[E-posta(Mail) Başlık Bilgileri]

E-posta Başlıklarından Bilgi Toplama

Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>

8/21/2009

E-postaların taşıdığı başlık bilgilerinden forensic analiz amaçlı bilgi edinme, çeşitli e-posta servis ve yazılımlarından bilgi toplama

İçerik

E-posta Kavramı

Internetin gelişmesiyle birlikte günümüz iletişim sistemlerinde telefondan sonraki adımı e-postanın almaya başladığını görüyoruz. Bunun çeşitli sebepleri vardır ama en önemli sebepleri arasında e-posta sisteminin ücretsiz olması ve basit, kolay kullanıma sahip olması sayılabilir. 3G hizmetinin yaygınlaşmasıyla birlikte kısa mesaj servisi SMS'in yerini e-postanın alacağı da uzmanlar tarafından öngörülüyor.

Artık her birimizin bir –ya da birden fazla- e-posta adresi var. E-postalarımızı sadece haberleşme için kullanmıyoruz. E-postalarımız internet üzerinde çoğu zaman sanal kimlik bilgisi olarak kullanılıyor. Çeşitli sitelerden hizmet alabilmek amaçlı üyeliklerimiz, paypal vs gibi sanal ödeme sistemlerinde yaptığımız işlemler hep e-postalarımız üzerinden yürümekte ve gün geçtikce e-postalarımızın güvenliğinin önemi artmakta.

Bugün e-postayı aktif olarak kullanan birilerinin hesap bilgileri başkaları tarafından ele geçirildiğinde çok zor durumda kalabilmektedir.

Bu yazıda e-posta sisteminin son kullanıcılara çok bir şey ifade etmeyen ama gerektiğinde çok işe yarayan " başlık bilgileri" konusunu inceleyeceğim.

E-posta Sistemi Nasıl Çalışır?

E-posta sistemi gerçek hayattaki posta hizmetinden örnek alınarak oluşturulmuş bir servistir. Gerçek dünyada bir mektup yazar bu mektubu zarfın içine koyarak üzerine gönderici alıcı vs gibi ek bilgileri yazıp postaneye bırakırız(dık). Mektubu alan görevliler zarf üzerindeki bilgilere(başlık bilgileri)bakarak mektubumuzu doğru adrese yönlendirirler.

E-posta da aynen bu şekilde çalışır, gerçek hayattan tek farkı aracı olarak insanların değil bilgisayar sistemlerinin kullanılmasıdır.

E-posta DNS İlişkisi

E-posta sisteminin sağlıklı çalışabilmesi için çeşitli etkenler vardır. Bunların başında isim çözümleme sistemi olan DNS gelir. DNS servisi çalışmadan sağlıklı bir e-posta servisinden bahsedilemez.

DNS'in e-posta sistemine etkisi şudur: bir e-postanın hangi adrese teslim edileceği DNS kayıtlarıyla belirlenir.

Mesela huzeyfe@lifeoverip.net adresine mail gönderebilmek için öncelikle bu adresin maillerini kabul edecek sistemin bilinmesi gerekir. Bu da DNS de MX kayıtlarında tutulur.

```
C:\Documents and Settings\Administrator>nslookup -q=mx lifeoverip.net 195.175.39.40
Server:  ttdns40.ttnet.net.tr
Address:  195.175.39.40

Non-authoritative answer:
lifeoverip.net  MX preference = 0, mail exchanger = mail02.lifeoverip.net
lifeoverip.net  MX preference = 10, mail exchanger = mail.lifeoverip.net

lifeoverip.net  nameserver = ns4.tekrom.com
lifeoverip.net  nameserver = ns3.tekrom.com
mail02.lifeoverip.net   internet address = 91.93.119.80
mail.lifeoverip.net     internet address = 91.93.119.80
ns3.tekrom.com  internet address = 70.84.223.226
```

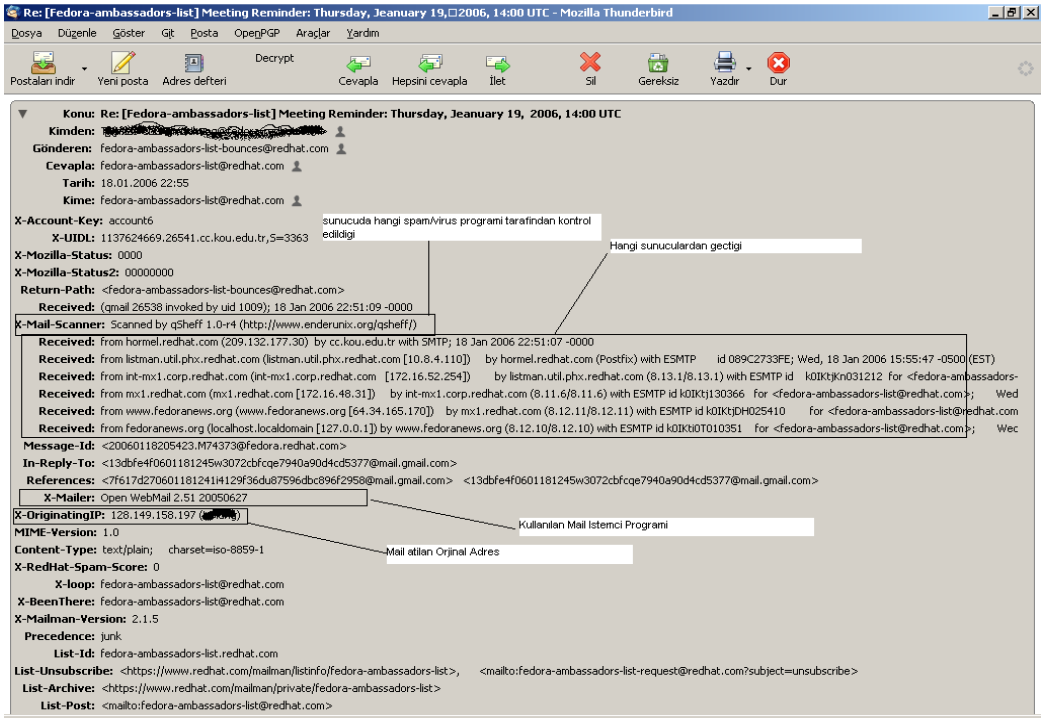
Bu adres(mail02.lifeoverip.net) @lifeoverip.net uzantılı mailleri kabul edecek sistemdir.

