YMT 311-Bilgi Sistemleri ve Güvenliği

Ağ Güvenliği

Konu Başlıkları

- Wireshark
- Wimax
- Güvenli İşletim Sistemleri

Wireshark

- Wireshark,1998 yılında Ethereal adıyla faaliyete başlayan bir projedir.
- Wireshark ismiyle çıkan bu yazılım bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Bir başka deyişle bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartı) tüm TCP/IP mesajlarını analiz eden bir programdır.
- Wireshark günümüzde çok amaçlı kullanılmaktadır.
- *Şebeke problemlerinde sorun çözme
- *Güvenlik problemlerini sınamak
- *Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
- *Ağ problemlerinin içindeki bilgileri öğrenebilmek amacıyla kullanılmaktadır.

WiRESHARK ÖZELLİKLERİ

- Windows,Unix,OS X,Solaris,FreeBSD,NetBSD ve birçok işletim sistemleri için uygundur.
- Yerel ağ arayüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.
- Tutulan bilgileri kaydetme özelliği vardır.
- Çeşitli kriterlerde paket arar ve filtreler.
- Çeşitli istatistikleri yapılan ayarlar doğrultusunda kullanıcıya sunar.
- Birçok protokol için şifre çözme desteği sunar. (IPsec,ISAKMP,Kerberos,SNMPv3, SSL/TLS, WEP, ve WPA/WPA2'yi içerir).

Wireshark kullanimi ile ilgili örnekler

- Ağ trafik tespiti
- Veri madenciliği
- Saldırı tespiti
- Port tarama tespiti
- Virüslerin bulaştığını veya Denial of Service(Dos) ataklarını bulma tespiti
- Bağlantı sorunu tespiti
- Casus yazılım tespiti

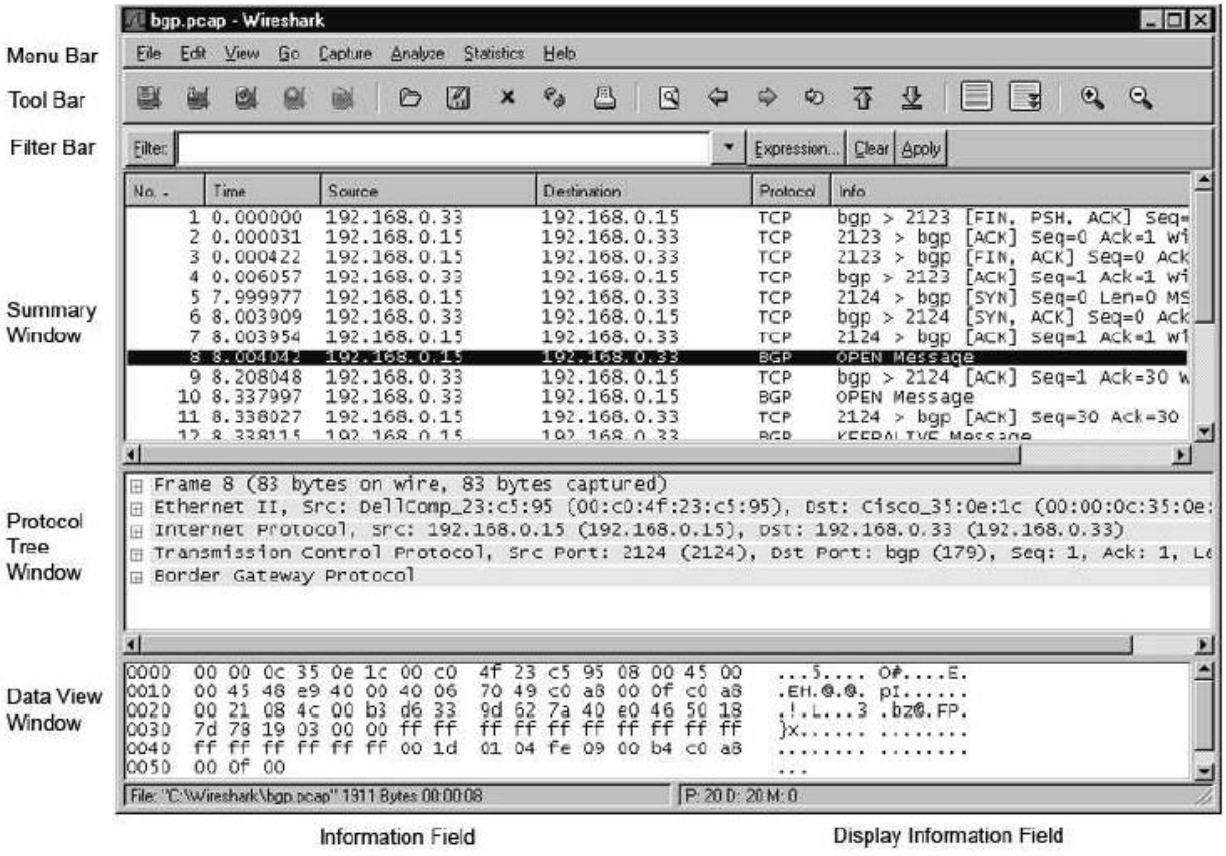
Wireshark bileşenleri

- Wireshark iletişim ağının iç yüzünde neler olduğunu kavramamızı sağlar.
- Bu özelliğiyle; uygulama protokollerinde, ağ uygulamalarındaki sorunları
- çözmede, ağı test etmede ve canlı ağ bağlantılarındaki sorunları
- çözmemizde bize yardımcı olur. Yani, iletişim ağı ile teknik düzey
- arasında etkileşim sağlayarak pek çok problemi çözmemizi sağlar. Bu
- bölümde wireshark'ın grafiksel kullanıcı ara yüzündeki ana bileşenleri
- tanımlayacağız :

Wireshark bileşenleri

- Main window
- Menu bar
- Tool bar
- Summary window
- Protocol Tree window
- Data View window
- Filter bar
- Information field
- Display information

Wireshark Görseli



ANA PENCERE (MAIN WINDOW)

Menu Bar	Menudeki maddelerin, grafiksel ara yüzünü içeren klasik bir uygulamadır.
Tool Bar	Wireshark'ın sık kullanılan fonksiyonlarının kısa yollarını içerir. Kullanıcıya göre ayarlanabilir.
Filter Bar	Yakalanan paketleri, istenilen sekilde ayrılarak gösterilmesini sağlar.
Summary Window	Yakalan paketlerin her biri için, bir satırlık özet bilgi sunar.
Protocol Tree Window	Summary window 'da seçili olan paketin detaylı bilgilerini, kullanıcıların anlayacağı şekilde düzenleyerek sunar.
Data View Window	Summary Window 'da seçili olan paketin, detaylı bilgilerini, herhangi bir düzenleme yapmadan sunar.
Display Information Field	Yakalanmış paketlerin numaralarını, güncel olarak gösterir.

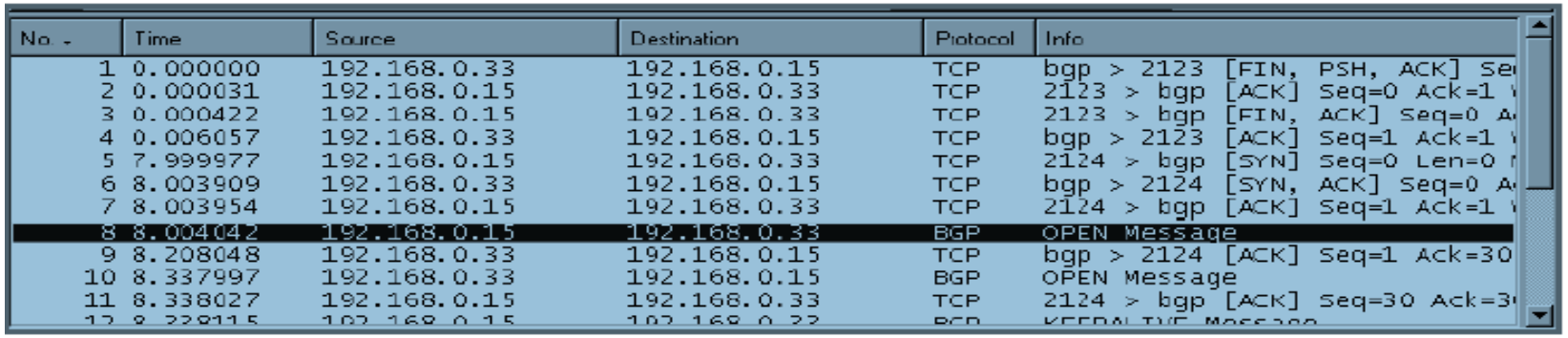
SUMMARY WINDOW

- Yakalanmış paketlerin tamamına buradan bakılabilir. Her bir dosyanın içeriği bir satır olarak sunulur, satırlar belli özelliklerine göre sütunlara ayrılır.

Sütun adı	Tanımı
No	Yakalanan dosyanın içindeki paketlerin numarasını temsil eder. Görüntüleme filtresi (display fitler)kullanılmadığı sürece bu numara değiştirilemez.
Time	Paketin zaman damgasıdır.
Source	Paketin nereden geldiğini gösterir.
Destination	Paketin nereye gittiğini gösterir.
Protocol	Protokol isminin kısa versiyonudur.
Info	Paket içeriği hakkında ekstra bilgi gösterir.

SUMMARY WINDOW

- Bu dosyalar daha ayrıntılıda incelenebilir. Herhangi bir dosya seçilirse "Packet Details" ve "Packet Bytes" pencereleri açılır. Bir paketin içeriğine bakılacak olursa, Ethernet paketinin içinde IP, onun içinde TCP bulunur. Ethernet tarayıcısı kendi bilgisini(örneğin Ethernet Adresleri) yazar, IP tarayıcısı onun üstüne kendi bilgisini(örneğin IP adresleri) yazar ve TCP tarayıcısı da onun üstüne IP bilgisini yazacaktır.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [FIN, PSH, ACK] Se
2	0.000031	192.168.0.15	192.168.0.33	TCP	2123 > bgp [ACK] Seq=0 Ack=1
3	0.000422	192.168.0.15	192.168.0.33	TCP	2123 > bgp [FIN, ACK] Seq=0 A
4	0.006057	192.168.0.33	192.168.0.15	TCP	bgp > 2123 [ACK] Seq=1 Ack=1
5	7.999977	192.168.0.15	192.168.0.33	TCP	2124 > bgp [SYN] Seq=0 Len=0
6	8.003909	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [SYN, ACK] Seq=0 A
7	8.003954	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=1 Ack=1
8	8.004042	192.168.0.15	192.168.0.33	BGP	OPEN Message
9	8.208048	192.168.0.33	192.168.0.15	TCP	bgp > 2124 [ACK] Seq=1 Ack=30
10	8.337997	192.168.0.33	192.168.0.15	BGP	OPEN Message
11	8.338027	192.168.0.15	192.168.0.33	TCP	2124 > bgp [ACK] Seq=30 Ack=3

Tablo 1.3 : Summary Window Sütunu

SUMMARY WINDOW

- Gözüktüğü gibi bu paket; Border Gateway Protocol (BGP) oturumunda, *192.168.0.15* ve*192.168.0.33* adresleri arasında yakalanmıştır. Bu paket seçilerek, açılan "Protocol Tree Window" ve "Data View Window" bölümlerinden daha da ayrıntılı incelenebilir.

PROTOCOL TREE WINDOW

- Paketi bütün protokollerin bir üst ağacı (tree) olarak canlandıralım. Her bir protokol için ağaç düğümü(tree node) oluşturulur. Bu ağaç düğümleri sayesinde, protokol alanı Daha geniş bir şekilde tanımlanabilir. Herhangi bir ağaç düğümünün alt ağaca sahip olması, Onun daha geniş bilgiler gösterecek şekilde genişletilebileceğini veya sadece özet bilgiler gösterecek şekilde daraltılabileceğini gösterir. Protocol tree window, wireshark'ın paketi çözümleyerek oluşturduğu ağacı denetleme imkanı sunmaktadır.

PROTOCOL TREE WINDOW

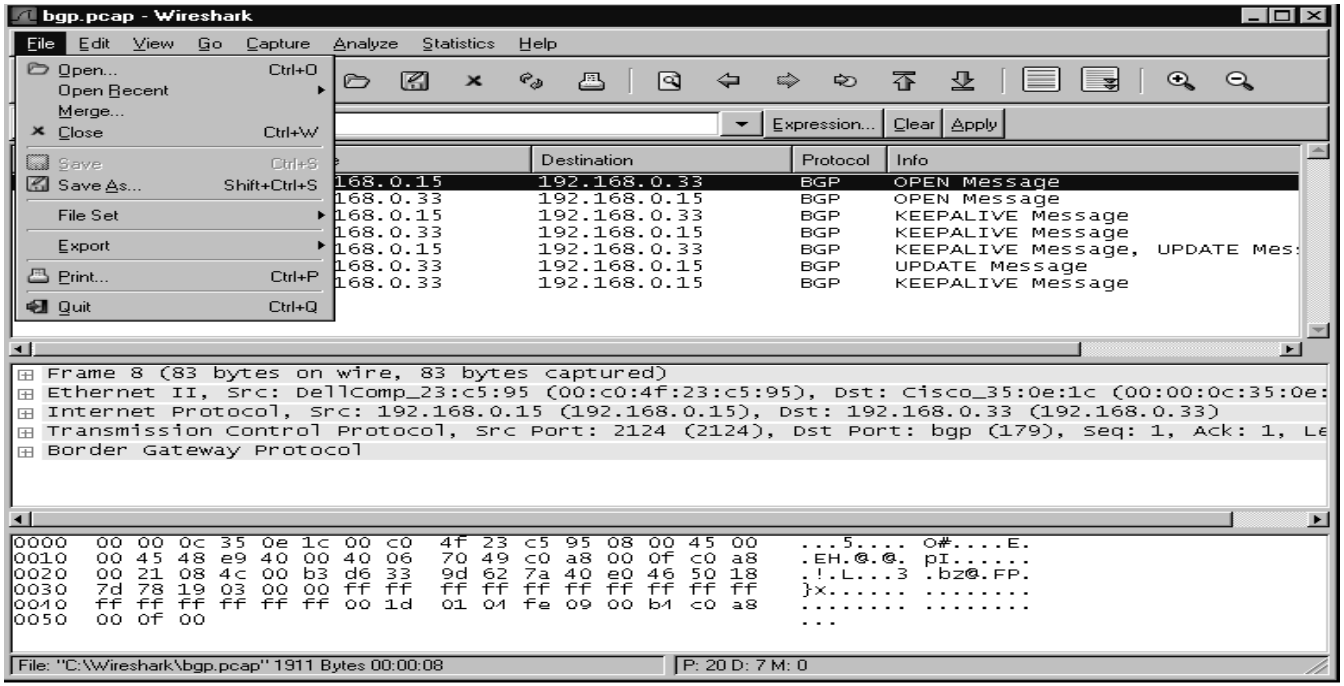
Wireshark arayüzü ;menü çubuğu, araç çubuğu, görüntüleme filtresi çubuğu, özet Alanı, protokol ağacı alanı ve veri alanı olmak üzere 6 bölümden oluşur. Menü Çubuğu;

- File (Dosya Menüsü)
- Edit (Ekleme Menüsü)
- View (Görüntü Menüsü)
- Go (Git Menüsü)
- Capture (Yakalama Menüsü)
- Analyze (Analiz Menüsü)
- Statistics (Statik Menüsü)
- Help (Yardım Menüsü)

olmak üzere 8 bölümden oluşmaktadır.

