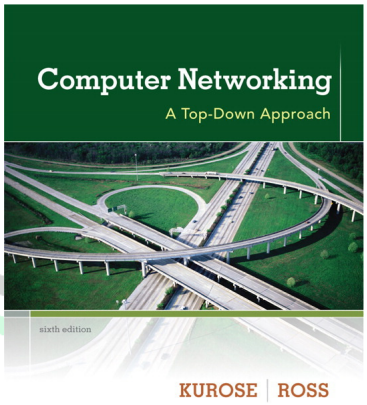
KOCAELİ ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Wireshark Lab: Getting Started v6.0



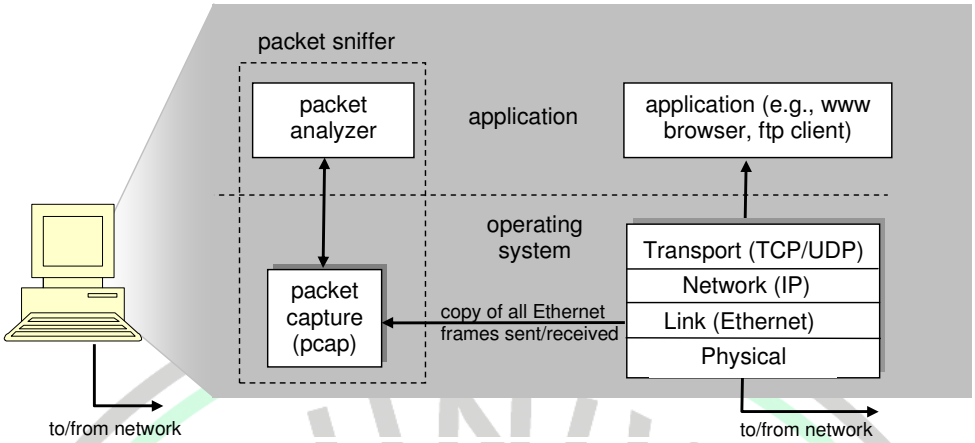
Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Çin Atasözü

Bu ilk Wireshark laboratuvarında Wireshark ile tanışmış olacaksınız ve bazı basit paket yakalama örnekleri yapıp bunları yorumlayacaksınız.

Yürütülen protokoller arasında gidip gelen mesajları gözlemlemek için kullanılan temel bir araç paket dinleyicisi (packet sniffer) olarak adlandırılır. Adından da anlaşılacağı gibi, bir paket dinleyicisi bilgisayarınıza gelen ya da bilgisayarınız tarafından gönderilen mesajları yakalar ("sniffs") ; ayrıca bu yakalanan protokol mesajlarına ait pek çok farklı alanı saklar ve / veya görüntüler. Bir paket dinleyicisinin kendisi pasiftir. Bilgisayarımızda çalışan uygulamalar ve protokoller tarafından gönderilen ve alınan mesajları gözlemler, ancak kesinlikle paketleri kendisi göndermez. Benzer şekilde alınan paketlerde kesinlikle açıkça paket dinleyicisini adreslemez. Bunun yerine, bilgisayarımızda çalışan uygulama ya da protokoller tarafından gönderilen ya da alınan paketlere ait bir kopya alır.

Şekil 1, bir paket dinleyicisinin yapısını göstermektedir. Şekil 1' in sağında bilgisayarımızda normal olarak çalışan protokoller (Buradaki durumda internet protokolleri) ve uygulamalar (örneğin bir web tarayıcı ya da ftp istemcisi gibi) bulunmaktadır. Şekil 1' de kesikli dikdörtgen içerisinde gösterilen paket dinleyicisi bilgisayarınızda var olan yazılım üzerine bir eklentidir, iki parçadan oluşur. **Paket yakalama kütüphanesi** bilgisayarınız tarafından gönderilen veya alınan her bağlantı katmanı çerçevesinin bir kopyasını alır. Mesajlar HTTP, FTP, TCP, UDP, DNS, veya IP gibi yüksek seviye protokoller aracılığıyla değiştirilir, bunların tamamı sonunda bağlantı katmanı çerçeveleri içerisinde kapsüllenir ve fiziksel ortam (örnek olarak Ethernet Kablosu) üzerinden iletilir. Şekil 1' de fiziksel ortam olarak Ethernet ortamı olduğu varsayılmıştır ve böylece tüm üst katman protokolleri sonunda bir Ethernet çerçevesi ile kapsüllenmiştir. Bilgisayarımızda çalışan uygulama ve protokollerin tamamından gönderilen ve alınan mesajlar bağlantı katmanı çerçevelerini yakalayarak elde edilmiş olur.