Internetten herhangi bir yerden @lifeoverip.net adresli hesaplara gönderilecek mailler mail02.lifeoverip.net adresine ulaşacaktır.

E-posta Başlıklarını Okuma

Her e-postanın bir ader başlık(header) ve gövdesi(body) vardır . Başlık bilgileri aynı günlük hayatımızdaki posta sistemindeki gibi adres bilgileri, kimden kime atıldığı ve özel not gibi bilgileri taşır. Gövde ise mesajın içeriğini taşır.

Mail başlıklarını doğru okuyabilmek forensic analiz ve bilgi toplama açısından oldukça önemlidir. Üzerinde dikkatle uğraşılmamış bir mail takip edilerek sahibine ait oldukça detaylı bilgiler edinilebilir.



Uzaktan bakıldığından anlamsız gözüken bu satırlar dikkatli bir göz tarafından incelendiğinde birçok bilgiyi ifşa edecektir.

Bundan 4-5 yıl önce üye olduğum bir arkadaş listesine tanımadığımız bir adresten grup arkadaşlarımızdan birini zor durumda bırakan e-posta gelmişti. Gönderen mail adresini hiçbirimiz tanımıyorduk fakat e-posta başlıklarını incelediğimde gönderenin kimlik bilgilerini rahatlıkla bulabilmiştim.

Gönderilen E-postanın başlık bilgilerinden edindiğim bilgiler şunlardı: gönderenin IP adresi, gönderenin iç ağda kullandığı ip aralığı, gönderenin Windows sisteminin bilgisayar adı(Received başlığı Helo/ehlo) ve gönderdiği program. Bu bilgileri kullanarak e-postayı gönderenin kim olduğunu konusunda kesin bilgi edinebilmiştim.

Received: from dsl88-14-20.adsl.ttnet.net.tr ***(HELO warcraft-ng)***
(zky@nett.com@88.14.1.164)
by mail.lifeoverip.net with SMTP; 19 Aug 2009 07:26:46 -0000

E-posta başlıklarından çıkarılabilecek temel bilgileri sırasıyla inceleyelim.

E-posta Başlıkları

E-posta başlık bilgisi çeşitli alanlardan oluşur. E-postayı gönderen, ileten , alan her sistem uygun başlıklar ekleyerek bu alanı çoğaltır. Hatta bazen bu başlık alanı gövdeyi geçer. E-posta başlıkları kolaylıkla değiştirilebilir, dolayısıyla tam güvenilir değildirler.

From: Başlık Bilgisi

From: Mailin kimden geldiğini gösteren başlık alanıdır. Çok kolay spoof edilebileceği için en az güvenilir başlık alanıdır denilebilir.

From: "Huzeyfe Onal" Huzeyfe.Onal@xyz.com.tr

Bir de From(**From:** değil) alani vardir ki bu standart mail başlığı değildir, bazı yazılımların mail alındığında eklediği bir başlık türüdür. Mesela Mbox formatında kaydedilen e-postaların ayırtedilebilmesi için kullanılır.

To: Başlık Bilgisi

E-postanın kime gönderildiği bilgisini taşır.

To: "Huzeyfe Onal" aslan@yaslan.com

Reply-To: Başlık Bilgisi

Dönen cevabın hangi adrese gönderileceğini bildirir.

Return-path: Başlık Bilgisi

Reply-to benzeri bir başlıktır. Dönecek hata mesajlarının hangi adrese gideceğini belirtir.

Received Başlık Bilgisi

Received başlığı mail iletilişimi ile ilgili verdiği detaylı ve gerçekci bilgiden dolayı oldukça önemlidir. Kullanıcı ile MTA(e-posta sunucu), MTA ile MTA arasındaki iletişimi geriye dönük takip edebilmek içi Recevied alanı kullanılır.

Postayı her teslim alan mta bir received başlığı ekler. Aşağıdan yukarı takip ederek gönderilen mailin hangi SMTP sunucularindan geçtiği belirlenebilir.

