ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/internet-ve-yerel-ag-sizma-testleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/%C4%B0nternet%20ve%20Yerel%20A%C4%9F%20S%C4%B1zma%20Testleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

iodine ile DNS Tünelleme
iodine adlı tool kullanılarak DNS protokolü üzerinden internet erişiminin engellendiği bir yerel ağda engellerin aşılıp internete çıkılabilmektedir. Böylece ilgili ağda bulunan bilgilerin dışarıya çıkartılması mümkün hale gelmektedir. Bu tool Kali'de yüklü olarak gelmektedir. Ubuntu'da ise aşağıdaki şekilde yüklenebilir:

> sudo apt-get install iodine

Benim NOT: Kullanımı hakkında bazı bilgiler verilmiş, ama somutlaşmadığından buraya not alınmamıştır.

(Page 3)

2)

Cain & Abel Kullanarak ARP Cache Poisoning Saldırısı // Denendi, Başarılı Olundu.

Gereksinimler

~/Downloads/Windows 7 Professional SP1 x64 - Cain _ Abel Materyaller.zip

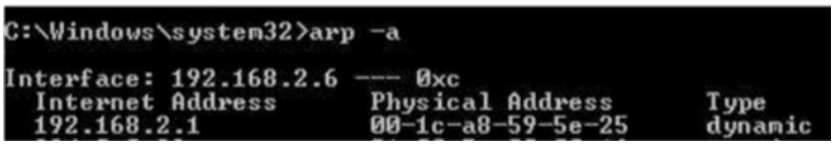
Zip İçeriği:

- Windows 7 Professional SP1 ISO
- Cain and Abel exe

Local ağda bulunan bir bilgisayarın ağ trafiğini dinleyebilmek için Cain & Abel yazılımı ile ARP Cache Poisoning yöntemini kullanalım. Diyelim ki IP adresleri şöyle olsun:

Gateway : 192.168.2.1
Saldırgan: 192.168.2.2
Kurban : 192.168.2.6

Saldırı öncesi kurbanın ARP tablosuna bir göz atalım. Zira ARP Cache Poisoning saldırısı ile kurbanın ARP tablosunu değiştireceğimiz için farkı gözümüzle görebilelim:



(Resim Temsili)

Görüldüğü üzere kurban gateway'i (192.168.2.1'i) 00-1c-a8-59-5e-25 olarak görüyor. Şimdi saldırıya başlayalım.

Öncelikle Cain and Abel programının düzgün çalışabilmesi için şu gereksinimlerin karşılanması gerekiyor:

Cain and Abel programı çalışmak için şu adımların uygulanmasını ister:

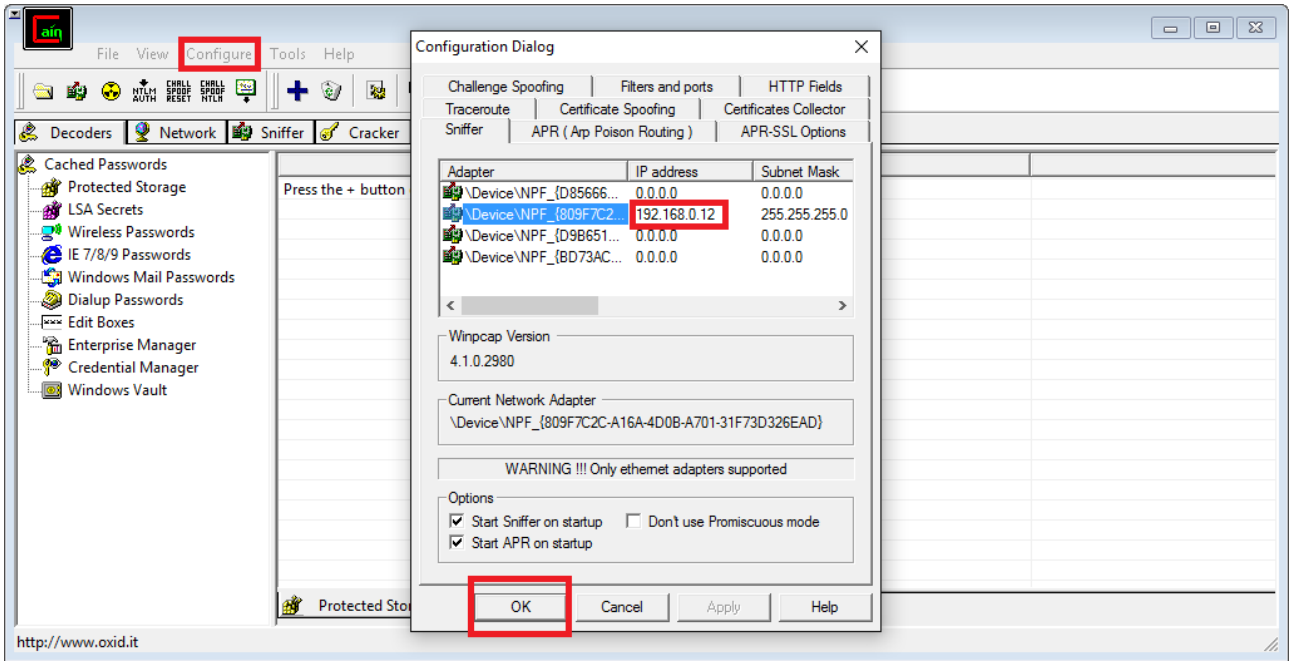
i) Windows 7 işletim sisteminde çalışmak.
ii) Windows Güvenlik Duvarını devredışı bırakmak.
iii) Gelişmiş Güvenlik ile Birlikte Windows Güvenlik Duvarı'nda Windows Güvenlik Duvarı Özellikleri'ni On'dan Off'a çevirmek.
iv) Yönetici olarak CMD çalıştırmak ve şu kuralı girmek:

```
netsh int ip set global taskoffload=disable
```

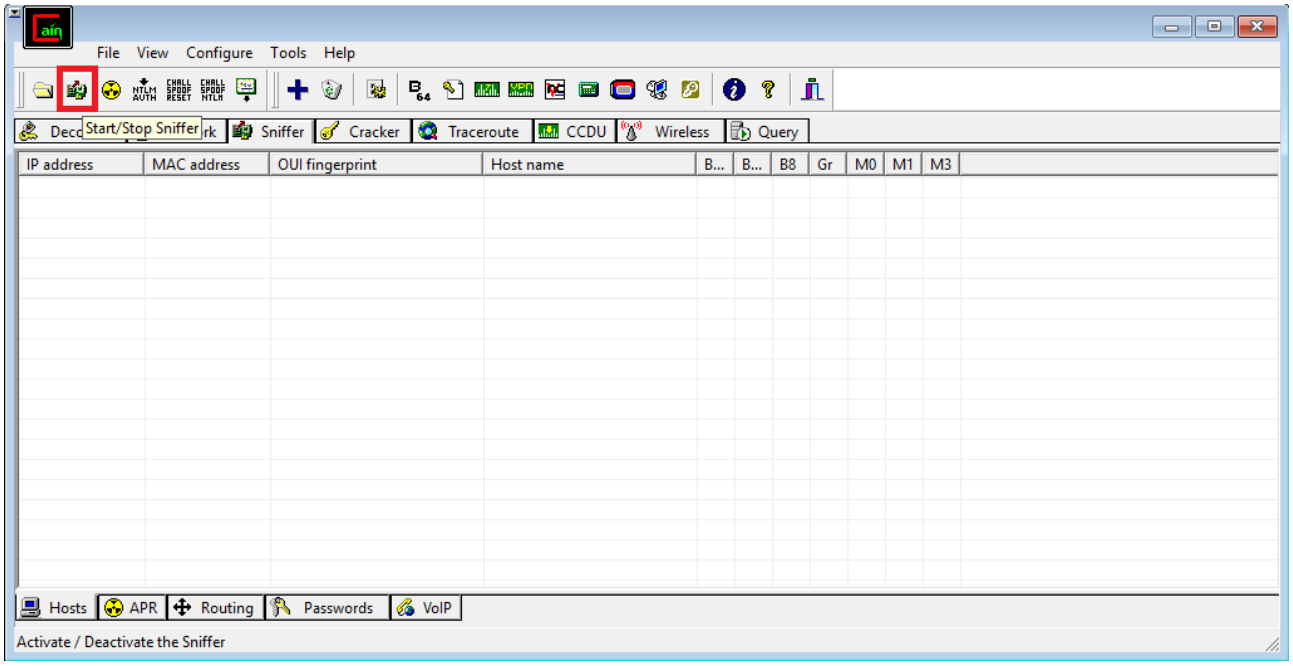
v) Kuralı girdikten sonra windows 7'de ethernet adaptörünü devre dışı bırakıp tekrar etkinleştirmek.
vi) Cain and Abel programını kapatıp yönetici olarak tekrar başlatmak.

Bu adımlar neticesinde Cain and Abel programında sıradaki saldırı adımları sorunsuzca uygulanabilir ve başarılı sonuç alınabilir.

