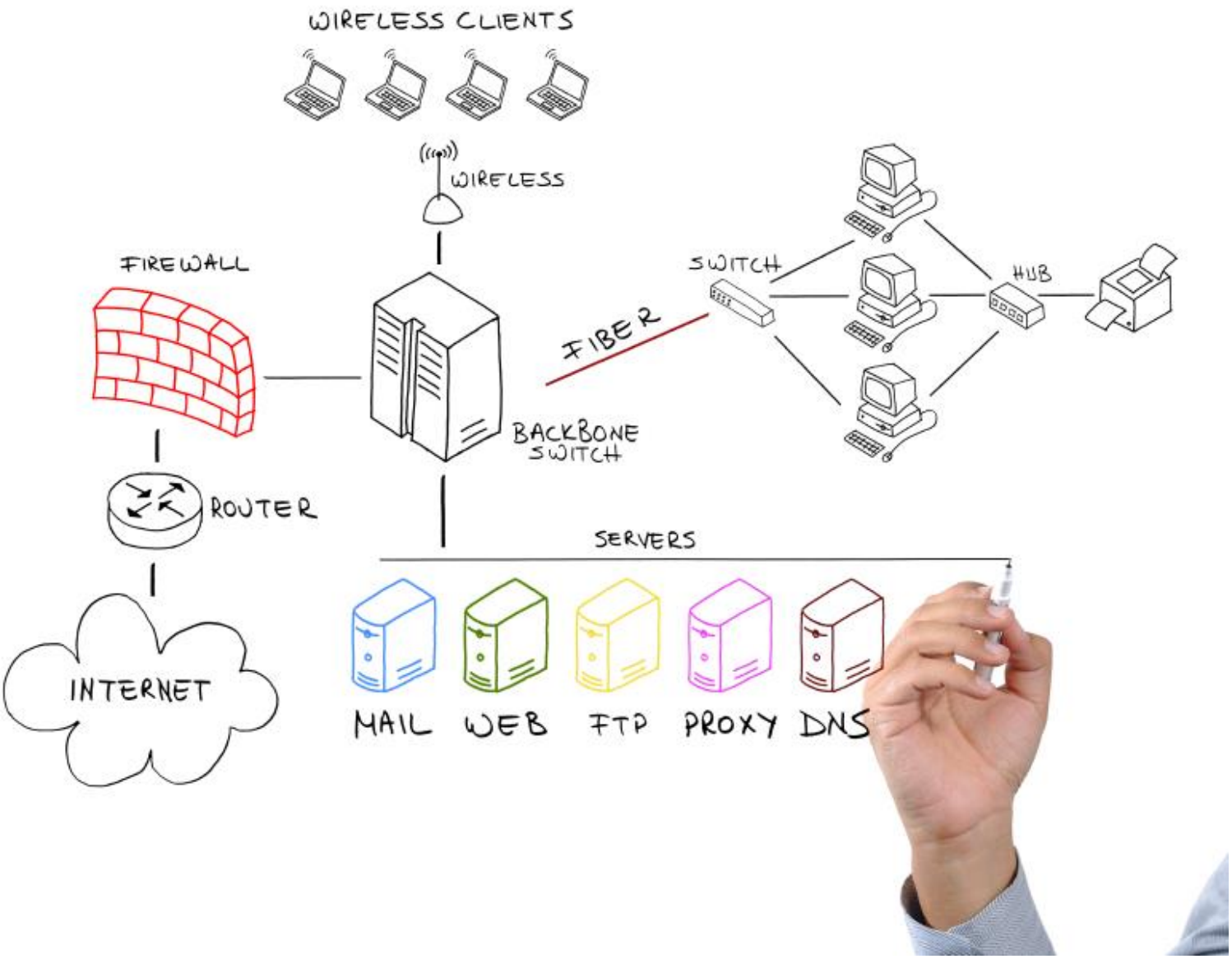
T.C.
FATİH
SULTAN
MEHMET
VAKIF ÜNİVERSİTESİ
2010