File(dosya menüsü)

- Bu menü dosya açma, kaydetme,yazdırma gibi temel işlevleri yapabileceğimiz bölümdür.



Tablo 1.4

File(dosya menüsü)

- Open (*ctrl+O*): Hazırda var olan önceden kaydedilmiş wireshark ya da başka
- desteklediği paket analiz yazılımlarının ürettiği dosyaları görüntülemek için
- kullanılır.
- Open Recent(Son dosyayı aç): Son kullanılan dosyaları açmada kolaylık sağlar.
- Merge(Birleştir): Kaydedilmiş dosyaları birleştirmede kullanılır.
- Close (*ctrl+W*): Açık olan dosyadan çıkar.
- Save (*ctrl+S*): Görüntülenmekte olan paketleri kaydeder.
- Save As (*ctrl+shift+S*): Farklı kaydeder.
- File Set(Dosya Ayarları):
- List Files(Dosya Listesi):Dosya listesini oluşum tarihi, son değişim tarihi, boyutu
- Şeklinde dosya dizisi içerisinde gösterir.
- Next File(Sonraki dosya): Dosya dizisi içinde varolanı kapatıp sonrakine atlar
- Previous File(Önceki dosya): Dosya dizisi içinde varolanı kapatıp bir öncekine atlar.

Export

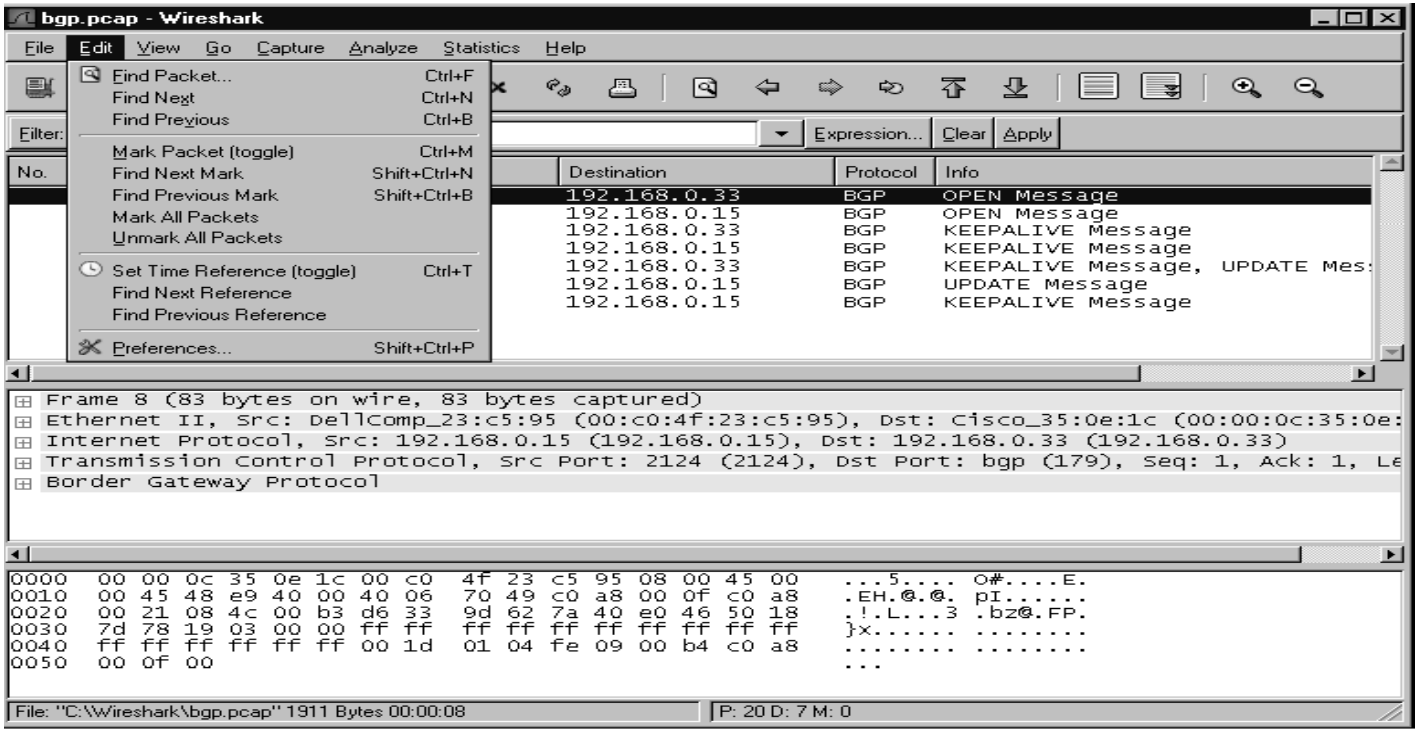
- As “Plain Text” File: Toplanan paketleri metin dosyası olarak dışa aktarmaya yarar. Özet ve ayrıntı bölümlerini aktarır.
- As “PostScript” File: İstenen paketleri postscript dosyası olarak dışa aktarmaya yarar. Wireshark seçilen ayrıntı bölümü bilgilerini aktarır.
- As "CSV" (Comma Separated Values packet summary) File: Wireshark özet bölümündeki bilgileri virgülle ayrılmış şekilde düz metin dosyası olarak dışa aktarır.
- As “C Arrays” Paket Bytes File: Paket veri değerlerini hex byteları olarak aktarır.
- As XML ”
- PSML” (Packet Summary) File: Paketleri PSML (packet summary markup language) XML
- dosya formatında dışa aktarmaya yarar.
- As "PDML" File: Paketleri PDML (packet details markup language) XML dosyası
- olarak aktarmaya yarar.

Selected Packet Bytes

- Objects > http : Paketler içerisinden http protokollü paketleri ve Objelerini dışarı aktarmaya yarar.
- Print (*ctrl+P*):Seçilen paketleri yazdırmaya yarar.
- Quit(*ctrl+Q*):Programdan çıkar.

Edit

- Edit menüsü kullanıcı tanımlı işlemleri ve paket arama gibi işlemleri yapmamızı sağlar. Edit menüsünün içeriği gösterilmiştir.



Edit

- Copy (*Shift+ctrl+C*): Veri bölmesinden tıklanan değeri filtre ifadesi olarak kopyalar. İstenilen bölüm seçilerek sağ fare menüsünden de yapılabilir .
- Find Packet (*ctrl+F*): Birçok kritere göre arama yapmanıza imkan sağlar. Display filter seçeneği seçiliyse wireshark filtreleme kriterlerine göre arama yapar. Basit protokol taramalarından kuvvetli filtreleme ifadelerine kadar birçok türde etkin arama yapabilirsiniz.
- Hex Value:Paket veri kümesi içerisinde belirtilen hex değerlerinde arama yapar.
- String: Girilen string i liste, ayrıntı ya da veri alanlarında belirlenen kriterlere göre arar .String options alanından arama büyük küçük harf duyarlı ve karakter seti belirtilerek yapılabilir. Direction alanında ise taramanın aşağı yada yukarı yapılacağı belirtilir.
- Find Next (*ctrl+N*): Belirlenen kriterde bir sonraki paketi bulur.
- Find Previous (*ctrl+B*) : Belirlenen kriterde bir önceki paketi bulur.

Edit

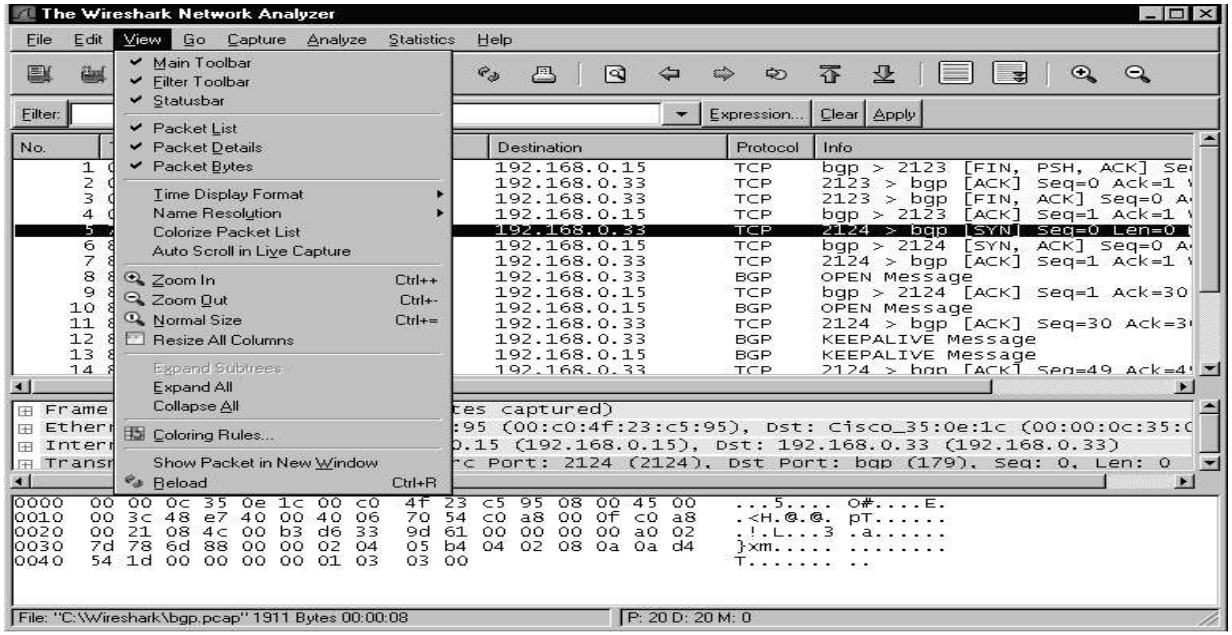
- Mark Packet (*ctrl+M*) : Seçilen paketi işaretler.
- Find Next Mark (*shift+ctrl+N*) : Bir sonraki işaretli paketi bulur.
- Find Previous Mark (*shift+ctrl+B*) : Bir önceki işaretli paketi bulur.
- Mark All Packet: Bütün paketleri işaretler.
- Unmark All Paket: Bütün işaretleri kaldırır.
- Set Time Referance (*ctrl+T*): Seçilen paketi zaman referansı olarak alır ve sonraki paketlerde o pakete göre zaman değerleri alır.
- Find Next Referance: Bir sonraki referans alınan paketi bulur.
- Find Previous Referance: Bir önceki referans alınan paketi bulur.
- Configuration Profiles (*shift+ctrl+A*): Profil ekle sil işlemlerini yapar.
- Preference (*shift+ctrl+P*): Programla ilgili ayarlamaları yaptığımız bölümdür.
- User İnterface bölümünde program için pencere düzeni, renk, font ayarlamaları ve bunlar gibi görünümü kişiselleştirmeye yarayan seçenekler bulunur.

Edit

- Capture : Paketleri yakalamak için kullanılacak default ağ arabirimi, eş zamanlı paket görüntüleme ve promiscouos mod seçimi (promiscouos mod : Yönlendirme olmadan bütün paketlerin bütün istemcilere dağıtıldığı durumda paketin hedefine bakılmadan bütün paketlerin takibi olayıdır. Root yetkisi gerektirir.), otomatik kaydırma çubuğu hareketi, ve yakalanan paketlerin türlerine göre sayıları ve % oranlarını veren info penceresinin saklanması seçenekleri bulunur.
- Printing: Yazdırmak için gereken ayarlar bulunmaktadır. Dosya çıktısı konumu, yazdırma komutu ve çıktı türü “düz metin ya da post script seçenekleri” Bulunmaktadır .Varsayılan yazdırma komutu lpr dir.
- Name Resolutions: Adres dönüşüm işlemlerini etkinleştirebileceğiniz alandır.
- Protocols: ihtiyaca göre wireshark üzerinde paketlerin protokollere göre kullanım ayarlamalarını yapabileceğiniz bölümdür.

View

- Wireshark ana ekranımızın görüntüsünü düzenlememizi sağlayan menüdür.
- Toolbar lar eklenebilir, çıkarılabilir, paketlere özel renk ayarları yapılabilir.



