Penetration Testing Security Analysis
Wireshark network packet analysis tool

TheMirkin
WhiteHat
themirkin@hotmail.com
themirkin.org | janissaries.org

#JanissariesTeam

Wires hark Nedir ?

Bu seferki Konumuz wires hark bu yazılım analiz işlemlerinde kullanılan yardımcı bir program olup network trafiğinin, bir grafik ara yüz üzerinden izlenmesini sağlayan bir programdır.

Uygulamanın kurulu olduğu bilgisayar üzerinden anlık network trafiği izlenebileceği gibi, Wires hark daha önce kaydedilmiş dosyaların incelenmesi amacı ile de kullanılabilir .

Ücretsiz bir yazılım olup bir çok alanda kullanılmaktadır ,
anlatım yapıyorum ama ne kadar işinizi görecektir bilinmez ama ciddi anlamda iş gören ve kullanılan programdır.
Anlatımlarımızı örnekleme ile birlikte yapacağımızdan kolay anlayacağınızı düşünüyorum

Wires hark Özellikleri?

Windows ve Unix sistemlerde çalışabilir.

- Ağ arabiriminden eş zamanlı paket yakalayabilir.
- Paketleri çok ayrıntılı bir şekilde protokol bilgileriyle görüntüler
- Yakaladığı paketleri kaydetme imkanı vardır
- Kriterlere göre paket filtreleme mevcuttur
- Kriterlere göre paket arama mevcuttur
- paket görünümleri renklendirilerek kullanım kolaylaştırılabilir.
- Çeşitli istatistikler yapabilir
- ...ve daha birçoğu

Wires hark diğer paket yakalama yazılımlarının açabileceği formatlar göz önünde bulundurularak tasarlanmıştır ... ve sürekli güncellenmektedir

- libpcap, tcpdump ve tcpdump formatındaki diğer araçlar
- (*.pcap,*.cap,*.dmp)
- 5Views (*.5vw)
- HPUX nettl (*.TRC0,*.TRC1)
- Microsoft Network Monitor NetMon (*.cap)
- Network Associates Sniffer DOS (*.cap,*.enc,*.trc,*fdc,*.syc)
- Network Associates Sniffer Windows (*.cap)
- Network Instruments Observer version 9 (*.bfr)
- Novell LANalyzer (*.tr1)
- Sun snoop (*.snoop,*.cap)
- Visual Networks Visual UpTime traffic (*.*)

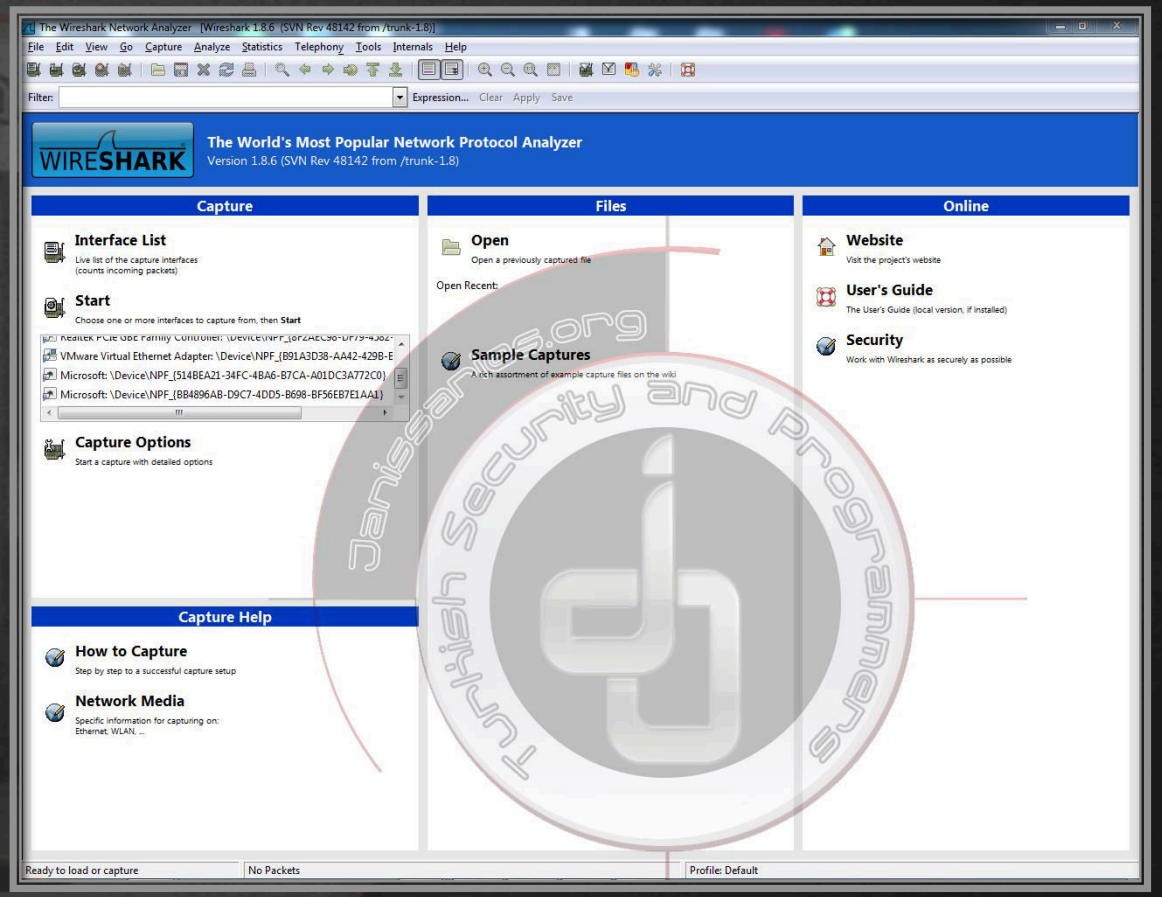
Nasıl Kullanılır?