BİLGİSAYAR AĞLARI

LABORATUVAR

6

1. Önkoşullar

1.1. Temel teknoloji kullanabilmeli
1.2. Bilgisayar kavramlarına hakim olmalı
1.3. Veri yapılarını bilmeli

2. Giriş

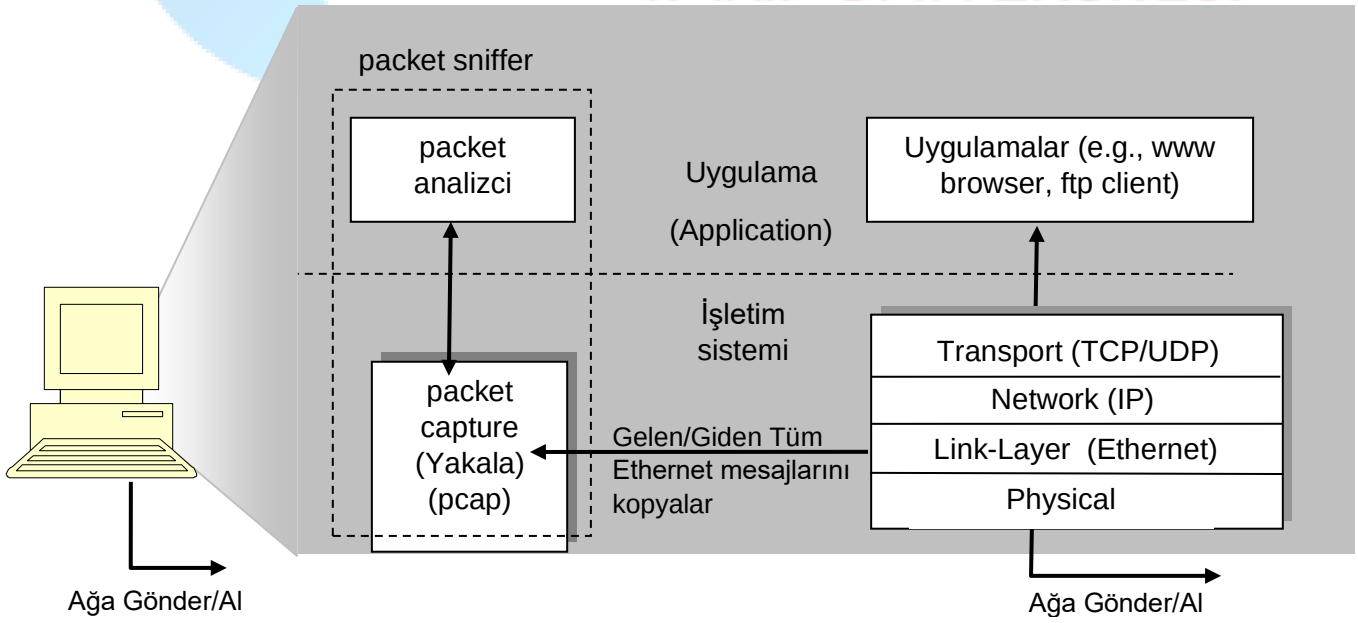
Bilgisayar teknolojisinin temellerinden olan bilgisayar ağlarını anlayabilmek, bu ağlarda kullanılan protokolleri anlamaktan geçiyor. Eğer bilgisayar ağlarını kavramak istiyorsak protokol mesaj döngüsü, protokol adımlarının detayları, birbirleri ile etkileşimde oldukları zaman olan işlemlerin amaçları ve sonuçları gibi işlemleri anlamalıyız. Bunun için simülasyonlardan yararlanabilir ya da gerçek çalışır bir sistem üzerinde incelemelerde bulunabiliriz. Wireshark lablarında çeşitli ağ uygulamalarını faklı senaryolarla çalıştıracak, amaçlarını ve sonuçları görmeye anlamaya çalışacağız.

Wireshark, bilgisayarınızda yapmış olduğunuz bütün ağ işlemlerini izleyebileceğiniz bir yazılımdır. “Wire” “kablo” demektir “Shark” ise “Köpek Balığı” ya da “Usta” anlamına gelir. Wireshark kurulu olduğu ve izlediği bilgisayara gelen tüm paketleri alır ve anlamlı bir şekilde kullanıcıya sunar. Wireshark bu özellikleriyle canlı bir laboratuvardır yani simülasyon değildir.

Uygulanan protokoller arası mesajları gözlemleyebilmek için kullandığı araca “packet sniffer (paket koklayıcı, dinleyici) adı verilmiştir. İsminden de anlaşılacağı gibi packet sniffer ilgili ağa gelen/giden mesajları yakalar/dinler ve bunları anlamlı bir şekilde kaydeder. Packet sniffer asla olmayan bir paketi göndermez ve almaz. O sadece bilgisayara gelen/giden paketlerin bir kopyasını saklar.

