بخش اول: Ethernet

گام های زیر را انجام دهید :

- ابتدا می بایست cache مرورگر خود را پاک کنید.
- وایرشارک خود را در حالت گوش دادن بسته‌ها قرار دهید.
- آدرس مقابل را در مرورگر خود وارد کنید : http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
- عملیات ضبط کردن بسته ها توسط وایرشارک را متوقف کنید.
- از آنجایی که در این تمرین به پروتکل های بالای لایه لینک نیازی نداریم در نتیجه لیست بسته های مورد نظر برای گوش دادن را تغییر بدهید : برای این کار در وایرشارک به منوی Analyze رفته و Enabled Protocols را انتخاب کنید و سپس تیک گزینه IP را بردارید .

بر اساس محتویات فریم اترنت مربوط به پیام HTTP GET به سوالات زیر پاسخ دهید .

۱. آدرس ۴۸ بیتی لینک اترنت کامپیوتر خود را بیابید .
۲. آدرس ۴۸ بیتی لینک اترنت مقصد را بیابید ، آیا این آدرس اترنت gaia.cs.umass.edu می باشد ؟ کدام دستگاه این آدرس لینک اترنت را دارد ؟
۳. مقدار Hexadecimal را برای دو بایت نوع فریم مشخص کنید؟ این دو بایت به چه پروتکلی از لایه بالایی مربوط می شود؟
۴. چند بایت از ابتدای فریم اترنت مربوط به کاراکتر G در "GET" می باشد؟

حال بر اساس محتویات فریم اترنت مربوط به HTTP Response به سوالات زیر پاسخ دهید .

۵. آدرس سورس را در فریم اترنت بیابید . آیا این آدرس کامپیوتر شما است یا gaia.cs.umass.edu ؟ کدام دستگاه این آدرس لینک اترنت را دارد ؟
۶. آدرس مقصد در فریم اترنت را بیابید . آیا این آدرس اترنت کامپیوتر شماست ؟
۷. مقدار Hexadecimal را برای دو بایت نوع فریم مشخص کنید ؟ این دو بایت به چه پروتکلی از لایه بالایی مربوط می شود ؟
۸. چند بایت از ابتدای فریم اترنت مربوط به کاراکتر O در "OK" می باشد ؟

بخش دوم: ARP

می‌دانیم پروتکل ARP معمولا جفت‌های دوتایی IP به Ethernet address translation را در یک cache نگه می‌دارد. دستور arp (هم در MS-DOS و هم در Linux/Unix) برای مشاهده و تغییر دادن محتوای این cache مورد استفاده قرار می‌گیرد. از آنجایی که دستور arp و پروتکل ARP اسم مشابهی دارند معمولا با هم اشتباه گرفته می‌شوند. اما در نظر داشته باشید که این دو متفاوت هستند. دستور arp برای مشاهده و تغییر محتوای cache در پروتکل ARP است در حالی که پروتکل ARP فرمت و معنای پیام‌هایی که ارسال می‌شوند و کارهایی که باید روی پیام‌ها هنگام ارسال و دریافت انجام می‌شوند را مشخص می‌کند.

MS-DOS : دستور arp در مسیر ۳۲c:\windows\system قرار دارد پس برای اجرای این دستور می‌توان "arp" یا "c:\windows\system32\arp" را در محیط command line تایپ کرد.

Linux/Unix/Mac OS : فایل قابل اجرای arp ممکن است در مسیرهای متفاوتی باشد اما به طور معمول برای Linux در مسیر /sbin/arp و برای برخی از انوع Unix در مسیر /usr/etc/arp قرار دارد.

- دستور arp بدون هیچ آرگومانی در ویندوز محتوای کش ARP در کامپیوتر شما را نمایش خواهد داد. دستور arp را اجرا کنید.