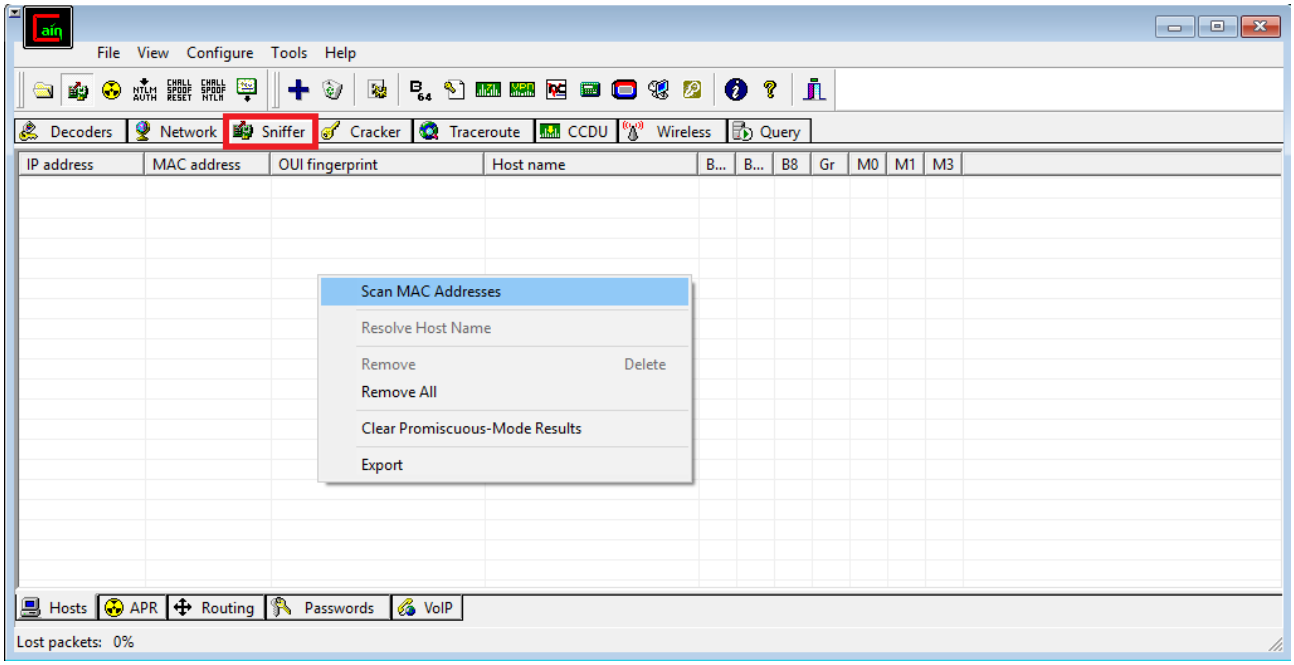
Cain & Abel programı başlatılır ve saldırı yapılacak ağ arayüzünü seçmek için menudeki Configure seçilir.



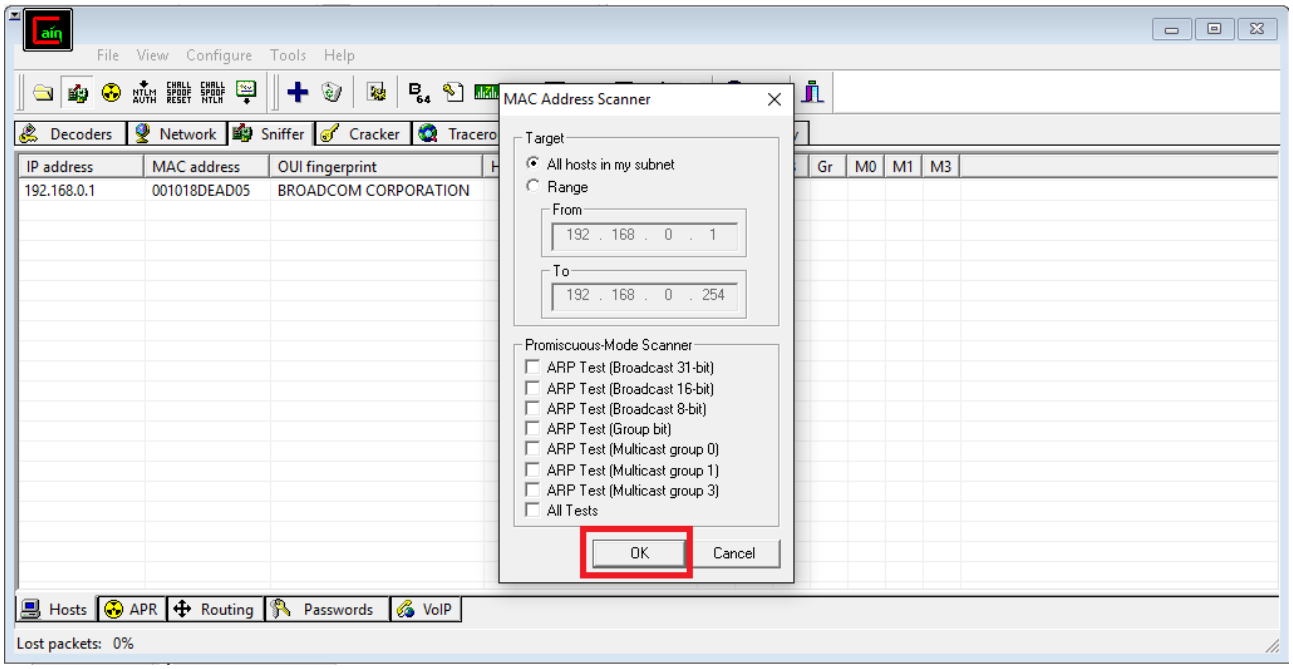
Kendi adaptörümüzü (interface'imizi) seçtikten sonra Options altındaki "Start Sniffer on startup" ve "Start APR on startup" tick'lenir, ve OK butonuna basılır. Ardından sniffer işlemi aşağıdaki belirtilen butonla enable edilir.



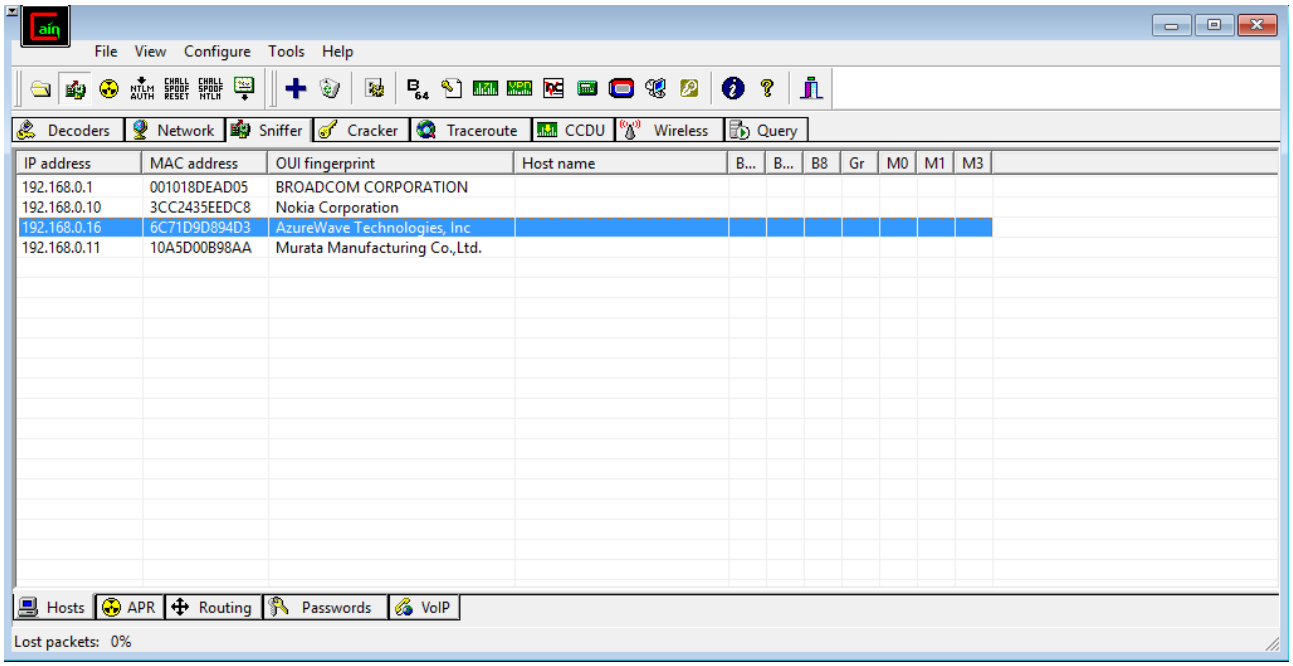
Daha sonra Sniffer sekmesine gelinir.



