

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** trafiginin, bir **grafik** ara yüz üzerinden izlenmesini sağlayan bir programdır.

Uygulamanın kurulu olduğu bilgisayar üzerinden **anlık** **network** trafigi 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.
Anlatımlarımıza örneklemme 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 görüntüleri 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 tcdump 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 trafiginin yakalanmasını sağlayan programdır. Wireshark bu uygulamadan gelen veriyi kullanarak size grafik bir ara yüz üzerinden Ethernet trafigini izleme/inceleme fırsatı sunar

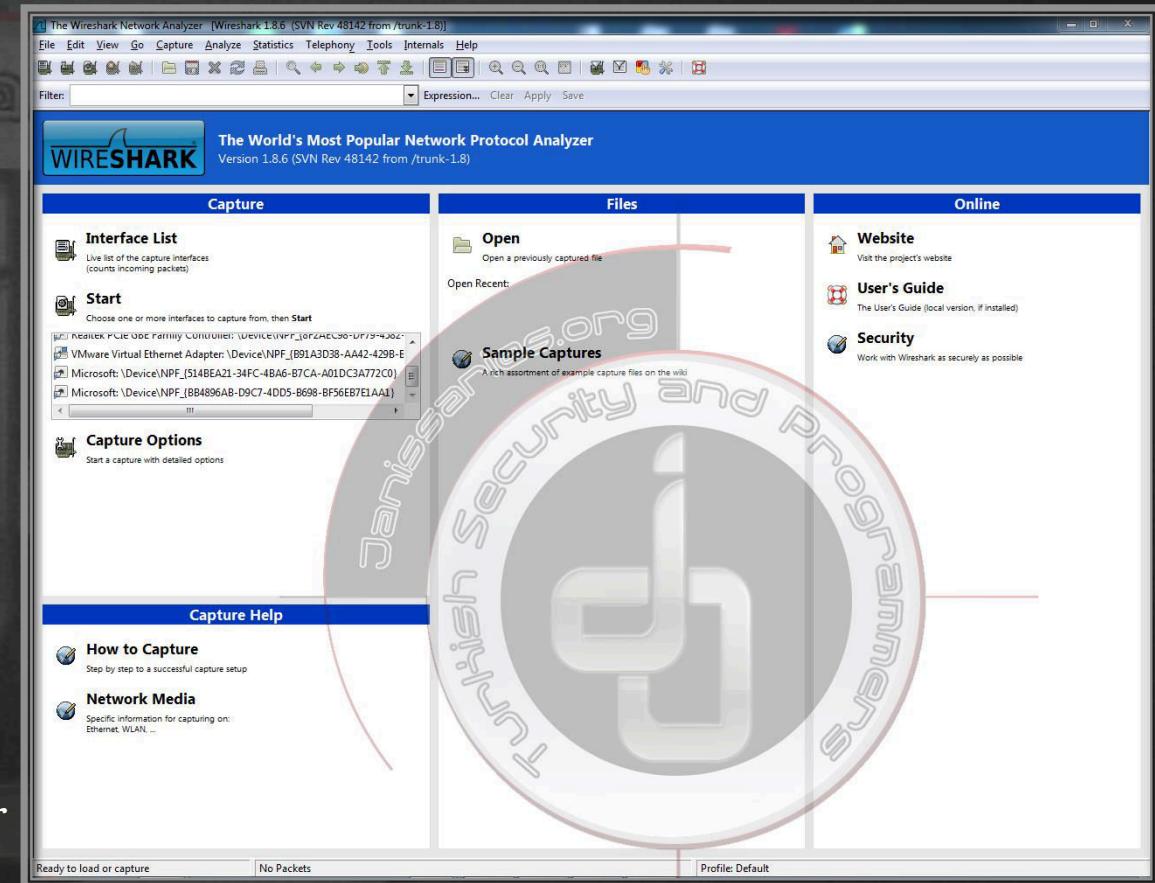
Uygulama başlatıldığında yandakine benzer bir ekran açılacaktır.

Burada Start bölümünün altında bilgisayarda algılanan Ethernet kartları listelenecektir.