Uygulama indirilip kurulduğunda, bu uygulama ile birlikte Windows yüklü bilgisayara WinPcap isimli bir uygulama daha kurulacaktır. WinPcap, kurulu olduğu bilgisayarın anlık Ethernet trafiğinin yakalanmasını sağlayan programdır.
Wireshark bu uygulamadan gelen veriyi kullanarak size grafik bir ara yüz üzerinden Ethernet trafiğini izleme/inceleme fırsatı sunar

Uygulama başlatıldığında yandakine benzer bir ekran açılacaktır.

Burada Start bölümünün altında bilgisayarda algılanan Ethernet kartları listelenecektir.

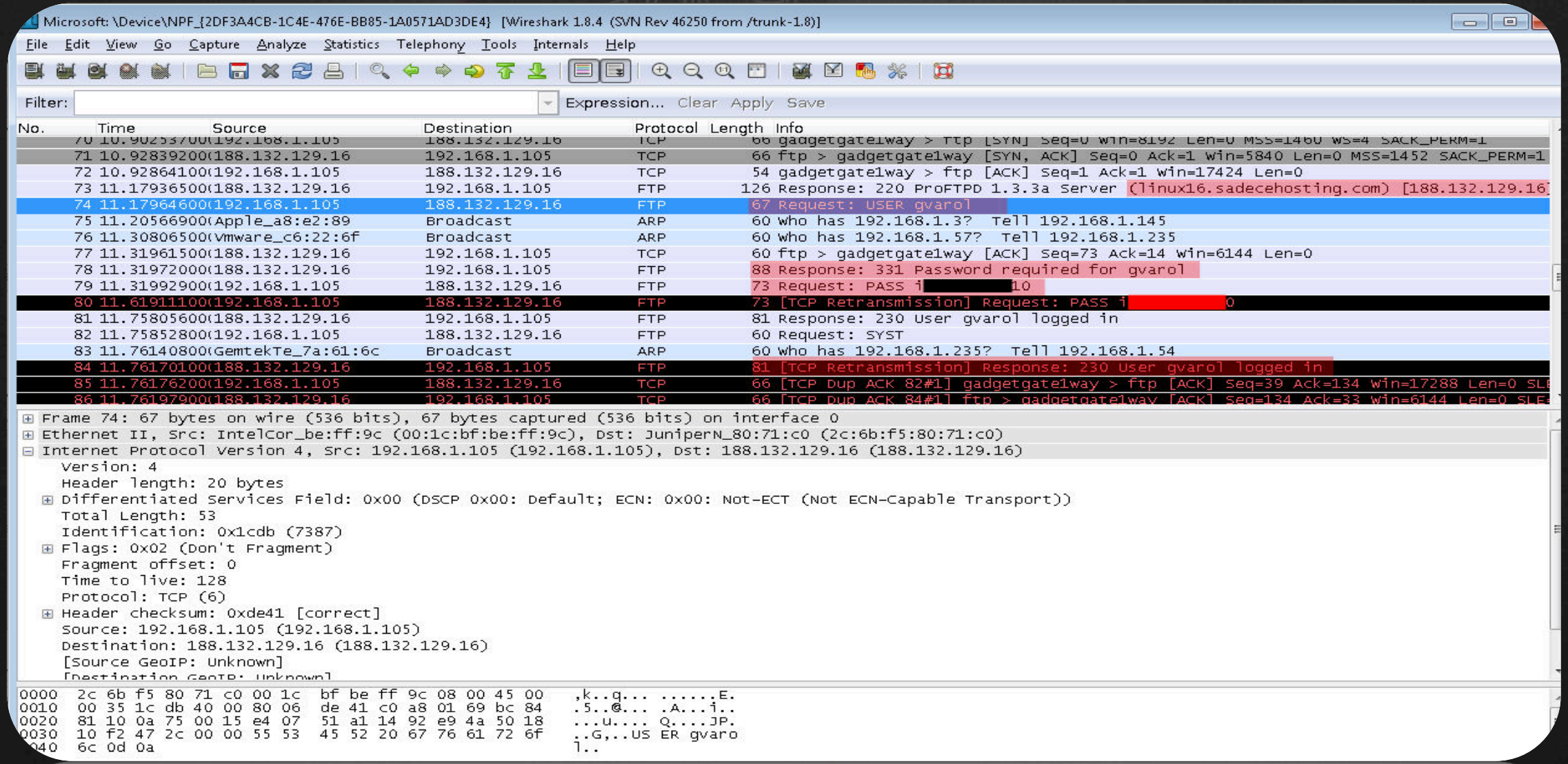
Bu kartlardan biri seçilir ve ardından Start butonuna tıklanırsa uygulama ilgili Ethernet kartının network trafiğini loglamaya başlar