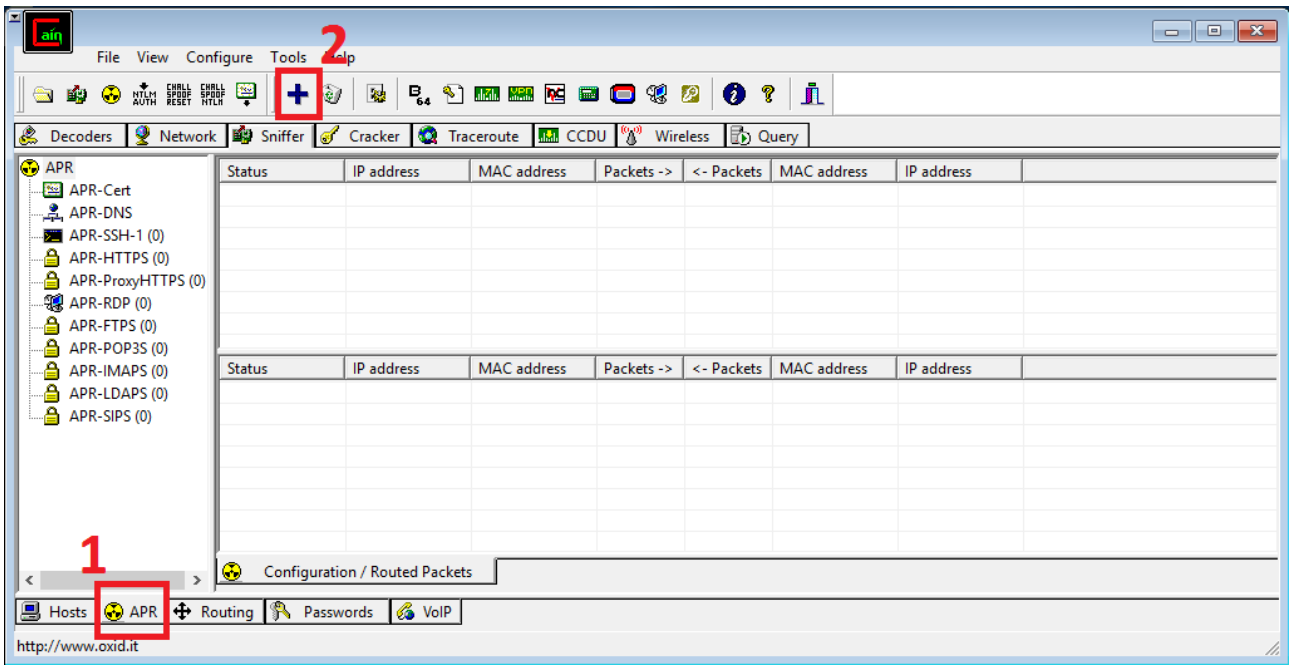
Sniffer ekranı gelince ekrana sağ tıklanır ve Scan MAC addresses seçilir. Sonra gelen ekrandaki pencereye OK denir.



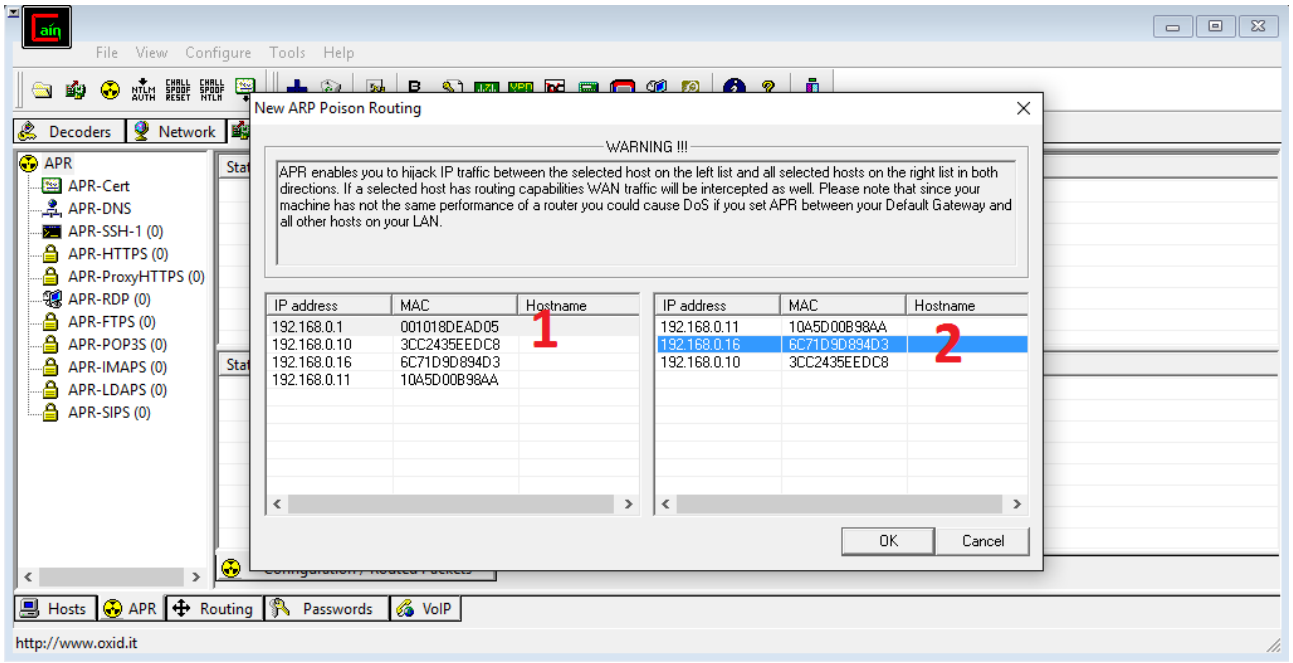
Böylece yerel ağdaki aktif bilgisayarların keşfi yapılır. Keşif işlemi bittikten sonra aşağıdaki gibi aktif cihazlar sıralanır.



Şimdi sıra geldi router'la kurban arasına girmeye. Bunun için öncelikle alt tarafta yer alan APR sekmesine tıklanılır. Sonra ekrandaki boş içerikli tabloya birkez tıklanılır ve böylece + butonu tıklanabilir olacağından +'ya basılır.



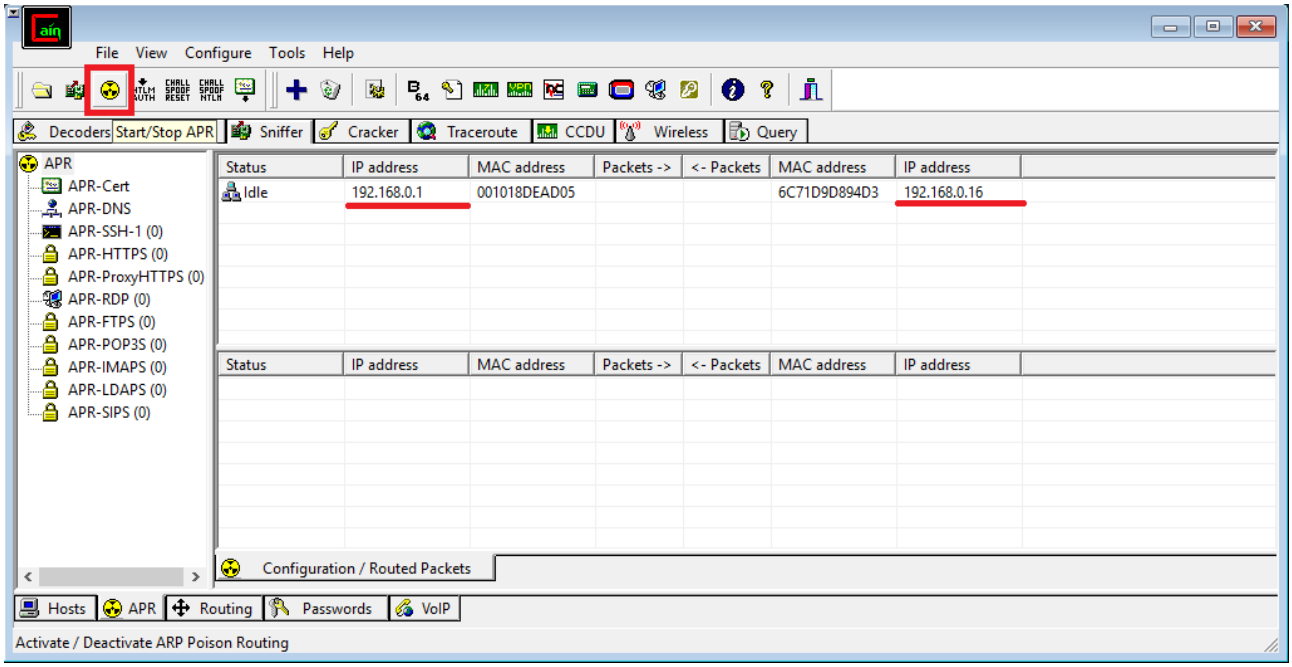
Bu tıklamalar sonucu ekrana gelen iki textarea'dan birinde gateway seçilir, diğerinde ise kurban seçilir.



NOT: Yukarıdaki ekran ilk göründüğünde sağ taraftaki textarea boş içerikle gelecektir. Ne zaman sol taraftaki textarea'dan bir hedef seçersen o zaman sağ taraftaki textarea doluverecektir.

Hedefler seçildikten sonra OK butonuna basılır ve Nükleer alarma benzeyen simgeye tıklanır.

NOT: En baştaki Configure aşamasında ayarda "başlangıçta otomatik sniff'le" dediğimiz için bu aşamada birkaç saniye içerisinde sniffing işlemi nükleer butona basmadan kendiliğinden başlayabilir ve "Idle" status'ündeki işlem "Sniffing" status'üne geçebilir.