Şekil 1: Paket Dinleyicinin Yapısı

Paket yakalayıcının ikinci bileşeni ise **paket çözümleyicisi**dir (packet analyzer), Paket çözümleyicisi bir protokol mesajı içindeki tüm alanların içeriğini görüntüler. Bunu yapabilmek için, paket çözümleyicisinin protokol tarafından gönderilip alınan tüm mesajların yapısını anlaması gerekir. Örneğin, Şekil 1' de http protokolü tarafından mesaj alışverişinde kullanılan farklı alanları görüntülemek isteyelim. Paket çözümleyicisi Ethernet çerçevelerinin formatını anlar ve bu yüzden bir Ethernet çerçevesi içerisindeki IP datagramını da tanıyabilir. Ayrıca IP datagram formatını da anlar, bu yüzden IP datagram içindeki TCP segmentini çıkartabilir. Son olarak TCP segmentinin yapısını anlar bu yüzden TCP segmenti içerisinde yer alan HTTP mesajını çıkarabilir. Sonuç olarak HTTP protokolünü anlar ve böylece örneğin; HTTP mesajının ilk byte' ının "GET," "POST," ya da "HEAD," kelimelerinden bir tanesi olduğunu bilir.

Wireshark'a Giriş

Wireshark'ı çalıştırmak için, Wireshark ve Libpcap veya WinPcap paket yakalama kütüphanelerini destekleyen bir bilgisayarın olması gerekir. Wireshark'ı yüklediğinizde işletim sisteminizde Libpcap yazılımı yüklü değilse, kendiliğinden yüklenmiş olacaktır. http://www.wireshark.org/download.html linkinden desteklenen işletim sistemleri ve Wireshark'ı indirebileceğiniz web sitelerinin adresine ulaşabilirsiniz.

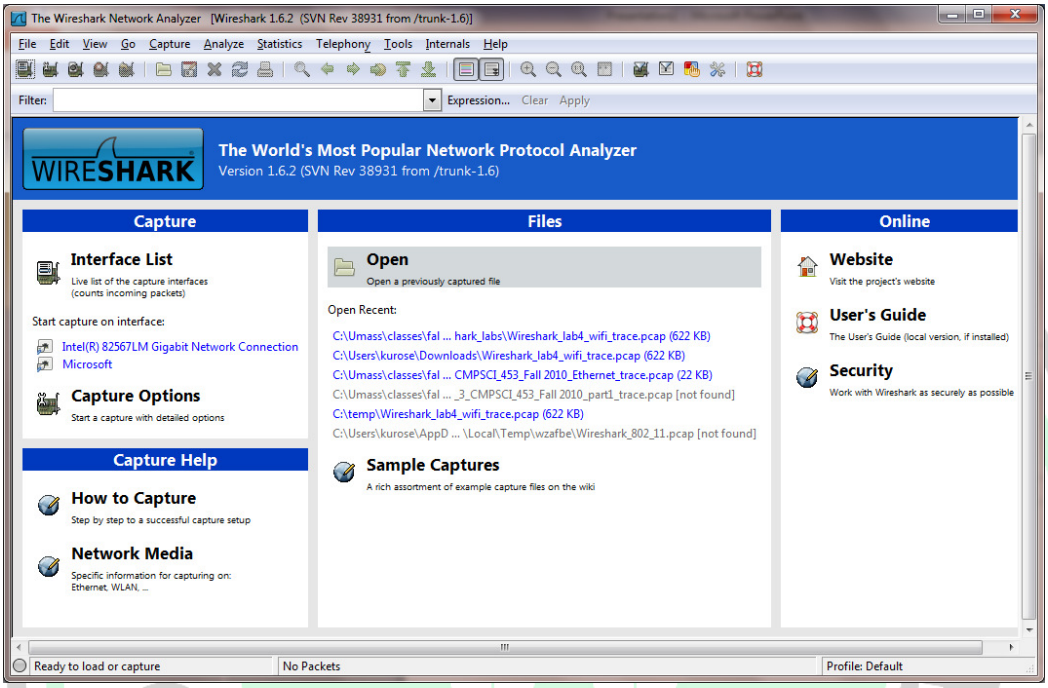
Wireshark yazılımın indirilmesi yüklenmesi:

- http://www.wireshark.org/download.html adresine gidin ve Wireshark ı bilgisayarınıza indirin.

Eğer yükleme veya Wireshark'ı çalıştırıken sorun yaşarsanız, sık sorulan sorular (FAQ) bölümünde pek çok yardımcı ve ilginç ipuçları bulunmaktadır.

Wireshark' ın Çalıştırılması

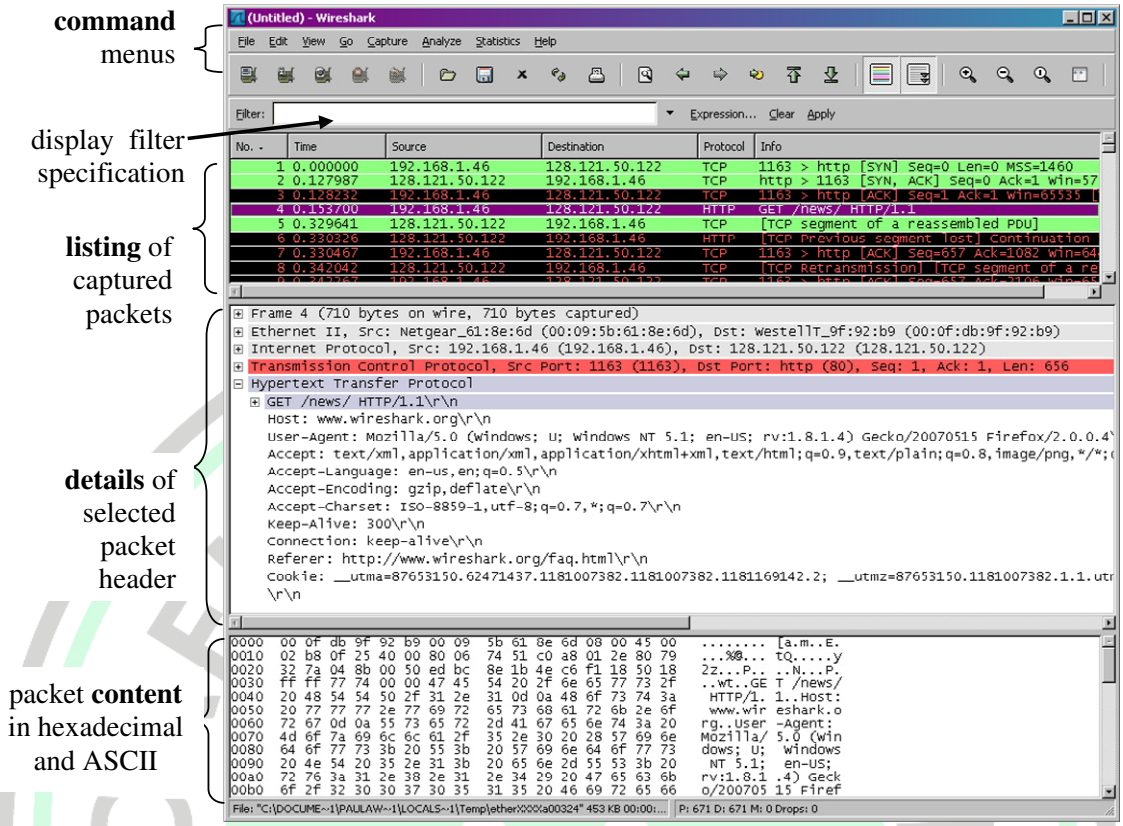
Wireshark programını çalıştırdığınızda aşağıda görülen başlangıç ekranı ile karşılaşırsınız:



Şekil 2: Wireshark Başlangıç Ekranı

Ekranın sol üst tarafına bir göz atarsanız – bir "Arayüz Listesi"göreceksiniz. Bu liste, bilgisayarınızdaki ağ ara yüzlerinin listesidir. Bir ara yüzü seçtiğinizde, Wireshark bu ara yüzdeki tüm paketlerini yakalayacaktır. Yukarıdaki örnekte, bir Ethernet ara yüzü (Gigabit ağ bağlantısı) ve kablosuz ara yüzü ("Microsoft") vardır.

Eğer paket yakalamayı başlatmak için bu ara yüzlerden birine tıklarsanız , aşağıdaki gibi bir ekran görüntülenecektir. Bu ekranda yakalanan paketlere ait bilgiler gösterilmektedir. Bir kere paket yakalamaya başladıktan sonra, "Capture" menüsünden Stop seçeneği seçilerek paket yakalamayı durdurabilirsiniz.



Şekil 3: Paket yakalama ve analizi sırasında Wireshark Grafiksel Kullanıcı Ara yüzü

Wireshark ara yüzünün beş ana bileşeni vardır:

- **Komut menüleri (command menus)** ana pencerenin üst kısmında bulunan standart açılan menülerdir. Şimdilik bizi ilgilendiren menüler File ve Capture menüleridir. File menüsü yakalanmış olan veri paketlerini kaydetmemizi ya da daha önce yakalanmış olan veri paketlerini açabilmemizi, ve Wireshark uygulamasından çıkmayı sağlar. Capture menüsü ise paket yakalamaya başlamayı sağlar.
- **Packet-listing penceresi (listing of captured packets)** yakalanmış olan her paket için bir satırlık açıklama içerir ve içerisinde Wireshark tarafından verilmiş paket numaraları(bu numara hiç bir protocol başlığı tarafından kullanılmayan bir numaradır), paketlerin yakalanma zamanı, paketlerin kaynak ve hedef adresleri, protokol çeşidi ve paket tarafından sağlanan protokole özgü bilgiler vardır. Paket listesi herhangi bir sütun adının üzerine tıklayarak bu kategorilerden herhangi birine göre sıralanabilir. Protokol tipi alanı bu paketleri gönderen ya da alan üst düzey protokollerin bir listesini içerir, (yani, bu protokol bu paket için kaynak ya da nihai alıcıdır)
- **Packet-header details penceresi (details of selected packet header)** packet-listing penceresinde seçilen (vurgulanan) paket hakkında ayrıntılı bilgi sağlar. (packet listing penceresinden bir paket seçmek için, farenin imlecini paketin tek satırlık özeti üzerine getirin farenin sol tuşu ile tıklayın.) Bu sayfa Ethernet

çerçevesi hakkında ve bu paketi içeren IP datagramı hakkında ayrıntılı bilgi içerir (gönderilen paketin Ethernet arayüzü üzerinden gönderilip alındığını varsayar) Packet details penceresindeki, Ethernet ve IP katmanına ait görüntülenen detaylı bilgi miktarı, Ethernet çerçevesi ya da IP datagramı hattının solundaki artı / eksi kutularına tıklayarak genişletilip küçültülebilir. Eğer paket TCP veya UDP üzerinden taşınmışsa, TCP veya UDP protokollerine ait detaylarda ayrıca görüntülenecektir. Bu detay pencereleri de benzer şekilde büyütülüp küçültülebilir. Son olarak, üst düzey protokole ait detaylar da ayrıca gösterilmektedir.

