# NetworkMiner

## NetworkMiner Nedir?

Herkese merhaba. İlk olarak NetworkMiner nedir? Sorusunu cevaplamadan önce Network Forensic nedir kısaca bunu cevaplayarak başlasak daha doğru olur diye düşünmekteyim.

Network Forensic, Ağ Adli Bilişimi olarak Türkçeye çevrilmektedir. Bilgisayarın ve internet bağlantısı olan herhangi bir aracın ağdaki trafiğini dinlemeye ve bu trafikten elde edilen kayıtların analizini yapmaya Network Forensic denilmektedir. Yapılan analizler sonucunda Adli Bilişim acısından önem teşkil edilebilecek çeşitli bilgilere ve delillere ulaşılmaktadır.

NetworkMiner da bu işlemi yapmak için kullanılan araçlardan bir tanesidir. Kolayca indirilebilmesi ve basit ara yüzü sayesinde rahatlıkla kullanılabilir. NetworkMiner piyasaya çıktığı tarihten itibaren adli alanlarda çalışma yapan kolluk kuvvetleri ve ekiplerce kullanılması oldukça tercih edilen bir ağ adli bilişim aracı olmuştur. Windows, Mac OS, Linux, FreeBSD gibi sistemler için geliştirilmiş açık kaynaklı bir yazılımdır. Ücretli ve ücretsiz sürümleri mevcuttur. Canlı ve çevrimdışı analiz yapma yeteneği mevcuttur. Çevrimdışı analiz sayesinde P-cap gibi dosya türlerini incelememizi sağlamaktadır.

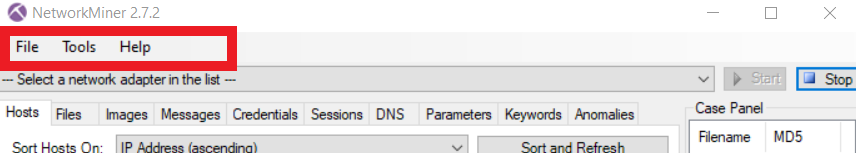
## NetworkMiner Nereden ve Nasıl İndirilir?

Netresec in web sitesinden NetworkMinir’ ı aşağıya bıraktığım bağlantıya tıklayarak kolaylıkla indirebilirsiniz

<https://www.netresec.com/?page=NetworkMiner>

NetworkMiner’ ı nasıl indirebileceğimizi de gösterdiğimize göre artık aracımızı kurup incelemeye başlayabiliriz. Aracımızı kullanmaya başlamadan önce NetworkMiner’ ın bilmenizi istediğim yazılım bölümlerinden bahsederek sizlere anlatmaya başlayacağım.

# NetworMiner Arayüzü Hakkında?

****

**File Bölümü:**

**Open(Ctrl+O):** Çevrim dışı analiz için pcap dosya türlerini açar ve inceler.

**Read From PacketCache:** Bir bilgisayarın ağ ara yüzlerini sürekli olarak izler ve elde edilen paketleri RAM’ de depolar.

**Exit(Ctrl+F4):** Programdan çıkış yapar.

**Tools Bölümü:**

**Start Capturing F5 ve Stop Capturing F8:** Canlı analiz paket yakalama başlatılır ve sonlandırır.

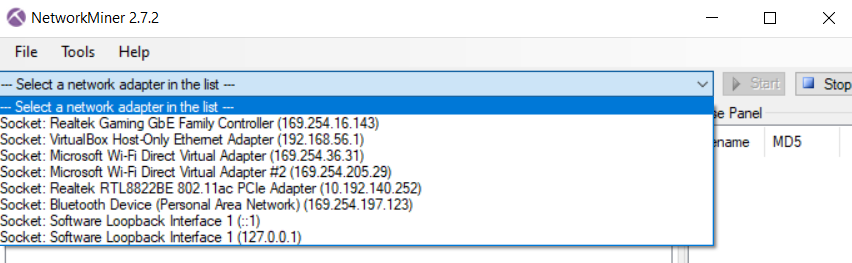
**Clear GUI(Ctrl+N):** Ara yüzü temizlemeye yarar.