Keylogger gibi düşünebilirsiniz bir bakıma bu dinlemeler üzerinde Siteye gönderdiğiniz post işlemleri dahil hepsini içerisinde barındırmaktadır

Sniffing işlemi yapmaktadır kısaca bu dinleme içerisinde sesli görüşme bir yana videolu görüşmeleriniz ve izlediğiniz videolar dahil işlendikten hemen sonra izlenmesi mümkün kılınmaktadır :) bununla ilgili örnek göstererek göstermeye çalışacağım

Sniffing


Microsoft: \Device\NPF_{2DF3A4CB-1C4E-476E-BB85-1A0571AD3DE4} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
71 10.92839200 188.132.129.16 192.168.1.105 TCP 66 ftp > gadgetgate1way [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM=1
72 10.92864100 192.168.1.105 188.132.129.16 TCP 54 gadgetgate1way > ftp [ACK] Seq=1 Ack=1 Win=17424 Len=0
73 11.17936500 188.132.129.16 192.168.1.105 FTP 126 Response: 220 ProFTPD 1.3.3a Server (linux16.sadecehosting.com) [188.132.129.16]
74 11.17964600 192.168.1.105 188.132.129.16 FTP 67 Request: USER gvarol
75 11.20566900 Apple_a8:e2:89 Broadcast ARP 60 Who has 192.168.1.3? Tell 192.168.1.145
76 11.30806500 Vmware_c6:22:6f Broadcast ARP 60 Who has 192.168.1.57? Tell 192.168.1.235
77 11.31961500 188.132.129.16 192.168.1.105 TCP 60 ftp > gadgetgate1way [ACK] Seq=73 Ack=14 Win=6144 Len=0
78 11.31972000 188.132.129.16 192.168.1.105 FTP 88 Response: 331 Password required for gvarol
79 11.31992900 192.168.1.105 188.132.129.16 FTP 73 Request: PASS i[redacted]10
80 11.61911100 192.168.1.105 188.132.129.16 FTP 73 [TCP Retransmission] Request: PASS i[redacted]0
81 11.75805600 188.132.129.16 192.168.1.105 FTP 81 Response: 230 User gvarol logged in
82 11.75852800 192.168.1.105 188.132.129.16 FTP 60 Request: SYST
83 11.76140800 GemtekTe_7a:61:6c Broadcast ARP 60 Who has 192.168.1.235? Tell 192.168.1.54
84 11.76170100 188.132.129.16 192.168.1.105 FTP 81 [TCP Retransmission] Response: 230 User gvarol logged in
85 11.76176200 192.168.1.105 188.132.129.16 TCP 66 [TCP Dup ACK 82#1] gadgetgate1way > ftp [ACK] Seq=39 Ack=134 Win=17288 Len=0
Frame 74: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: IntelCor_be:ff:9c (00:1c:bf:be:ff:9c), Dst: JuniperN_80:71:c0 (2c:6b:f5:80:71:c0)
Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 188.132.129.16 (188.132.129.16)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 53
Identification: 0x1cdb (7387)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0xde41 [correct]
Source: 192.168.1.105 (192.168.1.105)
Destination: 188.132.129.16 (188.132.129.16)
[Source GeoIP: Unknown]
0000 2c 6b f5 80 71 c0 00 1c bf be ff 9c 08 00 45 00 ,k..q... ......E.
0010 00 35 1c db 40 00 80 06 de 41 c0 a8 01 69 bc 84 .5..@... .A...i..
0020 81 10 0a 75 00 15 e4 07 51 a1 14 92 e9 4a 50 18 ...u.... Q....JP.
0030 10 f2 47 2c 00 00 55 53 45 52 20 67 76 61 72 6f ..G,..US ER gvaro
0040 6c 0d 0a l..