Resim 1’de packet sniffer yapısı gösterilmektedir. Resmin sağ tarafında protokoller (resimdeki durumda “internet protocol”) ve bilgisayarda çalışmakta olan uygulamalar (web browser, ftp client) bulunmaktadır. Resimde görülen paket yakalama kütüphanesi her link-layer (Ethernet) katmanında gelen/giden paketleri alır.

Diğer katmanlar ileride anlatılacağı gibi link-layer tarafından kapsüllendiği için tüm katman paketlerine erişim sağlanmış olur.



Resim 1: Packet sniffer (Paket Koklayıcı-İzleyici) Yapısı

Resim 1'de görülen diğer bir bileşen Packet Analyzer (Paket Analizci) ise yakalanan paket içerisindeki tüm alanların içeriğini gösterir. Yani, paket analiz bileşeni paket içerisindeki tüm mesajları düzgün bir şekilde parse ederek (ayırarak) yapısını anlamamızı sağlar.

3. Wireshark Kurulumu

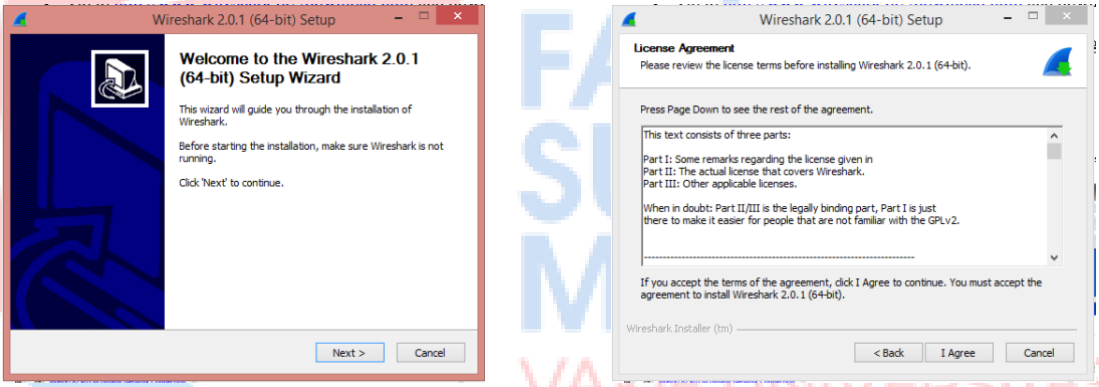
3.1. İndirme

Wireshark programını kurmak için öncelikle internet üzerinde bilgisayarınıza uygun olan Wireshark sürümünü indirmeniz gerekmektedir. İndirme linki aşağıda görülmektedir. Açılan sayfadan işletim siteminize uygun olan versiyonu indiriniz.

Link: https://www.wireshark.org/download.html

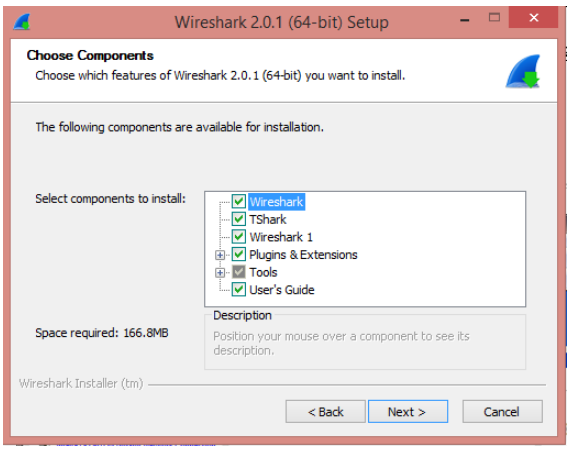
3.2. Yükleme

Windows kurulumu için indirmiş olduğunuz kurulum dosyasını yönetici modunda açınız ve sırasıyla "Next", "I Agree" deyiniz. (Resim 2)



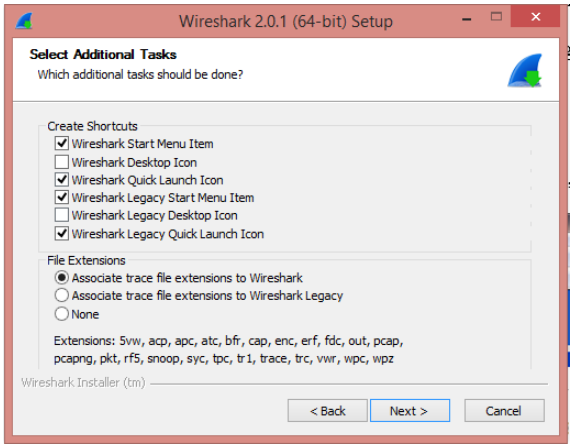
Resim 2: İlk Yükleme Adımları

Resim 3'te kurmak istediğimiz araçları (tool) seçiyoruz. "Androiddump" hariç hepsini seçiniz ve "Next"e tıklayınız.