**Delete Captured Data(Ctrl+Del):** Yakalanan paketleri silme işlemini gerçekleştirir.

**Help Bölümü:**

**Check for Updates:** Bu bölümden NetworkMiner’ a gelen güncellemeler kontrol edilir ve gerçekleştirilir.

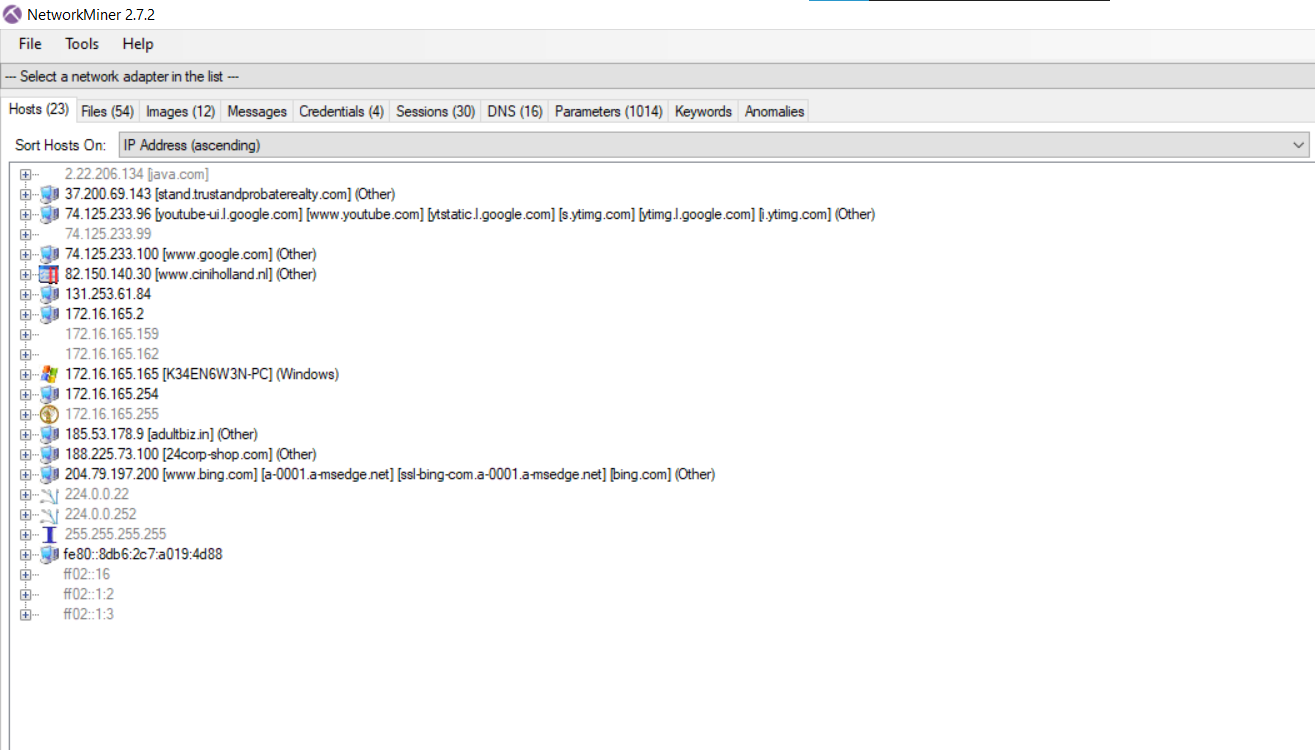
**About NetworkMiner:** Araç ile ilgili bilgi alınabilir.

****

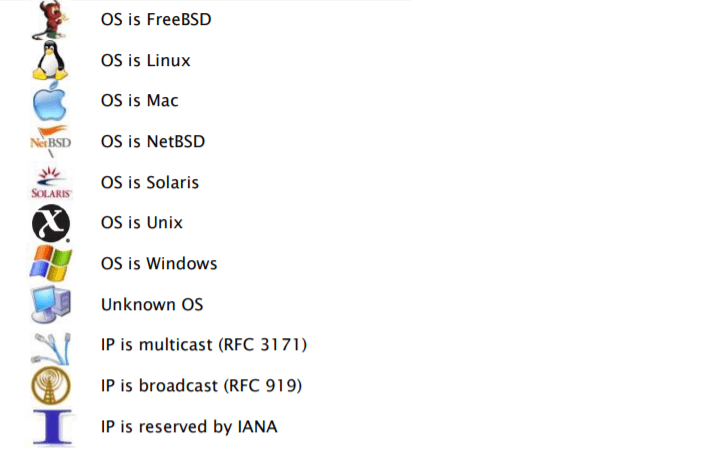
Canlı analiz için **---Select a network adapter in the list ---** bölümünden izlemek istediğimiz network adaptörünü seçip **–Start** diyerek canlı analiz yapabilirsiniz.

NetworkMiner’ ın ara yüzünden de kısaca bahsettiğimize göre gelin şimdi hep birlikte örnek bir P-cap dosyası inceleyerek **Host File, Images, Messanges, Credantials, Sessions, DNS, Parameters** ve **Keywords** sekmelerinin görevlerini öğrenelim.

