در وب است (برای درخواست صفحات وب).

DNS : برای تبدیل نام دامنه‌ها به آدرس‌های IP استفاده می‌شود.

DHCP : آدرس‌های IP را به طور خودکار به دستگاه‌های شبکه اختصاص می‌دهد.

پاسخ سوال دو:



گزارش تحلیل ترافیک شبکه با استفاده ازWireshark

در این گزارش، ترافیک کپچر شده هنگام باز کردن سایت www.w3schools.comبا استفاده از نرم‌افزار Wireshark تحلیل شده است. هدف از این تحلیل، بررسی ارتباط بین مرورگر و سرورهای مورد نیاز برای دسترسی به این سایت و همچنین شناسایی پروتکل‌های استفاده‌شده در این فرآیند است.

"تحلیل ترافیک"

۱. **پروتکل:DNS**

- در ابتدا، مرورگر برای تبدیل نام دامنه www.w3schools.comبه آدرسIP ، از پروتکل DNS استفاده کرده است.
- در بسته‌های شماره ۱ و ٤، درخواست‌های DNS (Query) به سرور DNS ارسال شده‌اند. درخواست شامل نام دامنه و نوع رکورد مورد نظر بوده است.
- پاسخ‌های DNS (Response) در بسته‌های شماره ۳ و ٦ دریافت شده‌اند که حاوی آدرس IPسرورهای مقصد است.

۲. **پروتکل:TCP**

- پس از دریافت آدرسIP ، ارتباط بین کلاینت و سرور آغاز شده است. در بسته‌های شماره ۱۰ و ۱۱، ارتباط TCP با استفاده از فرآیند **Three-Way Handshake**برقرار شده است:
  - **SYN**:کلاینت درخواست اتصال به سرور را ارسال می‌کند.
  - **SYN-ACK**:سرور این درخواست را تأیید می‌کند.
  - **ACK**:کلاینت پاسخ تأیید سرور را ارسال می‌کند.

۳. **پروتکل:TLS**

- از آنجا که سایت از HTTPS استفاده می‌کند، ارتباط ایمن از طریق پروتکل TLS برقرار شده است.

- در بسته‌های شماره ۱۴ و ۱۵، پیام‌های **Client Hello**و **Server Hello**مشاهده می‌شوند که برای شروع فرآیند رمزنگاری استفاده شده‌اند.
- مراحل دیگرTLS ، شامل **Change Cipher Spec**و **Application Data**، نشان می‌دهند که ارتباط رمزگذاری شده است.

۴. **تحلیل ترافیک:HTTP**

- پس از برقراری ارتباطTLS ، مرورگر شروع به ارسال درخواست‌های) HTTP در قالب (HTTPSمی‌کند. این درخواست‌ها احتمالاً شامل GETیا POSTبرای دریافت منابع سایت هستند. به دلیل رمزگذاری، جزئیات این درخواست‌ها در کپچر مشاهده نمی‌شود.

در نگاه کلی...

این ترافیک نشان‌دهنده فرآیند معمول باز کردن یک وب‌سایت است:

- ابتدا از **DNS**برای تبدیل نام دامنه به آدرس IP استفاده شده است.
- سپس اتصال TCP برقرار شده و از طریق **TLS**ارتباط رمزگذاری شده‌ای برای ارسال و دریافت داده‌ها ایجاد شده است.
- استفاده از پروتکل‌های استاندارد مانندDNS ، TCPو TLS امنیت و کارایی ارتباط را تضمین می‌کند.

این تحلیل نشان می‌دهد که هر یک از پروتکل‌ها نقش مهمی در برقراری ارتباط و انتقال داده‌ها در شبکه ایفا می‌کنند.