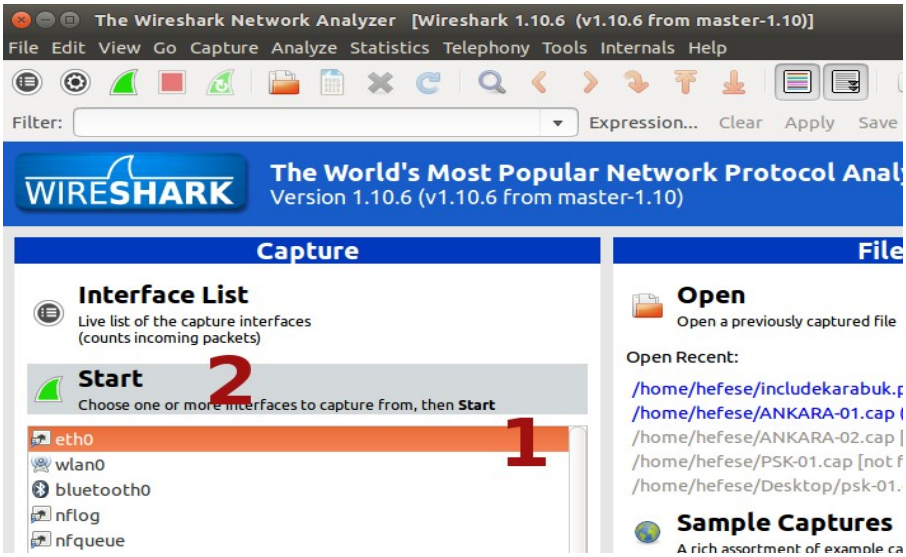
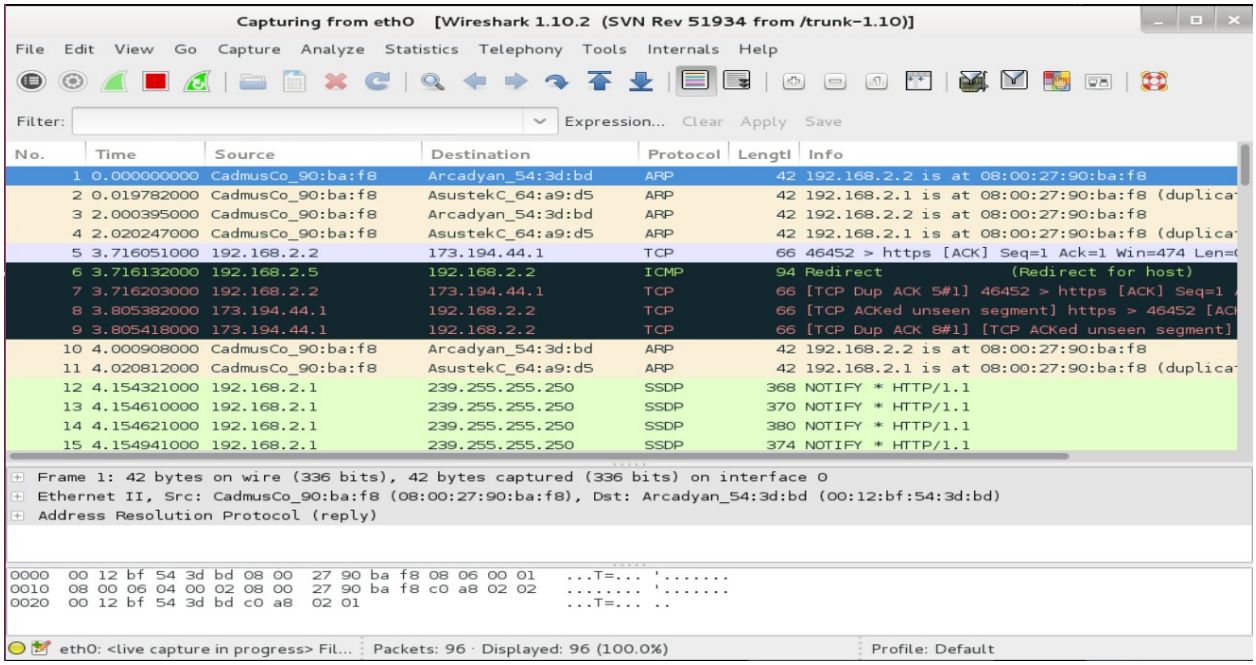
NetworkMiner ile Trafik Analizi

Wireshark'ı açtığımızı, bir interface seçtiğimizi ve Start butonuna basarak sniffing'e başladığımızı varsayalım.



Paketler ekrana akmaya başlayacaktır.