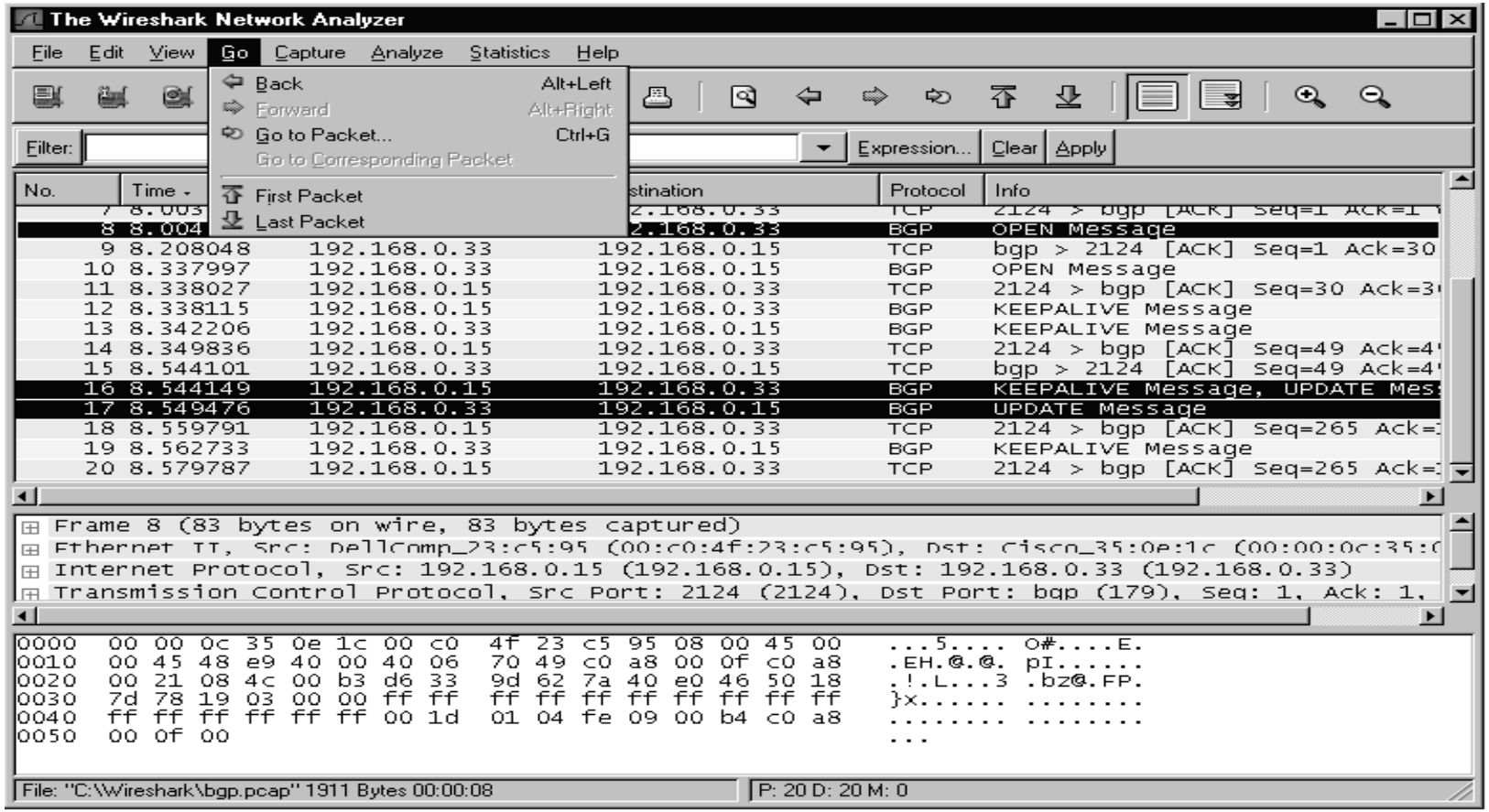
View

- Packet Details(Paket Detayları): Paketlerin detaylarını ASCII kodunda gösteren
- Bölgeyi ekler ya da kaldırır.
- Packet Bytes: Data Window penceresini ekler ya da kaldırır.
- Time Display Format Summary: Window da zaman görünümün nasıl gözükeceğini ayarlamamızı sağlar.
- Colorize Packet List: Paketlerin renk özelliğini açar ya da kapar.
- Auto Screen in Live Capture: Summary Windowun güncellenmesini açıp kapamaya yarar.
- Zoom In: Font ve column size ları büyütmeye yarar.
- Zoom Out: Font ve column size ları küçültmeye yarar.
- Normal Size: Zoom In ve out la büyütüp küçülttüğümüz fontları default değere döndürmemizi sağlar.
- Expand Subtrees: Protocol tree deki seçili alt diziyi açar.

View

- Expand All: Protocol tree deki bütün alt dizileri açar.
- Collapse All: Protocol tree deki bütün alt dizileri kapatır.
- Coloring Rules: Paketler için Renk ayarlarını yapmamızı sağlar.
- Show Packet in New: Window Paket detaylarını yeni bir pencerede görmemizi sağlar.

Go

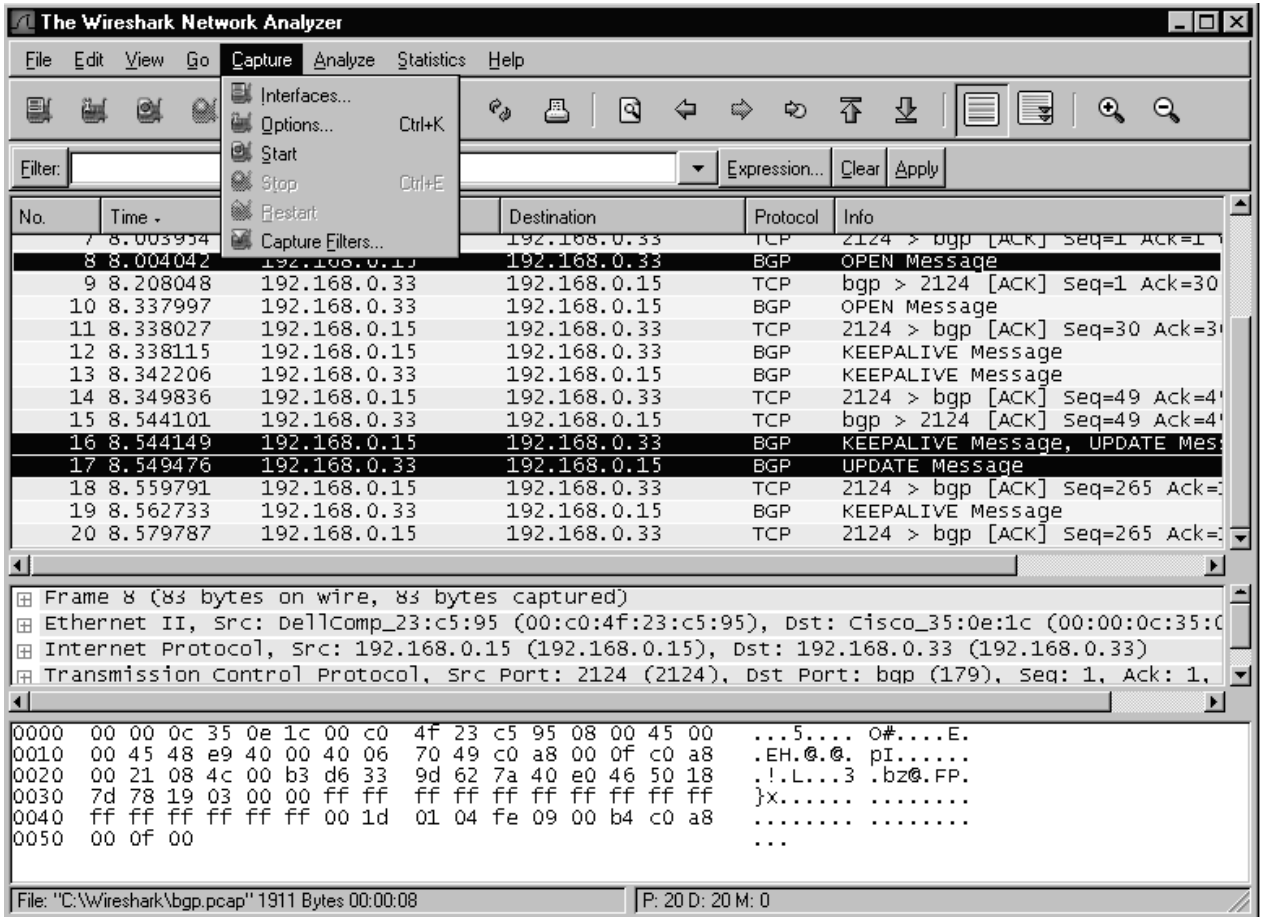

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Back Alt+Left
Forward Alt+Right
Go to Packet... Ctrl+G
Go to Corresponding Packet
First Packet
Last Packet
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
8 8.004 2.168.0.33 BGP OPEN Message
9 8.208048 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.337997 192.168.0.33 192.168.0.15 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
15 8.544101 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=49 Ack=4
16 8.544149 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message, UPDATE Mes
17 8.549476 192.168.0.33 192.168.0.15 BGP UPDATE Message
18 8.559791 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
19 8.562733 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
20 8.579787 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
Frame 8 (83 bytes on wire, 83 bytes captured)
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1,
0000 00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00 ...5.... O#....E.
0010 00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8 .EH.@.@. pI......
0020 00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18 .!.L...3 .bz@.FP.
0030 7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff ff }x...... ....
0040 ff ff ff ff ff ff 00 1d 01 04 fe 09 00 b4 c0 a8 ....
0050 00 0f 00 ...
File: "C:\Wireshark\bgp.pcap" 1911 Bytes 00:00:08
P: 20 D: 20 M: 0

Tablo 1.7

Go

- Back (*ctrl+sol*): Bir önceki baktığınız pakete atlar.
- Forward (*ctrl+sağ*): Ziyaret edilen bir sonraki pakete zıplar.
- Go To Packet (*ctrl+G*): Paket numarasına göre istenilen pakete zıplar.
- Go To Corresponding Packet: Seçilen pakete karşılık gelen pakete zıplar .
- Previous Packet (*ctrl+yukarı*): Seçili paketten önceki pakete zıplar.
- Next Packet (*ctrl+aşağı*): Seçili paketten sonraki pakete zıplar.
- First Packet: Yakalanan ilk pakete zıplar.
- Last Packet: Yakalanan son pakete zıplar.

Capture


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Interfaces...
Options... Ctrl+K
Start
Stop Ctrl+E
Restart
Capture Filters...
Filter:
Expression... Clear Apply
No. Time Destination Protocol Info
8 8.004042 192.168.0.33 BGP OPEN Message
9 8.208048 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.337997 192.168.0.33 192.168.0.15 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
15 8.544101 192.168.0.33 192.168.0.15 TCP bgp > 2124 [ACK] Seq=49 Ack=4
16 8.544149 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message, UPDATE Mes
17 8.549476 192.168.0.33 192.168.0.15 BGP UPDATE Message
18 8.559791 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
19 8.562733 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
20 8.579787 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=265 Ack=
Frame 8 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: DellComp_23:c5:95 (00:c0:4f:23:c5:95), Dst: Cisco_35:0e:1c (00:00:0c:35:0
Internet Protocol, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.33 (192.168.0.33)
Transmission Control Protocol, Src Port: 2124 (2124), Dst Port: bgp (179), Seq: 1, Ack: 1,
0000 00 00 0c 35 0e 1c 00 c0 4f 23 c5 95 08 00 45 00 ...5.... O#....E.
0010 00 45 48 e9 40 00 40 06 70 49 c0 a8 00 0f c0 a8 .EH.@.@. pI......
0020 00 21 08 4c 00 b3 d6 33 9d 62 7a 40 e0 46 50 18 .!.L...3 .bz@.FP.
0030 7d 78 19 03 00 00 ff ff ff ff ff ff ff ff ff ff }x...... ....
0040 ff ff ff ff ff ff 00 1d 01 04 fe 09 00 b4 c0 a8 ....
0050 00 0f 00 ...
File: "C:\Wireshark\bgp.pcap" 1911 Bytes 00:00:08
P: 20 D: 20 M: 0

Capture

- İnterfaces: Wiresharkın kullanacağı ağ arabirimi ve özellikleri ayarlanır.
- Options: Uygulama sırasında kullanılacak ağ arabirimi seçimi adres çözümleme özellikleri, görünüm özellikleri uygulama durdurmak için ayarlanacak özellikler gibi bir çok ayarlanabilir bölüm içermektedir.
- IP address: Seçilen ağ arabirimin sahip olduğu ip adresidir.
- Limit each packet to n bytes : Paket yakalama işlemi sırasında uyulacak tampon sınırdır. Seçili olmadığı durumda default değeri 65535 bytes tır. Default değerde bırakmanız önerilir.
- Capture packets in promiscuous mode : Hub kullanılan ağlarda yalnızca kullanılan makine ile ilgili paketleri değil gelen bütün paketleri hedeflerine bakmadan toplama özelliğidir.
- Capture Filter: Paket yakalama sırasında filtreleme özelliği sunar. İstenmeyen paketlerin yakalanmasını engelleyerek hem analiz işlemini kolaylaştırır hemde programın çalışması sırasında daha az paket ile sistem kaynaklarını idareli kullanır.

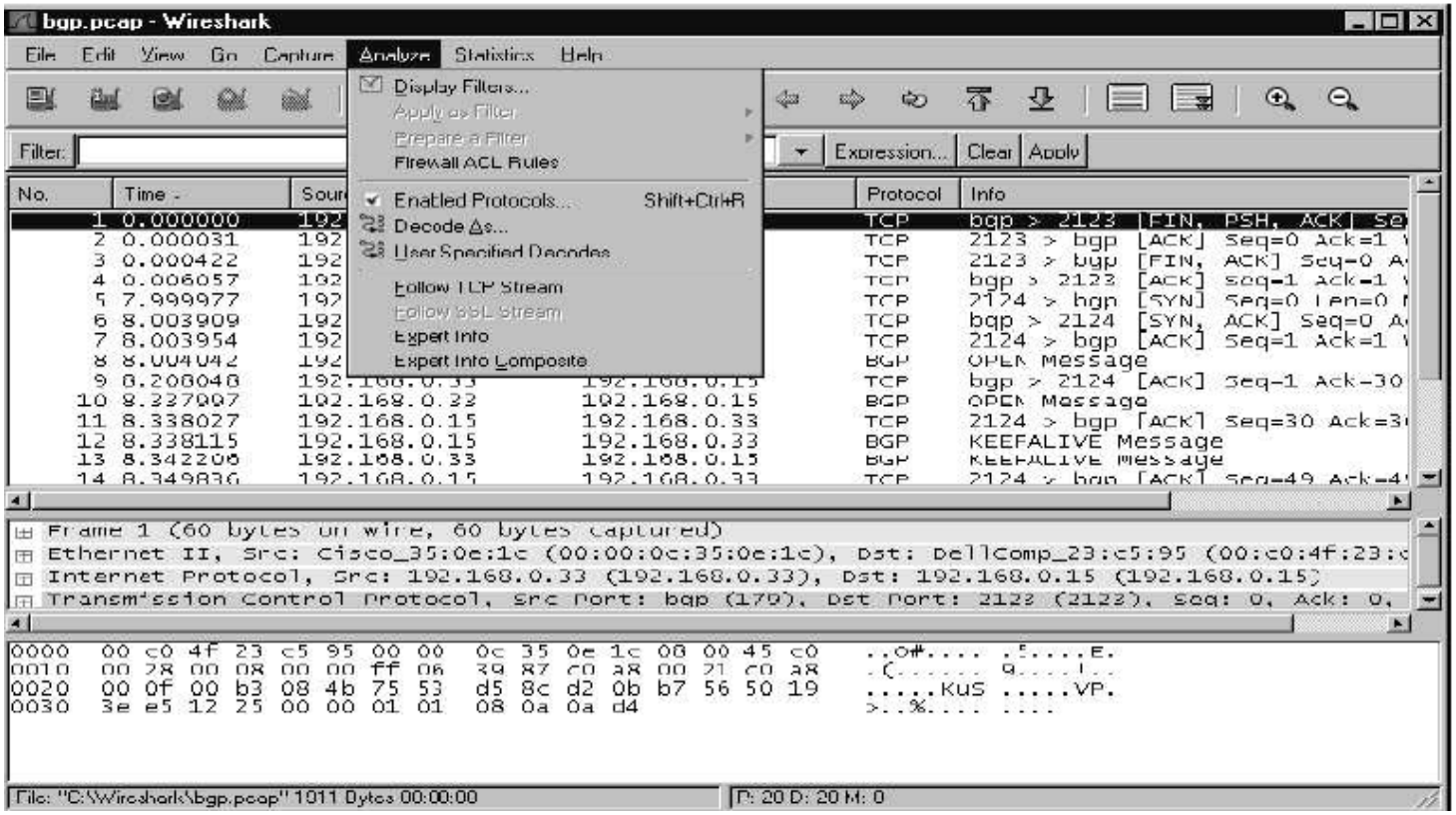
Capture File(s) Alanı

- File: Yakalama dosyası olarak kullanılacak dosya ismi belirtmene yarar. Default olarak boştur.
- Use multiple files: Tek dosya kullanımı yerine wireshark otomatik olarak yeni bir dosyayla yer değiştirir.
- Next file every n megabyte(s): Belirtilen boyutta (kilobyte,megabyte,gigabyte) paket yakalandıktan sonra bir diğer dosyaya geçer.
- Next file every n minute(s): Belirtilen süre geçtikten sonra diğer dosyaya geçer.
- Ring buffer with n files: Belirtilen sayıda dosya aşıldığında en eski dosyayı siler.
- Stop capture after n file(s):Belirtilen sayıda dosya değiştikten sonra yakalama işlemini durdurur.