Received başlık alanı formatı şu şekildedir:

Received: from **string** (hostname [host IP address])

by recipient host (MTA Bilgisi)

with protocol id message ID

for recipient;

timestamp

string ile hostname(gönderici MTA/host) genelde aynı olur fakat string kısmı farklı olabilir.

Hostname, gonderici MTA'nin ters DNS kaydi ile elde edilir. String degistirilebilir oldugu icin dikkate alınmayabilir.

recipient host*:* Maili teslim alan MTA

MTA Bilgisi : Maili teslim alan MTA yazılım bilgileri. Bu alan kullanılan yazılıma ve yapılan ayarlara göre çok detaylı bilgi de verebilir, sadece yazılım ismi de.

Örnek MTA Bilgisi.

Received: from defiant.ddtechcg.com ([72.90.237.196])
by vms044.mailsrvcs.net **(Sun Java System Messaging Server 6.2-6.01 (built Apr** 3 2006)) *endmail*

by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4heF4002161;

Not: esmtp id maili alan sunucunun kendi içerisinde kullanılabilecek bir değerdir.

Message ID**:** Mailin ilk çıktığı makine tarafindan oluşturulan başlık değeri. Kullanılan mta'ya göre ufak tefek farklılıklar gösterse de genel tanım itibari ile id@smtp_sunucu formatındadır.

<1168358378.14189.ezmlm@huzeyfe.net>

Bu ID mail istemcisi tarafindan olusturulur ve mail sunucuda belirli bir mesajin aranmasinda kolaylik saglar.

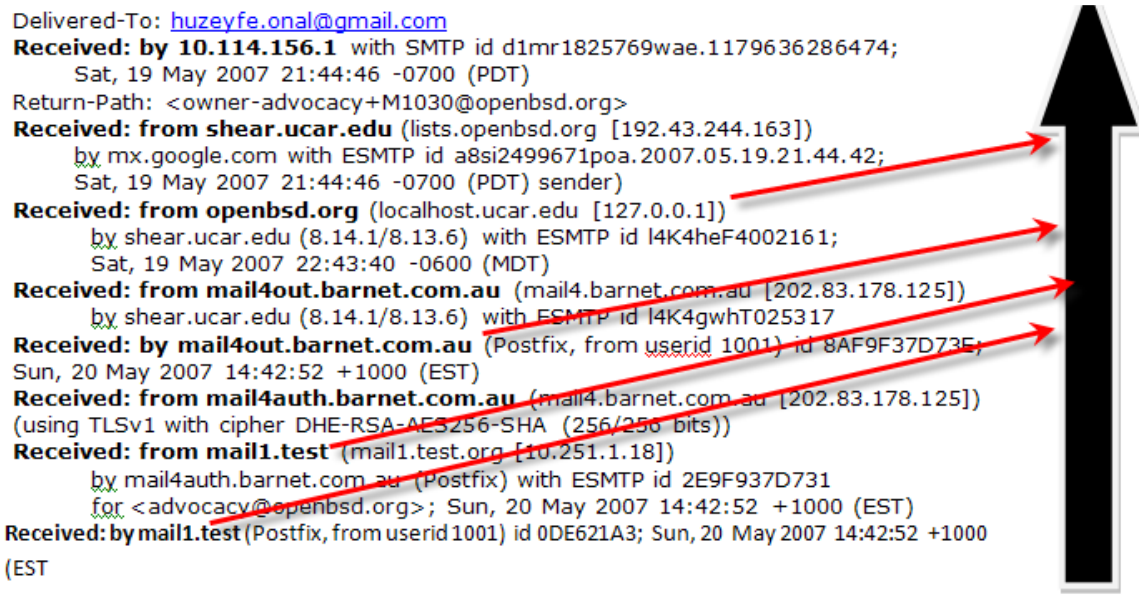
timestamp: mesajin alici taraftaki MTA'ya ulastigi zaman. Ilk ve son timestamp bilgilerine bakılarak e-posta sunucularin performanslarına dair bir fikir edinilebilir.

Örnek:

Received: (from rapsodi@localhost)
by synack.anonim.net (8.13.8/8.13.8/Submit) id l4JNzXCJ032364;
Sat, 19 May 2007 16:39:34 -0700
-0700 Greenwitch'in 7 saat gerisinde manasindadir.

***For recipient*:** alıcı mail adresi. Mailin kim için olduğu bilgisi.

Received alanı da diğer başlık alanları gibi değiştirilebilir fakat son Received bilgisi mutlak surette gönderici sunucu tarafından ekleneceğinden gerçek bilgi verecektir. Mail başlığını incelerken en üstteki Received alanı en son yapılan iletişimi gönderir. Aşağıdaki çıktıda gönderilen e-posta 8 farklı MTA'dan geçmiştir ve son olarak 10.114.156.1'de alıcısına teslim edilmiştir.



Date Başlık Bilgisi

Mailin ilk kaynakta oluşturulma zamanı.

Date: Sat, 19 May 2007 10:31:37 -0400

User-Agent Başlık Bilgisi

User-agent başlık bilgisi e-posta göndericinin hangi yazılımı kullandığını gösterir.

Örnek:

User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1b3pre) Gecko/20090513 Fedora/3.0-2.3.beta2.fc11 Thunderbird/3.0b2

X-Başlıkları

İstemci ve mta harici yardımcı yazılımların eklediği başlıklar gerçek başlık değerleri ile karışmaması için X- ile başlar.