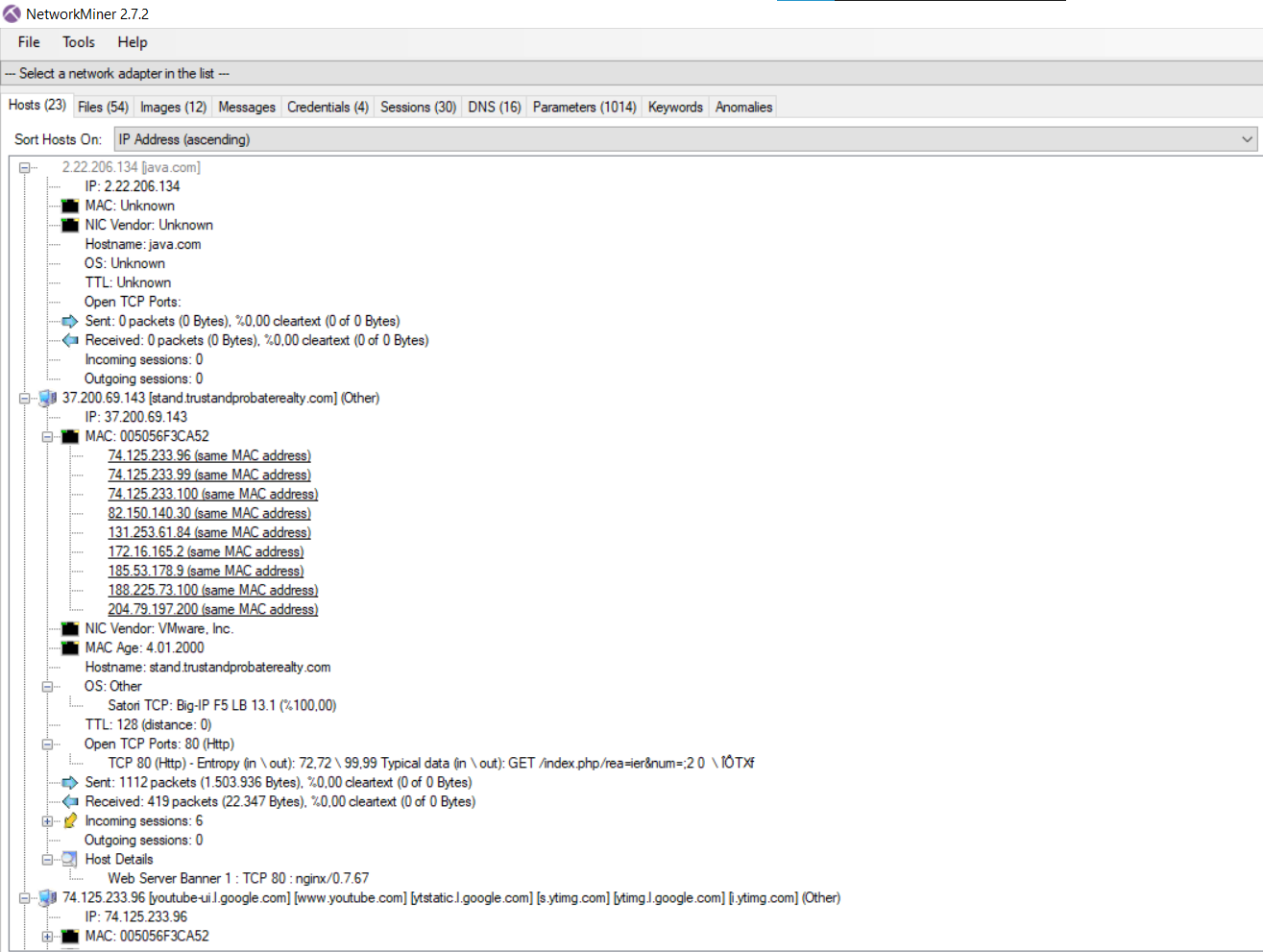
**HOST SEKMESİ:**



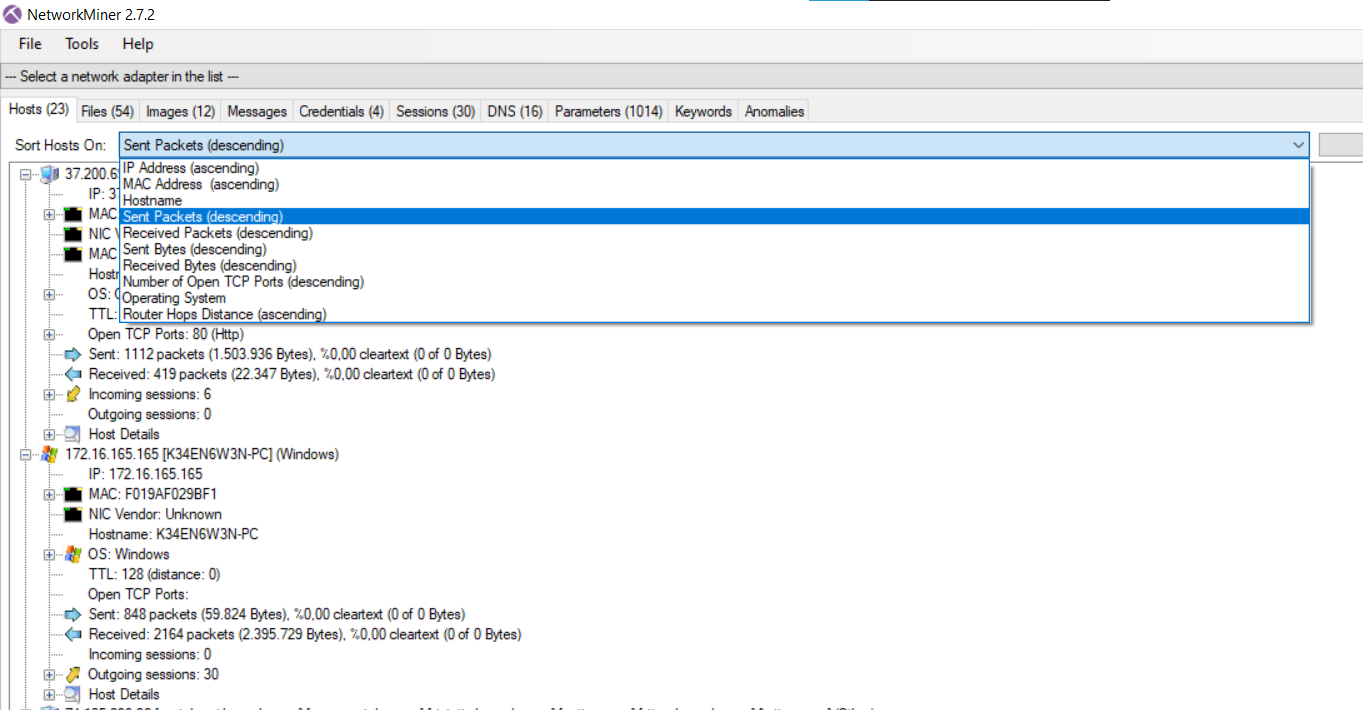
Host sekmesinde görüldüğü gibi analiz edilmiş trafikteki tüm IP adresleri mevcuttur.



Host sekmesindeki ikonların ne anlama geldiği yukarıdaki görselde belirtilmiştir.