Stop Capture. Alanı

- ... after n packet(s) : Belirtilen sayıda paket yakalandıktan sonra yakalama işlemini durdurur.
- ... after n megabytes(s): Belirtilen kb,mb,gb miktardan sonra yakalama işlemini durdurur.
- ... after n minute(s): Belirtilen süre sonunda (saniye, dakika, saat, gün) yakalama işlemini durdurur.
- Display Options Alanı:
- Update List Of Packets İn Real Time: Yakalanan paketleri eşzamanlı olarak anında ekranda görmenize yarar.
- Automatic Scrolling in Live Capture: Kaydırma çubuğu otomatik olarak son yakalanan pakete göre iner.
- Hide Capture info Dialog: Yakalanan paketlerin protokollere göre sayı ve Oranını veren bilgi penceresini saklar.

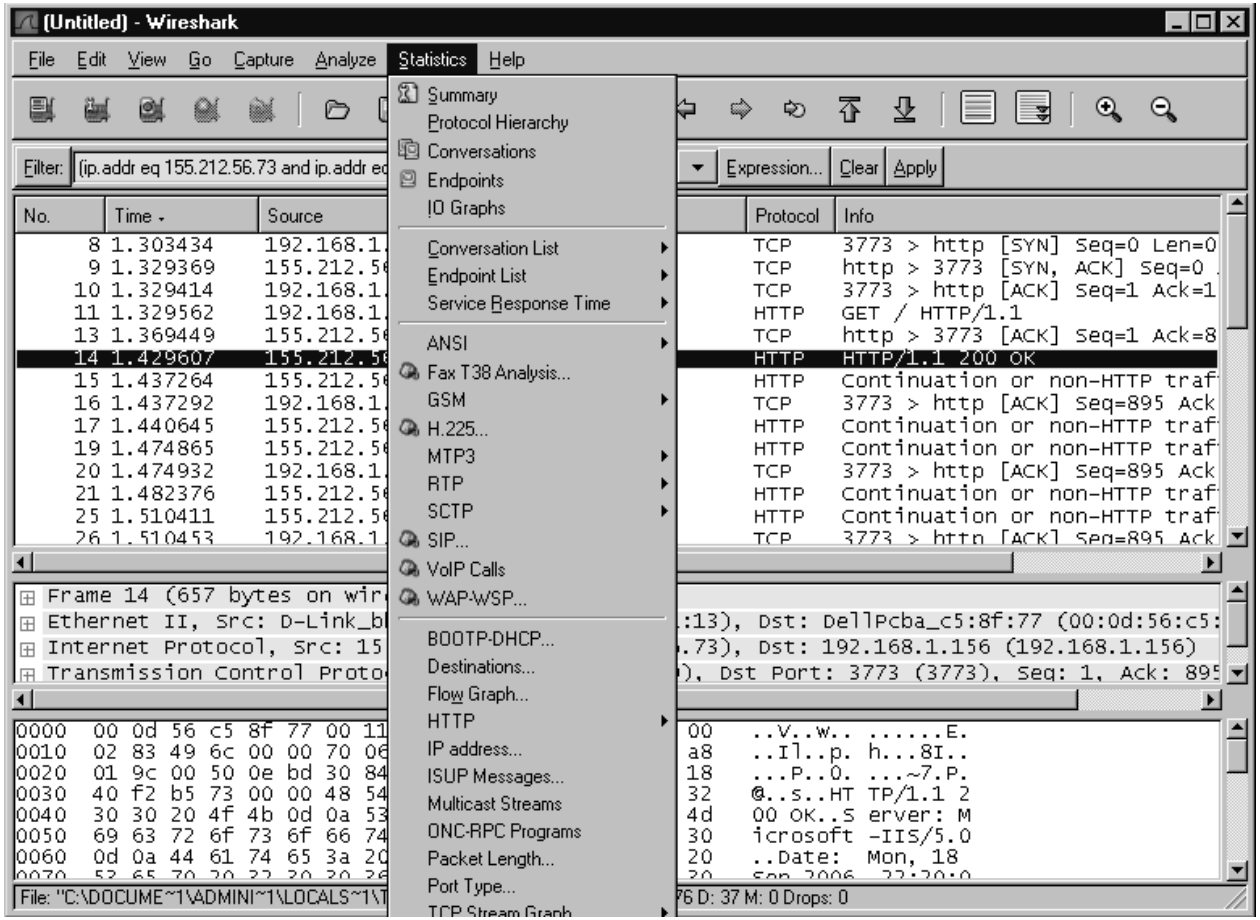
Analyze


bgp.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Display Filters...
Apply as Filter
Prepare a Filter
Firewall ACL Rules
Enabled Protocols... Shift+Ctrl+R
Decode As...
User Specified Decodes
Follow TCP Stream
Follow SSL Stream
Expert Info
Expert Info Composite
Filter:
Expression... Clear Apply
No. Time - Protocol Info
1 0.000000 TCP bgp > 2123 [FIN, PSH, ACK]
2 0.000031 TCP 2123 > bgp [ACK] Seq=0 Ack=1
3 0.000422 TCP 2123 > bgp [FIN, ACK] Seq=0
4 0.006057 TCP bgp > 2123 [ACK] Seq=1 Ack=1
5 7.999977 TCP 2124 > bgp [SYN] Seq=0 Len=0
6 8.003909 TCP bgp > 2124 [SYN, ACK] Seq=0
7 8.003954 TCP 2124 > bgp [ACK] Seq=1 Ack=1
8 8.004042 BGP OPEN Message
9 8.208048 TCP bgp > 2124 [ACK] Seq=1 Ack=30
10 8.327997 BGP OPEN Message
11 8.338027 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=30 Ack=3
12 8.338115 192.168.0.15 192.168.0.33 BGP KEEPALIVE Message
13 8.342206 192.168.0.33 192.168.0.15 BGP KEEPALIVE Message
14 8.349836 192.168.0.15 192.168.0.33 TCP 2124 > bgp [ACK] Seq=49 Ack=4
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_35:0e:1c (00:00:0c:35:0e:1c), Dst: DellComp_23:c5:95 (00:c0:4f:23:c
Internet Protocol, Src: 192.168.0.33 (192.168.0.33), Dst: 192.168.0.15 (192.168.0.15)
Transmission Control Protocol, Src Port: bgp (179), Dst Port: 2123 (2123), Seq: 0, Ack: 0,
0000 00 c0 4f 23 c5 95 00 00 0c 35 0e 1c 08 00 45 c0 ..O#.... .5....E.
0010 00 28 00 08 00 00 ff 06 39 87 c0 a8 00 21 c0 a8 .(...... 9....!..
0020 00 0f 00 b3 08 4b 75 53 d5 8c d2 0b b7 56 50 19 .....KuS .....VP.
0030 3e e5 12 25 00 00 01 01 08 0a 0a d4 >..%.... ....
File: "C:\Wireshark\bgp.pcap" 1011 Bytes 00:00:00
P: 20 D: 20 M: 0

Analyze

- Display Filter: Yakalanan paketleri belirtilen ifadelere göre sıralar.
- Apply As Filter: Seçilen paketin kaynak ve hedef adresine göre filtreleme yapar. And (&&), or(||), and not (&& !) ve or not (|| !) eklemeleriyle ifade güçlendirilir ve daha özelleşmiş arama yapılabilir.
- Prepare a Filter: Filtre ifadesini değiştirir ama hemen uygulamaz. Üstteki filtre uygulaması koşulları bunun içinde geçerlidir.
- Firewall ACL Rules :Cisco IOS, Linux Netfilter (iptables), OpenBSD pf ve Windows Firewall (via netsh) için firewall kural ifadesi oluşturur. Yeni kullanıcılar için mükemmel ötesi bir özelliktir.
- Decode As: Paketleri belirli protokollere göre decode eder.
- Enabled Protocols (*shift+ctrl+R*): Yakalama işlemi sırasında istenmeyen protkollerin kaldırılmasına imkan verir. Capture filter gibi düşünülebilir.
- Decode As: Geçici olarak protokol çevrim işi yapar.
- User Specified Decodes: Hali hazırda var olan çevrimleri görüntüler.
- Follow TCP Stream: Seçilen paketle ilgili tcp bağlantılarının tüm tcp segmentlerini ayrı bir pencerede gösterir.
- Follow SSL Stream: Follow TCP stream ile aynı özelliktedir fakat SSL stream için çalışır.

Statistics


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Summary
Protocol Hierarchy
Conversations
Endpoints
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANSI
Fax T38 Analysis...
GSM
H.225...
MTP3
RTP
SCTP
SIP...
VoIP Calls
WAP-WSP...
BOOTP-DHCP...
Destinations...
Flow Graph...
HTTP
IP address...
ISUP Messages...
Multicast Streams
ONC-RPC Programs
Packet Length...
Port Type...
Filter:
Expression... Clear Apply
No. Time Source Protocol Info
8 1.303434 TCP 3773 > http [SYN] Seq=0 Len=0
9 1.329369 TCP http > 3773 [SYN, ACK] Seq=0
10 1.329414 TCP 3773 > http [ACK] Seq=1 Ack=1
11 1.329562 HTTP GET / HTTP/1.1
13 1.369449 TCP http > 3773 [ACK] Seq=1 Ack=8
14 1.429607 HTTP HTTP/1.1 200 OK
15 1.437264 HTTP Continuation or non-HTTP traf
16 1.437292 TCP 3773 > http [ACK] Seq=895 Ack
17 1.440645 HTTP Continuation or non-HTTP traf
19 1.474865 HTTP Continuation or non-HTTP traf
20 1.474932 TCP 3773 > http [ACK] Seq=895 Ack
21 1.482376 HTTP Continuation or non-HTTP traf
25 1.510411 HTTP Continuation or non-HTTP traf
Frame 14 (657 bytes on wir
Ethernet II, Src: D-Link_b
Internet Protocol, Src: 15
Transmission Control Proto
0000 00 0d 56 c5 8f 77 00 11
0010 02 83 49 6c 00 00 70 06
0020 01 9c 00 50 0e bd 30 84
0030 40 f2 b5 73 00 00 48 54
0040 30 30 20 4f 4b 0d 0a 53
0050 69 63 72 6f 73 6f 66 74
0060 0d 0a 44 61 74 65 3a 20
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\T
D: 37 M: 0 Drops: 0