Mesela bazı webmail programları gönderdikleri e-postalara X-Originating-IP: [88.228.40.6] şeklinde başlık alanı ekler ve bu başlık bilgisi istemcinin IP adresini gösterir.

X- Başlık alanına bazı örnekler:

X-OriginalArrivalTime: 17 Aug 2009 11:44:12.0615 (UTC)
FILETIME=[0A5BA570:01CA1F30]
X-Disclaimer-Added-By: avc.com.tr
X-Mail-Scanner: Scanned by qSheff-II-2.1-r3
X-Mailer: Evolution 2.24.3

Detaylı Başlık Analizi

Mail sunucunun dns ismi ve makine ismi farklı olursa

Received: from smtp2.abc.com.tr (HELO smtp2.xyz.com.tr) (2.1.1.7)

by gelisimplatformu.org with SMTP; 29 Dec 2006 13:12:24 -0000

from satırında maili gönderen sunucunun smtp2.abc.com.tr olduğu gözüküyor, fakat aynı adrese dns sorgulaması yaptığımızda farklı bir isim çözüyorsa bu başlığın değiştirilmiş olduğundan şüphelenilebilir.

Bazen de maili gönderen makinenin DNS ismi ile kendi üzerinde tanımlanmış ismi farklı olur ve Received kısmında iki farklı isim gözükür . Yukarıdaki örnek aslında tam da bunu göstermektedir: makinenin ismi smtp2.xyz.com.tr olarak tanımlanmış fakat dns kaydı smtp2.abc.com.tr şeklindedir.

Webmail Üzerinden Gönderilen E-postalarda Başlık Bilgileri

Gmail, Yahoo, Hotmail gibi webmail servisleri üzerinden gönderilen e-postalarda gönderici MTA webmailin çalıştığı sistem olduğu için received alanlarından bilgi edinilemez(bazı istisnalar vardır).

Yani webmail üzerinden gönderilen e-postalardaki Received alanları incelenecek olursa kullanıcının değil webmail sisteminin ip adreslerine ulaşılır. Webmail üzerinden gönderilen e-postalarda X- başlıkları takip edilerek göndericinin ip adresi hakkında bilgi edinilebilir.

E-posta Başlık Bilgilerini İsteğe Göre Düzenleme

E-posta başlık bilgileri e-posta istemci yazılımları, aracı smpt sunucular tarafından eklenebileceği gibi isteğe göre de ekleme/çıkarmalar yapılabilir. Özellikle spam göndericiler AntiSpam yazılımlarını atlatabilmek için bu tip değişiklikleri sık sık kullanırlar.

İsteğe Göre Düzenlenmiş e-posta Gönderimi

Aşağıdaki loglar bir smtp sunucu üzerinden başlık bilgilerinin isteğe göre düzenlenerek gönderilmesi esnasında alınmıştır. SMTP sunucular üzerinden başlık bilgilerini değiştirmek için ek bir programa ihtiyaç duyulmaz, 25. Porta telnet çekerek ilgili smtp komutları kullanılabilir.

Dikkat edilmesi gereken husus e-posta başlık bilgilerini Data kısmından sonra eklenmesi gerektiğidir.

```
root@home-labs-fw#telnet 172.16.10.2 25
Trying 172.16.10.2...
Connected to 172.16.10.2.
Escape character is '^]'.
220 snort.openu.edu.tr ESMTP
EHLO firewallum-ben
250-snort.openu.edu.tr
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-PIPELINING
250 8BITMIME
MAIL FROM: kacak@lifeoverip.net
250 ok
RCPT TO: huzeyfe@lifeoverip.net
250 ok
DATA
354 go ahead
Received: from yolcu1.yollarbos.net (yolcu1.yollarbos.net [1.2.3.4]) by
sondurak.yollarbos.net (100.0.2) id 0021; Sun, May 20 2007 11:36:21
From: kacak@lifeoverip.net (Ismi Soylemez)
To: huzeyfe@lifeoverip.net
Date: Sun, May 20 2007 11:36:21
Message-Id: <kacak-qmail123456789@sondurak.yollarbos.net>
X-Mailer: EvYapimiThunderbird
Subject: Sahte mail dukkani?
```

Deneme maili...

.
250 ok 1179657667 qp 93701

QUIT
221 snort.openu.edu.tr
Connection closed by foreign host.

Görüleceği üzere bir e-postaya ait tüm başlık bilgilerini kendimiz düzenleyebiliriz. Bu e-postayı inceleyecek bir sistem yöneticisi aşağıdaki başlık bilgilerini görecektir.

...

Received: from 2007.open.edu.tr (HELO snort.openu.edu.tr) (19.7.2.8)
by mail.sistembil.com with SMTP; 20 May 2007 10:36:57 +0300

Received: (qmail 93701 invoked by uid 1013); 20 May 2007 10:36:45 -0000

Received: from yubam-sahte (HELO firewallum-ben) (19.7.2.8)
by snort.openu.edu.tr with SMTP; 20 May 2007 10:36:45 -0000

Received: from yolcu1.yollarbos.net (yolcu1.yollarbos.net [1.2.3.4]) by sondurak.yollarbos.net (100.0.2) id 0021; Sun, May 20 2007 11:36:21

From: kacak@lifeoverip.net (Ismi Soylemez)

To: huzeyfe@lifeoverip.net

Date: Sun, May 20 2007 11:36:21

Message-Id: <kacak-qmail123456789@sondurak.yollarbos.net>

X-Mailer: EvYapimiThunderbird

Subject: Sahte mail dukkani?