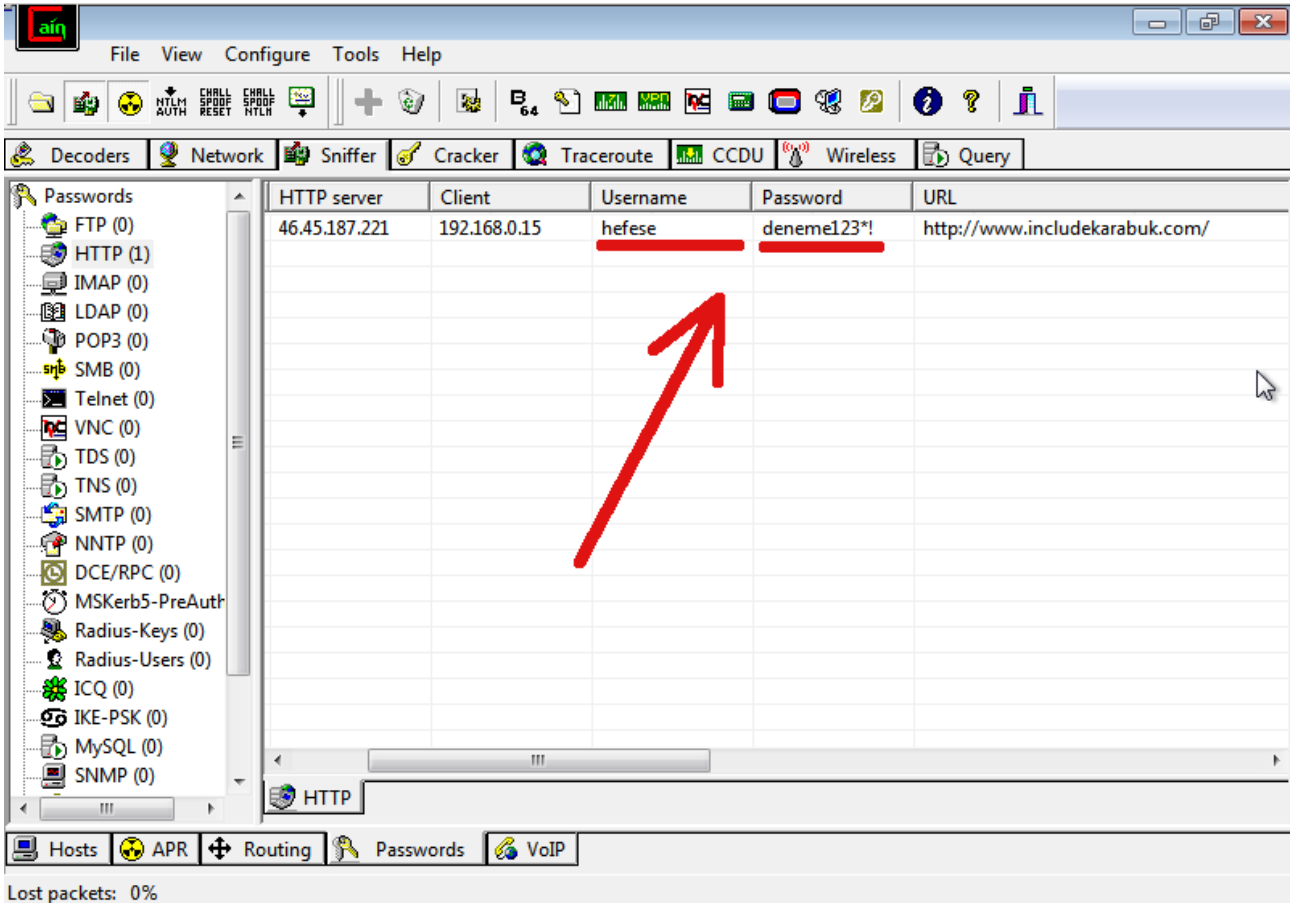


Böylece zehirleme işlemi başlar. Zehirleme işlemi ile önce kurbanın makinasına gateway olarak saldırganın MAC'i yollanır. Bunu kurbanın ARP tablosuna tekrar bakarak görebiliriz.

(Resim Temsili)

Görüldüğü üzere kurbanın ARP tablosunda 192.168.2.1 IP adresli gateway önceden 00-1c-a8-59-5e-25 adresine sahipken şimdi 00-1a-73-fb-09-8a adresine sahiptir. Yani MAC adresi olarak kurbanın tablosuna gateway diye saldırganın makinası yerleşmiştir. Bu manipulasyon gateway'in ARP tablosunda da gerçekleştirilir ve gateway'e kurban diye saldırganın MAC'i yollanır. Böylelikle kurban paketlerini gateway'e yolluyorum diye saldırgana yollayacaktır ve saldırgan da bu paketleri gateway'e forward edecektir. Aynı zamanda gateway dışarıdan gelen paketleri kurbana yolluyorum diye saldırgana yollayacaktır ve saldırgan da bu paketleri kurbana forward edecektir. Yani kurbanın trafiği ortada yer alan saldırganın üzerinden kusursuzca geçecek ve internet erişimi forward'lar sayesinde sekteye uğramayacaktır.

Cain & Abel uygulamasında bu zehirleme işlemi sonrası yapılan dinlemelerde sniff'lenenler FTP, SMTP, HTTP, …. şeklinde parse edilerek sınıflandırılacaklardır. Bu sınıflandırmaları ve sniff'lenenleri görmek için programın alt sekmelerindeki Passwords'e tıklanılır.



Yukarıda sniff'lenen bir HTTP hesabını görmektesiniz.

(Page 5-8)

3)

DHCP Spoofing ve DHCP Resource Starvation Denemeleri
Amacımız yerel ağda bulunan bir DHCP sunucusunun dağıtacağı IP havuzunu tüketmek ve böylece DHCP sunucusunu IP isteklerine cevap veremez hale getirmektir. Sonrasında ise saldırgan olarak biz bir DHCP sunucusu gibi davranarak kurbanlara IP dağıtmaya çalışacağız. Böylelikle yerel ağdaki başkalarının trafiğini üzerimizden geçirmiş olacağız. Öncelikle pig.py adlı tool'u kullanarak ağdaki DHCP sunucusunun tüm IP havuzunu tüketelim:

```
> pig.py eth0                    // pig.py tool'u Kali'de yüklü olarak gelmektedir.
```