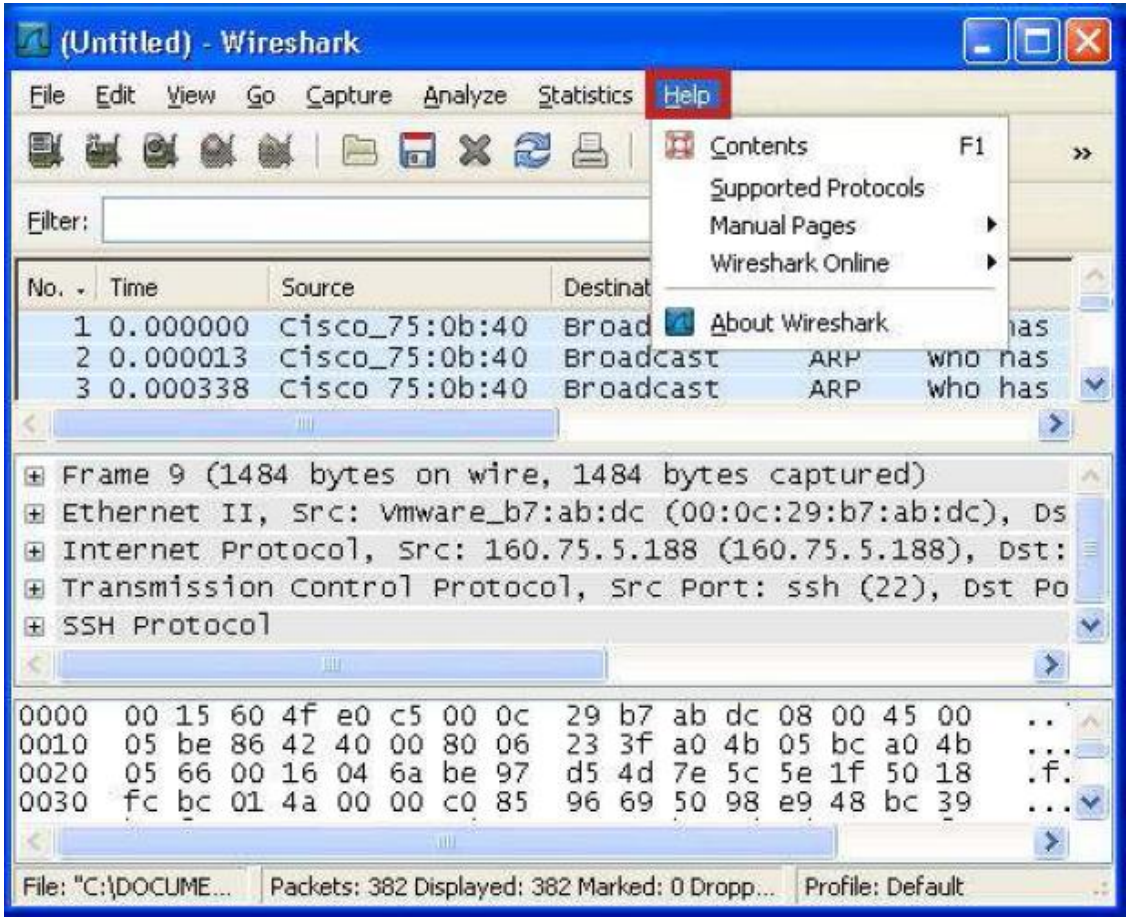
Statistics

- Summary: Açık olan yakalama dosyasında dosya formatı, paket sayısı, boyut, ilk ve son paket yakalama zamanları , filtre ve yakalama arabirimine ilişkin verileri içerir.
- Protocol Hierarchy : Yakalanan paketlerin ağaç şeklinde katman ve protokol hiyerarşisini gösterir. Her sıra bir protokole ait istatistiksel değerleri tutar. Seçilen sıra filtre ifadesi olarak kullanabilir.
- Conversations: Kaynak ve hedef noktaları arasındaki trafiğin istatistik bilgisini verir. Noktalar arasındaki toplam gelen giden paket ve byte miktarı portlara göre listelenir. Conversations penceresi endpoint penceresiyle benzerdir. Listedeki her bir sıra bir diyaloğun istatistiksel değerlerini verir. Adres çözümleme özelliği Conversations penceresi içinde, programın başlangıcında “capture options” bölümünden, preferences altında name resolutions bölümünden ya da view menusu altında name resolutions bölümünden seçildikten sonra kullanılabilmektedir. Limit to display filter özelliği ise herhangi bir filtreleme yönergesi tanımlandığı durumda kullanılabilmektedir.
- Endpoints: Hedef ve kaynak adresi ayrımı yapmadan her son nokta için istatistik bilgisini verir. Desteklenen her protokol için ayrı bir sekme mevcuttur .Her sekmede yakalanan son nokta sayıları belirtilmektedir.

Statistics

- IO Graphs: Belirtilen özelliklerde paketlerin zamana göre akış grafiğini verir. Ağda durum kontrolü için oldukça faydalı bir özelliktir. Bu özellikle normal paket akış diyagramında ağda meydana gelecek herhangi bir anormallik hemen farkedilebilir.
- Graphs: Grafik ayarlamalarının yapıldığı kısımdır.
- Service Response Time: İstek ve cevap arasındaki zamanı gösterir. Service response time istatistikleri DCERPC,Fibre, Channel, H.225 RAS, LDAP,MGCP, ONCRPC, SMB, ANSI,GSM,H.225 gibi protokoller için kullanılır.
- Wlan Traffic Statics: Yakalanan kablosuz ağ trafiğinin istatistik bilgisinin sunar.

Help


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Contents F1
Supported Protocols
Manual Pages
Wireshark Online
About Wireshark
Filter:
No. Time Source Destinat
1 0.000000 Cisco_75:0b:40 Broad
2 0.000013 Cisco_75:0b:40 Broadcast ARP who has
3 0.000338 Cisco 75:0b:40 Broadcast ARP who has
Frame 9 (1484 bytes on wire, 1484 bytes captured)
Ethernet II, Src: Vmware_b7:ab:dc (00:0c:29:b7:ab:dc), Ds
Internet Protocol, Src: 160.75.5.188 (160.75.5.188), Dst:
Transmission Control Protocol, Src Port: ssh (22), Dst Po
SSH Protocol
0000 00 15 60 4f e0 c5 00 0c 29 b7 ab dc 08 00 45 00
0010 05 be 86 42 40 00 80 06 23 3f a0 4b 05 bc a0 4b
0020 05 66 00 16 04 6a be 97 d5 4d 7e 5c 5e 1f 50 18
0030 fc bc 01 4a 00 00 c0 85 96 69 50 98 e9 48 bc 39
File: "C:\DOCUME... Packets: 382 Displayed: 382 Marked: 0 Dropp... Profile: Default

Help

- Help kısmı Wireshark'ın yardım menüsünün bulunduğu kısımdır.
- Contents: Wireshark online yardımı gösterir.
- Supported Protocols: Desteklenen protokolleri gösterir.
- Manual Pages :UNIX-Style kullanıcı sayfalarına ulasan bir alt menüdür.
- Wireshark Online: Online wireshark kaynaklarına ulaşmak için bir alt menüdür.
- About Wireshark :Wireshark ile ilgili bilgileri gösterir.

Filtreleme

- Filtre özelliği,
- Wiresharkta dinleme sırasında veya dinlemenin ardından paketler arasında istenilen özellikteki paketleri görüntülemekte kullanılabilir. Capture options penceresinden belirtilen capture filter, paket yakalama sırasında wiresharkın uyacağı koşulları belirtir. Capture filter penceresinde Wiresharkın paket yakalama sırasında uyacağı kurallar için bir liste sunulmuştur.
- Ethernet address 00:08:15:00:08:15 : Ethernet II altında kaynak veya hedef adreslerinde belirtilen mac adresine ait paketleri yakalar.
- not broadcast and not multicast: Broadcasting ve multicasting paketlerini yakalamaz.
- not arp: Arp paketlerini yakalamaz.

Filtreleme

- IP address 192.168.0.1 : Belirtilen ip adresini hedef yada kaynak adres kısımlarında barındıran paketler yakalanır.
- IPX only : İlgili protokole ilişkin paketleri yakalar.
- TCP only : İlgili protokole ilişkin paketleri yakalar.
- UDP only : İlgili protokole ilişkin paketleri yakalar.
- TCP or UDP port 80 (http) : Port 80 için tcp ve udp paketlerini yakalar.
- HTTP TCP port (80) : Port 80 için http ve tcp paketlerini yakalar.
- No ARP and no DNS : DNS ve ARP paketleri harici paketleri yakalar NonHTTP and nonSMTP to/from www.wireshark.org : Belirtilen adres için http ve smtp harici paketleri yakalar.

EN ÇOK KULLANILAN FİLTRELER

- 1.IP FILTERS

Filter	Tip	Tanım
ip.addr	IPv4 adresi	Source(kaynak) veya Destination(hedef)kaynak
ip.src	IPv4 adresi	Source adres
ip.dst	IPv4 adresi	Destination adres
ip.host	Karakter dizisi	Source veya Destination host adres
İp.src.host	Karakter dizisi	Source host adres
İp.proto	8 bit integer	Protokol
İp.version	8 bit integer	IP versiyonu

EN ÇOK KULLANILAN FİLTRELER

- 2.ETHERNET FILTERS

Filter	Tip	Tanım
eth.addr	6 bit mac adres	Source(kaynak) veya Destination(hedef) adres
eth.src	6 bit mac adres	Source adres
eth.dst	16 bit integer	Destination adres
eth.len	16 bit integer	Uzunluk
eth.type	16 bit integer	Tip

EN ÇOK KULLANILAN FİLTRELER

- 3.TCP FILTERS

Filter	Tip	Tanım
tcp.ack	32 bit integer	Acknowledgement numarası
tcp.analysis.ack_lost_segment	-	Ack yapılmıs kayıp paket tcp.analysis.duplicate_ack - Tekrar edilmis ack
tcp.analysis.duplicate_ack	-	Tekrar edilmiş ack
tcp.analysis.duplicate_ack_num	32 Bit integer	Tekrar edilen ack numarası
tcp.analysis.flags	-	TCP analiz bayrakları(uyarı)
tcp.port	16 bit integer	Source veya Destination port numarasına göre

IEEE 802.16 ve WiMAX

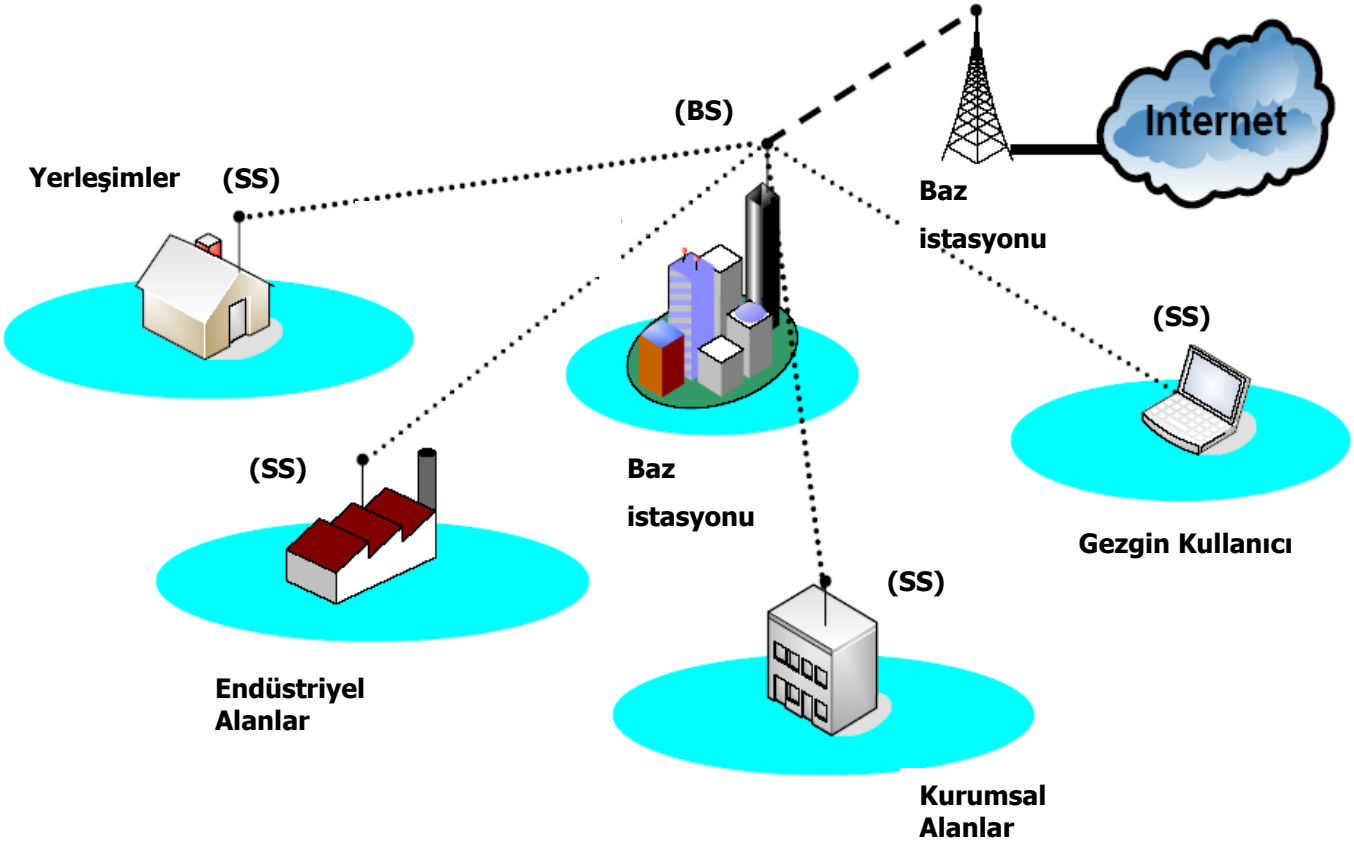
- IEEE 802.16: Telsiz Kentsel alan ağı standardı (Wireless MAN),(1999).
- WiMAX (Worldwide Interoperability for Microwave ACCess):

  802.16 standardını destekleyen uç birimlere telsiz alanda yüksek bandgenişliği (BWA) sağlamayı amaçlayan bir forumun standardı (2001).
- Yüksek hızda kesintisiz telsiz iletişim
  - 70 Mbps
  - Kapsama alanı: 50-70 km'ye kadar
  - Veri
  - Ses (isteğe-bağlı)
  - Görüntü (isteğe-bağlı)
  - VoIP
  - Videokonferans