Deneme maili...

Yukardaki çıktıda ilk Received alanı sahte başlıktır sonraki başlık bilgileri smtp sunucular tarafından otomatik eklenmiştir.

Received alanları da değiştirilebildiğine göre gerçek gönderici nasıl bulunabilir?

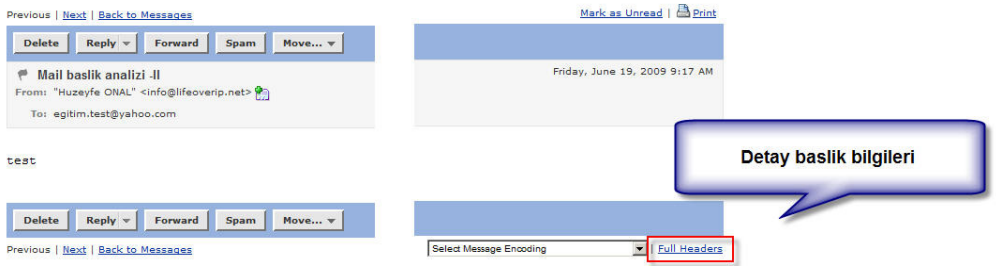
Her ne kadar Received alanları değiştirilebilse bile bu maili alan her SMTP sunucu Received başlığı ekleyecektir. E-posta başlıklarını okumayı bilen bir admin Received alanını yukardan aşağı okuyarak mailin kaynağını rahatlıkla tespit edebilir.

Bazen Received , from alanı boş mailler görürüz bunlar akıllı spamcilerin kendi makilerinde kullandıkları özel smtp servisleri kullanarak bu alanları sakladıkları bir yöntem sonucu oluşmuş olabilir.

Çeşitli E-posta Programlarında Başlık Bilgisi Alanı

Yahoo Webmail Üzerinden Başlık Bilgilerini İnceleme

Yahoo Webmail "Full Headers" linki üzerinden gelen e-postaların detay başlıklarına bakılmasına izin verir.

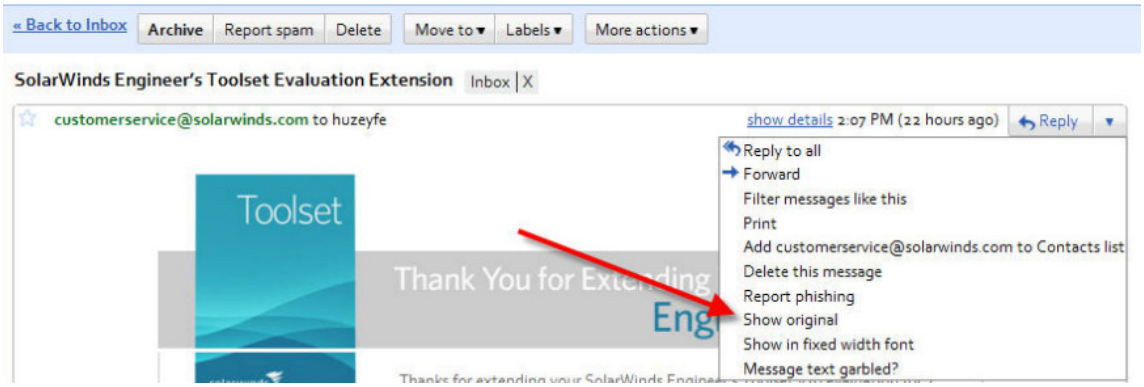


Yahoo Webmail Full Headers aracılığıyla gözüken başlık bilgileri:

From Huzeyfe ONAL Fri Jun 19 02:17:05 2009
Return-Path: <info@lifeoverip.net>
Received: from 91.93.119.80 (HELO mail.sistembil.com) (91.93.119.80) by mta146.mail.re4.yahoo.com with SMTP;
Received: from unknown (HELO ?10.20.4.1?) (info@lifeoverip.net@86.108.1.9) by mail.sistembil.com with SMTP; 19 Jun 2009 12:16:31 -0000
Message-ID: <4A3B5791.8090302@lifeoverip.net>
Date: Fri, 19 Jun 2009 12:17:05 +0300
From: Huzeyfe ONAL <info@lifeoverip.net> Add sender to Contacts
User-Agent: Thunderbird 2.0.0.21 (Windows/20090302)
To: egitim.test@yahoo.com
Subject: Mail baslik analizi -II

Gmail webmail üzerinden Başlık Bilgilerini İnceleme

Gmail gelen e-postalarda öntanımlı olarak detay başlık bilgilerini göstermez. E-posta açıldığında ekranın sağında kalan "show details">Show Original yolu takip edilirse detay başlık bilgilerine ulaşılabilir.