Wireshark Nerelerde Kullanılır

Bu konu aslında göreceli bir kavram bana göre ama ben şimdilik programın kullanımını simgeleyen 2 bölüm yaptım pentest1 ve pentest2 1 ve 2 aslında bir bütündür ama kısa bir anlatım için ayırdım ...
Pentest 1 buna baktığınızda bireysel işlem gibi durmaktadır ama Pentest 2 gören kişi %80 civarında kesin hack içeriği var bunda diyerek göz süzdürmektedir , ama işin aslı her ikisine de ihtiyaç olması ve kullanılabilir olmasıdır ...

Pentest 1

- Ag trafik tespiti
- Baglantı sorunu tespiti
- Port tarama tespiti

Pentest 2

- Veri madenciligi
- Saldırı tespiti
- Port tarama tespiti
- Casus yazılım tespiti
- Veri inceleme (okuma)

Örnek 1

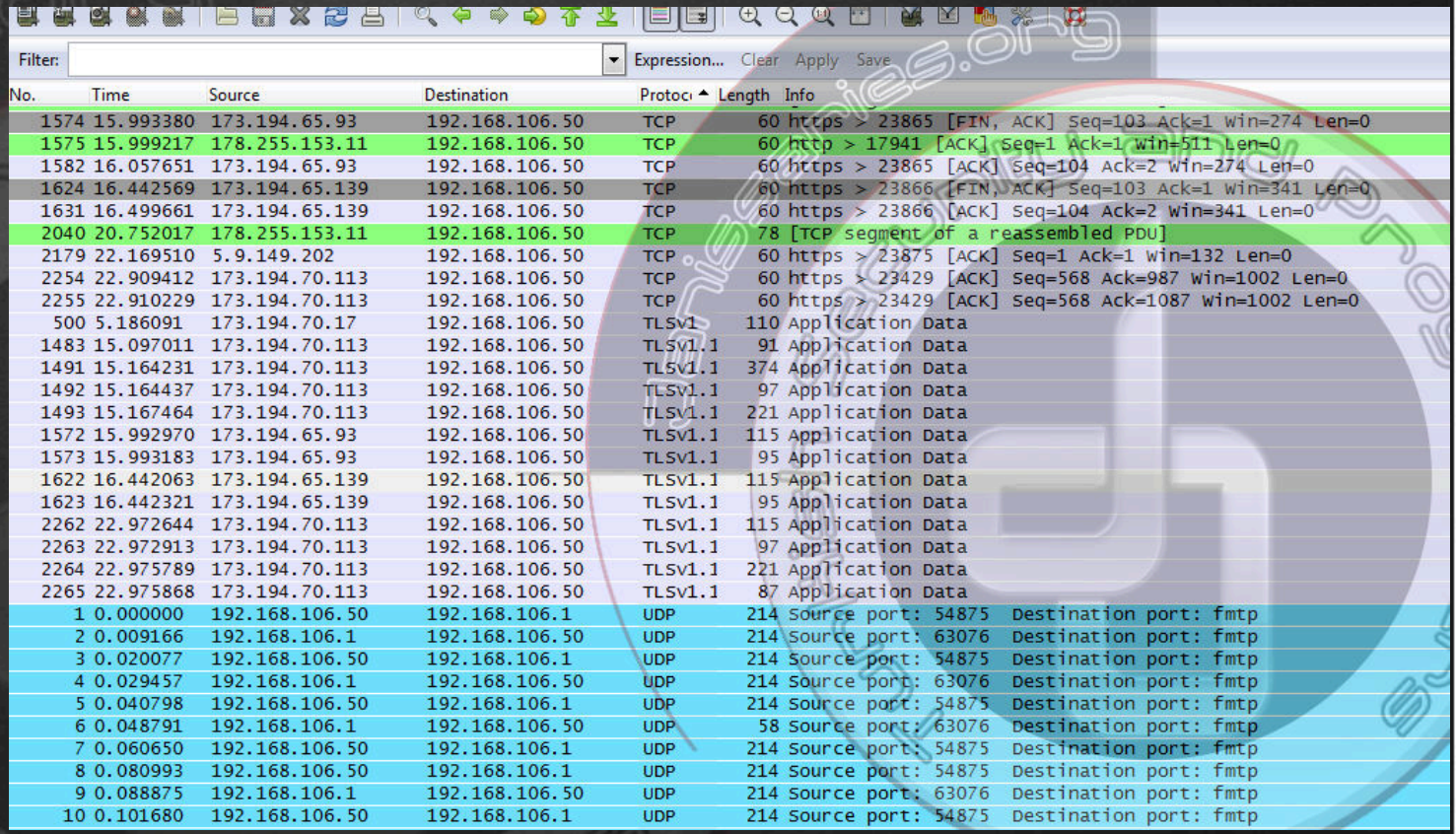
Bu örneğimizde Daha önce paketlenmiş olan bir dosyamız var bu dosyamızı inceleyerek ele alacağız