Diyelim ki includekarabuk'ün admin paneline giriyoruz.

www.includekarabuk.com/adminPaneli/index.php

Kullanıcı adı ve şifreyi girdikten sonra Wireshark'a dönelim. Girdiğimiz kullanıcı adı ve şifreyi taşıyan paketi bulmak için yapabileceğimiz en iyi şey Wireshark filtrelerini kullanmak olucaktır. Dolayısıyla includekarabuk'ün IP'si üzerinden bir paket filtreleme yapalım. Bunun için önce includekarabuk'ün IP'sini öğrenelim.

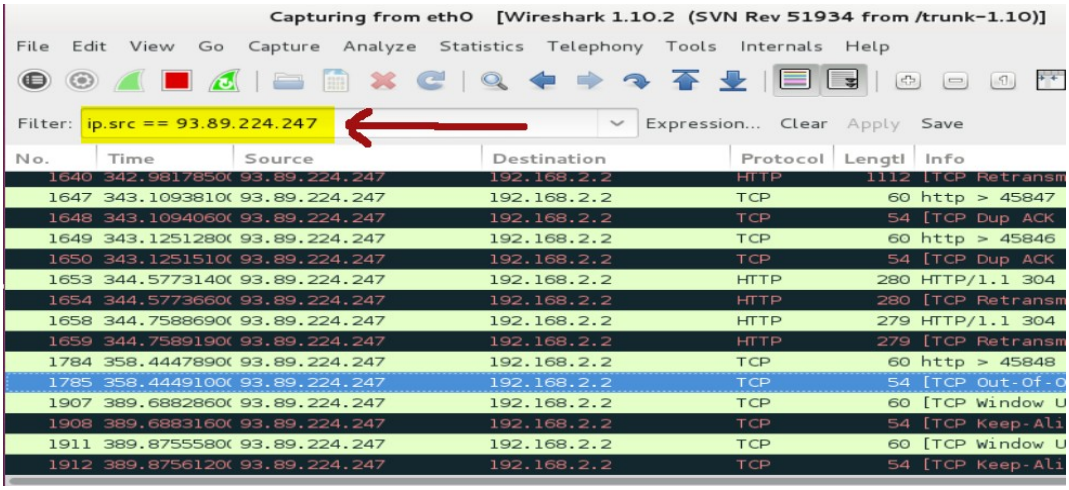
> nslookup www.includekarabuk.com

Output:

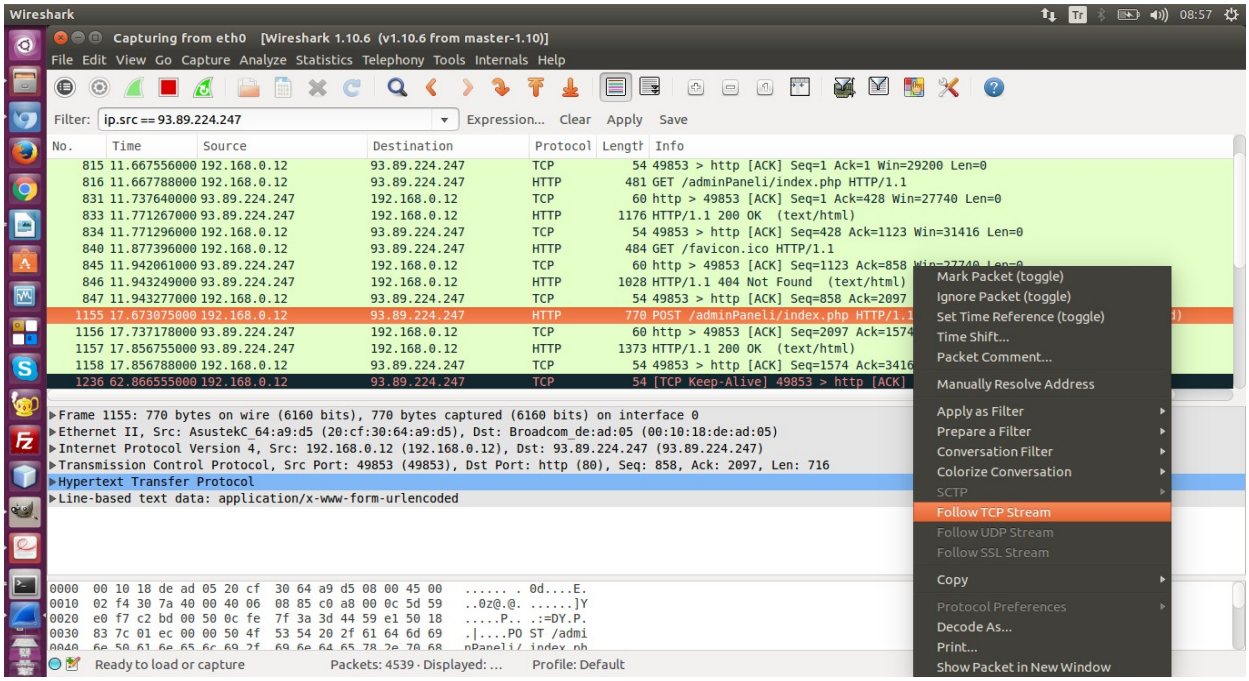
93.89.224.247

Ardından Wireshark filtresini hazırlayalım ve Wireshark'taki ilgili kutucuğua girelim:

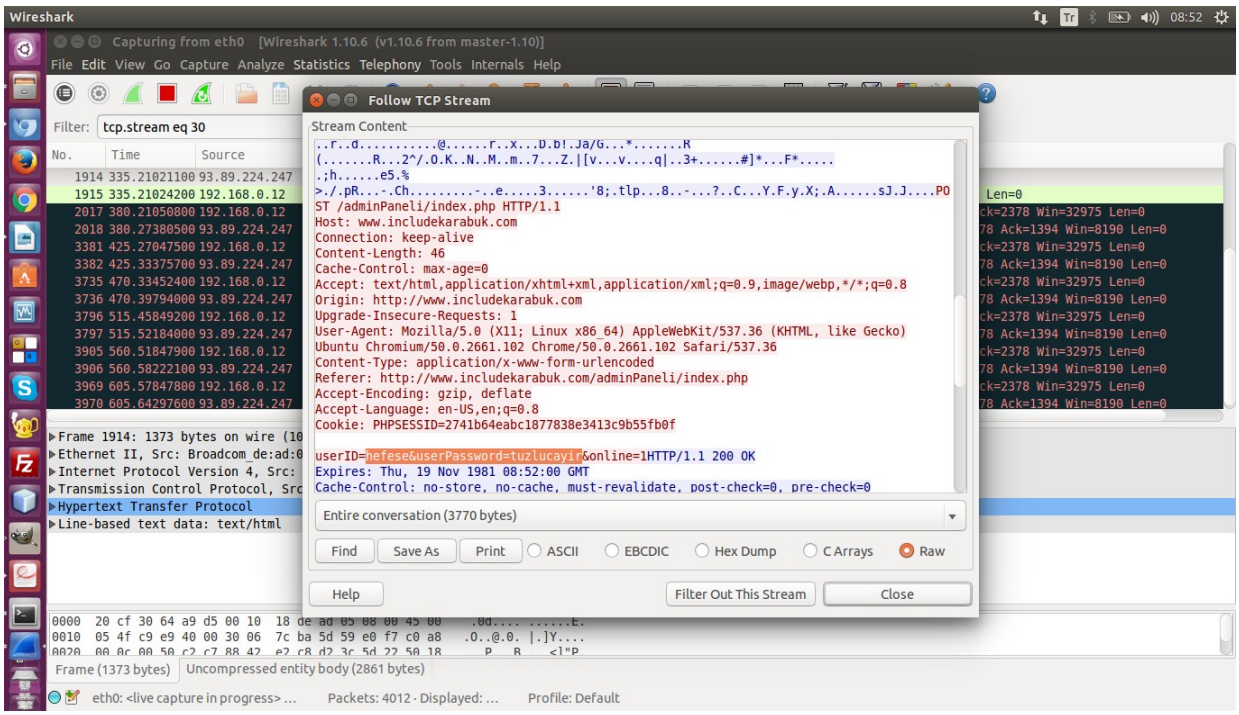
ip.src == 93.89.224.247



Enter'ladığımız takdirde sadece includekarabuk'e ait paketleri görür hale geliriz. Şimdi göz kararınca includekarabuk'e ait paketler arasından HTTP POST paketi arayalım.

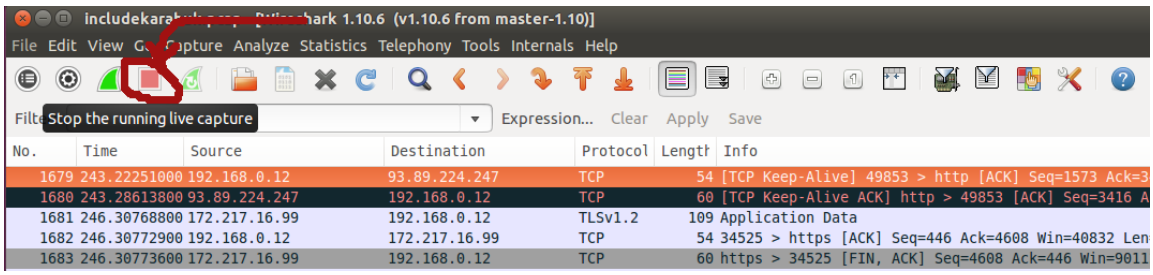


Görüldüğü üzere bir tane HTTP POST paketi bulduk. Şimdi ona sağ tıklayalım ve Follow TCP Stream diyelim. Böylece tıkladığımız paketin içini okuyabilelim.