Bu kartlardan biri seçilir ve ardından Start butonuna tıklanırsa uygulama ilgili Ethernet kartının network trafigini 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 |
|-----|-----------------|-------------------|----------------|----------|--------|---|
| 70 | 10.902537000 | 192.168.1.105 | 188.132.129.16 | TCP | 66 | gadgetgate1way > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 71 | 10.928392000 | 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 | 10.928641000 | 192.168.1.105 | 188.132.129.16 | TCP | 54 | gadgetgate1way > ftp [ACK] Seq=1 Ack=1 Win=17424 Len=0 |
| 73 | 11.11.179365000 | 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 | 11.179646000 | 192.168.1.105 | 188.132.129.16 | FTP | 67 | Request: USER gvarol |
| 75 | 11.205669000 | Apple_a8:e2:89 | Broadcast | ARP | 60 | who has 192.168.1.3? Tell 192.168.1.145 |
| 76 | 11.308065000 | VMware_c6:22:6f | Broadcast | ARP | 60 | who has 192.168.1.57? Tell 192.168.1.235 |
| 77 | 11.319615000 | 188.132.129.16 | 192.168.1.105 | TCP | 60 | ftp > gadgetgate1way [ACK] Seq=73 Ack=14 Win=6144 Len=0 |
| 78 | 11.319720000 | 188.132.129.16 | 192.168.1.105 | FTP | 88 | Response: 331 Password required for gvarol |
| 79 | 11.319929000 | 192.168.1.105 | 188.132.129.16 | FTP | 73 | Request: PASS i 10 |
| 80 | 11.619111000 | 192.168.1.105 | 188.132.129.16 | FTP | 73 | [TCP Retransmission] Request: PASS i 10 |
| 81 | 11.758056000 | 188.132.129.16 | 192.168.1.105 | FTP | 81 | Response: 230 User gvarol Logged in |
| 82 | 11.758528000 | 192.168.1.105 | 188.132.129.16 | FTP | 60 | Request: SYST |
| 83 | 11.761408000 | GemtekTe_7a:61:6c | Broadcast | ARP | 60 | who has 192.168.1.235? Tell 192.168.1.54 |
| 84 | 11.761701000 | 188.132.129.16 | 192.168.1.105 | FTP | 81 | [TCP Retransmission] Response: 230 User gvarol Logged in |
| 85 | 11.761762000 | 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 SLE: |
| 86 | 11.761979000 | 188.132.129.16 | 192.168.1.105 | TCP | 66 | [TCP Dup ACK 84#1] ftp > gadgetgate1way [ACK] Seq=134 Ack=33 Win=6144 Len=0 SLE: |

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]
 [Destination GeoIP: Unknown]

```

0000  2c 6b f5 80 71 c0 00 1c bf be ff 9c 08 00 45 00 ,k..@... . ....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 1..
```

```

0040  ec 00 09 j...
0050  j0 45 41 5c 00 00 22 23 42 25 50 01 5e 0t 15 0t ..C...U2 EB dvarlo
0060  8t j0 09 12 00 t2 64 0t 05 6e 49 20 t8 ..C...S...eb.
0070  00 32 jc qp 40 00 80 00 46 q5 0t 0d pc 84 .2..@... .
0080  sc ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0090  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00a0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00b0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00c0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00d0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00e0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
00f0  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0100  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0110  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0120  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0130  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0140  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0150  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0160  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0170  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0180  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0190  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0200  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0210  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0220  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0230  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0240  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0250  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0260  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0270  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0280  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0290  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0300  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0310  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0320  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0330  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0340  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0350  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0360  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0370  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0380  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0390  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0400  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0410  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0420  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0430  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0440  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0450  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0460  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0470  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0480  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0490  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0500  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0510  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0520  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0530  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0540  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0550  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0560  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0570  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0580  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0590  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0600  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0610  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0620  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0630  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0640  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0650  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0660  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0670  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0680  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0690  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0700  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0710  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0720  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0730  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0740  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0750  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0760  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0770  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0780  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0790  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0800  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0810  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0820  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0830  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0840  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0850  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0860  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0870  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0880  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0890  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0900  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0910  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0920  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0930  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0940  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0950  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0960  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0970  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0980  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
0990  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1000  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1010  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1020  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1030  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1040  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1050  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1060  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1070  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1080  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1090  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1100  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1110  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1120  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1130  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1140  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1150  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1160  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1170  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1180  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1190  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1200  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1210  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1220  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1230  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1240  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1250  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1260  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1270  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1280  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1290  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1300  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1310  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1320  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1330  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1340  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1350  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1360  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1370  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1380  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1390  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1400  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1410  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1420  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1430  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1440  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1450  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1460  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1470  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1480  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1490  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1500  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1510  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1520  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1530  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1540  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1550  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1560  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1570  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1580  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1590  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1600  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1610  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1620  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1630  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1640  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1650  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1660  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1670  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1680  5c ep 42 80 t2 c0 00 jc sd fd 44 0c 08 00 42 00 .2..@... .
1690  5c ep 42 80 t2 c0 00 jc sd
```