۹. محتوای کش ARP کامپیوترتان را بنویسید. معنای مقدار هر ستون چیست؟

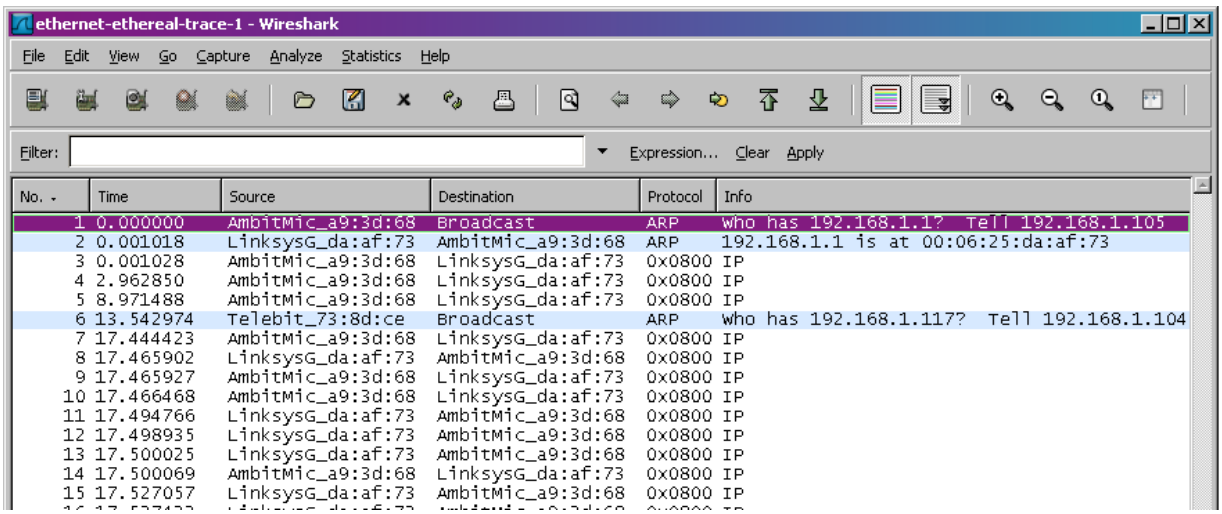
برای اینکه مطمئن شویم کامپیوتر شما پیام‌های ARP را ارسال و دریافت می‌کند، باید کش ARP را پاک کنیم. زیرا در غیر این صورت کامپیوتر شما احتمالا زوج IP به Ethernet address translation مورد نظر را در کش ARP پیدا می‌کند و نیازی به ارسال پیام ARP نخواهد داشت.

- MS-DOS : دستور "arp -d *" حافظه‌ی کش ARP را پاک می‌کند. علامت d- نشان‌دهنده‌ی عملیات پاکسازی و کاراکتر * مشخص می‌کند که همه جدول‌های موجود حذف شوند.
- Linux/Unix/Mac OS : دستور "arp -d *" حافظه‌ی کش ARP را پاک می‌کند. برای اجرای این دستور نیاز به دسترسی root دارید. اگر دسترسی root ندارید و نمی‌توانید wireshark را روی یک ماشین با سیستم عامل ویندوز اجرا کنید، می‌توانید بخش trace collection این آزمایش را انجام ندهید و فقط از trace بحث‌شده در پانویس قبلی استفاده کنید.

مراحل زیر را انجام دهید:

- همانند توضیحات بالا کش ARP را پاک کنید.
- سپس مطمئن شوید کش مرورگرتان خالی است. (اگر خالی نیست آن را خالی کنید.)
- ضبط کردن بسته‌ها در wireshark را آغاز کنید.
- آدرس http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html را در مرورگر خود وارد کنید. (مرورگر شما باید دوباره سند حقوق ایالات متحده را نمایش دهد.)

- ضبط کردن بسته‌ها در wireshark را متوقف کنید. بازهم کاری به IP یا پروتکل‌های لایه‌های بالاتر نداریم، پس پنجره‌ی "listing of captured packets" را تغییر دهید تا فقط پروتکل‌های زیر لایه‌ی IP را نمایش دهد. برای این کار می‌توان وارد مسیر Analyze->Enabled Protocols شد و تیک IP را برداشت و OK را انتخاب کرد. حال باید پنجره wireshark شما مانند شکل زیر باشد.



به سوالات زیر پاسخ دهید:

۱۰. مقدار hex آدرس مبدا و مقصد در Ethernet frame حاوی پیام درخواست ARP چیست؟

۱۱. مقدار hex برای فیلد ۲بایتی type در Ethernet Frame چیست؟ این مقدار با چه چیزی از پروتکل‌های بالایی مطابقت دارد؟

۱۲. مشخصات ARP را از این لینک دریافت کنید. همچنین این لینک می‌تواند مفید باشد.

بعد از چند بایت از اول Ethernet frame فیلد opcode مربوط به ARP آغاز می‌شود؟

آیا پیام ARP حاوی آدرس IP فرستنده است؟

کجای یک درخواست ARP سوال مبتنی بر آدرس Ethernet ماشینی که مرتبط با IP است پرسیده می‌شود.

۱۳. حال پیام ARPی که در جواب درخواست ARP فرستاده شد را پیدا کنید.

بعد از چند بایت از اول Ethernet frame فیلد opcode مربوط به ARP آغاز می‌شود؟

کجای پیام ARP جواب مربوط به ARP قبلی ظاهر می‌شود؟

۱۴. مقدار hex آدرس مبدا و مقصد در Ethernet frame حاوی پیام جواب ARP چیست؟

۱۵. مقدار زمانی که یک عضو در کش ARP باقی می‌ماند چقدر است؟ می‌توانید با مانیتور کردن کش این مقدار را بیابید یا در سند مربوط به سیستم عامل خود آن را پیدا کنید. اگر از روش مانیتور کردن جواب را یافتید روش کار را شرح دهید و اگر تحقیق کردید منبع را مشخص کنید.