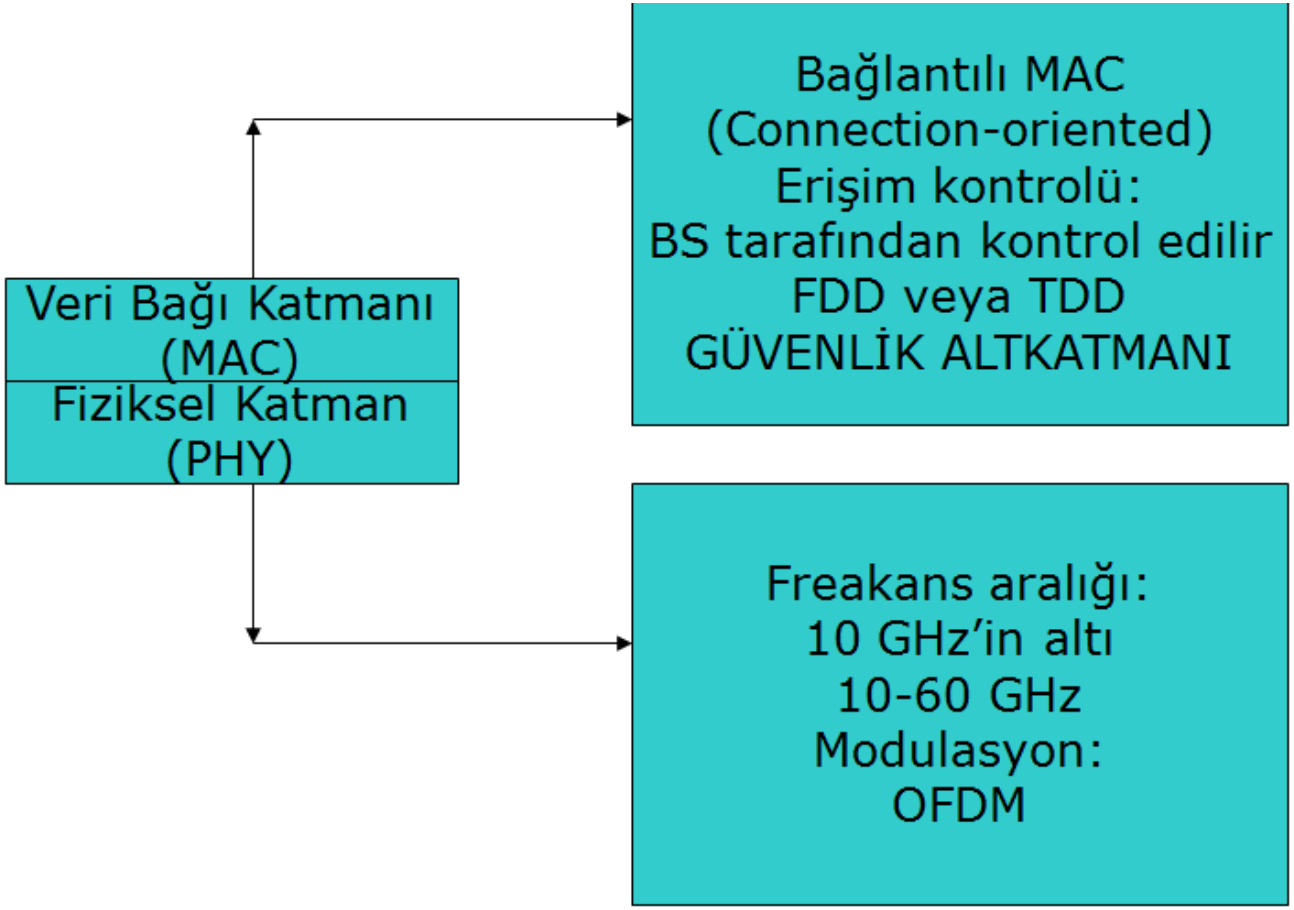
IEEE 802.16 ve WiMAX

- İletişim Türleri:
  - Baz istasyonu(BS)→ Kullanıcı İstasyonu(SS): Downlink
  - Kullanıcı İstasyonu(SS)→ Baz İstasyonu(BS): Uplink
  - Baz İstasyonu(BS)-kullanıcı İstasyonları (SS) arası
    - Tek noktadan Çok noktaya (PMP)
  - Kullanıcı İstasyonları arası
    - Ağ (mesh) yapısı

WiMAX Genel Yapısı



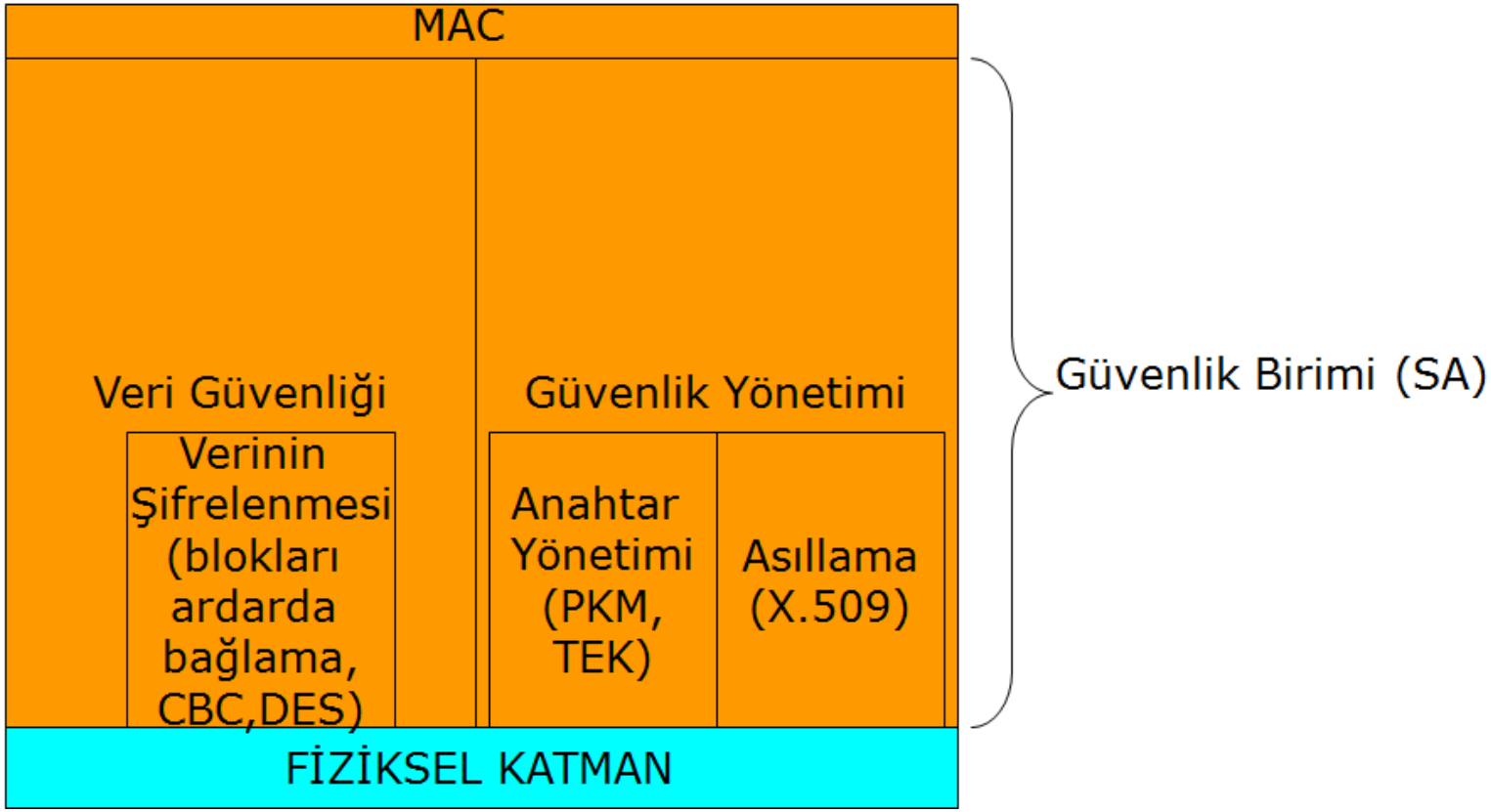
WiMAX katmansal Analiz



802.16 Güvenlik Standardı

- 5 kavrama dayalı bir yapı
  - Veri Şifreleme
    - MAC başlığı dışındaki kısma uygulanıyor
  - Anahtar Yönetimi
    - PKM
  - “Güvenlik Birimi” nin oluşturulması
    - Birimler arasında saydam bir iletişim kontrolü
  - Bağlantıların güvenlik birimine iletilmesi
  - Kriptografik süreç
    - Güvenlik biriminin veri şifrelemesi, asıllama ve anahtar alışverişi sırasında uyguladığı metodlarve girdiği durumlar

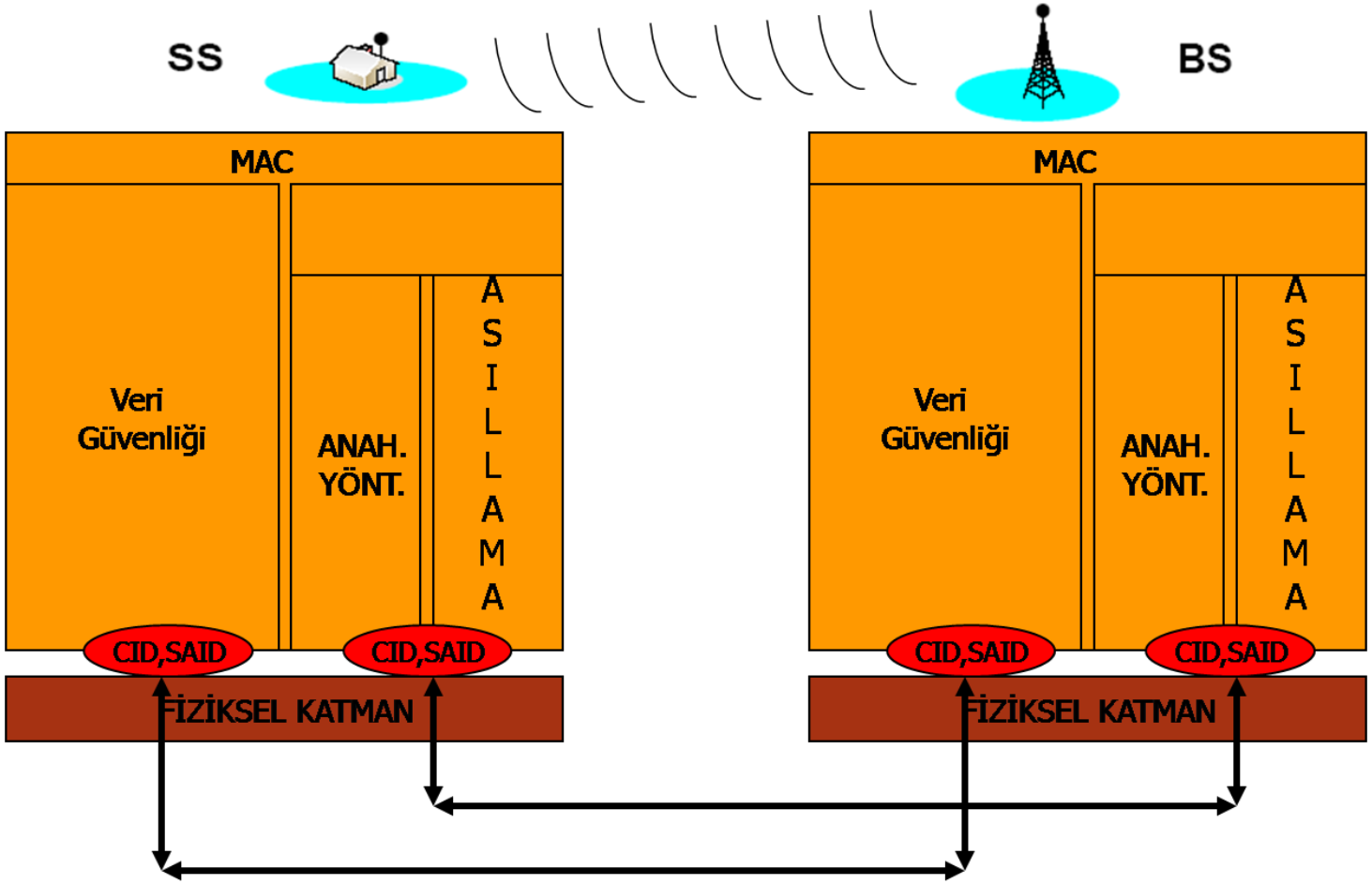
WiMAX Güvenlik Altkatmanı(1/2)



WiMAX Güvenlik Altkatmanı(2/2)

- Güvenlik Birimi (SA):
  - BS-SS arasındaki her türlü güvenlik bağlantısını sağlar.
  - 16-bitlik bir belirteci vardır (SAIP).
  - Tutulan parametler:
    - Her düzey için bir bağlantı ID'si(CID).
    - Kriptografik bilgiler(CBC, DES vs)
    - Güvenlik Bilgileri(Anahtar, IV)

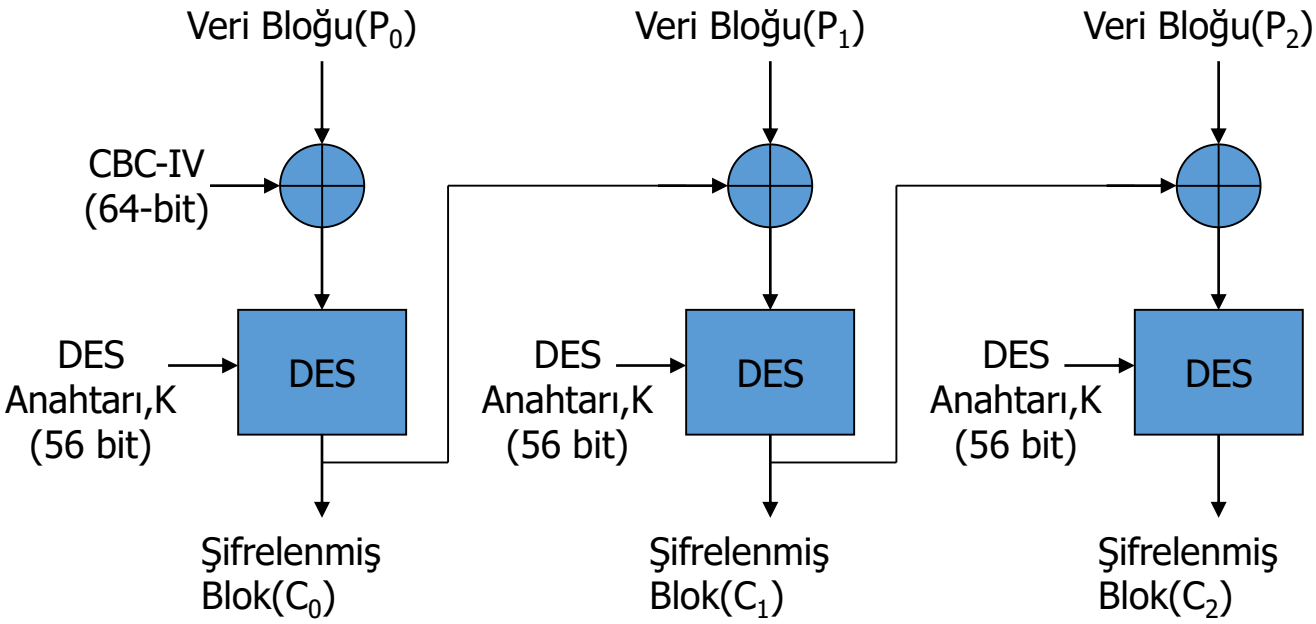
WiMAX Güvenlik Altyapısı



Veri Güvenliği (1/2)

- Şifreleme
  - Kullanılan Algoritma
    - DES
      - 56 bit anahtar
      - 64 bitlik bloklar
  - Kullanılan Şifreleme Kipi
    - “Şifreleme Bloklarını ardarda Bağlama Kipi” (Cipher Block Chaining,CBC)
    - CBC-IV: başlama vektörü TEK anahtar değiştokuşu sırasında öğrenilir
    - XOR: Çerçevedeki senkronizasyon alanında belirtilir.