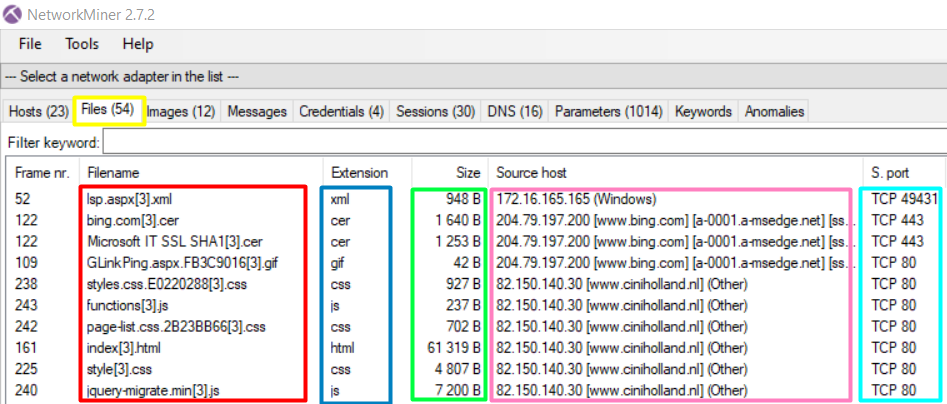
Host sekmesinde IP adreslerinin başındaki + işaretlerine basarak daha detaylı bilgiler olduğunu bulabiliriz. Buradan MAC adresi, işletim sistemi bilgileri, host, adresi, alınan ve gönderilen paketlerin boyutu, bağlantı kurulan port bilgileri gibi bilgilere ulaşılabilir.