Yan tarafta gördüğünüz daha önce kaydedilmiş bir proje diyelim biz buna şimdilik bu proje içerisinde bir ses işlemi var Biz bunu nasıl ortaya çıkartıp dinleyebiliriz ?

Cevap :

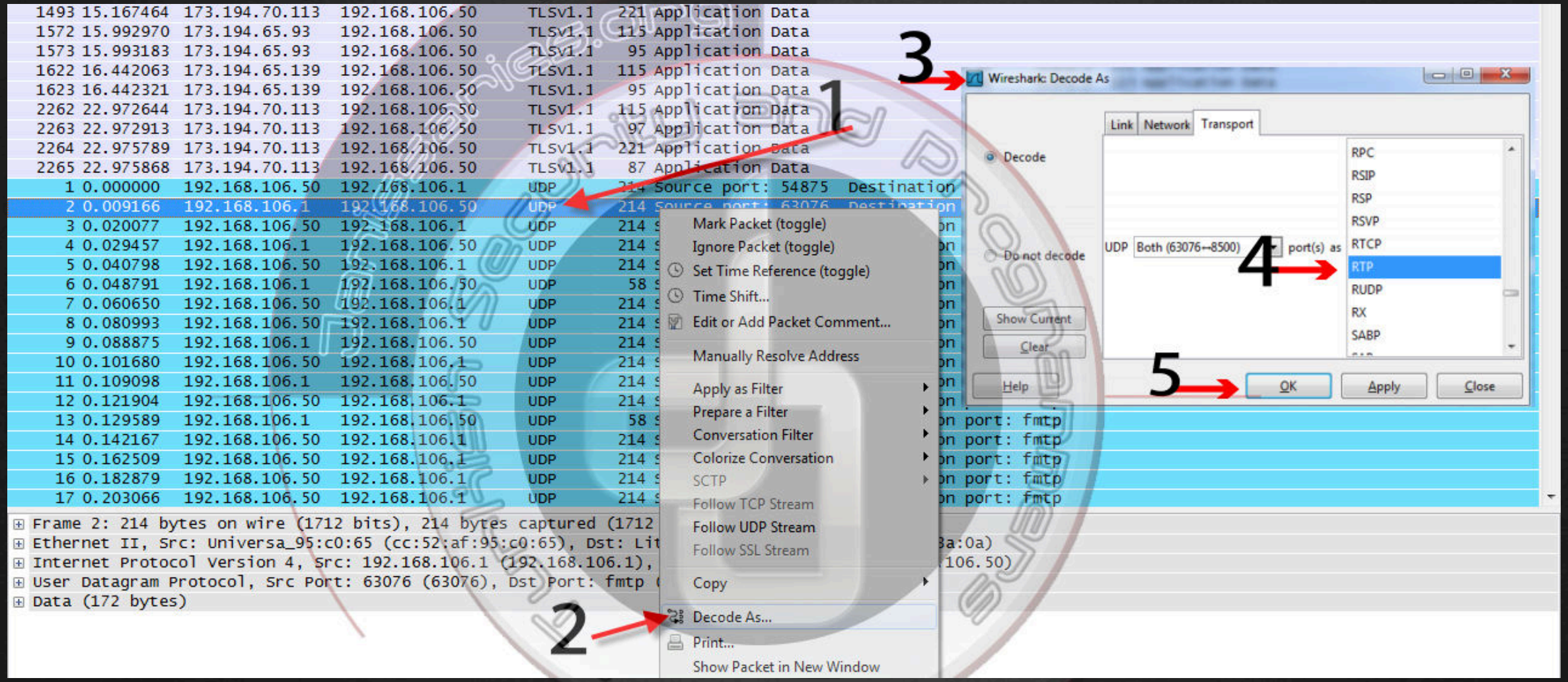
Şimdi yan taraftaki resme bakarsanız protokol bölümünde TCP – UDP – SSDP – HHTP gibi protokoller mevcut bu nu dinleyebilmemiz için bir Dönüştürme işlemi yapmamız gerekmektedir ilk olarak bizim UPT protokolünü RTP ye çevirmemiz daha sonrasında decode ederek işlenebilir hale çekmemiz gerekmektedir bunun için