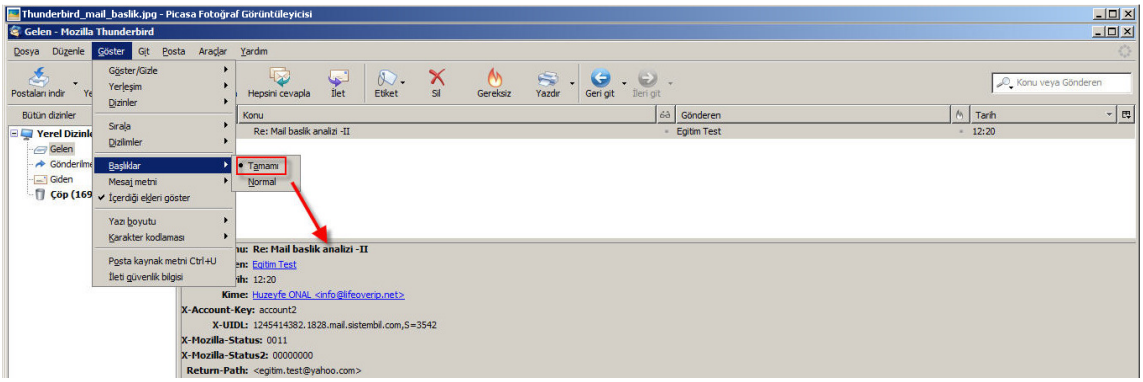


Google Webmail Full Headers aracılığıyla gözüken başlık bilgileri:

Delivered-To: huzeyfe.onal@gmail.com
Received: by 10.86.51.14 with SMTP id y14cs73672fgy;
Thu, 18 Jun 2009 04:08:23 -0700 (PDT)
Received: by 10.204.124.7 with SMTP id s7mr1231274bkr.105.1245323303274;
Thu, 18 Jun 2009 04:08:23 -0700 (PDT)
Return-Path: <customerservice@solarwinds.com>
Received: from mail.sistembil.com ([91.93.119.80])
by mx.google.com with SMTP id 22si2388329bwz.14.2009.06.18.04.08.21;
Thu, 18 Jun 2009 04:08:21 -0700 (PDT)
Received: (qmail 93579 invoked by uid 89); 18 Jun 2009 14:07:39 -0000
Delivered-To: huzeyfe@lifeoverip.net
Received: (qmail 93570 invoked by uid 89); 18 Jun 2009 14:07:39 -0000
Received: from coronalrain.solarwinds.com (65.89.32.74)
by mail.sistembil.com with SMTP; 18 Jun 2009 14:07:37 -0000
Received: from AUS-WWW-02 ([1.10.11.11])
by coronalrain.solarwinds.com (8.13.1/8.13.1) with ESMTP id n5IB8DeL028881
for <huzeyfe@lifeoverip.net>; Thu, 18 Jun 2009 06:08:15 -0500
Message-Id: <200906181108.n5IB8DeL028881@coronalrain.solarwinds.com>
From: customerservice@solarwinds.com
To: huzeyfe@lifeoverip.net
Date: 18 Jun 2009 06:07:58 -0500
Subject: =test

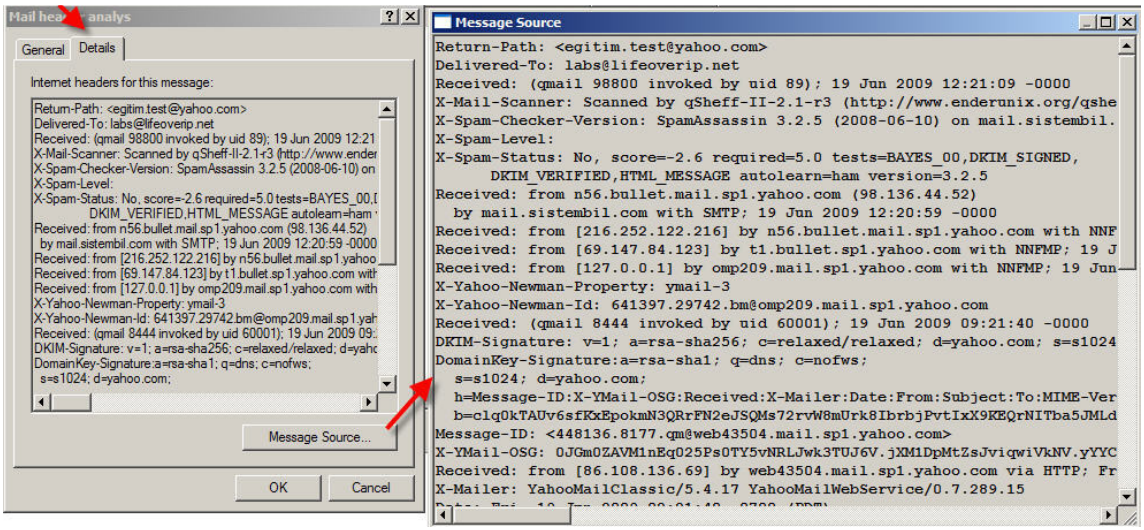
Thunderbird Üzerinden Başlık Bilgilerini Okuma

Ana menünden Göster>Başlıklar>Tamamı yolu izlenerek gelen e-postalara ait detay başlık bilgileri incelenebilir.