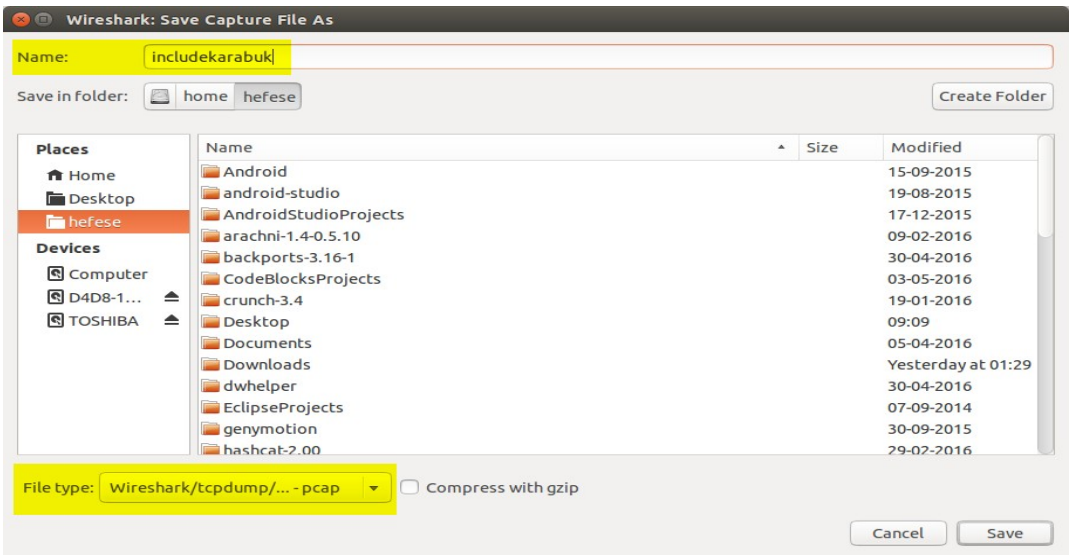


Ve işte sonuç: userID=hefese&userPassword=tuzlucayir. Görüldüğü gibi kullanıcı adı ve şifre bilgisine biraz paketler üzerinde göz gezdirme yaparak ulaşabildik. Peki milyonlarca paket olsaydı...?

NetworkMiner Wireshark, tcpdump gibi trafik sniff'leyen araçlardan gelen trafiği (pcap uzantılı dosyaları) parse işlemine tabi tutarak kritik bilgileri bizim yerimize kendisi bulan bir araçtır. Şimdi az önce elle yaptığımız şifre bulma işini bu sefer Network Miner'a otomatize bir şekilde yaptıralım. Bu iş için ilk olarak Wireshark'tan elde edilen paketleri pcap uzantılı bir dosyaya toplamamız gerekmektedir. Fakat pcap dosyalamasını yapabilmek için önce Wireshark'ın paket sniff'leme işlemini kırmızı kareye tıklayarak durdurmamız gerekir.



Şimdi File -> Save As diyerek ekrana gelen penceredeki dosya uzantısı kısmına Wireshark/tcpdump – pcap diyelim ve isim olarak da örneğin includekarabuk demiş olalım.



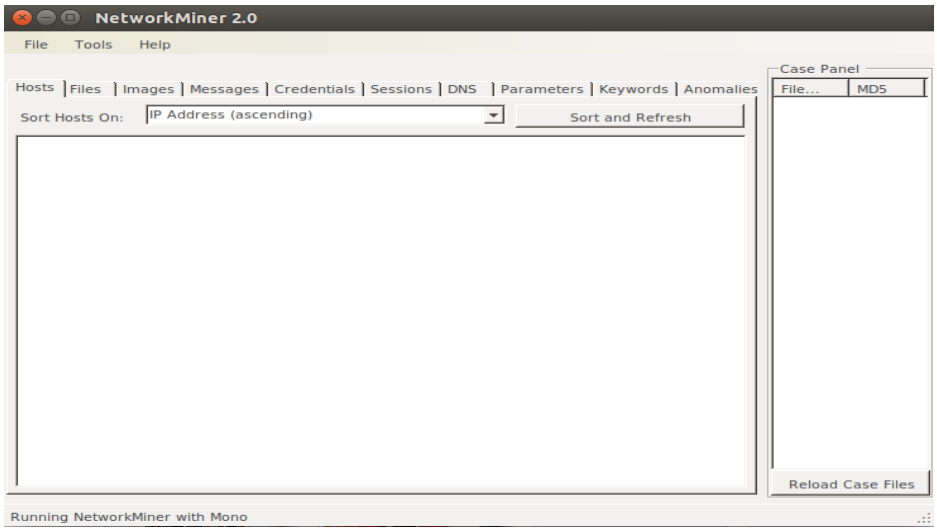
Save diyerek pcap dosyasını oluşturalım. Dosya oluştuktan sonra sırada dosyayı Network Miner'a vermek vardır. Önce NetworkMiner'ı kuralım.