Bu işlemi sırası ile sizlere vereceğim ama ezber yerine uygulama yapınız >>>>>>>>



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protoc	Length	Info
1574	15.993380	173.194.65.93	192.168.106.50	TCP	60	https > 23865 [FIN, ACK] Seq=103 Ack=1 Win=274 Len=0
1575	15.999217	178.255.153.11	192.168.106.50	TCP	60	http > 17941 [ACK] Seq=1 Ack=1 Win=511 Len=0
1582	16.057651	173.194.65.93	192.168.106.50	TCP	60	https > 23865 [ACK] Seq=104 Ack=2 Win=274 Len=0
1624	16.442569	173.194.65.139	192.168.106.50	TCP	60	https > 23866 [FIN, ACK] Seq=103 Ack=1 Win=341 Len=0
1631	16.499661	173.194.65.139	192.168.106.50	TCP	60	https > 23866 [ACK] Seq=104 Ack=2 Win=341 Len=0
2040	20.752017	178.255.153.11	192.168.106.50	TCP	78	[TCP segment of a reassembled PDU]
2179	22.169510	5.9.149.202	192.168.106.50	TCP	60	https > 23875 [ACK] Seq=1 Ack=1 Win=132 Len=0
2254	22.909412	173.194.70.113	192.168.106.50	TCP	60	https > 23429 [ACK] Seq=568 Ack=987 Win=1002 Len=0
2255	22.910229	173.194.70.113	192.168.106.50	TCP	60	https > 23429 [ACK] Seq=568 Ack=1087 Win=1002 Len=0
500	5.186091	173.194.70.17	192.168.106.50	TLSv1	110	Application Data
1483	15.097011	173.194.70.113	192.168.106.50	TLSv1.1	91	Application Data
1491	15.164231	173.194.70.113	192.168.106.50	TLSv1.1	374	Application Data
1492	15.164437	173.194.70.113	192.168.106.50	TLSv1.1	97	Application Data
1493	15.167464	173.194.70.113	192.168.106.50	TLSv1.1	221	Application Data
1572	15.992970	173.194.65.93	192.168.106.50	TLSv1.1	115	Application Data
1573	15.993183	173.194.65.93	192.168.106.50	TLSv1.1	95	Application Data
1622	16.442063	173.194.65.139	192.168.106.50	TLSv1.1	115	Application Data
1623	16.442321	173.194.65.139	192.168.106.50	TLSv1.1	95	Application Data
2262	22.972644	173.194.70.113	192.168.106.50	TLSv1.1	115	Application Data
2263	22.972913	173.194.70.113	192.168.106.50	TLSv1.1	97	Application Data
2264	22.975789	173.194.70.113	192.168.106.50	TLSv1.1	221	Application Data
2265	22.975868	173.194.70.113	192.168.106.50	TLSv1.1	87	Application Data
1	0.000000	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp
2	0.009166	192.168.106.1	192.168.106.50	UDP	214	Source port: 63076 Destination port: fmtp
3	0.020077	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp
4	0.029457	192.168.106.1	192.168.106.50	UDP	214	Source port: 63076 Destination port: fmtp
5	0.040798	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp
6	0.048791	192.168.106.1	192.168.106.50	UDP	58	Source port: 63076 Destination port: fmtp
7	0.060650	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp
8	0.080993	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp
9	0.088875	192.168.106.1	192.168.106.50	UDP	214	Source port: 63076 Destination port: fmtp
10	0.101680	192.168.106.50	192.168.106.1	UDP	214	Source port: 54875 Destination port: fmtp