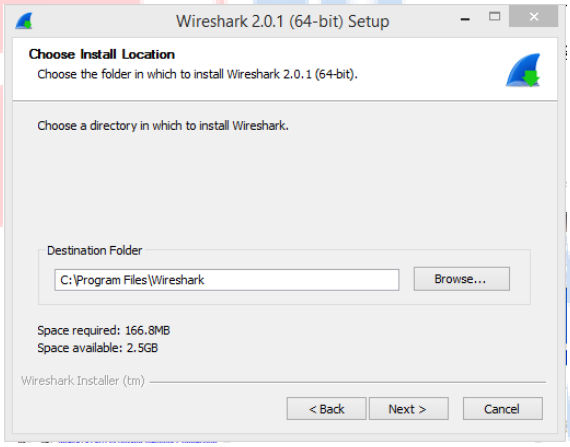
Resim 3: Araçların Seçimi

Resim 4'te kısayolları ve kapsayacağı dosya uzantılarını seçiyoruz. Aynı şekilde bırakınız ve "Next"i tıklayınız.



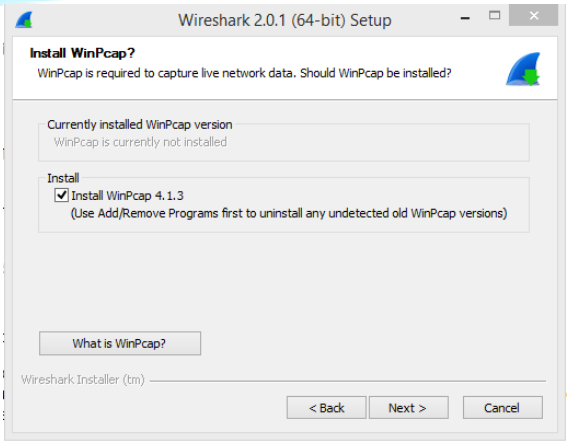
Resim 4: Kısayollar

Resim 5'te kurulum yapılacak dosya yolunu belirtiniz. Özel bir dosya yolu seçiminiz yoksa "Next"i tıklayınız.



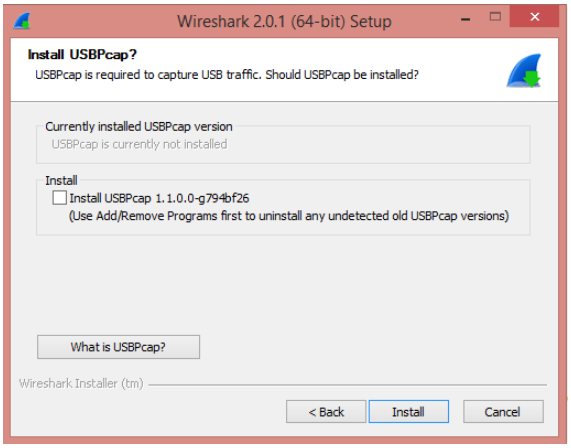
Resim 5: Dosya Yolu

Wireshark çalışabilmek için "WinPcap" kütüphanesine ihtiyaç duyar eğer yüklü değilse Resim 6'yı aynı bırakınız.



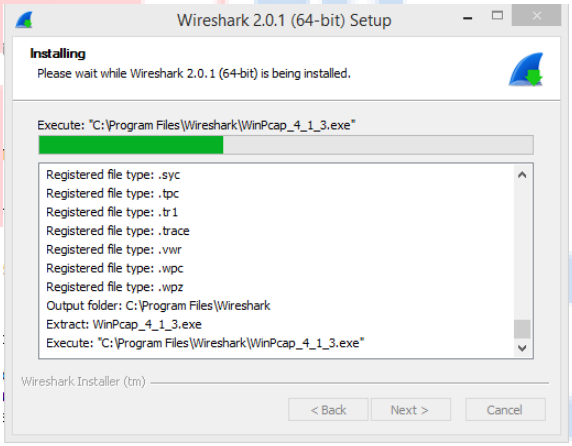
Resim 6: WinPcap Kütüphanesi

Eğer bilgisayarınızdaki USB trafiğini de dinlemek istiyorsanız “USBPcap” kütüphanesini de kurmanız gerek. Seçiminizi yapınız ve “Next”e basınız.