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 arasında 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 madenciliği

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

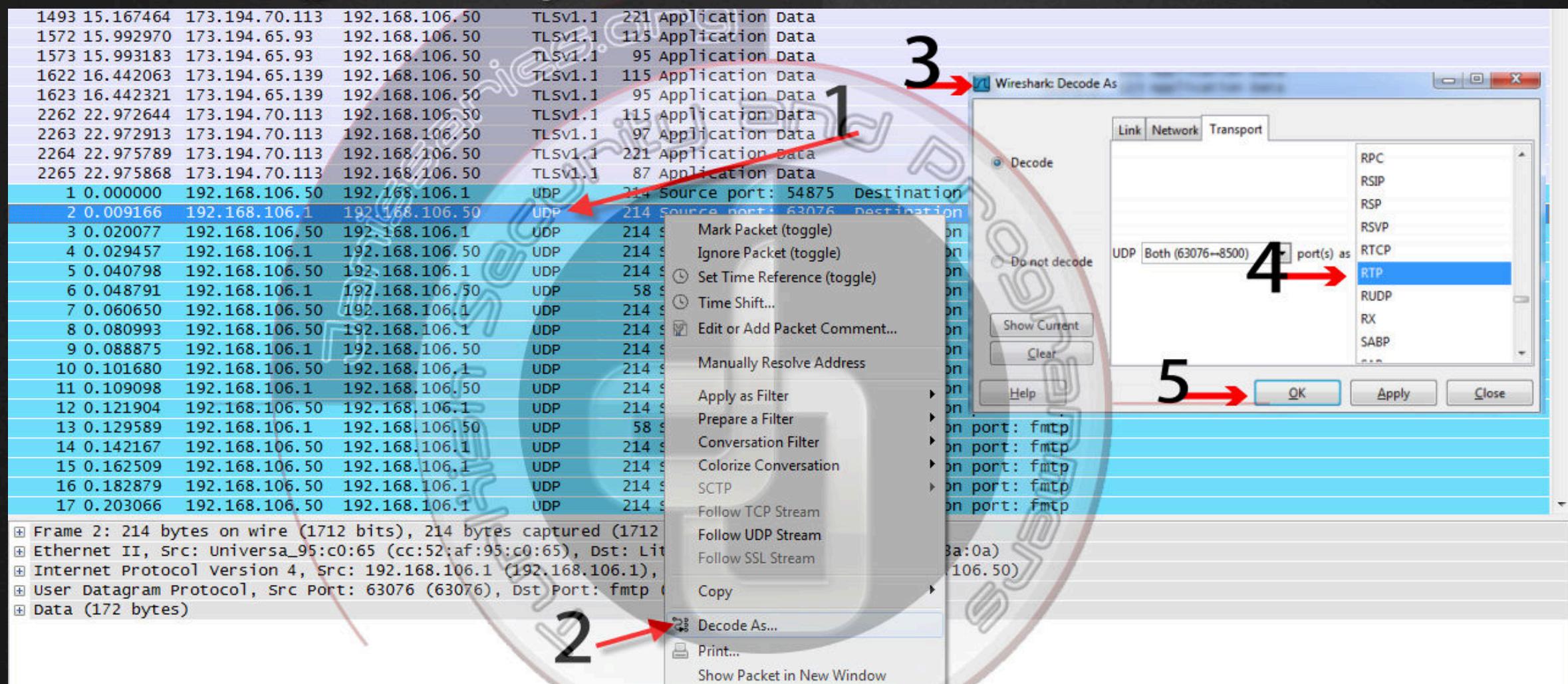
Yan tarafta gördüğünüz daha önce kaydedilmiş bir proje diyelim biz buna şimdilik bu proje içerisinde bir ses işlemi var Biz bunu nasıl ortaya çıkartıp dinleyebiliriz ?

