فرم گزارش کار آزمایشگاه شبکه

نام و نام خانوادگی	فرهاد امان	شماره دانشجویی	۹۹۳۱۰۰۶	نام و شماره آزمایش	۷ TCP تحلیل با استفاده از Wireshark
هدف آزمایش	در این آزمایش، با ابزارwiresharkرا بیشتر کار می‌کنیم و آمار و نمودارهای ارائه شده در آن را برای بسته‌های TCP را بررسی می‌کنیم.				
ابزارهای مورد نیاز	Wireshark				
شرح آزمایش	سوال ۱: در پنجره‌ای که باز می‌شود، سه بخش"Hosts" ، "Ports"و "Capture file comments" را مشاهده می‌کنید. در بخش"Hosts" ، Mac addressمتناظر با هاست‌ها نمایش داده می‌شود Mac . addressیک شناسه منحصر به فرد است که به رابط شبکه‌یک دستگاه اختصاص داده شده است و در لایه‌ی پیوند داده مدل OSI برای شناسایی دستگاه‌های شبکه محلی (local) استفاده می‌شود و در قالب هگزادسیمال نمایش داده می‌شود. در بخش"Ports" ، نام سرویس‌ها همراه با portو نوع سرویس آن‌ها مشخص شده است. در بخش ""Capture file comments، Commentهایی که در فایل‌ها ضبط شده‌اند، به نمایش در می‌آیند. سوال ۳: در این بخش، انواع پروتکل‌های به کار رفته در لایه‌های مختلف به صورت سلسله مراتبی با ترتیب لایه‌ها نمایش داده شده‌اند. برای هر پروتکل، درصد packetهایی که آن پروتکل را دارند، تعداد آن packetها، درصد بایت و تعداد آن، سرعت بر حسب bits/s و غیره به صورت آمار نمایش داده شده است.				

	سوال ۴: همانطور که در تصویر بالا نیز نمایش داده شده است،95.3درصد از ارتباط های IPv4از TCPاستفاده میکنند. سوال ۵: در این بخش، نشست‌های مختلف با دسته‌بندی پروتکل‌های مختلف نمایش داده می‌شوند. برای هر نشست، اطلاعاتی اعم از آدرس دو طرف conversation، تعداد packetها و اندازه مجموع آن‌ها، تعداد packetهای ارسال شده از هر host به دیگری و غیره نمایش داده شده است. سوال ۶: در پنجره‌ای که باز می‌شود، شما اطلاعات آماری هر نقطه پایانی (endpoint) را مشاهده می‌کنید. این اطلاعات شامل نمایش اطلاعات هر endpoint در دسته‌بندی‌های مختلف بر اساس پروتکل است و شامل مواردی مانند آدرس آن، تعداد و اندازه packetهایی که با آن در ارتباط بوده‌اند (ارسال یا دریافت) و نیز تعداد بسته‌های دریافت شده و ارسال شده و اندازه مجموع هر کدام می‌باشد. سوال ۷: ابتدا آدرس ipسیستم خود را با استفاده از دستور ipconfig /all مشاهده میکنیم. حال، در بخش TCPدر پنجره endpoints، آدرس‌هایی که برابر با ip addressما نیستند را میتوان آدرس هایی دانست که با آن ها در ارتباط بوده ایم. سوال ۸: سیستم محلی ما بیشتر از سایر آدرس‌ها در ارتباط‌های ضبط شده شرکت کرده است. بنابراین، معمولاً تعداد بسته و یا حجم داده مبادله شده توسط آدرس ما، از سایر آدرس‌ها بیشتر است. در اینجا، دو Mac address وجود دارند که حجم داده بسیار زیادی انتقال داده اند. بیشترین داده مربوط به آدرس مشخص شده است و احتمال داده می‌شود مربوط به سیستم محلی ما باشد. حالا، با دستور "ipconfig /all" در cmd می‌توانیم آدرس Mac خود را مشاهده کنیم و با آدرس بالا مقایسه کنیم.
نتیجه‌گیری	بخش‌های مختلف آمارهای ارائه شده توسط Wireshark مانند Resolved Addresses ، Protocol Hierarchy، و نمودارهایی مانند I/O graph و نیز نمودارهای مختلف TCP streamرا مشاهده و اطلاعات موجود در هر یک را بررسی کردیم. همچنین آمارهایی اعم از conversation های موجود، endpointها و ... را نیز مشاهده کردیم و اطلاعات هر یک را مورد بررسی قرار دادیم.