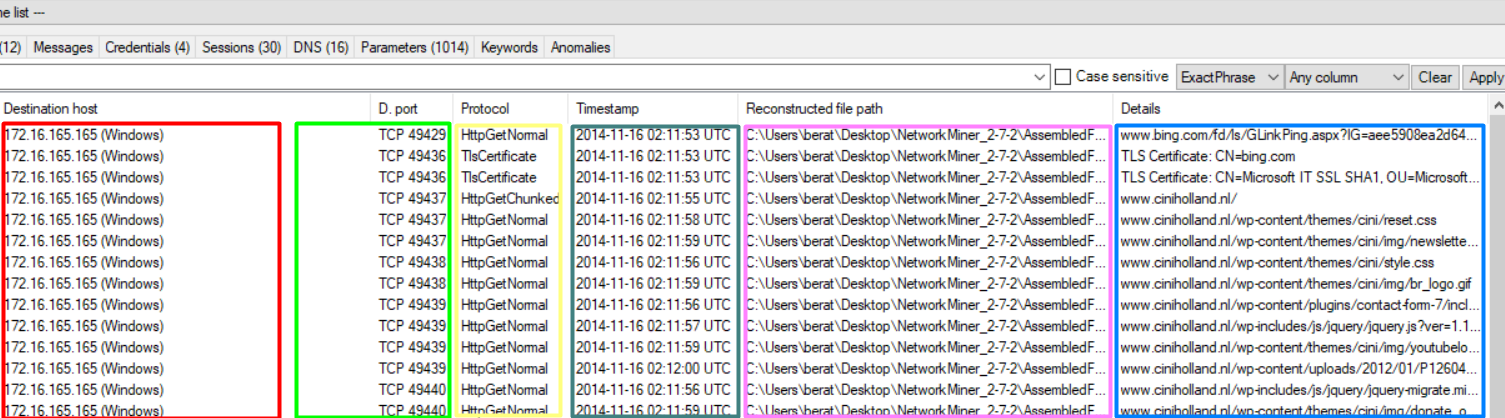
**Sort Hosts On** kısmından adresleri çeşitli parametrelere göre sıralayabiliriz.

1. IP Adress (ascending): IP adreslerini küçükten büyüğe doğru sıralar.
2. MAC Adress (ascending): MAC adreslerini küçükten büyüğe doğru sıralar.
3. Hostname: bilgisayar isimleri hakkında bilgiler verir.
4. Sent Packets (descending): Adreslerdeki gönderilen paket boyutlarını çoktan aza doğru sıralar.
5. Received Packet (descending): Adreslerdeki alınan paket boyutlarını çoktan aza doğru sıralar.
6. Sent Bytes (descending): Gönderilen byte ları çoktan aza doğru sıralar.
7. Received Bytes (descending): Alınan byte ları çoktan aza doğru sıralar.
8. Number of Open TCP Ports ( descending): Açık TCP portlarını çoktan aza doğru sıralar.
9. Operating System: İşletim Sistemi hakkında bilgiler verir.
10. Router Hops Distance: Router(yönlendirici) atlama mesafesi hakkında bilgiler içerir.

**FILES SEKMESİ:**



1 2 3 4 5

 6 7 8 9 10 11

**Files** bölümünde ise NetworkMiner tarafından extract (çıkarılan) edilen dosyalara ait bilgiler yer alır. Bir pcapt dosyası açıldığında veya NetworkMiner canlı bir analize başladığında HTPP, SMB, FTP ve TFTP protokollerinden dosyaları otomatik olarak indirir.

Bu dosyalar geçici olarak saklanır ve istenilen dosyanın üzerine gidilip sağ tık yapılarak **Open Files** seçilir ve dosya açılır veya da klasöre ulaşılabilir.

Files sekmesinden elde edebileceğimiz bilgiler aşağıdaki gibidir:

1.Bölümde; extract (ayıklanmış) edilmiş dosyanın ismine,

2.Bölümde; dosyanın uzantısına,

3.Bölümde; dosyanın boyutuna,

4.Bölümde; dosyanın kaynak adres bilgilerine,

5.Bölümde; kaynak iletişim portuna,

6.Bölümde; IP bilgilerine, Host name’ ne,

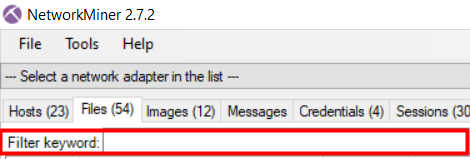
7.Bölümde; hedef iletişim portuna,

8.Bölümde; Protocol bilgilerine,

9. Bölümde; Tarih ve Saat bilgilerine,

10. Bölümde; Bulunduğu geçici dosya yollarına,

11. Bölümde ise detaylı bilgilere ulaşılır.

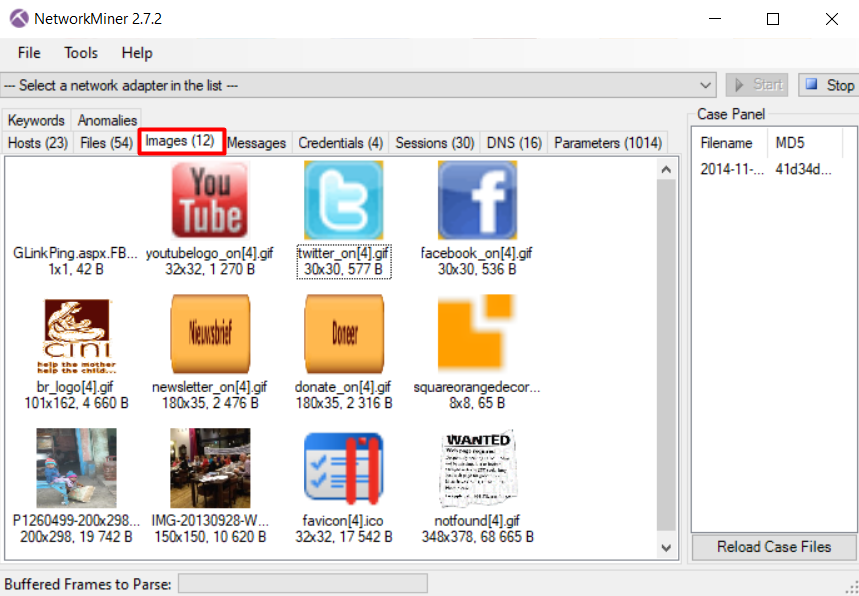


**Filter Keyword** kısmındın ise dosya isimleri, uzantısı, boyutu gibi filtrelemeler yapabilirsiniz.

**MESSAGE SEKMESİ:**

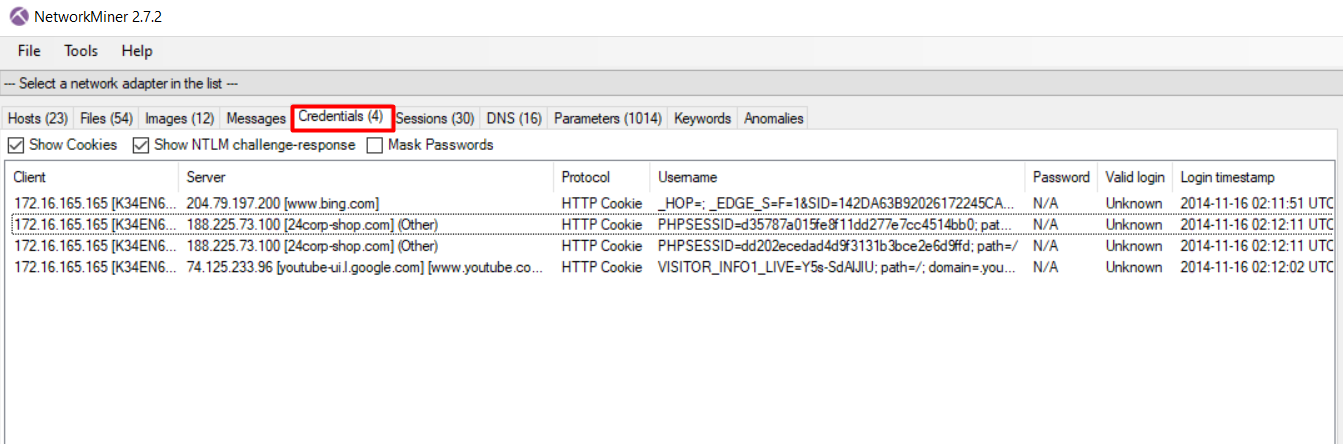
Bu sekmede E- Mail’ den alınan tüm mesajlar, IM(Instant Messaging), IRC(INTERNET RELY CHAT) ve sosyal medya mesajlarına erişilir.