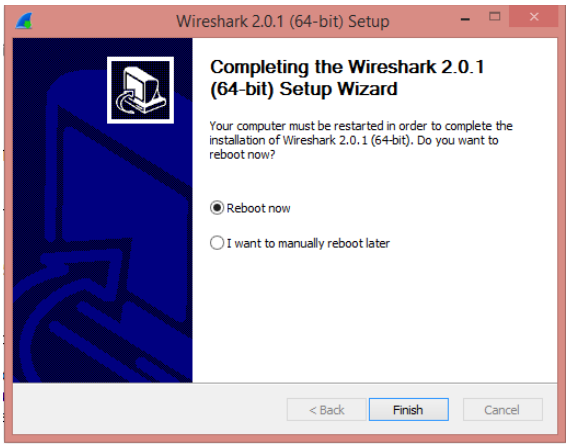
Resim 7: USBPcap Kütüphanesi

Kurulum yüklemesini göreceksiniz (Resim 8). Eğer karşınıza başka bir kurulum ekranı çıkarsa bu diğer kütüphanelerin kurulumudur sadece “Next” deyip geçiniz.



Resim 8: Yükleme İlerlemesi

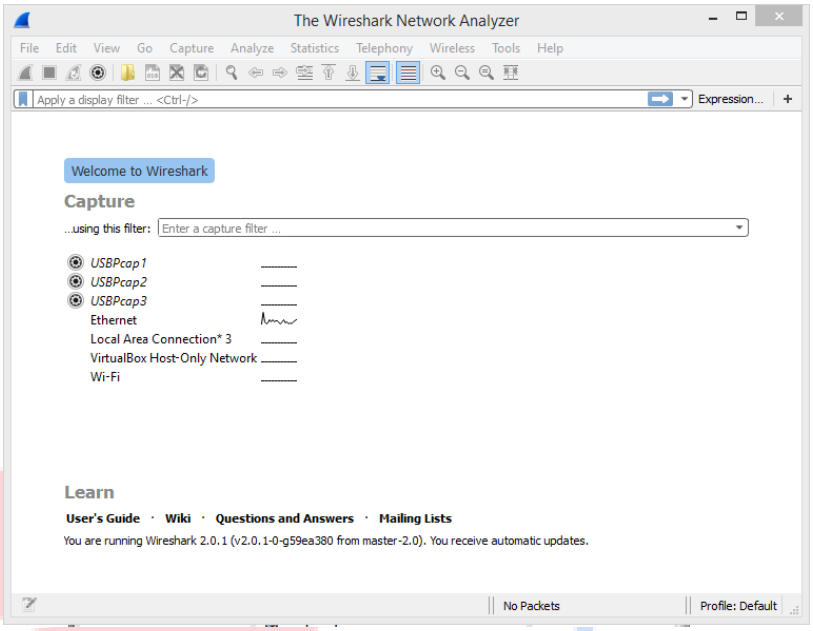
En son olarak bilgisayarınızı “Reboot” ediniz (yeniden başlatınız).