Cevap :

Şimdi yan taraftaki resme bakarsanız protokol bölümünde TCP – UDP – SSDP – HHTP gibi protokoller mevcut bu nü dinleyememiz için bir Dönüşürme 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 >>>>>

| No. | Time | Source | Destination | Protocol | 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: ftmp |
| 2 | 0.009166 | 192.168.106.1 | 192.168.106.50 | UDP | 214 | Source port: 63076 Destination port: ftmp |
| 3 | 0.020077 | 192.168.106.50 | 192.168.106.1 | UDP | 214 | Source port: 54875 Destination port: ftmp |
| 4 | 0.029457 | 192.168.106.1 | 192.168.106.50 | UDP | 214 | Source port: 63076 Destination port: ftmp |
| 5 | 0.040798 | 192.168.106.50 | 192.168.106.1 | UDP | 214 | Source port: 54875 Destination port: ftmp |
| 6 | 0.048791 | 192.168.106.1 | 192.168.106.50 | UDP | 58 | Source port: 63076 Destination port: ftmp |
| 7 | 0.060650 | 192.168.106.50 | 192.168.106.1 | UDP | 214 | Source port: 54875 Destination port: ftmp |
| 8 | 0.080993 | 192.168.106.50 | 192.168.106.1 | UDP | 214 | Source port: 54875 Destination port: ftmp |
| 9 | 0.088875 | 192.168.106.1 | 192.168.106.50 | UDP | 214 | Source port: 63076 Destination port: ftmp |
| 10 | 0.101680 | 192.168.106.50 | 192.168.106.1 | UDP | 214 | Source port: 54875 Destination port: ftmp |



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 dönüşecktir 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
işlemi Göstermiş
olduk bu dosyayı ek
olarak sizlere
vereceğim üzerinde
çalışıp göz
gezdirerek hiç
yoktan deneme
yanılma işlemleri
yaparak ta
öğrenebilirsiniz

Wireshark: RTP Stream Analysis

Forward Direction Reversed Direction

Analysing stream from 192.168.106.50 port 54875 to 192.168.106.1 port 8500 SSRC = 0x5F78

| Packet | Sequence | Delta(ms) | Filtered Jitter(ms) | Skew(ms) | IP BW(kbps) | Marker | Status |
|--------|----------|-----------|---------------------|----------|-------------|--------|--------|
| 1 | 14216 | 0,00 | 0,00 | 0,00 | 1,60 | | [Ok] |
| 3 | 14217 | 20,08 | 0,00 | -0,08 | 3,20 | | [Ok] |
| 5 | 14218 | 20,72 | 0,05 | -0,80 | 4,80 | | [Ok] |
| 7 | 14219 | 19,85 | 0,06 | -0,65 | 6,40 | | [Ok] |
| 8 | 14220 | 20,34 | 0,07 | -0,99 | 8,00 | | [Ok] |
| 10 | 14221 | 20,69 | 0,11 | -1,68 | 9,60 | | [Ok] |
| 12 | 14222 | 20,22 | 0,12 | -1,90 | 11,20 | | [Ok] |
| 14 | 14223 | 20,26 | 0,13 | -2,17 | 12,80 | | [Ok] |

Max delta = 28,94 ms at packet no. 2184
 Max jitter = 2,06 ms. Mean jitter = 0,81 ms.
 Max skew = -11,69 ms.
 Total RTP packets = 1342 (expected 1342) Lost RTP packets = 0 (0,00%) Sequence errors = 0
 Duration 26,82 s (-1 ms clock drift, corresponding to 8000 Hz (-0,00%))

Save payload... Save as CSV... Refresh Jump to Graph Player Next non-Ok Close

test.pcap - VoIP - RTP Player

From 192.168.106.50:54875 to 192.168.106.1:8500 Duration:26,84 Drop by Jitter Buff:0(0,0%) Out of Seq: 0(0,0%) Wrong Timestamp:
 View as time of day

Jitter buffer [ms] 50 Use RTP timestamp

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>