- **Packet-contents penceresi** yakalanmış olan çerçevenin tüm içeriğini görüntüler, İçeriği hem ASCII hem de hexadecimal formatta görüntüler.
- Wireshark grafik kullanıcı ara yüzünün üst kısmına doğru olan alan **packet display filter** alanıdır**.** Bu alanın içerisine packet-listing penceresine yer alan bilgileri filtrelemek için protokol ismi ya da farklı bilgiler girilebilir. (aynı işlem packet-header ve packet-contents pencerelerinde de uygulanabilir.). Aşağıdaki örnekte, packet-display filter alanını kullanarak saklı Wireshark paketlerinin HTTP mesajlarından bazılarını bulacağız.

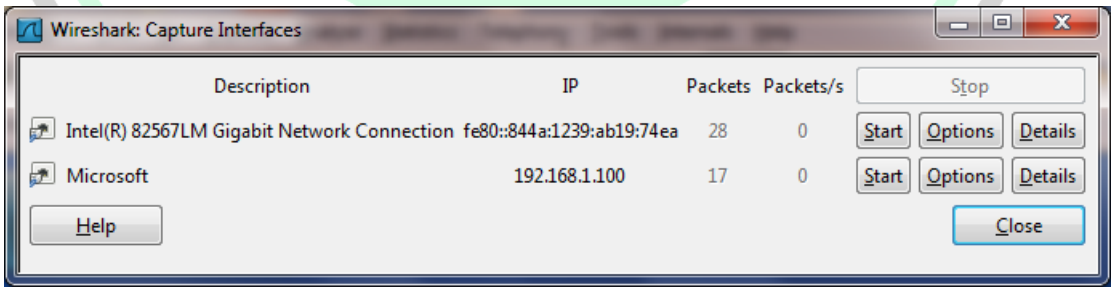
Wireshark ile Filtreleme Örneği

Herhangi bir yazılımın yeni bir bölümünü öğrenmek için en iyi yol denemektir! Aşağıda adımlarını gerçekleştirin:

1. Seçmiş olduğunuz ana sayfayı açacak favori web tarayıcınızı açın.

2. Wireshark yazılımını başlatın. Şekil 2 ‘ de gösterilen ekran benzeri bir ekran ile karşılaşacaksınız. Wireshark henüz paket yakalamaya başlamamıştır.

3. Paketleri yakalamaya başlamak için, Capture menüsünü seçin ve buradan da Interfaces’ı *seçiniz*. Bu işlem ile Şekil 4’ te de gösterildiği gibi “Wireshark: Capture Interfaces” penceresi açılacaktır.



Şekil 4: Wireshark Capture Interface Penceresi

4. Açılan pencerede bilgisayarınızda yer alan ara yüzlerin listesinin yanı sıra şimdiye kadar bu ara yüzler üzerinde gözlemlenen paketlerin sayısını da göreceksiniz. Paketleri yakalamayı istediğiniz ara yüz için Start a tıklayın. (Bu örnek de Intel (R) 82567LM Gigabit Network Connection arayüzü seçildiği durum). Paket

yakalama işlemi şimdi başlayacaktır.- Wireshark şimdi bilgisayarınız tarafından gönderilen ve alınan paketleri yakalıyor!

5. Paketleri yakalamaya başladığınızda, Şekil 3 de görülen pencere benzeri bir pencere görünecektir. Bu pencere yakalanmış olan paketleri gösterir. *Capture* pulldown menüsünü ve *Stop* seçeneğini seçerek, *paket* yakalama işlemini durdurabiliriz. Ancak şu anda paket yakalama işlemini durdurmayın. İlk olarak bazı ilginç paketleri yakalamayı deneyelim. Bunu yapmak için, bir ağ trafiğinin oluşturulmasına ihtiyacımız var. Trafiği web tarayıcıyı kullanarak oluşturalım. Web tarayıcısı bir web sitesinden herhangi bir içeriği indirmek için bizim detaylı olarak ele alacağımız HTTP protokolünü kullanacaktır.