Outlook Express Üzerinden Başlık Bilgilerini Okuma

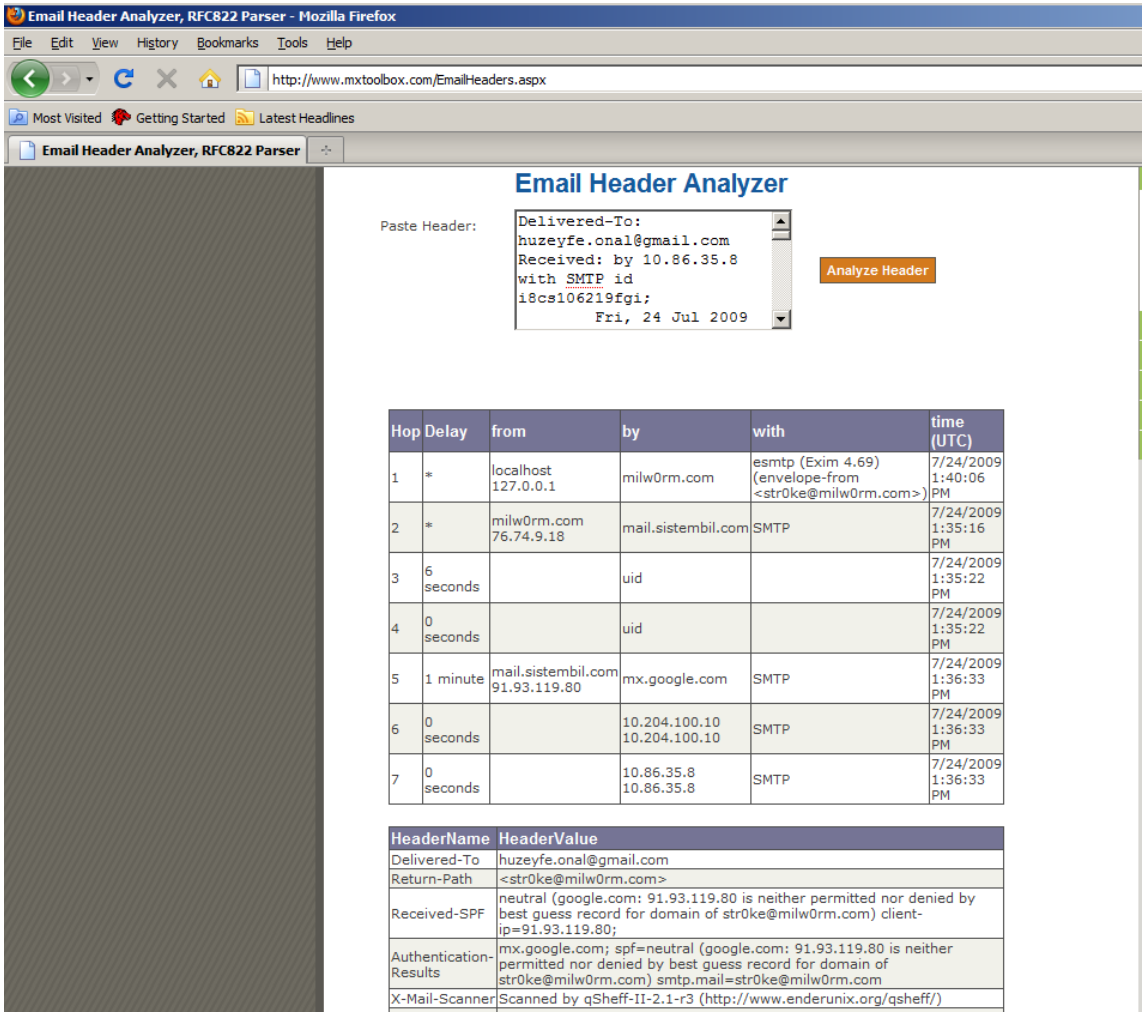
Detay başlık bilgilerini okumak için ilgili e-postanın üzerinde sağ tıklayarak Özellikler seçilir ve sonrasında aşağıdaki ekran görüntüsü takip edilerek e-postanın detay başlık bilgilerine ulaşılabilir.



Hazır E-posta başık Analiz Yazılımları

E-posta başlık bilgilerini yorumlamakta zorluk çekiyorsanız bu işi daha kolay yapmanın yolu hazır web araçlarını kullanmaktır. Internet üzerinde e-posta başlık bilgilerini düzenli bir şekilde gösteren ve yorumlayabilen çesitli web sayfalarına ulaşabilirsiniz.

Yorumlamakta güçlük çekerseniz bu sayfalardan birine tüm mail basligini aktarmaniz yeterli olacaktir.