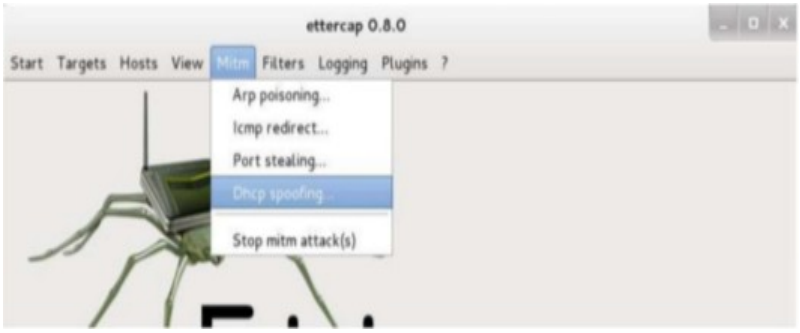
Betik yukarıdaki gibi çalıştırıldığında aşağıdaki gibi ardı ardına IP talep çıktıları üretecektir.

```
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. O an geldiğinde DHCP sunucusu gibi davranalım ve başkalarının trafiğini üzerimizden geçirelim. Bunun için ettercap'i başlatalım:

> ettercap -G

Kullanacağım ağ arayüzünü seçelim ve ardından sırayla aşağıdaki resimlerin gösterdiği işlemleri yapalım.



Bu son resim için “saldırıda kullanılacak alanlar doldurulur” denmiş. Fakat neye göre kime göre anlaşılamadı. Bu değerler rasgele mi veriliyor?

Benim NOT: PDF bu aşamada bırakmış. Tahminimce bu son resimdeki OK butonuna basarak local ağdaki istemciler IP'yi bizden almaya başlayacaklar ve biz de bir şekilde istemcilerin trafiğini dinleyebilir konuma geleceğiz. Böylece kritik bilgileri sniff'leyebileceğiz.

(Page 9-10)

4)

Wireshark Kullanımı
Eski adı Etheral olan Wireshark açık kaynak kodlu bir sniffer aracıdır. İki tür filtreye sahiptir:

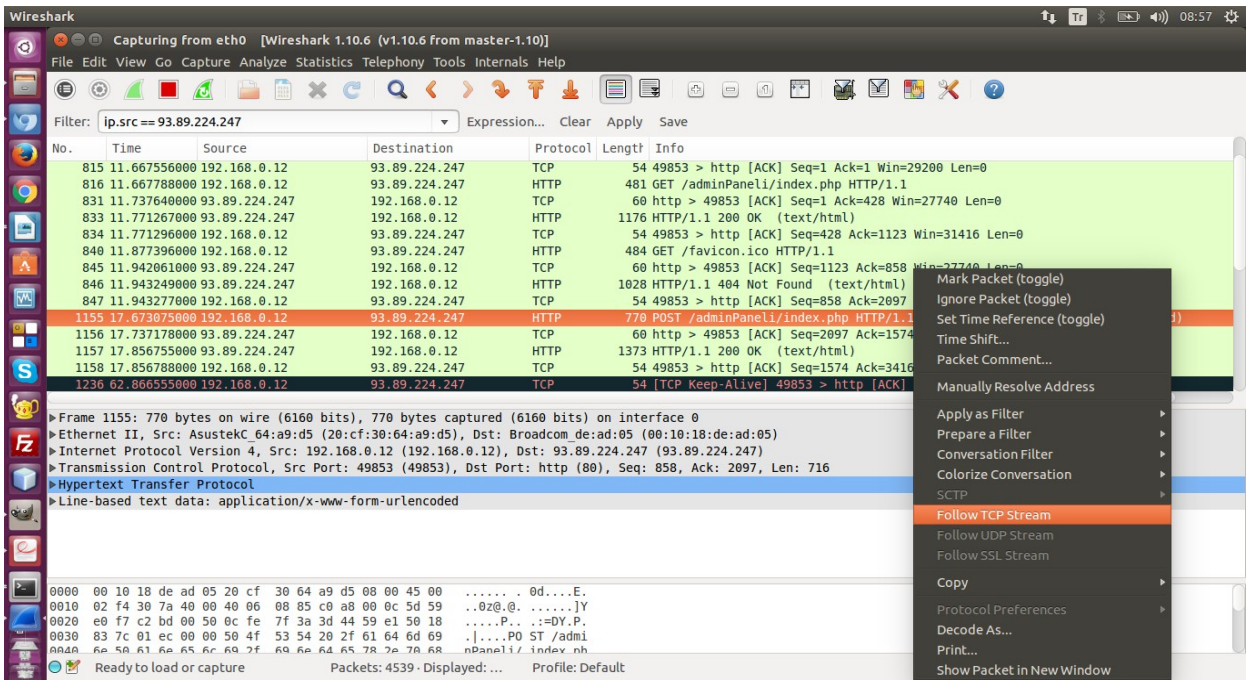
a. Capture Filter
- Yakalanacak paketleri belirli kriterlere (tipine, portuna, protokolüne) göre yakalatmaya capture filter denir.

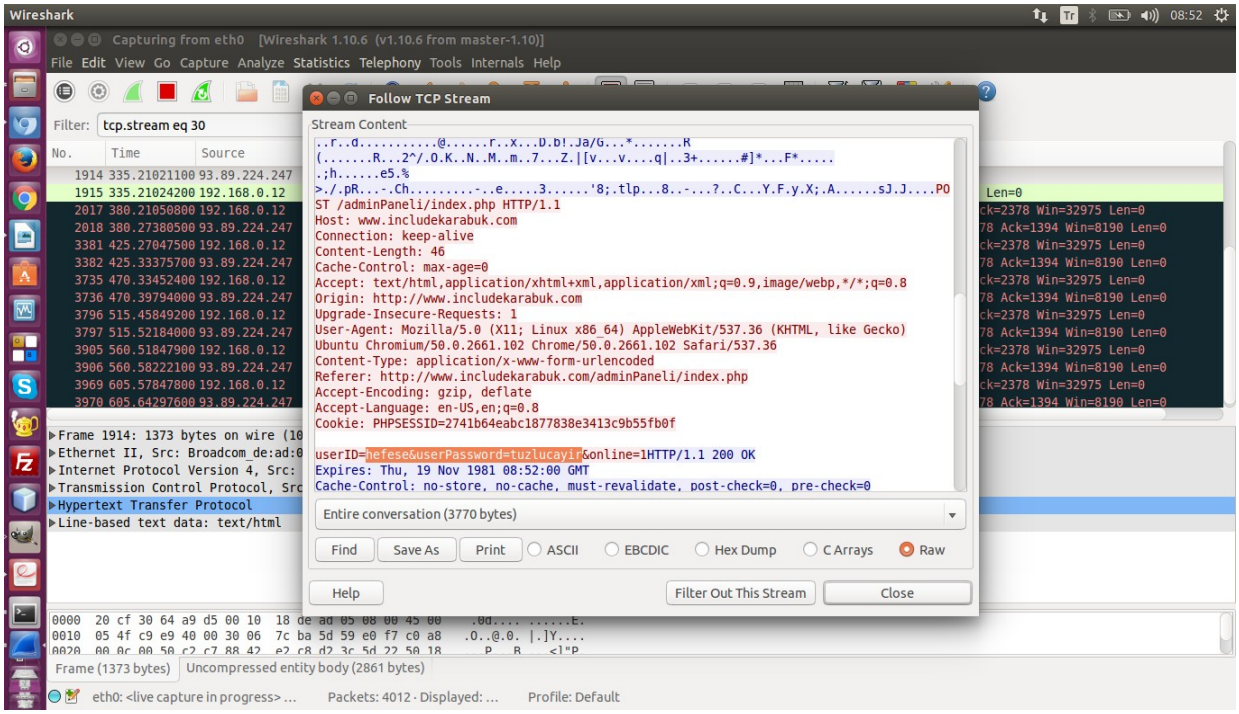
b. Display Filter
- Yakalanmış paketler içerisinde belirlenen özelliklere sahip olanları ayıklamaya da display filter denir.

Yani capture filter ile hangi paketlerin yakalanması gerektiğini Wireshark'a söylerken display filter ile yakalanmış bir yığın paket içerisinden hangisinin gösterilmesi gerektiğini belirtiyoruz.