**IMAGES SEKMESİ:**



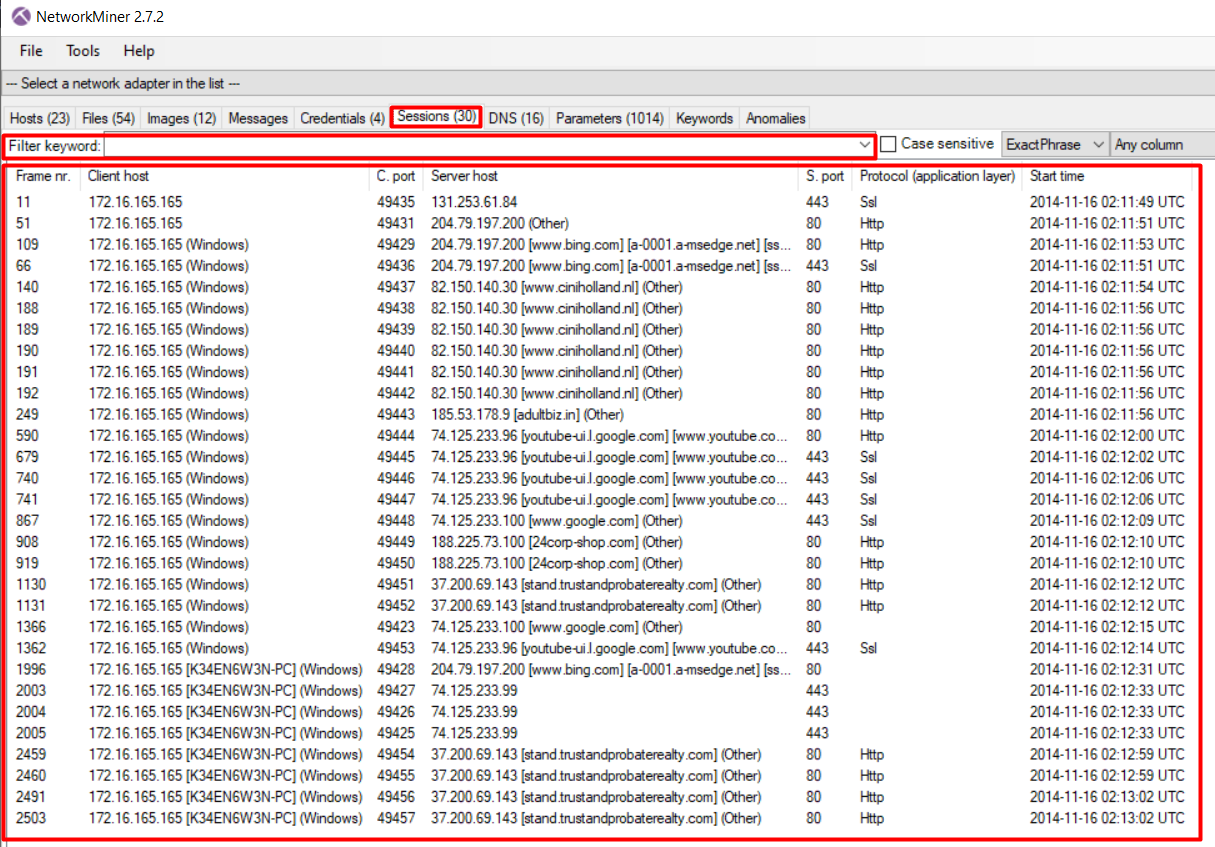
**Images** sekmesinde ayıklanmış tüm görüntü dosyalarını bize ön görüntü resmi halinde gösterilir. İstenilirse ön görüntü resimlerin üzerine çift tıklanarak ön görüntü resimler açılabilir veya mouse ile resimlerin üzerine gelinerek ön görüntü resimleri hakkında bilgiler alınılabilir.

**CREDENTIALS SEKMESİ:**



Credentials kısmında ise kullanıcı adları ve parolaları gibi bilgiler bulunur. Ayrıca trafikte yer alan HTTP ve FTP çerezleri (cookie), NTML challenge-response mesajları da bulunabilir.

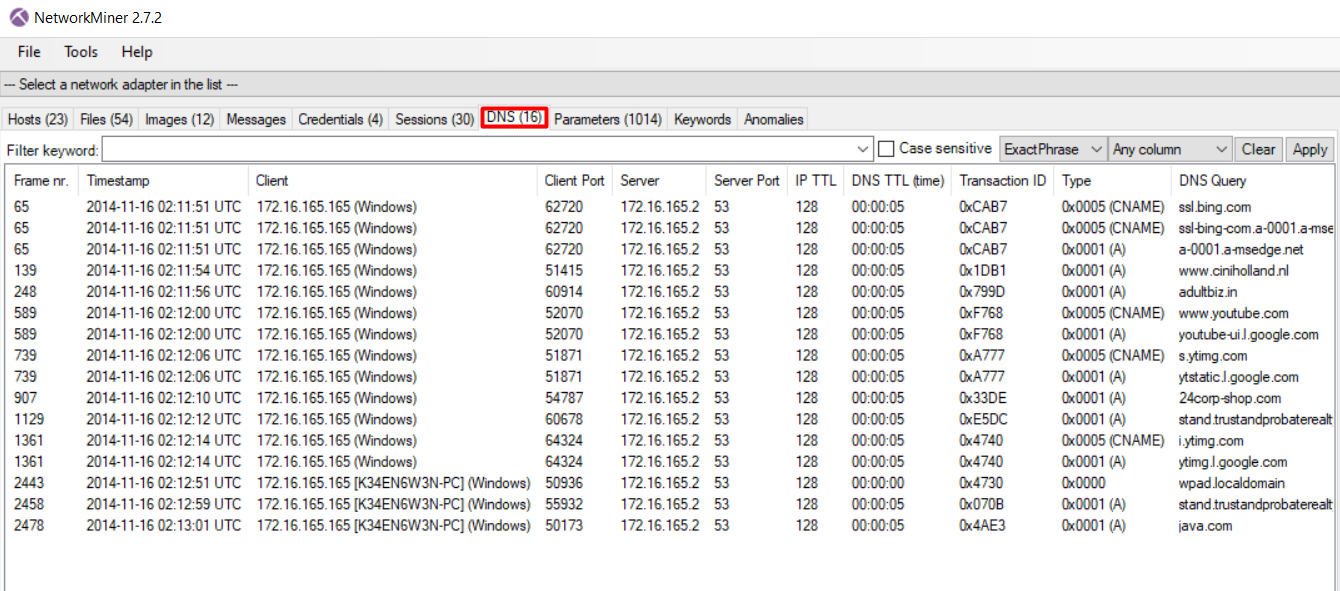
**SESSIONS SEKMESİ:**



**Sessions** sekmesinde client-server bağlantıları, aralarındaki iletişim, port bilgileri, protokol bilgileri ve zamanlamalar daha net gözükmektedir.