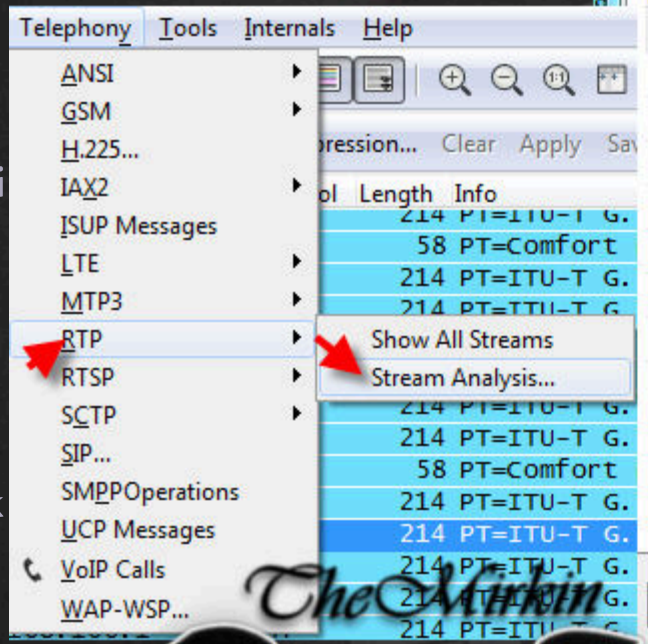


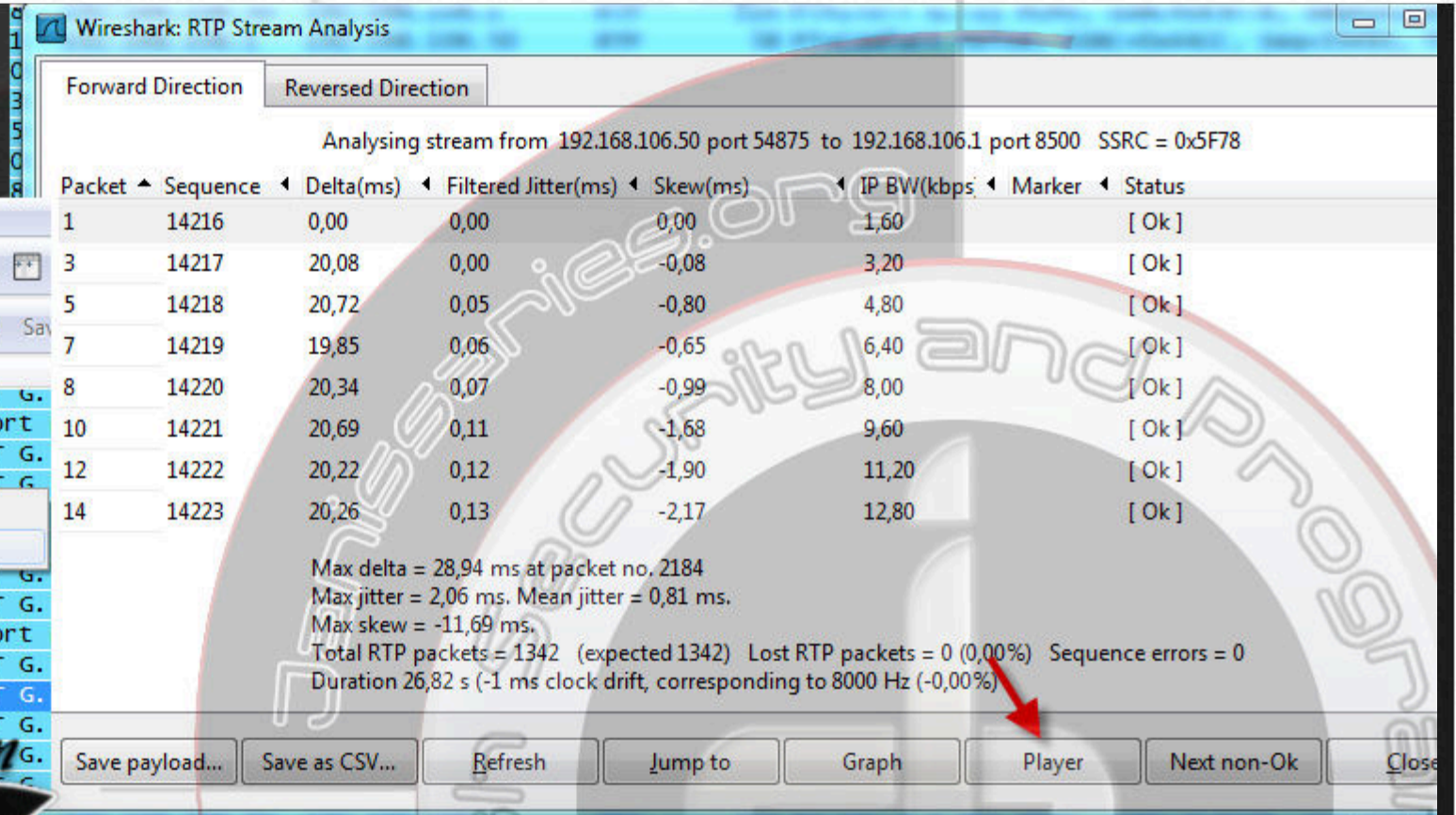
1 UTP protokolünde olan herhangi bir işleme sağ tıklayarak Decode As seçeneğine tıklayın