> 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

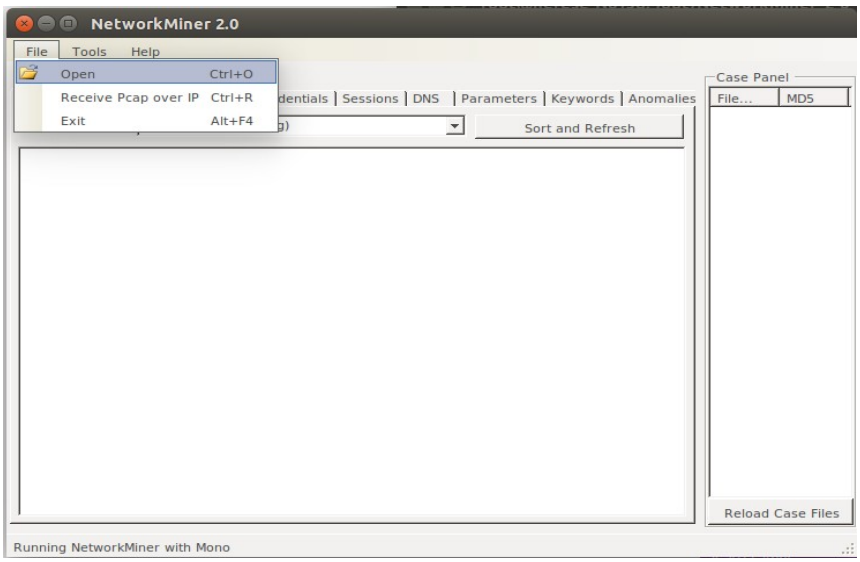
NOT: Eğer program zaten kuruluysa programı başlatmak için şu iki satırı girmen yeterli:

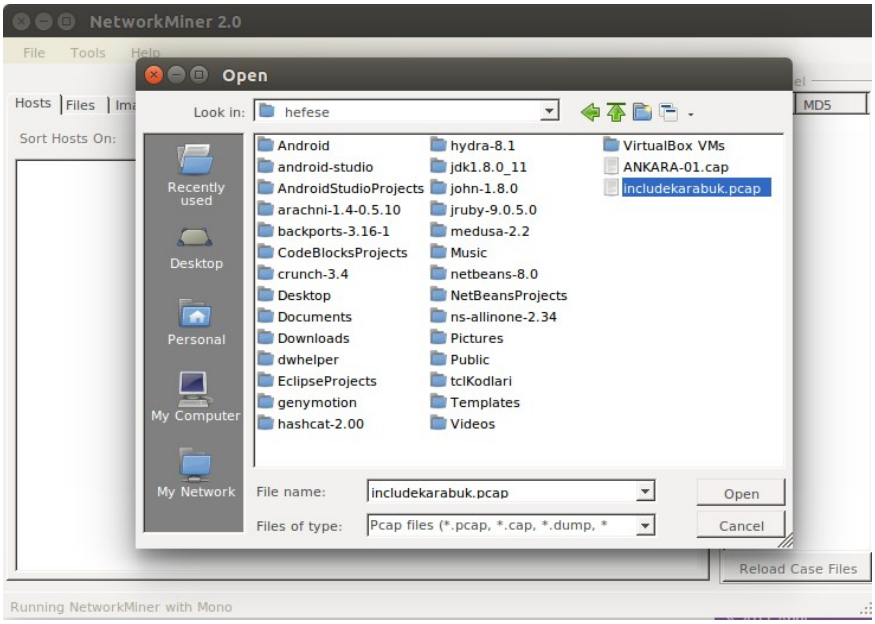
> cd /opt/NetworkMiner*
> mono NetworkMiner.exe

NetworkMiner programı başladığında karşımıza aşağıdaki ekran gelecektir:

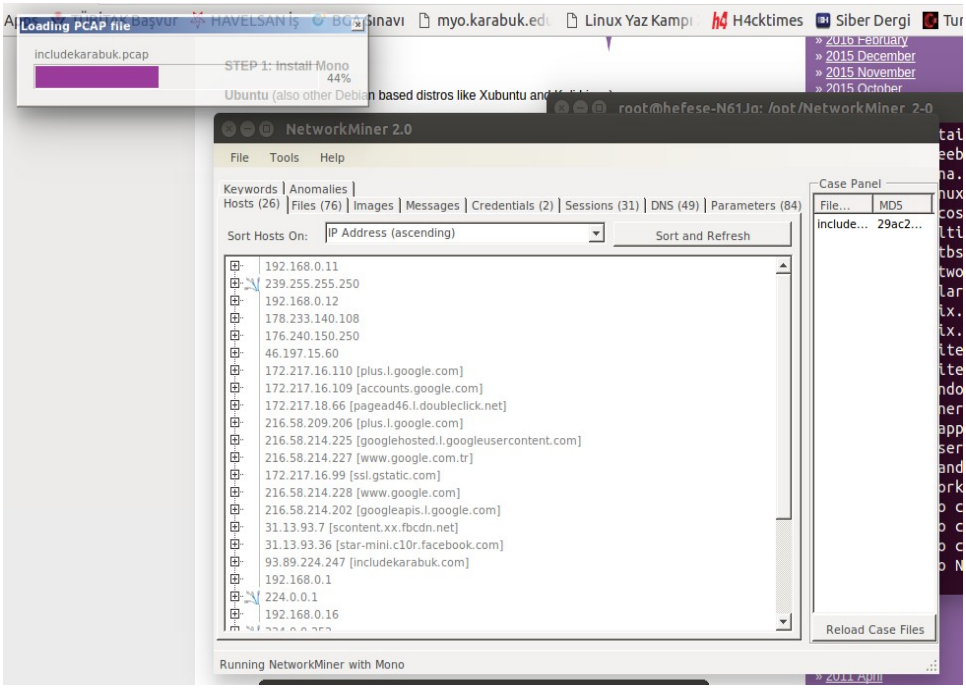


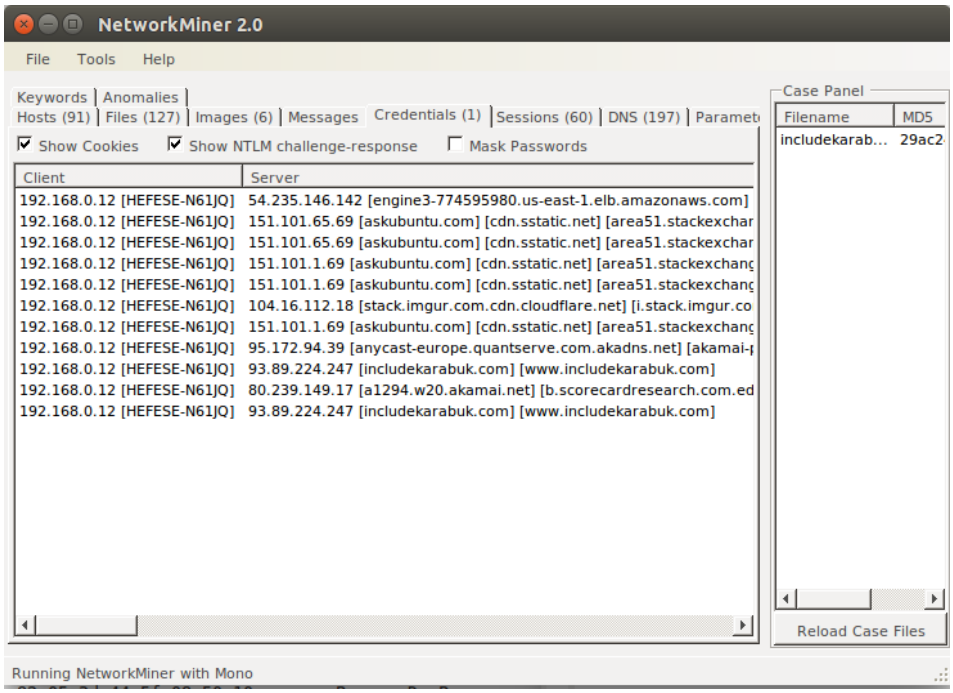
Şimdi Wireshark'tan elde ettiğimiz pcap dosyasını NetworkMiner'a verelim.