(Page 11)
5)

Herhangi bir pakete sağ tıklayıp “Follow TCP Stream” diyerek tıklanılan paketin içeriği okunabilmektedir. Aşağıda ip.src == 93.89.224.247 filtresi kullanılarak includekarabuk'ün paketleri sıralanmıştır ve içlerinden POST yazan HTTP paketine sağ tıklayıp Follow TCP Stream denmiştir.



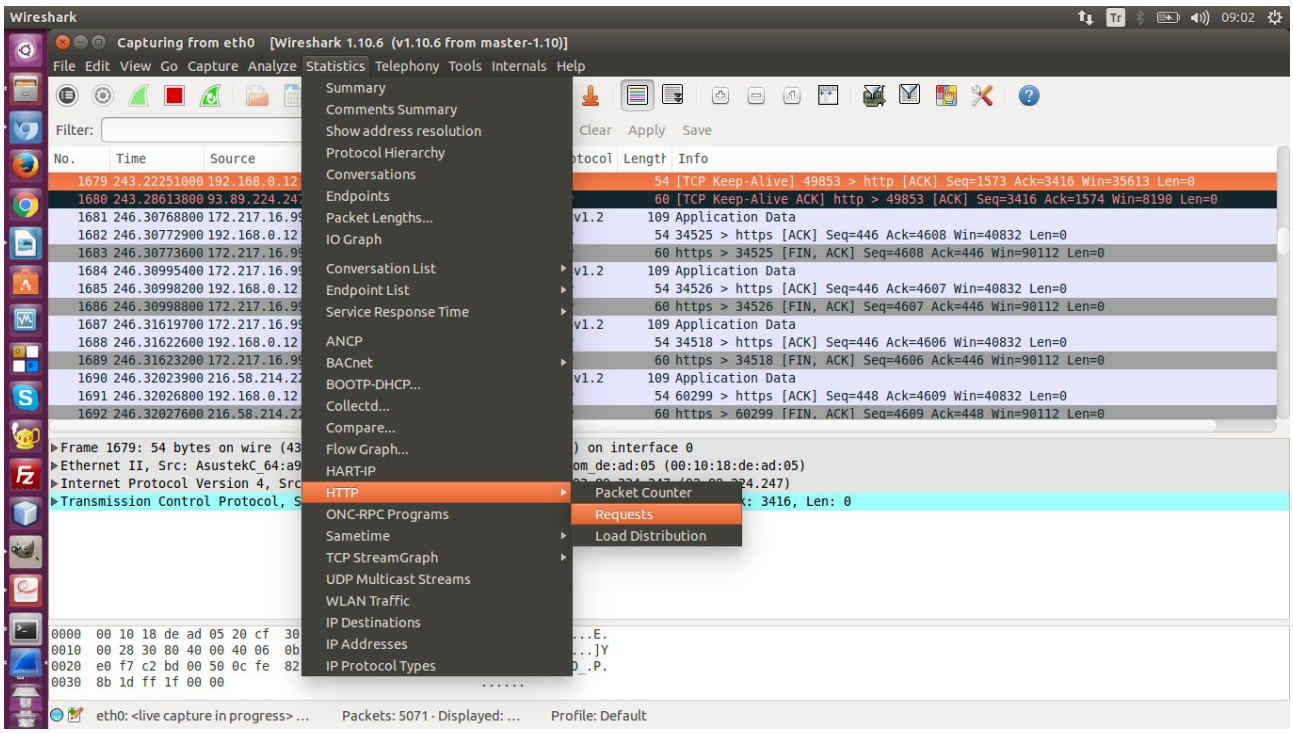


Böylece includekarabuk'ün admin panelinden POST'lanan kullanıcı adı ve şifre paket içerisi açılarak okunabilmiştir.

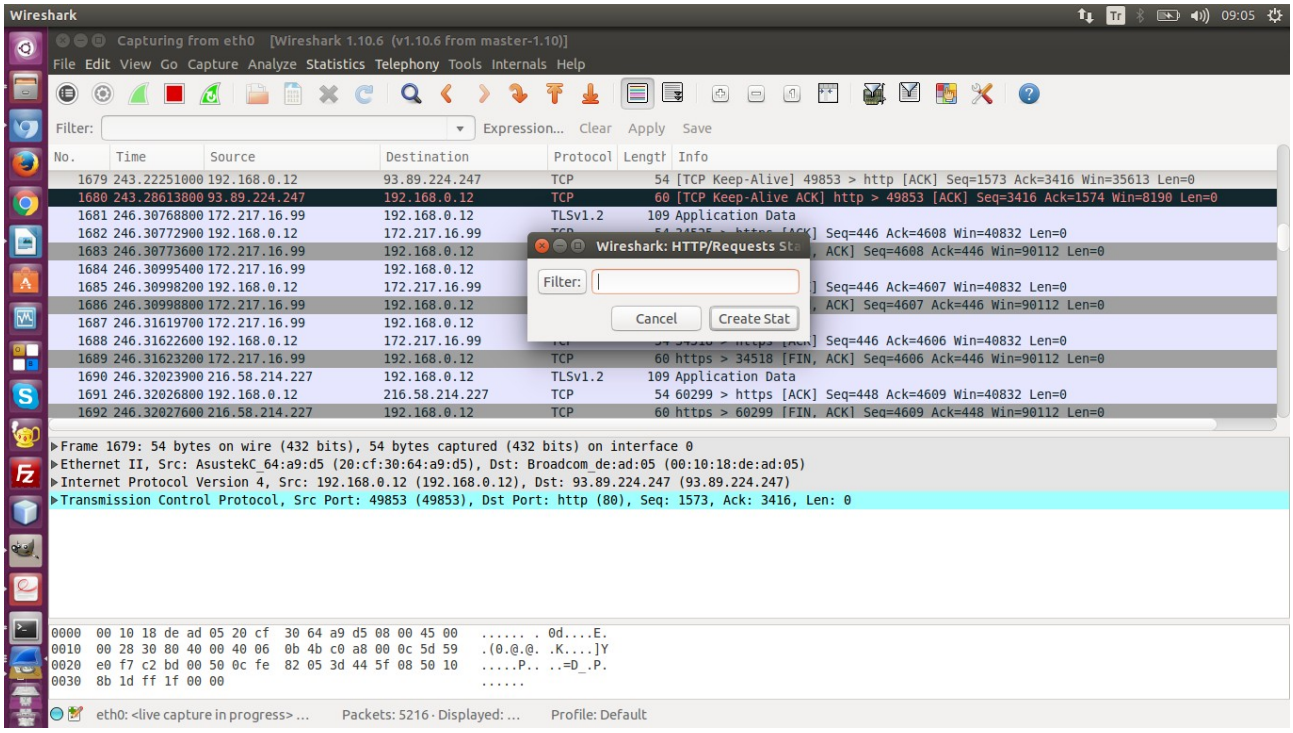
(Page 14-15)

6)

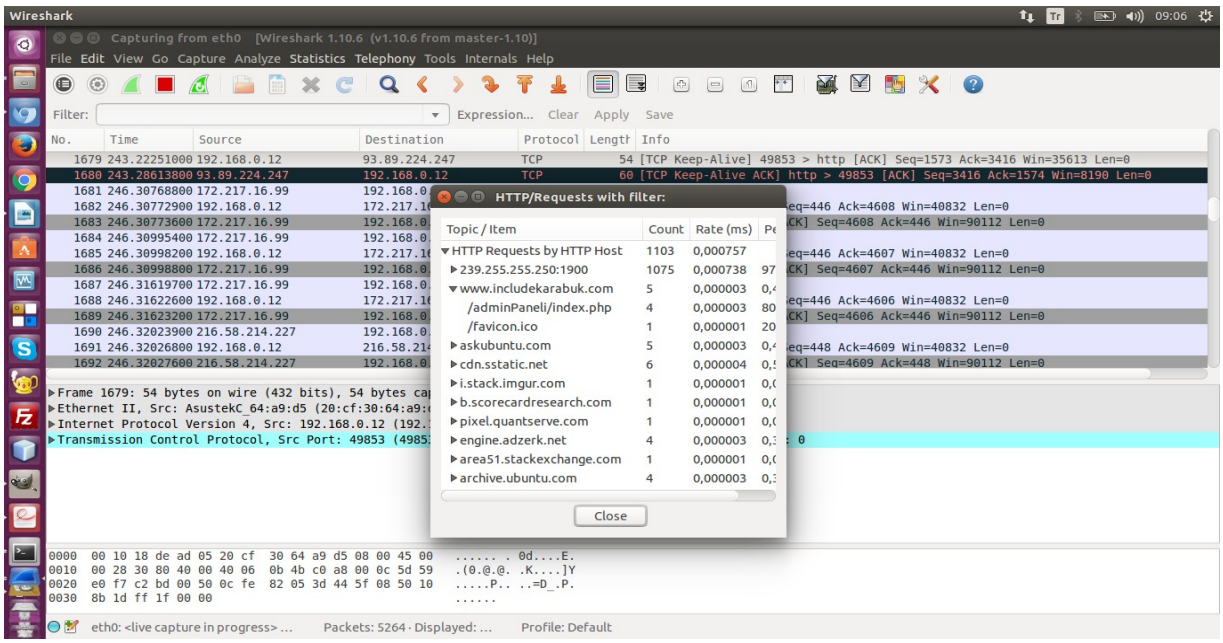
Ziyaret Edilen Web Sitelerini Listeleme ve DOS Tespiti
Wireshark'ın Statistics menüsünden dinlenen trafikten geçen ziyaret edilmiş web sitelerini dökümünü anlık etkileşimli olarak alabilirsiniz. Bu işlem için aşağıdaki seçenekleri işaretleyin.



Ve ekrana gelen filtre kutucuğunu boş geçip Ok deyin.



Böylece ekrana ziyaret edilen web siteleri gelecektir.

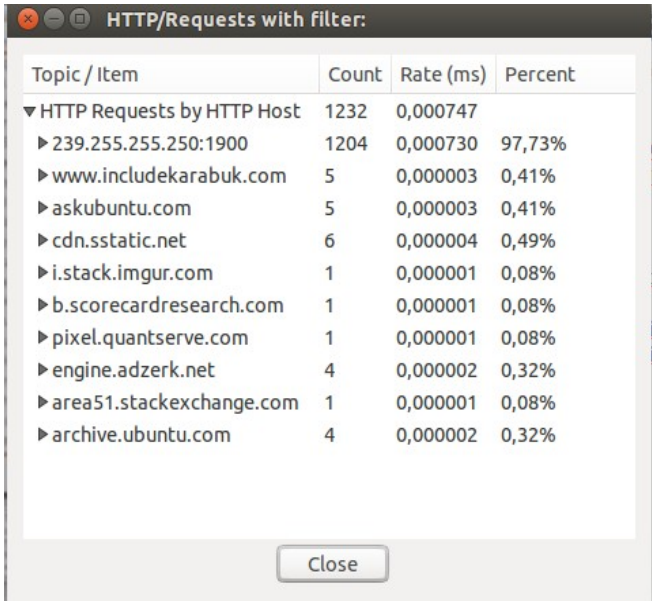


Eğer dinlenilen trafikteki sadece belirli bir istemcinin ziyaret ettiği web sitelerini görmek istersek o zaman az önce gelen filtre kutucuğuna

ip.src == istemciIP

filtresi girilerek arzulanan sonuca ulaşılabilir.

Bunların yanısıra ziyaret edilen web sitelerinin görüntülendiği ekrandan bir DOS atağı yapılıp yapılmadığı da tespit edilebilir.

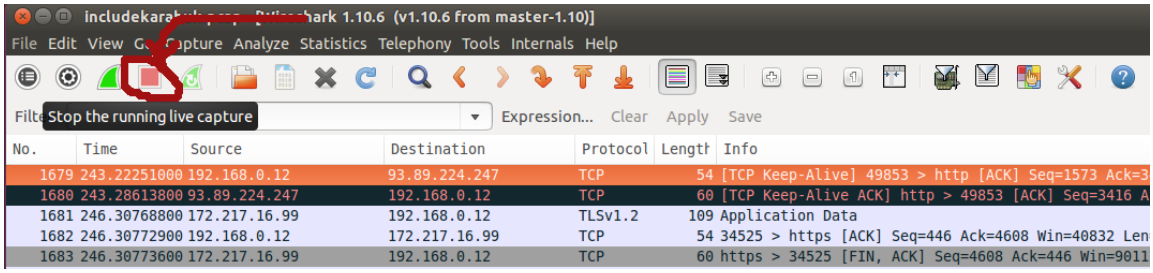