Resim 9: Son Ekran

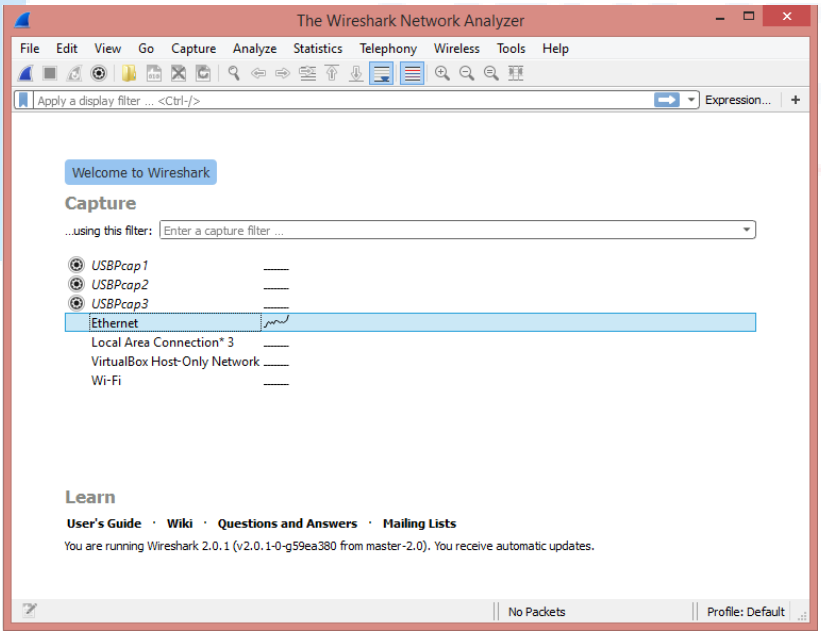
4. Wireshark İlk Kullanım

"Wireshark Network Analyzer" programını açtığınızda karşınıza Resim 10'da görülen görsel çıkacaktır. Bu ekranda bilgisayarınızdaki USB portlar, Ethernet, Wi-Fi gibi bilgisayarınızda tanımlı donanımsal ve yazılımsal ilgili bileşenler bulunmaktadır. Burada var olan birleşenleri Wireshark programıyla dinleyebilirsiniz.



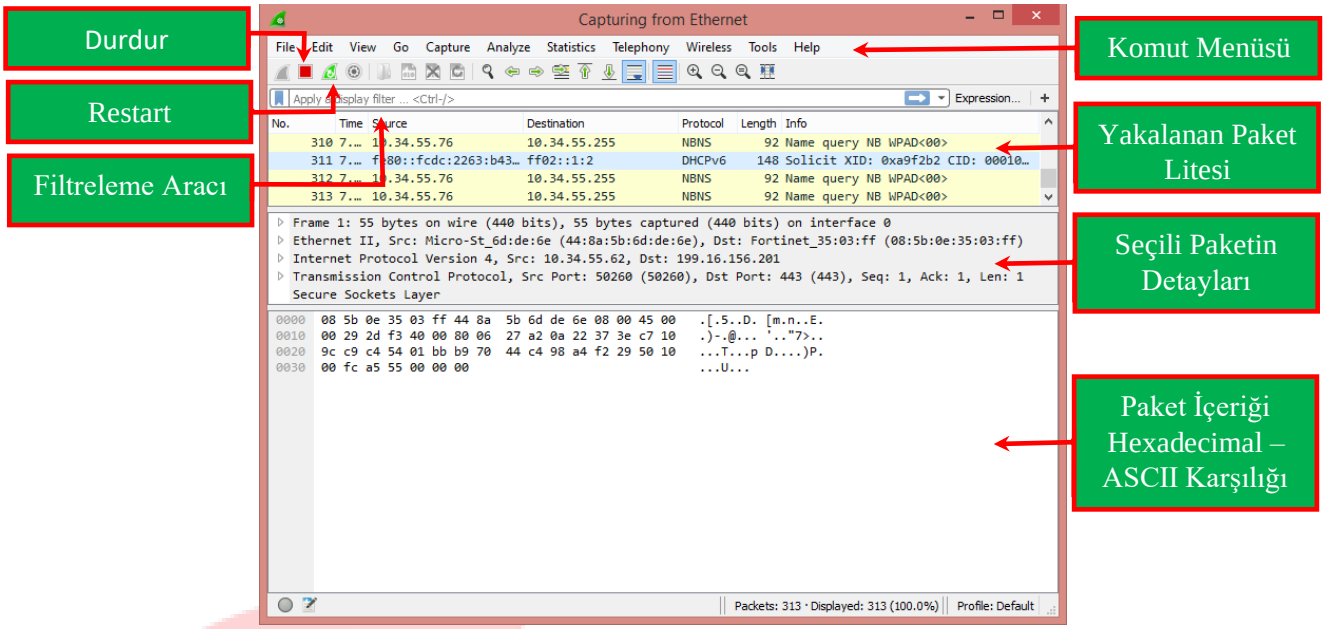
Resim 10: Programın Ekran Görüntüsü

Dinlemek istediğiniz bileşeni seçiniz ve yukarıda gördüğünüz köpek balığı yüzgeci şekline ile gösterilen "Start Capturing Packets" butonuna tıklayınız.



Resim 11: Ethernet Dinlemesi Yapma

Eğer Ethernet seçeneğini seçtiyseniz ve bilgisayarınızda bir internet trafiği varsa anında ekranda birçok veri göreceksiniz.



Resim 12: Arayüzün İşlevsel Özellikleri

Resim 12'de temel birleşenler kısa biçimde gösterilmiştir. Bir kere dinleme başlatıldıktan sonra internet trafiğini Resim 12'te görülen "Durdur" butonuna basılana kadar dinlemeye devam eder. Yakalanan paket listesine birçok verinin geldiğini göreceksiniz. Burada gelen her paket ayırım yapılmaksınız listelenir. Eğer "Restart" butonuna basarsanız ekranda görülen tüm veriler silinecektir ve dinleme yeniden başlatılacaktır.