Hop	Delay	from	by	with	time (UTC)
1	*	localhost 127.0.0.1	milw0rm.com	esmtp (Exim 4.69) (envelope-from <str0ke@milw0rm.com>)	7/24/2009 1:40:06 PM
2	*	milw0rm.com 76.74.9.18	mail.sistembil.com	SMTP	7/24/2009 1:35:16 PM
3	6 seconds		uid		7/24/2009 1:35:22 PM
4	0 seconds		uid		7/24/2009 1:35:22 PM
5	1 minute	mail.sistembil.com 91.93.119.80	mx.google.com	SMTP	7/24/2009 1:36:33 PM
6	0 seconds		10.204.100.10 10.204.100.10	SMTP	7/24/2009 1:36:33 PM
7	0 seconds		10.86.35.8 10.86.35.8	SMTP	7/24/2009 1:36:33 PM

HeaderName	HeaderValue
Delivered-To	huzeyfe.onal@gmail.com
Return-Path	<str0ke@milw0rm.com>
Received-SPF	neutral (google.com: 91.93.119.80 is neither permitted nor denied by best guess record for domain of str0ke@milw0rm.com) client-ip=91.93.119.80;
Authentication-Results	mx.google.com; spf=neutral (google.com: 91.93.119.80 is neither permitted nor denied by best guess record for domain of str0ke@milw0rm.com) smtp.mail=str0ke@milw0rm.com
X-Mail-Scanner	Scanned by qSheff-II-2.1-r3 (http://www.enderunix.org/qsheff/)

http://www.mxtoolbox.com/EmailHeaders.aspx

Yahoo Webmail Üzerinden Gönderilen E-posta İncelemesi

Yahoo Webmail üzerinden gönderilen e-postalarda göndericinin IP adresi gözükmektedir.

Eğer gönderici proxy kullanmadıysa ilk Received satırından From: kısmı maili gönderenin IP adresidir. Benzer şekilde bazı maillerde göndericinin IP adresi X-Originating-IP: başlık bilgisinde bulunur.

```
Return-Path: <egitim.test@yahoo.com>
Delivered-To: labs@lifeoverip.net
Received: (qmail 98800 invoked by uid 89); 19 Jun 2009 12:21:09 -0000

Received: from n56.bullet.mail.sp1.yahoo.com (98.136.44.52)
  by mail.sistembil.com with SMTP; 19 Jun 2009 12:20:59 -0000
```

Received: from [216.252.122.216] by n56.bullet.mail.sp1.yahoo.com with NNFMP; 19 Jun 2009 09:21:40 -0000
Received: from [69.147.84.123] by t1.bullet.sp1.yahoo.com with NNFMP; 19 Jun 2009 09:21:40 -0000

Received: from [127.0.0.1] by omp209.mail.sp1.yahoo.com with NNFMP; 19 Jun 2009 09:21:40 -0000
Received: from [86.108.1.2] by web43504.mail.sp1.yahoo.com via HTTP; Fri, 19 Jun 2009 02:21:40 PDT

X-Mailer: YahooMailClassic/5.4.17 YahooMailWebService/0.7.289.15
Date: Fri, 19 Jun 2009 02:21:40 -0700 (PDT)
From: Egitim Test <egitim.test@yahoo.com>
Subject: Mail header analys
To: labs@lifeoverip.net

Hotmail Webmail Üzerinden Gönderilen E-posta İncelemesi

Hotmail üzerinden gönderilen maillerde en önemli başlık X-Originating-IP alanıdır. Bu alandaki bilgi e-postayı gönderenin IP adresini gösterir.

Delivered-To: huzeyfe.onal@gmail.com
Received: by 10.86.54.4 with SMTP id c4cs124014fga;
Tue, 11 Aug 2009 00:00:04 -0700 (PDT)
Return-Path: <abc@hotmail.com>
Received: from mail.sistembil.com ([91.93.119.80])
by mx.google.com with SMTP id 23si23570509mun.13.2009.08.11.00.00.03;
Tue, 11 Aug 2009 00:00:04 -0700 (PDT)
Received: (qmail 22896 invoked by uid 89); 11 Aug 2009 06:58:22 -0000
Delivered-To: huzeyfe@lifeoverip.net
Received: (qmail 22891 invoked by uid 89); 11 Aug 2009 06:58:22 -0000
Received: from col0-omc4-s19.col0.hotmail.com (65.55.34.221)
by mail.sistembil.com with SMTP; 11 Aug 2009 06:58:15 -0000
Received: from COL103-W24 ([65.55.34.200]) by col0-omc4-s19.col0.hotmail.com with Microsoft SMTPSVC(6.0.3790.3959);
Mon, 10 Aug 2009 23:59:54 -0700
X-Originating-IP: [88.228.40.6]
From: Mustafa ... <abc@hotmail.com>
To: <huzeyfe@lifeoverip.net>
Subject: RE: [tcpip-09] Re: Egitim Notlari & Degerlendirme Formu
Date: Tue, 11 Aug 2009 09:59:53 +0300
X-OriginalArrivalTime: 11 Aug 2009 06:59:54.0007 (UTC)
FILETIME=[54282270:01CA1A51]

Gmail Webmail Üzerinden Gönderilen E-posta İncelemesi

Gmail üzerinden gönderilen e-postalarda kullanıcıya ait özel bilgiler gizlenmektedir(http://mail.google.com/support/bin/answer.py?answer=26903). Dolayısıyla Gmail üzerinden gönderilen bir e-postayı takip için yapılacak tek işlem

Google'la iletişime geçerek ilgili logları istemek olacaktır ki bu da yasal süreçler olmadan gerçekleşmez.

Gmail'i web üzerinden değil de SMTP üzerinden kullananlar için böyle bir gizleme yok. E-posta gönderenin tüm bilgileri başlıklardan edinilebilir.