Görüldüğü üzere ziyaret edilen web siteleri yanında ziyaret edilme sayısı da yer almaktadır. Bu sayı aşırıya kaçtığı takdirde bu ekran bir DOS atağının habercisi olabilir.

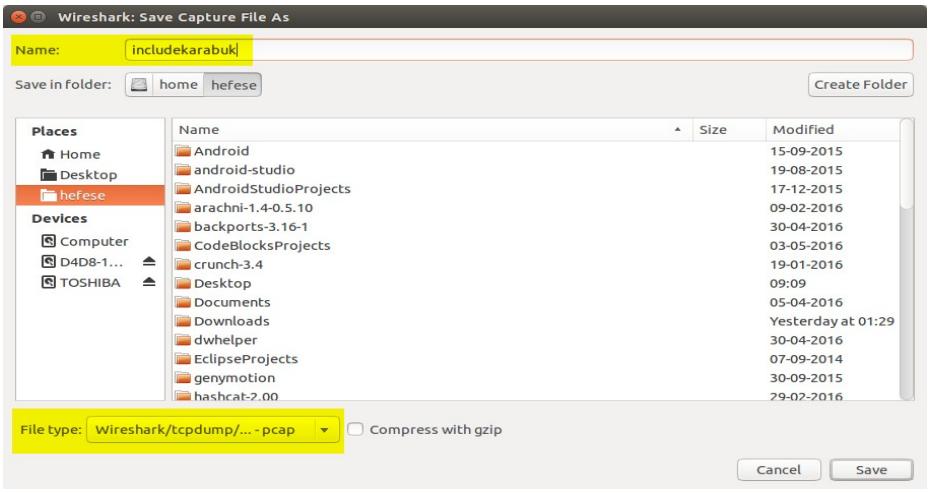
(Benim Notum)

7)

Network Miner ile Trafik Analizi // Denendi ve başarıldı.
Network Miner programı sniff'lenen trafik dosyaları içerisinde parse işlemi yaparak kritik bilgilere ulaşmamızı sağlayan bir madencilik programıdır. Şimdi az önce elle yaptığımız şifre bulma işini bu sefer Network Miner'a otomatize bir şekilde yaptıralım. Öncelikle az önce dinlenilen eth0 interface'inden elde edilen paketleri pcap uzantılı bir dosyaya toplayalım. Bunun için Wireshark'ın paket sniff akışını durdurman gerekir.



Ardından File -> Save As diyelim. Ekrana gelecek ayarlardan dosya ismi olarak herhangi bir şey, dosya uzantısı olarak ise wireshark/tcpdump/ – pcap diyelim.



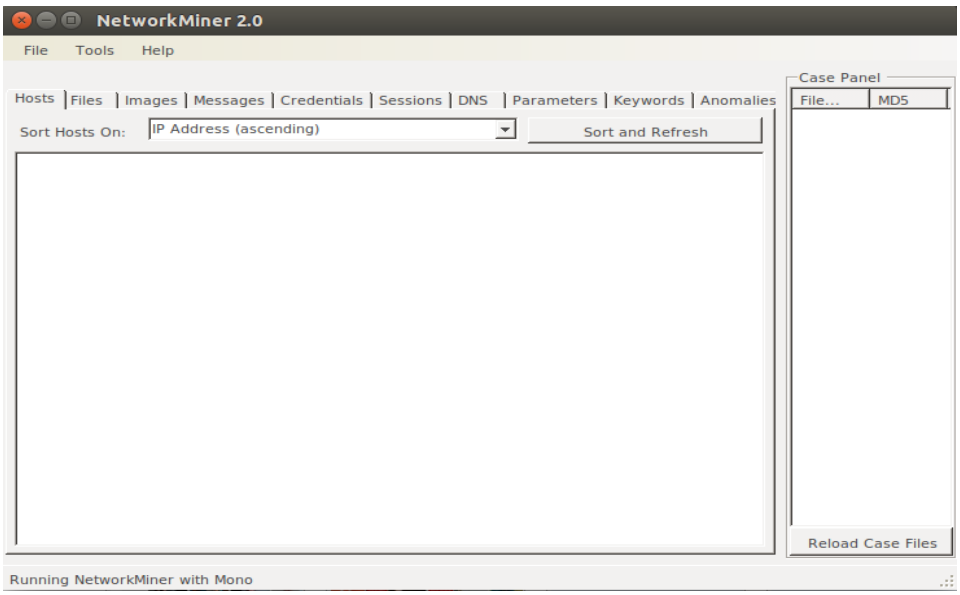
pcap dosyamızı oluşturduktan sonra Network Miner'ı Ubuntu'ya kurmak için aşağıdaki kodları sırasıyla terminale girelim.

> sudo apt-get install libmono-winforms2.0-cil
> wget www.netresec.com/?download=NetworkMiner -O /tmp/nm.zip
> sudo unzip /tmp/nm.zip -d /opt/
> cd /opt/NetworkMiner*
> sudo chmod +x NetworkMiner.exe
> sudo chmod -R go+w AssembledFiles/
> sudo chmod -R go+w Captures/
> mono NetworkMiner.exe

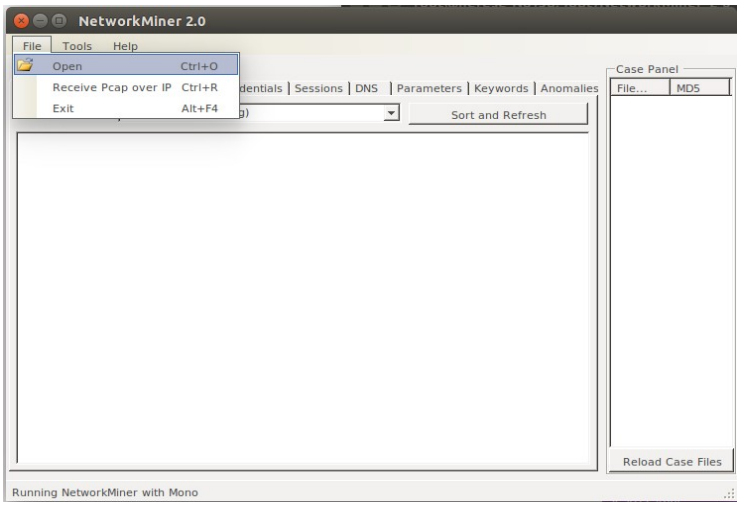
NOT: Eğer program zaten kuruluysa programı başlatmak için şu iki satırı girmen gerekir:

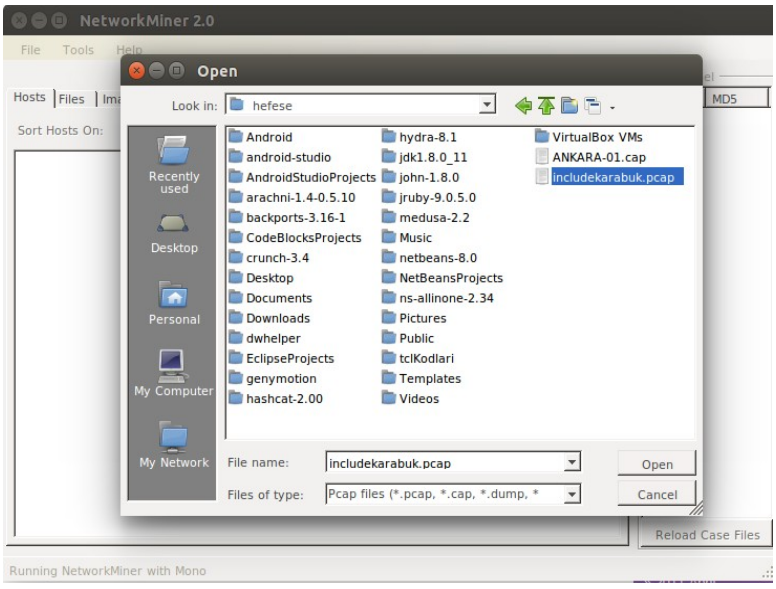