6. Wireshark çalışırken tarayıcıya aşağıdaki URL' yi yazın:

   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
   ve sayfayı tarayıcınız aracılığıyla görüntüleyin. Bu sayfayı görüntülemek için tarayıcınız gaia.cs.umass.edu' nun HTTP sunucusu ile iletişime geçecektir ve bu sayfayı indirmek yerine sunucu ile HTTP mesajlarını değişecektir. Bu HTTP mesajlarını içeren Ethernet çerçeveleri (bunun yanında Ethernet adaptöründen geçen diğer çerçevelerde) Wireshark tarafından yakalanacaktır.

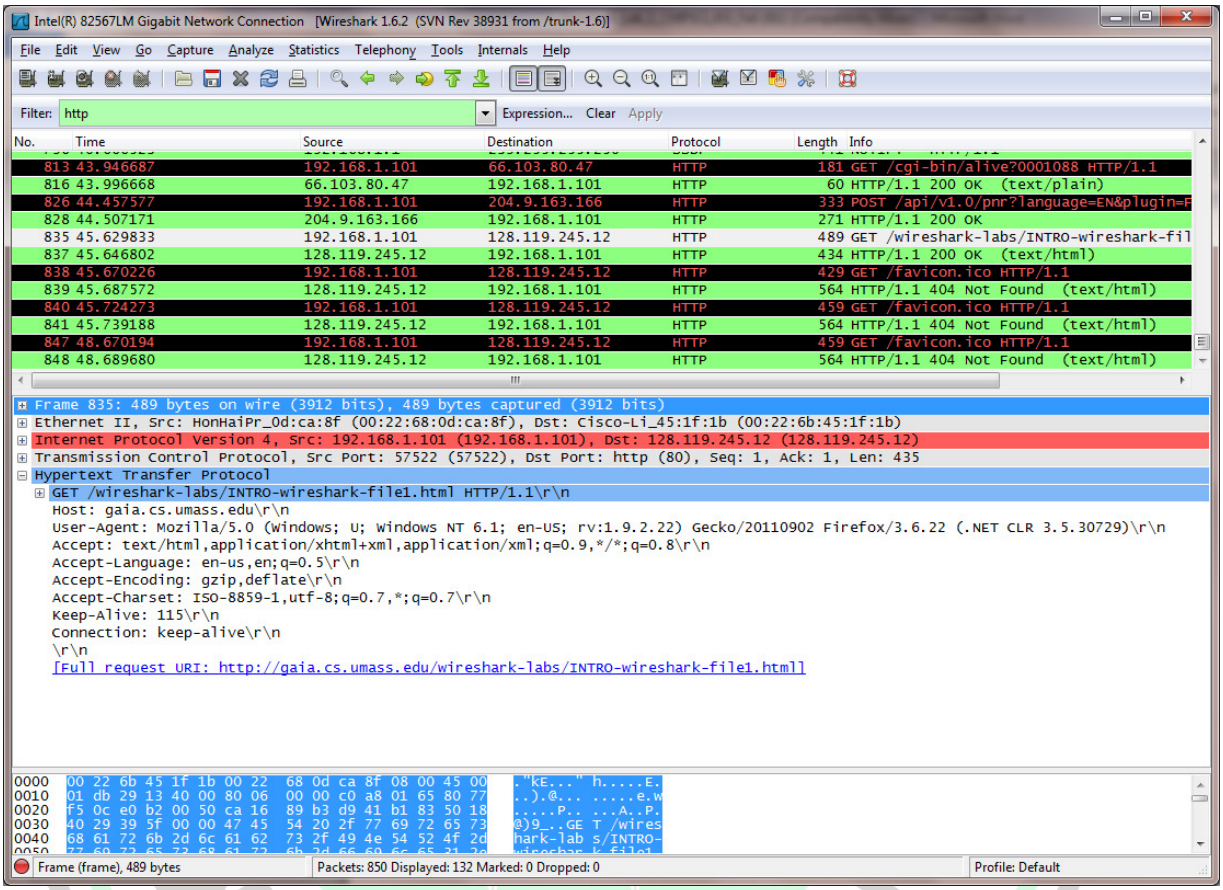
7. Tarayıcınız INTRO-wireshark-file1.html sayfasını görüntüledikten sonra Wireshark capture penceresinden stop seçeneğini seçerek paket yakalamayı durduruyoruz. Wireshark ana penceresi şimdi Şekil 3 benzeri bir pencere olarak gözükmelidir. Şu anda canlı veri paketlerine sahipsiniz ve bu paketler bilgisayarınız ile diğer ağ elemanları arasında gidip gelen tüm protokol mesajlarını içeriyor! gaia.cs.umass.edu web sunucusu ile yapılan HTTP mesaj değişimleri yakalanan paket listesinin bir yerinde görünmelidir. Ancak bunun yanında görüntülenen pek çok farklı tip paket de olacaktır. (Örnek olarak Şekil 3 te protokol kolonunda yer alan farklı tip protokollere bakınız.) Yaptığınız işlem sadece bir web sayfasını indirmek olsa bile, bilgisayarınızda çalışan ve kullanıcılar tarafından görülmeyen pek çok farklı protokol vardır.