Veri Güvenliği (2/2)



Şifreleme:

$$C_i = K[P_i \oplus C_{i-1}]$$

Şifre Çözme:

$$P_i = C_{i-1} \oplus K^{-1}[C_i]$$

Güvenlik Yönetimi(1/7)

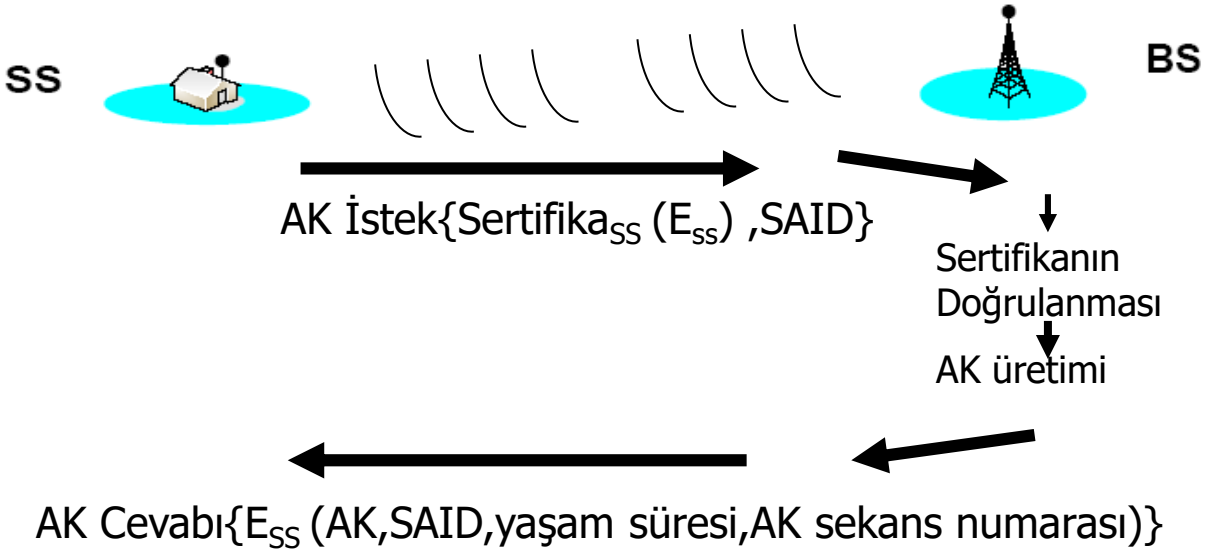
- Asıllama
  - Açık anahtarlı kriptografi kullanılır.
  - SS ile BS arasında SAID alışverişi
  - SS için kullanılan yöntem: X.509 sertifikalama
    - Üretici Sertifikası
      - Kendi kendine veya üçüncü kişi tarafından
      - Üretici bilgileri(WiMAX forumuna uygunluk)
    - SS sertifikası
      - Üretici tarafından
      - SS'in Seri numarası
      - SS'in MAC adresi
    - SS'ler açık-gizli anahtar çiftleri ile donatılmıştır
      - RSA tabanlı bir algoritma ile
      - Herhangi bir lokal algoritmayla dinamik olarak

Güvenlik Yönetimi(2/7)

- BS için ayrıca asıllama yok
  - BS, üretici sertifikasının açık anahtarını kullanarak SS'i asıllar.
  - Böylece standarda uygunluk anlaşılmış olur.
  - SS'in gizli anahtarının iyi saklandığı varsayılır.

Güvenlik Yönetimi(3/7)

- Asıllama anahtarı(AK,128-bit) alışverişi yapılır
  - Açık anahtar ile şifreli olarak gönderilir.
  - BS ve SS AK'yı elde ettikten sonra asıllama tamamlanmış olur.
  - SS periyodik olarak AK tazelemesi yapar.



Güvenlik Yönetimi(4/7)

- Anahtar oluşumu
  - Privacy Key Management (PKM)
  - Güvenlik birimi(SA) tarafından yönetilir.
  - SS'ler, PKM protokolünü BS'den asıllama ve trafik güvenliği parametrelerini almak için kullanır.
  - Asıllama anahtarı ve oturum tazeleme de PKM tarafından yönetilir.

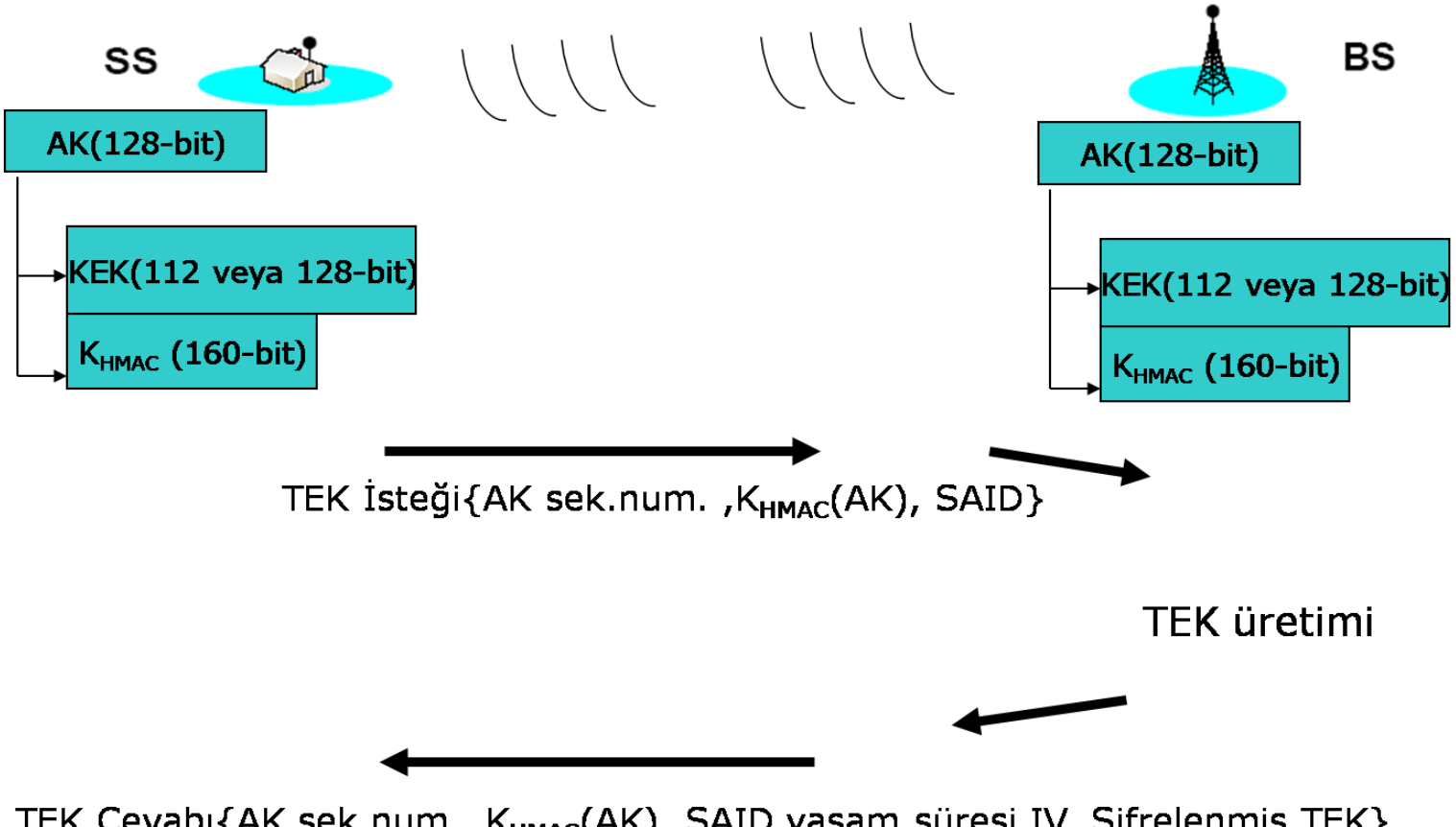
Güvenlik Yönetimi(5/7)

- Anahtar alışverişi
  - AK oluşumundan sonra, Traffic Encryption Keys (TEK) alışverişi yapılmalıdır.
    - TEK'ler 56-bitlik DES anahtarlarıdır.
    - Bu aşamda da AK'dan yardım alınır.
      - AK, BS'te anahtar oluşturulmasında kullanılacak olan Key-Encyrption Key(KEK) oluşturulmasında(112 yada 128 bit olabilir) ve HMAC'teki K anahtarı olarak kullanılır.
      - TEK, yukarıdaki anahtarlardan bağımsız olarak BS tarafından üretilir

Güvenlik Yönetimi(6/7)

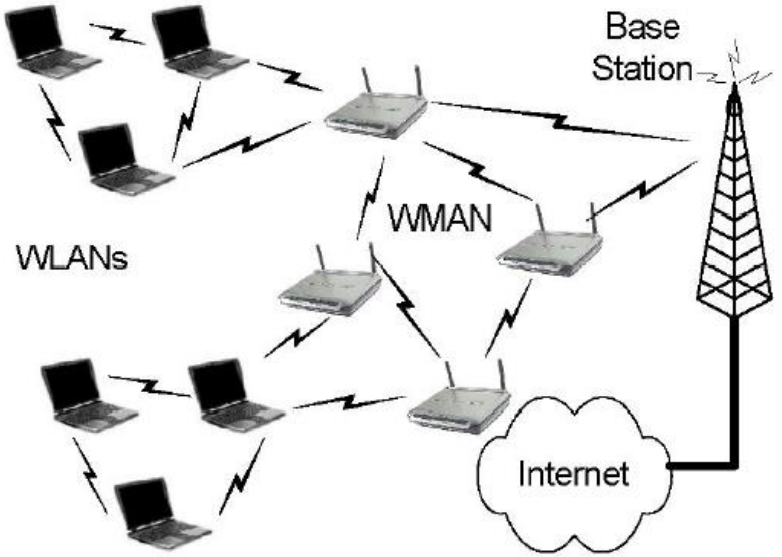
- TEK'in gönderilmesi:
  - 3DES ile
    - (112-bitlik KEK ile)
  - RSA ile
    - (SS'in Açık anahtarı ile)
  - AES ile
    - (128-bitlik KEK ile)
- Anahtar alışverişindeki asıllama,AK doğrulaması ve bütünlük HMAC-SHA1 ile sağlanır.

Güvenlik Yönetimi(7/7)



WiMAX Ağ(Mesh) yapısında Güvenlik(1/2)

- SS'ler BS olmadan birbirleriyle haberleşebilir→Mesh yapının en önemli özelliği BS'nin kapsama alanında artış olur
- Ağda bir düğüm çöktüğünde yada BS çöktüğünde tüm iletişim kesilmez.



WiMAX Ağ(Mesh) yapısında Güvenlik(2/2)

- Ağa katılmak isteyen bir düğüm kendisine en yakın düğümü “sponsor düğüm” ilan eder.
- İstemci düğüm,kendisini asıllaması için elçi düğüme mesaj gönderir.
- PMP’teki güvenlik işlemlerinin benzeri sponsor düğüm tarafından yapılır.
- Asıllama işini yapan gerçek düğümle bir tünel kuran elçi düğüm, istemci düğüme mesajları iletir.
  - Asıllama mesajları
  - Anahtar alışverişi
- Mesh’e dahil olan düğüm, diğer düğümlerle iletişime geçebilir.

Güvenlik Altyapısının Analizi(1/5)

- Veri şifrelemesindeki sorunlar
  - DES algoritması günümüzde kırılabilir bir algoritma haline gelmiştir.
    - Deneme-yanılma ve Brute-Force saldıralarına dayanıksızdır.
    - 128-bitlik AES kullanılabilir
      - Daha yavaş ama güvenliği arttırıcı bir yöntem

Güvenlik Altyapısının Analizi(2/5)

- Tekrar saldıralarına dayanıksızdır.
  - Aktif saldırılar gerçekleştirilebilir.
    - Telsiz ortamın doğasından kaynaklanan araya girebilme özelliğini ortadan kaldıracak bir yapı yok
    - Tekrar saldıraları için
      - Rastgele bir sayı
      - Paket numarası
      - Sekans numarası

Güvenlik Altyapısının Analizi(3/5)

- CBC Başlangıç vektörü tahmin edilebilir.
  - Seçilen Açık metin saldırısı yapılarak gerçek metin elde edilebilir.
  - Bazı çözümler
    - Başlangıç vektörü için
      - Her bir metin için değil, her bir çerçeve için IV üretimi
      - Bu IV'nin veriye gömülmesi
      - Şifreleme yükü artar!

Güvenlik Altyapısının Analizi(4/5)

- Anahtar Yönetimindeki sorunlar:
  - TEK'te kullanılan sekans numarasının 2-bit olması
    - Her bir tekrar saldırısında %25 bir olasılıkla TEk bulabilinir!
  - Rastgele üretilen TEK'lerin nasıl bir rassal fonksiyonla üretildiği konusunda bilgilendirme yapılmıyor.
    - Değişik üreticilerin oluşturduğu bir ağda güvensizlik ve dengesizlik yaratabilir.
  - BS tarafından oluşturulan AK'nin tazeligine güvenilmeli!
    - SS bunu kontrol etmiyor.