Komut menüsünde standart menü araçları bulunmasının yanında Wireshark programına özel menüler de bulunmaktadır. Yeri geldikçe bu menüde bulunan araçlara değineceğiz.

Yakalanan paket listesi bilgisayara gelen/giden tüm paketleri gösteren penceredir. Wireshark'ın çalıştığı bilgisayardaki tüm ağ trafiğini buradan izleyebilirsiniz. Burada "No" (işlem sırası), "Time" (işlem zamanı), "Destination" (hedef), "Protocol", "Length"(mesaj uzunluğu), "Info" (bilgi) bilgilerini kısa haliyle bir paket için görebilirsiniz.

Eğer Wireshark programına bir filtre uygulamak istiyorsak yani sadece belirli paketleri görmek istiyorsak "Filtreleme Aracına" filtrelemek istediğimiz kriteri girmeliyiz. Örneğin sadece TCP paketlerini görmek için filtreye "TCP" yazın ve Enter'a basın, sadece TCP protokolünü içeren paketlerin listelendiğini göreceksiniz.

Yakalanan paketlerin detaylarına erişim için; yakalanan paket listesinden istenilen pakete tıkladığınızda "Seçili Paketin Detayları" penceresinde paket içeriğini göreceksiniz. Burada paket katmanlarına ayrılmış halde görülmektedir. Eğer daha detaylı bir görünüm istiyorsanız yandaki açılır/kapanır ok işaretlerine tıklayabilirsiniz. Ok işaretine tıkladığınızda paketin daha anlaşılır bir görünümüne ulaşacaksınız.

Paket içeriklerinin Hexadecimal-ASCII karşılığını gösteren pencere paketlerin bu şekilde görselleştirilmiş halidir. Hexadecimal-ASCII bilgisayar ağlarında oldukça sık kullanılan veri formatıdır. Bu bilgilere ihtiyacınız olduğu yerde ilgili paketi seçerek bu pencereden bilgilere ulaşabilirsiniz.

5. Filtre Uygulama

Wireshark dinlemeye başladığından itibaren birçok paketi yakalar. Bu paketler oldukça fazla ve karmaşık olabilir. Ağ trafiğimizde bulunan tüm mesajlar ekranımıza dolar. Bu karmaşadan çıkış yolu filtre uygulamaktır. Wireshark çeşitli filtrelerin uygulanmasına izin verir. Filtre maskesinin iyi yazılması gereksiz paketlerden bizi kurtarır. Filtre uygulamaları için programlamada da gördüğümüz mantık operatörleri geçerlidir.

&& -> And – Ve –

|| -> Or –Veya-

^^ -> Xor - Özel veya-

! -> Not – Değil-

[…] Subsitring –kesme operatörü-

== -> eşit

!= -> eşit değil

> -> büyük

< -> küçük

>= -> büyük eşit

<= -> küçük eşit

Bu mantıksal operatörlerle çeşitli filtre maskelerini bir araya getirebilirsiniz. Şimdi filtre maske örneklerimize geçelim. Filtre boşluğuna:

- http -> içerisinde sadece http protokolü geçen paketler
- tcp -> içerinde sadece tcp protokolü geçen paketler
- ip.src==192.168.0.0 -> kaynak adresi verilen IP olan paketler
- ip.dest==192.168.0.0 -> hedef aderesi verilen IP olan paketler
- tcp || udp -> tcp ya da udp olan paketler
- tcp.window_size == 0 && tcp.flags.reset != 1 -> window size 0 olan ve bayrağı bir olmayan paketler
- udp.port==3245 -> 3245 nolu porta sahip udp paketler

