به نام خدا

# تجزیه و تحلیل بسته‌ها

# آشنایی با نرم‌افزار وایرشارک

# و پروتکل‌های HTTP و DNS

**بخش اول)** در حالی که وایرشارک در حال اجرا است، آدرس دلخواه خود را در مرورگر وارد کنید. پس از نمایش وبسایت مدنظر شما، وایرشارک را متوقف کرده و به سوالات زیر پاسخ دهید:

۱) پروتکل‌های مختلفی را که در ستون Protocol در پنجره‌ی Packet-Listing ظاهر شدند را فهرست نمایید.
۲) از زمان ارسال HTTP GET تا زمان دریافت HTTP OK چقدر طول کشیده است؟
۳) اولین پروتکلی که فعال می‌شود، چیست؟ درخواست خروجی از سیستم شما ابتدا به چه آدرسی رفته است؟ این آدرس متعلق به کجاست؟

**بخش دوم) پروتکل HTTP**

- مرورگر را باز کنید.
- وایرشارک را باز و در قسمت فیلتر، http را تایپ نمایید.
- لینکی که در قسمت قبل وارد کرده بودید را مجددا وارد نمایید. و به سوالات زیر پاسخ دهید:

۱) مرورگر شما کدام نسخه http را اجرا می‌کند؟
۲) آدرس آی پی کامپیوتر شما و سرور چیست؟

۳) از کدام پروتکل لایه انتقال استفاده می‌شود؟
۴) پورت مبدا و مقصد را مشخص نمایید.
۵) Status Code که از سرور به مرورگر شما برگشته چیست؟ این کد بیان‌کننده چیست؟

**بخش سوم) ردیابی DNS**

وایرشارک را اجرا کرده و آدرسی که در بخش‌های قبل وارد کرده بودید را مجددا در مرورگر وارد نمایید. سپس وایرشارک را متوقف کرده و به سوالات زیر پاسخ دهید:

۱) آدرس فرستنده DNS query و آدرس پیام‌های پاسخ[1] را بیابید. به وسیله UDP فرستاده شده‌اند یا TCP؟
۲) پورت مقصد پیام DNS Query و پورت مبدا پیام DNS Response را مشخص نمایید. این شماره پورت مربوط به چه سرویسی است؟
۳) پیام DNS Query به کدام آدرس آی پی فرستاده شده است؟
۴) پیام DNS Query را بررسی و نوع (Type) آن را مشخص نمایید.
۵) صفحه وب مدنظر شامل تصاویری بود. آیا قبل از بازیابی هر تصویر، میزبان شما DNS Query جدیدی فرستاده است؟

**بخش چهارم)**

وایرشارک را اجرا نمایید.

۱) دستور ping (به آدرس دلخواه) را در ویندوز اجرا کرده و نتیجه را مشاهده کنید.
۲) نتایج به دست آمده را تحلیل کنید. در زمان اجرای این دستور چه پروتکلی فعال می‌شود؟
۳) با استفاده از گزینه ... save as از منوی File بسته‌های دریافت شده را تحت نام "MyOwnCapture" ذخیره کنید.
۴) حال در لیست، همه‌ی بسته‌های از نوع پروتکل فعال شده را مشخص نموده و سعی کنید تا با گزینه ... save as این بسته‌ها را در فایلی تحت نام "MyOwnProtocol" ذخیره کنید.

[1] Response Messages