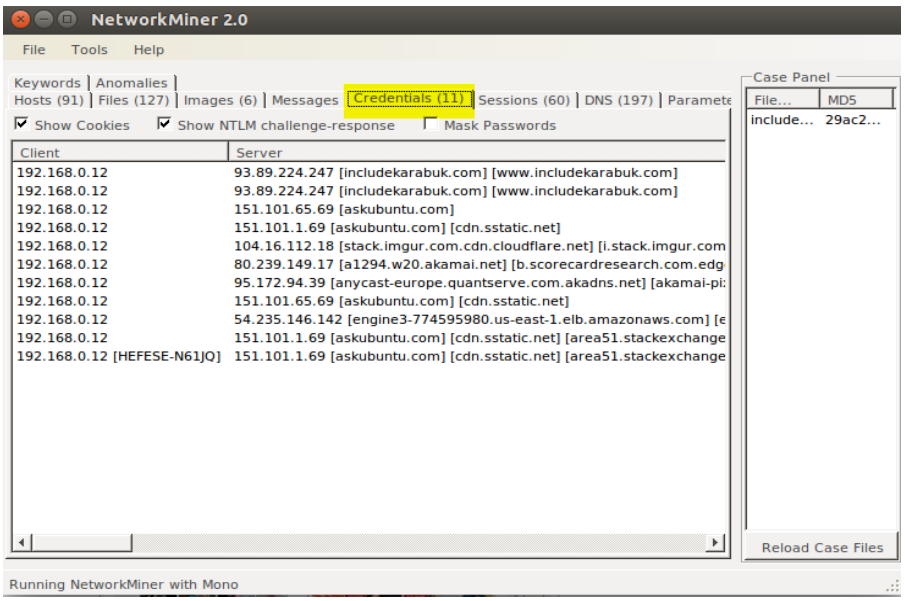


Pcap dosyası aşağıdaki gibi NetworkMiner'a yüklenecektir.