> cd /opt/NetworkMiner*
> mono NetworkMiner.exe

Son kod ile NetworkMiner programı başlayacaktır.

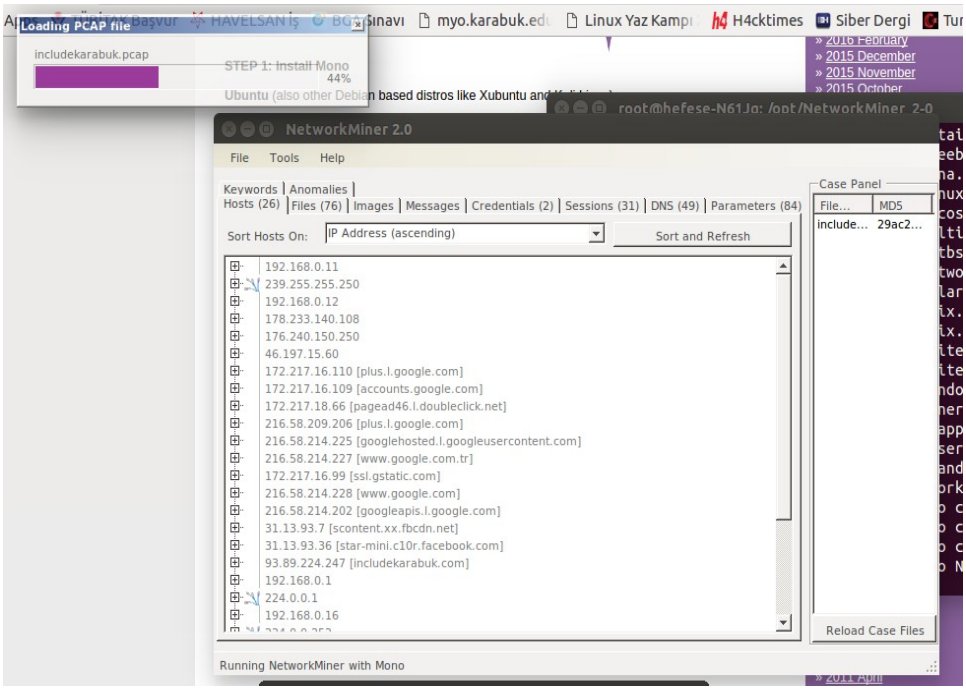


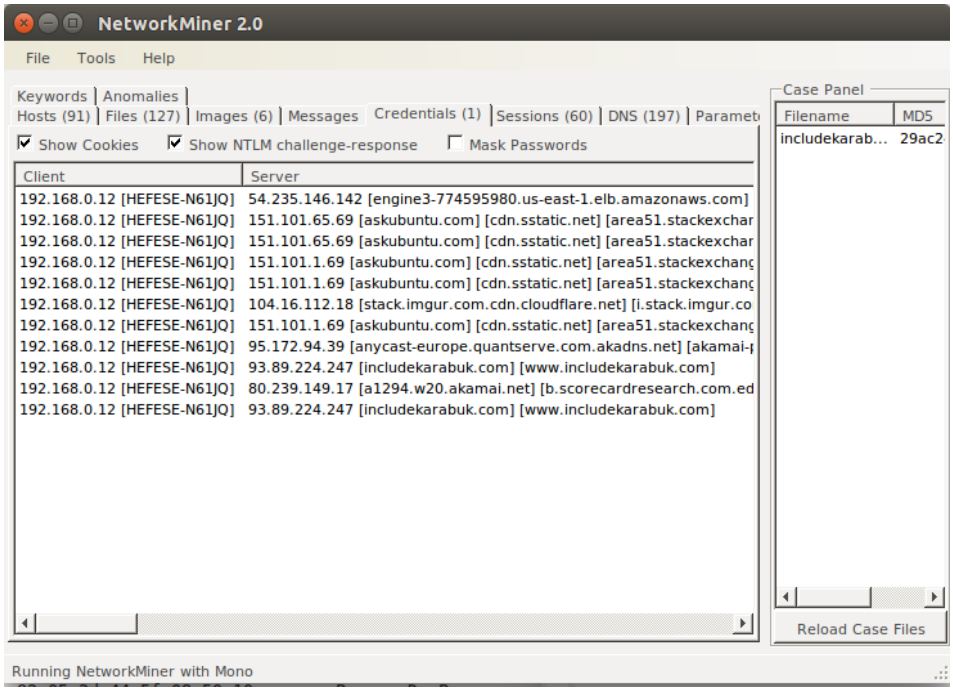
Wireshark'tan elde ettiğimiz pcap dosyasını NetworkMiner'a verelim.



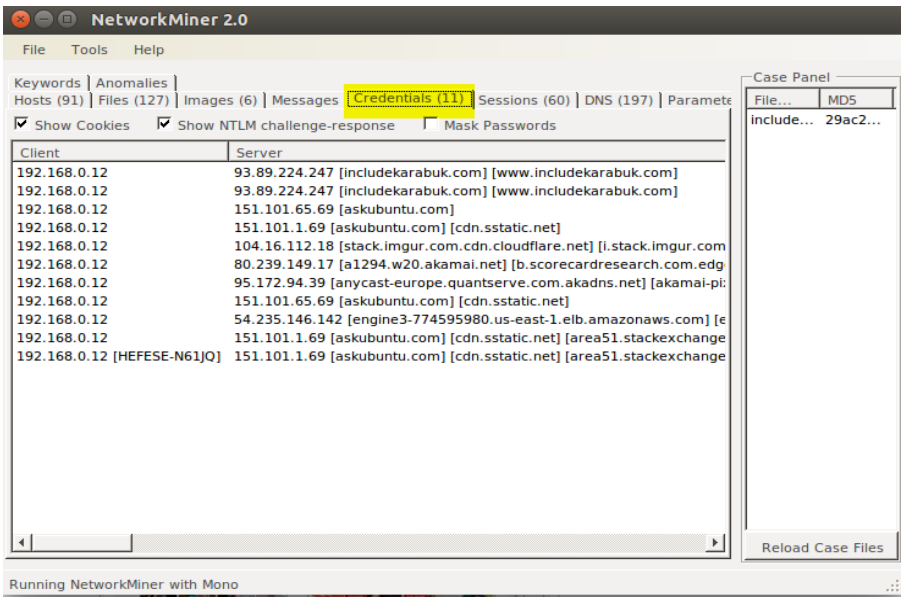


Pcap dosyası aşağıdaki gibi NetworkMiner'a yüklenecektir.

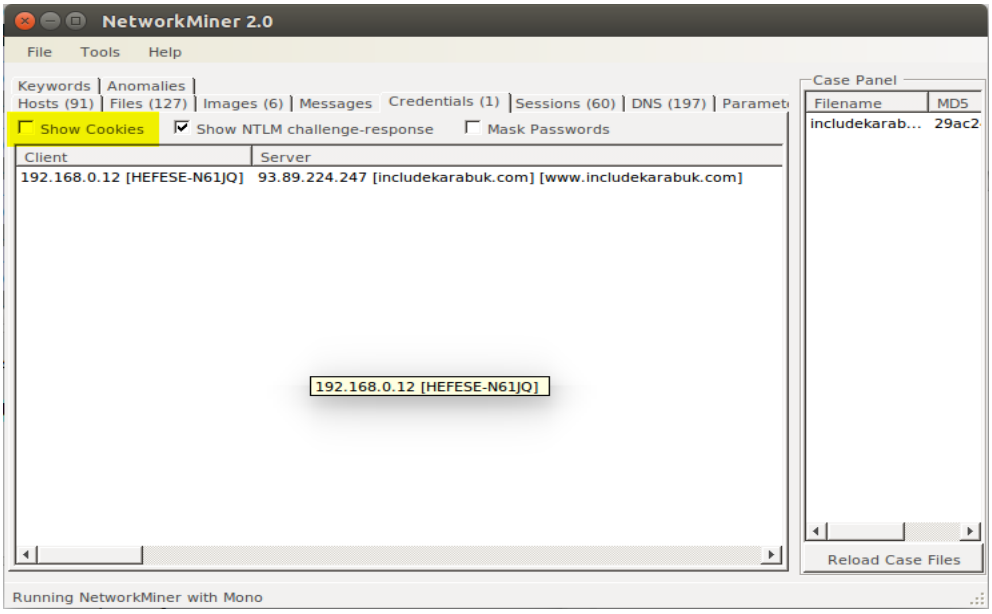




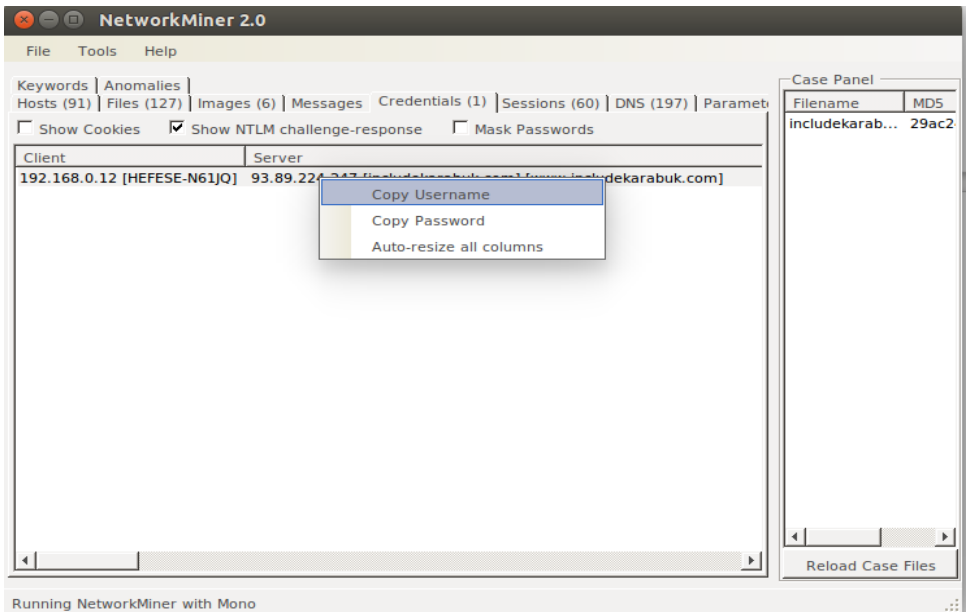
Paket yüklenmiştir ve parse işlemi de son bulmuştur. Credentials sekmesine geçildiğinde aşağıdaki ekran gelecektir.

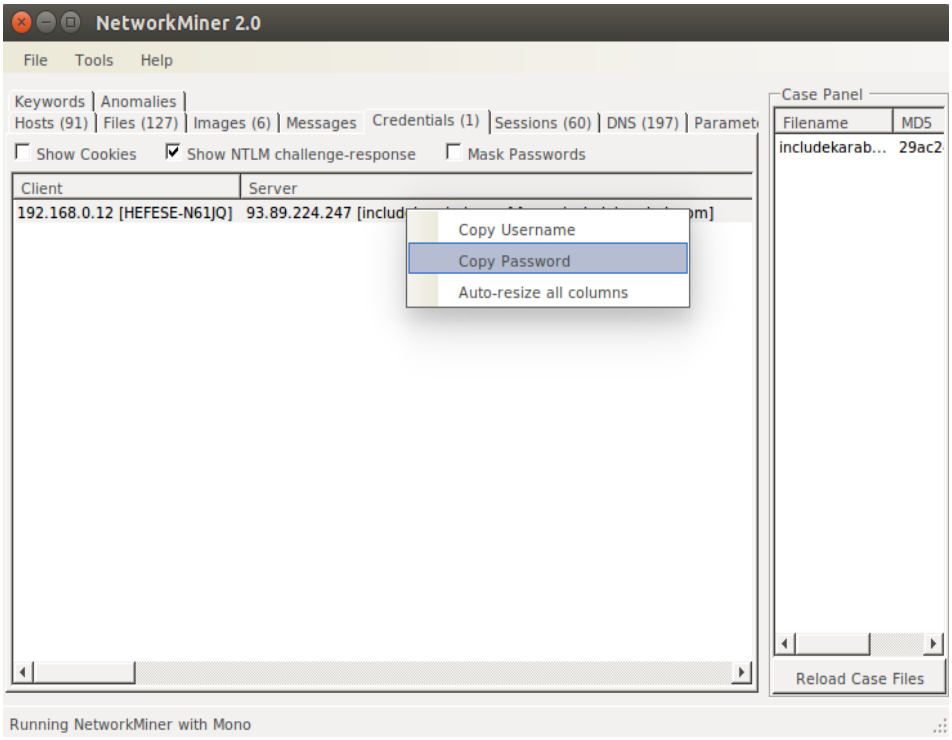


Görüldüğü üzere 11 tane credential tespit edildiği söylenmiştir. Bunlardan çoğu çerez olacağı için çerezleri ayıklayalım. Bunun için Show Cookies tick'ini kaldıralım.



Geriye bir tane credential kalmıştır. İşte o bizim includekarabuk'ün admin panelinden POST ettiğimiz kullanıcı adı ve şifreyi tutmaktadır. Kullanıcı adı ve şifreyi çekmek için sırasıyla ilgili satıra sağ tıklanır ve bir Copy username denir, bir de Copy Password denir. Böylece admin hesap bilgileri elimize geçmiş olur.





Sonuç olarak fark ettiysen Wireshark'ta kullanıcı adı ve şifreyi bulmak için onca paket yığını içerisinde boğuşuyorduk ve elimizle filtreler girerek sonuca ulaşmaya çalışıyorduk. NetworkMiner'da ise bu filtreleme işini bizim yerimize NetworkMiner yapıyor ve şıp diye trafik içerisinde bulduğu kullanıcı adı ve şifreyi önümüze sunuyor.

(Page 17-20)