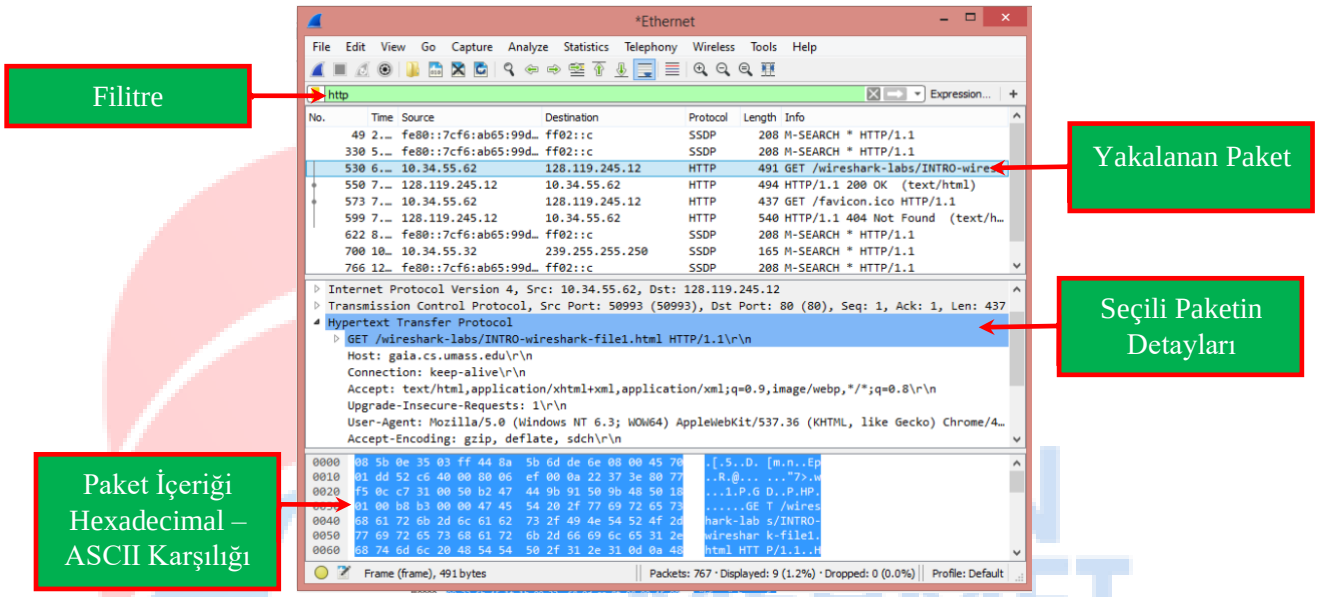
6. Wireshark Test Sürüşü

Bir şeyi öğrenmenin en iyi yolu test etmektir. Wireshark programıyla ne kadar çok incelemede bulunursanız programı anlamanız ve kullanımınız iyileşecektir. Bununla birlikte bilgisayar ağları mantığını da daha iyi anlamış olacaksınız.

Wireshark temel anlatımları takip ettiyseniz artık ilk testimize başlayabiliriz.

1. Herhangi bir tarayıcıyı açınız.
2. Wireshark programını çalıştırınız fakat henüz herhangi bir dinleme başlatmayınız.
3. Wireshark ekranında dinleyebileceğiniz arayüzleri görüyorsunuz

4. Biz bu testimizde Network'ü dinlemek istiyoruz. Network ile ilgili arayüzü seçiniz ve dinlemeyi başlatınız.
5. Şu anda bilgisayarınıza gelen/giden verileri görüyor olmalısınız. Eğer herhangi bir trafik yoksa bir paket göremeyeceksiniz.
6. Wireshark dinleme çalışmaya devam ediyorken tarayıcımıza http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html adresini yazınız ve giriş yapınız.
7. Şu anda başka bir bilgisayara bağlanarak paket alışverişi yaptınız ve bir ağ trafiği oluşturdunuz. Şimdi dinleme işlemini durdurunuz.
8. Bilgisayarımıza bir HTML sayfası paketi geldi. HTML Sayfaları HTTP protokolüyle çalışır (daha sonra bu protokolü derinlemesine inceleyeceğiz).
9. Filtre çubuğuna "HTTP" yazınız ve Enter'a basınız. Şimdi sadece "HTTP" paketlerini göreceksiniz.
10. HTTP paketlerinden GET yazan paketi tıklayınız.
11. Paket detayları ekranından HTTP açılır okunu açınız. Görülenleri inceleyiniz.
12. Paket içeriği hex/ascii alanındaki verileri inceleyiniz.



Resim 13: Çalışma Sonucu

7. Lab Değerlendirme

7.1. Wireshark nedir? Nerelerde kullanılabilir? Neler yapılabilir?
7.2. Yakalanan paket alanındaki sütunlar nelerdir? Ne işe yararlar?
7.3. Seçili paketin detaylarında hangi alanlar bulunmaktadır.
7.4. Labı bir başka html sayfası için tekrar ediniz.

8. Kaynaklar

8.1. http://www-net.cs.umass.edu/wireshark-labs/
8.2. Computer Networking: A Top-Down Approach, 6th edidtion. J.F. Kurose and K.W. Ross