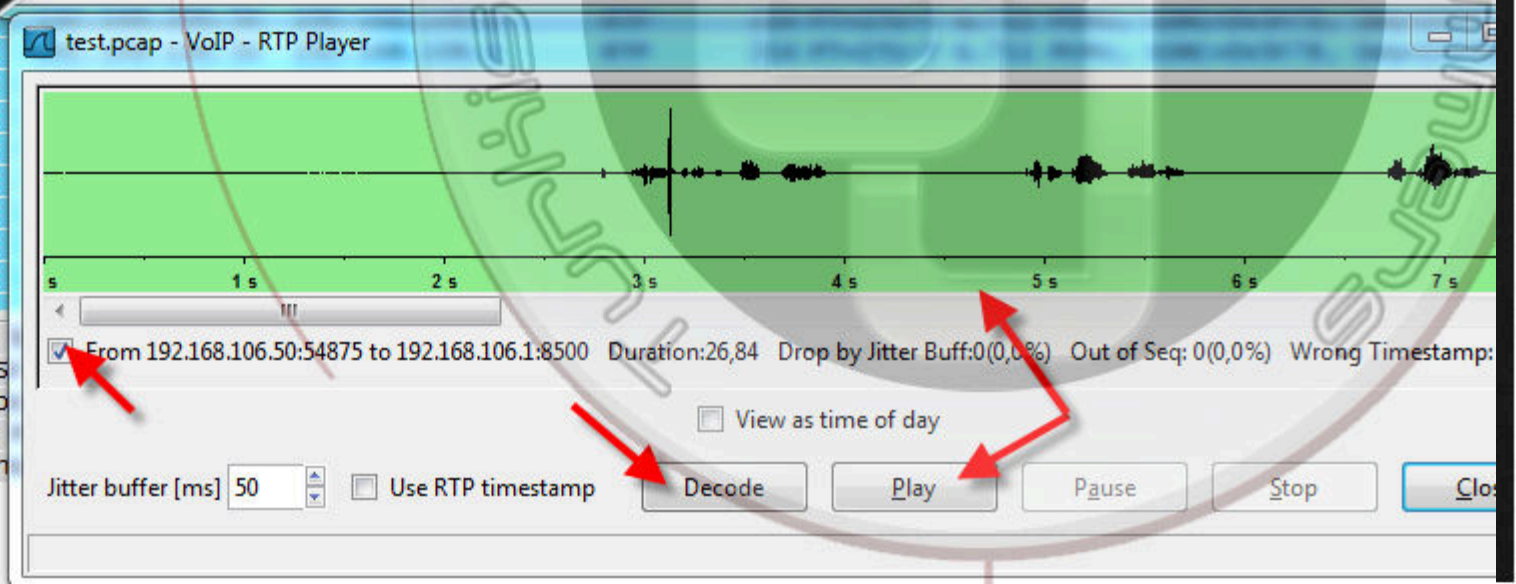
2 Açılan Menü Bizim UDP protokolündeki paketi çevireceğimiz Paket türünü seçmemizi ister Burada RTP Türünü seçeceğiz

3 Seçim yapıldığında Proje içerisinde olan Tüm UDP paketleri RTP'ye dönüşecektir ve bizlere yanılmıyorsak dinleme imkanı vericektir Devam edelim Konu sonunda video ile de sizlere bu örneği hızlı bir şekilde gösterimini yapacağım ...

Burada ilk olarak hangi paketi ele alarak işleyeceğimizi daha sonrasında ise ele alınan paketin decode ve dinleme işlemini Göstermiş olduk bu dosyayı ek olarak sizlere vereceğim üzerinde çalışıp göz gezdirerek hiç yoktan deneme yanılma işlemleri yaparak ta öğrenebilirsiniz







Zaman oldukça
Videolu ve konu anlatımlı
örneklerle açıklanacaktır

Penetration Testing Security Analysis
Wireshark network packet analysis tool

TheMirkin
WhiteHat
themirkin@hotmail.com
themirkin.org | janissaries.org

#JanissariesTeam

http://youtu.be/sCx7runj4ko