8. Ana wireshark penceresinin üstünde yer alan "Display filter specification" penceresine "http" yazın (tırnak işaretleri olmadan, küçük harflerle, wireshark içerisinde tüm protokol isimleri küçük harflerle yazılır). Sonra ("http" kelimesini girdiğiniz yerin sağında yer alan) Apply seçeneğini seçin. Böylece packet-listing penceresinde yalnızca HTTP mesajları görüntülenecektir.

9. Bilgisayarınızdan gaia.cs.umass.edu HTTP sunucusuna gönderilen HTTP GET mesajlarını bulunuz. "yakalanan paketlerin listesinde" ("listing of captured packets") (Şekil 3' te Wireshark'ın bir bölümü olarak gösterilmiştir.) HTTP GET mesajını arayınız. HTTP GET mesajını seçtiğinizde Packet Header penceresinde Ethernet çerçevesi, IP datagramı, TCP segmenti ve HTTP mesaj başlık bilgisi görüntülenecektir.

10. Wireshark' tan çıkın.

Tebrikler ! İlk laboratuvarı tamamladınız.



Şekil 5: 9. Adımdan Sonra Wireshark Penceresi

Neler Öğrendik?

Wireshark deneyiminize dayanarak aşağıdaki soruları cevaplayınız:

1. 7. Adımda yer alan filtrelenmemiş packet-listing penceresinde yer alan protokollerden üç farklı protokolü gösteriniz.

2. HTTP GET mesajı gönderilip cevap olarak HTTP OK mesajı gelene kadar ne kadar zaman geçmiştir?
   (Varsayılan olarak packet-listing penceresinde yer alan zaman değeri saniye olarak Wireshark izlemeye başladığı zamandan itibaren geçen zamanı gösterir. Time kolonunun formatını time-of-day formatına dönüştürmek için Wireshark'ın View menüsünüden Time DisplayFormat seçeneğini seçip ardından gelen seçeneklerden Time-of-day seçeneğini seçmelisiniz.)

3. gaia.cs.umass.edu 'nun internet adresi nedir? (www-net.cs.umass.edu olarak da kllanılabilir)? Sizin bilgisayarınızın internet adresi nedir?
   - **http://whatismyipaddress.com/** web sitesine girdiğinizde bilgisayarınızın internet adresini öğrenebilirsiniz. Wireshark da bulduğunuz bilgisayarınızın internet adresi **http://whatismyipaddress.com/** da gösterilen internet adresinden **farklı mı ?** Farklı ise bu fark neden kaynaklanıyor belirtiniz.

4. Yukarıdaki 2. Soruda bahsedilen HTTP GET ve HTTP OK mesajlarının çıktısını alınız.
   (Bu işlemi yapabilmek için Wireshark'ın File menüsünden Print seçeneğini seçiyoruz. Ardından "*Selected Packet Only*" seçeneğini ve *"Print as displayed"* butonunu seçip OK butonuna tıklayarak işlemimizi tamamlıyoruz.)