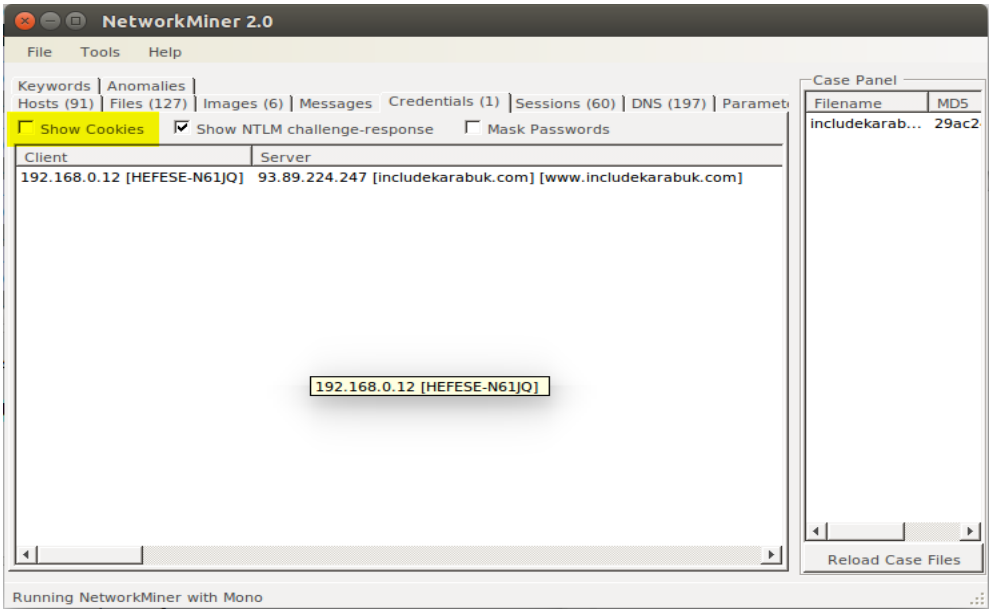




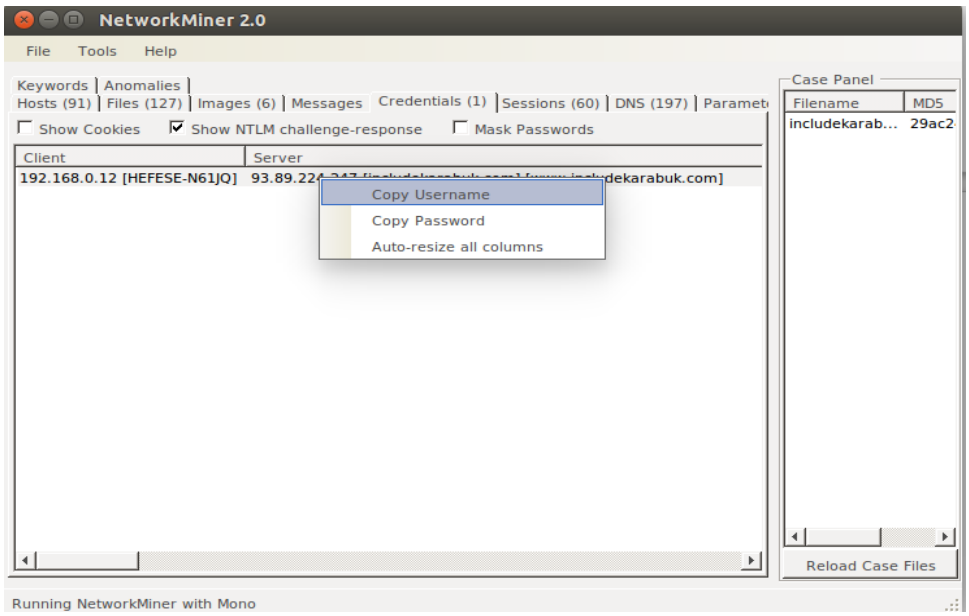
Pcap dosyası böylece NetworkMiner'a yüklenmiştir ve parse işlemi de son bulmuştur. Şimdi Credentials sekmesine geçelim.

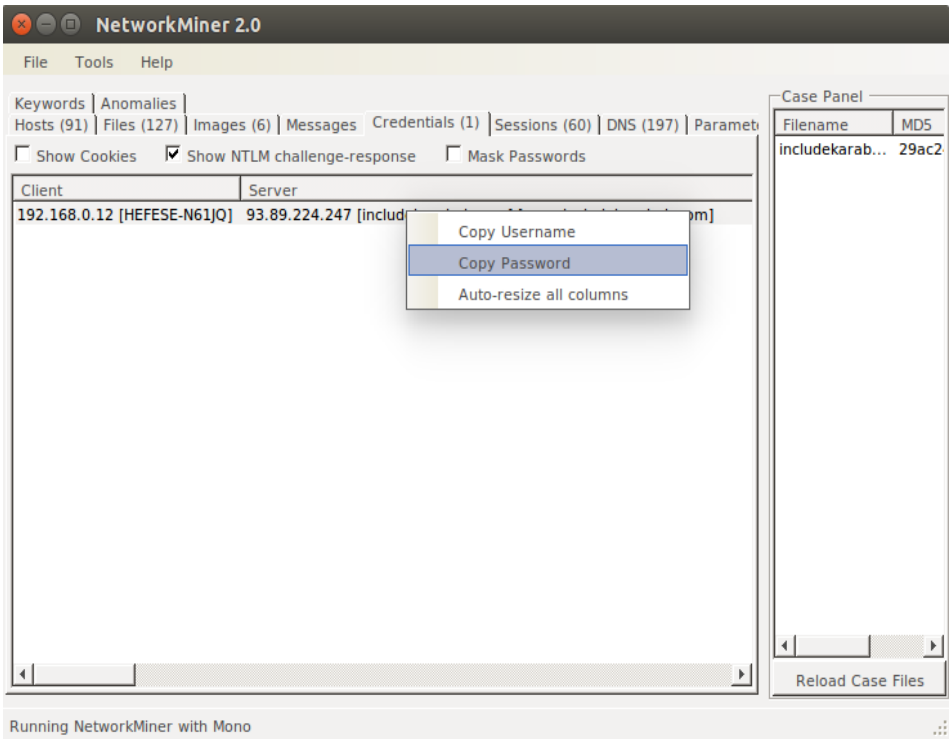


Görüldüğü üzere 11 tane credentials tespit edildiği gösterilmektedir. Bunlardan çoğu çerez olacağı için çerezleri ayıklayalım. Bunun için Show Cookies tick'ini kaldıralım.



Geriye bir tane credential kalmıştır. İşte o bizim includekarabuk'ün admin paneline girerken POST ettiğimiz kullanıcı adını ve şifreyi tutan pakettir. Kullanıcı adı ve şifreyi çekmek için sırasıyla ilgili satıra sağ tıklayalım ve bir Copy Username diyelim, bir de Copy Password diyelim.





Kopyaladıklarımızı sırasıyla bir metin belgesine yapıştırarak kullanıcı adı ve şifre bilgisine erişmiş oluruz. 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 programın kendisi yapıyor ve şıp diye trafik içerisinde bulduğu kullanıcı adı ve şifreyi önümüze sunuyor.

NOT: NetworkMiner normalde bir Windows yazılımıdır ve ayrıca Windows'ta exe'si indirildiği takdirde bir kuruluma gerek kalmadan direk çift tıkla - çalıştır pratikliğindedir.