Güvenlik Altyapısının Analizi(5/5)

- Asıllamadaki problemler
  - Çift taraflı bir asıllama yok.
    - BS asıllanmıyor.
      - Ortadaki adam saldırısı yapılabilir.
  - Asıllama protokolunde gönderilen mesajlar doğrulama için yetersiz
    - EAP(Extensible Authentication Protocol) tabanlı bir asıllama yapılabilir.
      - EAP-TLS(Transport Layer Securty)
      - EAP-MD5

GÜVENLİ İŞLETİM SİSTEMLERİ

- ✓ **Tarihçe**
- ✓ **Linux İşletim sistemi nedir , nelerden oluşur**
- ✓ **Linux Mimarisi**
- ✓ **Neden Linux ?**
- ✓ **Linux İşletim Sistemlerinin Özellikleri**

LINUX

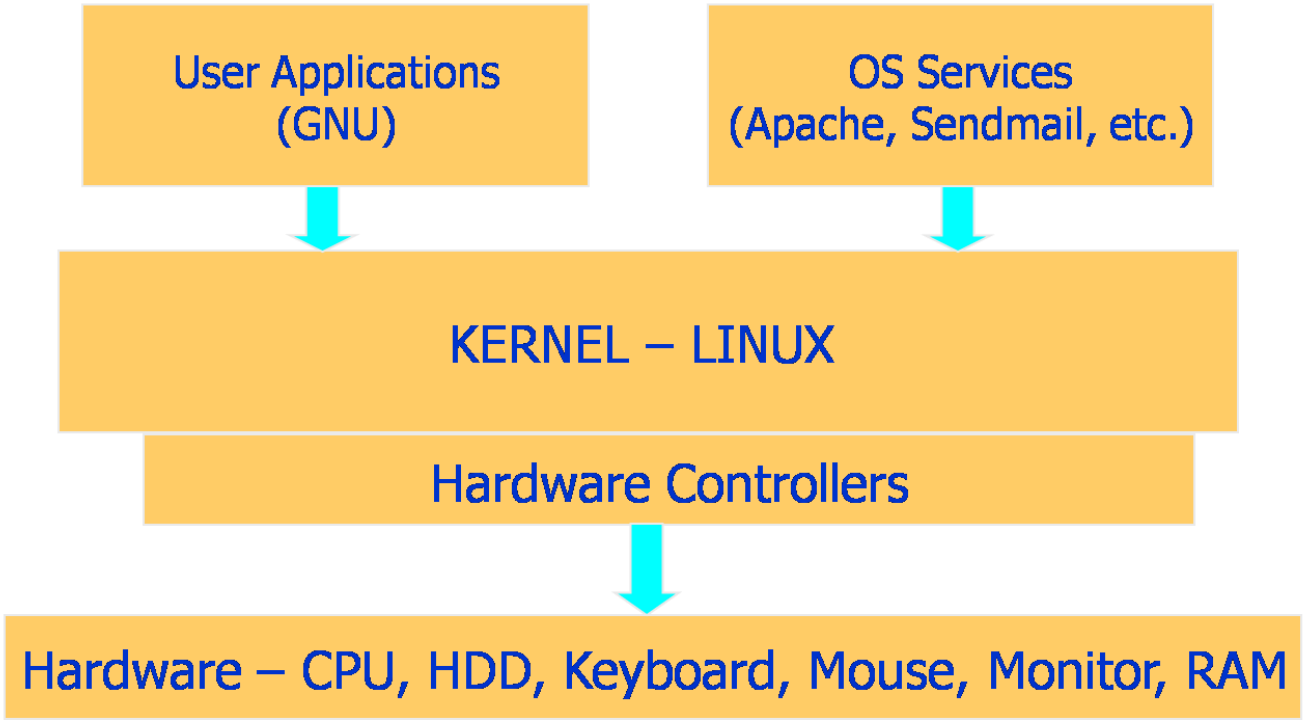
- Tarihçe
  - 1991'de Linus Torvalds adında Finlandiyalı bir öğrenci bilgisayar mühendisliği eğitimi alırken Intel'in 80386 geliştirmek için çıkartmıştır.
  - Minix de olmasını istediği özellikleri yeni işletim sistemine ekledi.
  - 5 Ekim 1991 de Linux un ilk sürümü 0.02 yi MIT'nin haber listelerinde Dünya ya duyurdu.

Linux işletim sistemi nedir?

- Unix bir işletim sistemi ailesine verilen ortak bir isimdir.
- Linux (resmi olarak olmasa da), OpenBSD, FreeBSD, Irix, Solaris, Aix... çeşitli Unix türevleridir.
- Linux, Unix sistemlerinin tüm avantajlarını taşır.Çok kullanıcılı ve bilgisayar ağlarında kullanılmak üzere tasarlanmıştır.
- Linux dağıtımları ;
  - Suse, Red Hat, Fedora, Knoppix vs

Linux işletim sistemi

LINUX MİMARİSİ



Neden LINUX ?

- Hız
- Maliyet
- Yaygınlık
- Güvenlik
- Sağlamlık

LINUX İşletim Sistemi Özellikleri

- Birden çok kullanıcı desteği
- Çok görevli olması
- Çok işlemci desteği
- TCP/IP desteği
- Dosya yapısı
- Kabuklar (shell)

1.Fiziksel Güvenlik

- **1.1 BIOS Güvenliği**

➢Parola ayarı yapmak gerekir .

➢ Konulan parola caydırıcı etki yapabilir.

➢ Tam anlamıyla güvenli sayılmaz.

2. Çekirdek (Kernel) Güvenliği

- Güncel tutmak
- Yamalı Çekirdek olmasından emin olmak
- Çekirdeğin derlenmesi gerekir.

3. Kullanıcı Güvenliği

- Kullanıcılara yeni hesap açarken onlara gerekli olan kadar , minimum imtiyaz hakkı verilmelidir.
- Ne zaman login ,log-off olduklarını belirleyen kayıtlar mutlaka tutulmalıdır.
- Aktif olmayan hesaplar silinmelidir.Aktif olmayan hesaplar log dosyaları kontrol ederek görülebilir.

3. Kullanıcı Güvenliği

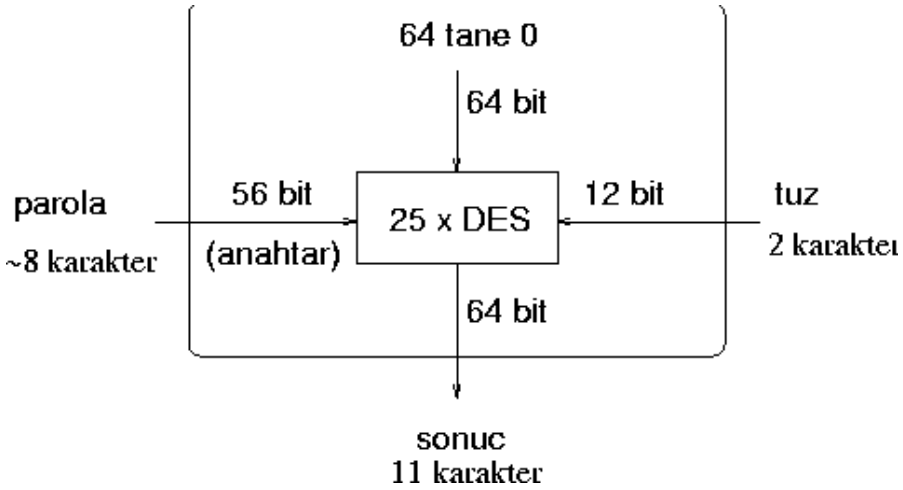
- Root hesabı adına dikkat edilmesi gerekenler ;
- Root olarak giriş izni çok kullanıcıya verilmemelidir.
- Root olarak rlogin/sh/rexec(r-utilities) kullanılmamalıdır. Kesinlikle .rhosts dosyası yani özel erişim dosyası yaratılmamalıdır.

4. Parolalar

- Çok-kullanıcılı işletim sistemlerinde kullanıcının kimliğinin belirlenmesi büyük önem taşımaktadır. Hem sistemi kullanmaya yetkisi olmayan kişilerin sisteme girmelerinin engellenmesi, hem de sistemdeki kullanıcıların birbirlerinden ayırt edilebilmeleri için, her kullanıcıya bir parola verilir ve sisteme giriş başta olmak üzere tüm kritik işlemlerde kullanıcıya parolası sorulur.
- Parolalar, diğer kullanıcı bilgileriyle birlikte, parola dosyasında (**/etc/passwd**) tutulur. Bu dosyadaki her satir, bir kullanıcı ile ilgili bilgileri saklar. Bir satırdaki alanlar, sırasıyla, kullanıcı adı, parola, kullanıcı numarası, grup numarası, ad, kişisel dizin ve komut yorumcusudur.

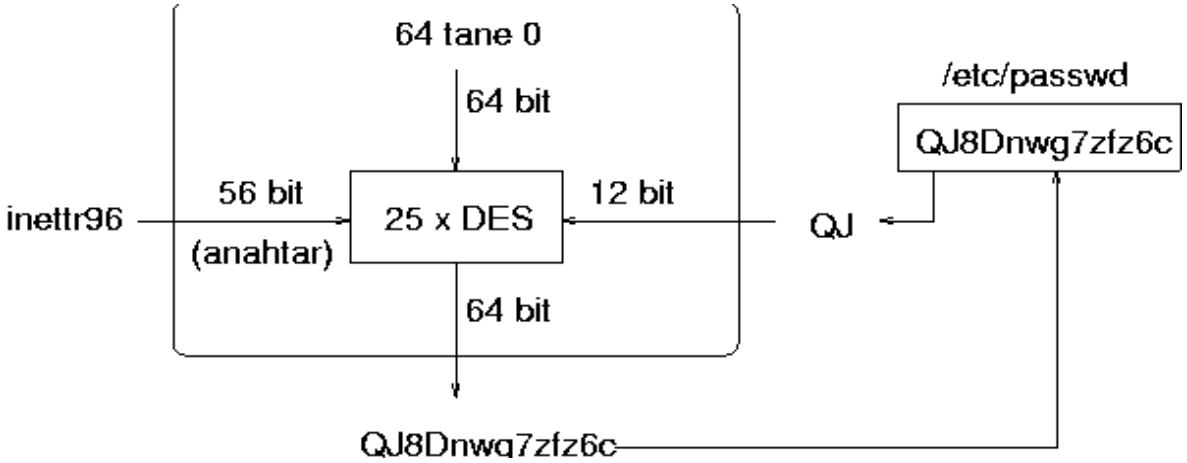
4.1 Parolaların Şifrelenmesi

- **Crypt** fonksiyonu ile şifreleme



4.1 Parolaların Şifrelenmesi

- **Parola Denetimi**



4.2 Parola Seçimi

Şu tip parolalar kolay tahmin edilebilen parolalar sayılmaktadır:

- Kullanıcı ile yakinliği olan kişilerinkiler (kendisi, ailesi, arkadaşları, yakınları) basta olmak üzere bütün erkek ve kadın isimleri
- Doğum tarihleri
- Kullanıcı ile ilgili herhangi bir bilgi (kullanıcı adı, oda numarası, telefon numarası, arabasının plaka numarası, sosyal güvenlik numarası)
- Yer isimleri
- Bilgisayar terimleri
- Klavyede belli bir düzene göre ardarda gelen harflerden oluşan parolalar (qwerty)
- Anlamlı bir sözcük
- Yalnızca küçük (ya da yalnızca büyük) harflerden oluşan parolalar
- Yukarıdakilerden birinin başına ya da sonuna bir rakam eklenerek oluşturulan parolalar
- Yukarıdakilerin ters yazılışları

4.2 Parola Seçimi

İyi bir parola üretmek için önerilen iki yöntem vardır:

- İki sözcüğün arasına bir rakam ya da noktalama işareti konarak birleştirilmesi
- Seçilen bir cümlenin sözcüklerinin bas harfleri

4.3 Tehlikeler

Bir saldırganın parola dosyasını eline geçirmesi birkaç şekilde mümkün olabilir:

- Bir kullanıcının parolasını elde ederek sisteme girer ve dosyayı alır.
- Bazı programlardaki hatalardan yararlanarak sisteme girmeden dosyayı alır.
- Sistemdeki bir kullanıcı parola dosyasını saldırgana gönderir.
- Saldırgan, sistemdeki kullanıcılardan biridir.

4.4. Önlemler

- Parola Seçiminin Kullanıcıya Bırakılmaması
  - Sistem sorumlusu ya da rasgele parola üreten program tarafından parola verilmesi gerekir.
  - mkpasswd programı
- Parola Seçiminin Kısıtlanması
  - anlpasswd
- Parola Dosyasının Sistem Sorumlusu Tarafından Kırılması
  - crack
- Parolaların Geçerlilik Surelerinin Kısıtlanması
- Gölge Parolalar
  - Parolalar gölge dosyasına (/etc/shadow) şifrelenmiş parolalar konur.
  - Shadow Password Suite

5. Dosya Güvenliği

- Her dosyanın bir sahibi, bir de grubu vardır. Dosya üzerinde kimin hangi işlemleri yapabileceğine dosyanın sahibi olan kullanıcı karar verir. Erişim hakları, dosyanın sahibi, grubu ve diğerleri için ayrı ayrı belirtilir.
- Her biri için dosyanın okunmasına (read), yazılmasına (write) ve çalıştırılmasına (execute) izin verilebilir. Böylece her dosya için üç tane üçlüden oluşan bir erişim hakları listesi elde edilir.

-rwxr-x--- 1 karin users 4030 Dec 4 15:30 deneme

- Örnekteki ``deneme'' dosyasının sahibi “karin" kullanıcısı, grubu "users" grubudur. “karin” kullanıcısı dosyayı okuyabilir, yazabilir ve çalıştırabilir; "users" grubundaki kullanıcılar okuyabilir ve çalıştırabilir; diğer kullanıcıların ise hiçbir hakki yoktur.

5.1. Tehlikeler

- **Dosyanın izinsiz Olarak Okunması**
  - Kullanıcıların kişisel dosyalarının ve e-postalarının okunması
- **Dosyanın Yetkisiz Kişilerce Değiştirilmesi**
  - Sistem dosyalarının değiştirilmesi
  - Yetkili kullanıcı yaratılabilir
  - Kayıt dosyalarının silinebilmesi

5.2. Önlemler

- **Dosya Değişikliklerinin Denetimi**
  - Dosya imzaları oluşturma
  - Tripwire paketi kullanılmalı
- **Şifreleme**
  - PGP (Pretty Good Privacy) kullanılması
  - CFS (Cryptographic File System)

Sonuç

- 802.16 standardındaki 2 düzeyli yapı,802.11'e göre geliştirilmeye daha elverişli bir altyapı oluşturmakta.
- Sertifika otoriteleri hakkında daha açık bilgiler verilmeli.
- Veri şifreleme yöntemi:DES yetersiz
- Tek taraflı bir asıllama söz konusu
  - Geliştirilmesi gereken bir nokta
  - EAP kullanılabilir
- Anahtar üretiminde problemler var
  - Tekrar saldırıların engellenebilmesi için rastgele sayıların üretilmesi gerekiyor.

Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "***Air Interface for Fixed Broadband Wireless Access Systems***".
- [2] David Johnston ve Jesse Walker--INTEL: "***Overview of IEEE 802.16 Security***"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "***IEEE 802.16 WiMax Security***"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"***Security issues in WiMAX/IEEE 802.16 BWA System***"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"***Security of 802.16 in Mesh Mode***"

Kaynaklar

- http://www.linuxplanet.com/linuxplanet/interviews/4495/1
- www.linuxsecurity.com
- www.linux.org.tr
- IMPROVING THE SECURITY OF YOUR UNIX SYSTEM ,David A. Curry, Systems Programmer ,Information and Telecommunications Sciences and Technology Division
- Linux Sistem Güvenliği Raporu ,2003