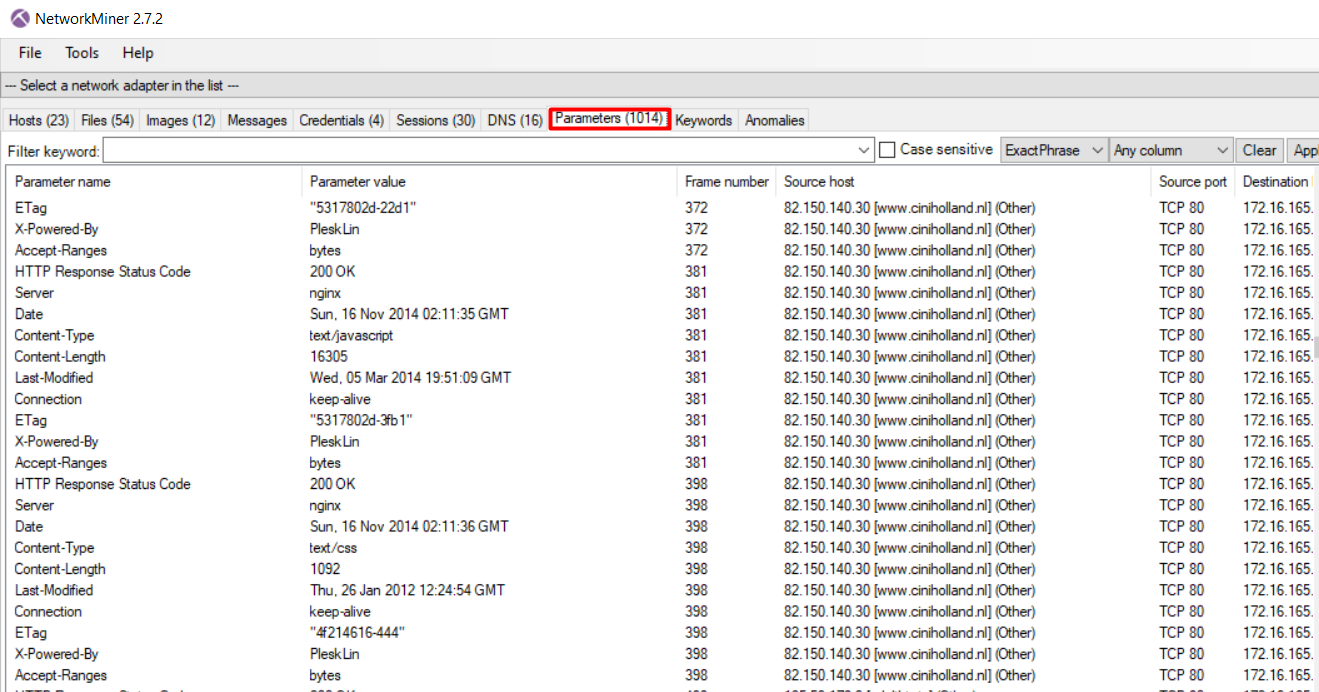
**Filter Keyword** kısmından ise istenilen porta yönelik filtrelemeler yapılabilir.

**DNS SEKMESİ:**



**DNS** sekmesinde SSL sertifikalarılisteleri, site içeriği, kara liste vb. gibi bilgileri bulabiliriz.

**PARAMETRES SEKMESİ:**



**Parametres** sekmesinden trafikte çıkarılan her türlü bilgiye ulaşılabilir. HTPP sorgu değerleri, dizileri, GET ve POST değişkenleri ve daha birçok şey bu sekmede mevcuttur.

**KEYWORDS SEKMESİ:**

**Keywords** sekmesinde ise trafik kaydı içerisinde belirli bir karakter dizisi aramak için kullanılır.

Bu makalede, bir Adli Bilişim Mühendisinin NetworkMiner yazılımını kullanarak nasıl Ağ Adli Bilişimi yani Network Forensic yaptığını, örnek bir P-cap dosyası üzerinden çevrim dışı analizin nasıl gerçekleştirdiğini öğrendiniz. Adli Bilişim Mühendisliği ile ilgili daha fazla makale okumak istiyorsanız takipte kalın. Bizleri Linkedin üzerinden takip edebilir ve çıkardığımız diğer makaleleri ilk görenler siz olabilirsiniz. Okuduğunuz için teşekkürler!