BGA

BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

Adli Bilişim Açısından E-posta Sistemi

@2014

Örnek Eğitim Notu

bilgi@bga.com.tr

Bölüm İçeriği

- E-posta çalışma mantığı
  - SMTP, POP, IMAP protokolleri
  - SMTP Ve DNS ilişkisi
- SMTP 25. port ve 587(Submission) farklılıkları
- E-posta başlık incelemesi
  - E-posta göndericisinin IP adresi ve lokasyonunun bulunması
  - Sahte e-posta başlık bilgileri kullanarak posta gönderimi
  - Yahoo webmail üzerinden gönderilen e-postaların incelenmesi
  - Gmail webmail üzerinden gönderilen e-postaların incelenmesi
  - Hotmail webmail üzerinden gönderilen e-postaların incelenmesi
  - Diğer web tabanlı e-posta servisleri üzerinden gönderilen postaların incelenmesi
- Anlık e-posta gönderim servisleri
- Facebook üzerinden gönderilen mesajların kimliğini belirleme
- Hotmail, Yahoo, Gmail, gibi webmail hizmetlerinde e-posta göndericisini bulma
- Spam mantığı ve incelemesi
- Spam gönderen firmaların bulunması
- E-posta takip programları ve çalışma yapıları
  - E-postanızı kaç kişi okudu?
  - E-postanızı hangi bilgisayarlardan kimler okudu?
  - E-postanız kaç kişiye iletildi(forward)

E-Posta Nedir?

- Sosyal hayattaki posta servisinin siber dünyaya uyarlanmış hali
- Günümüz iletişim dünyasının en önemli haberleşme araçlarındandır
- Yakın gelecekte SMS'in yerini alması öngörülmektedir
- İş dünyasının en önemli iletişim aracıdır

E-posta Güvenliği

- Günümüz E-posta sistemlerinin büyük çoğunluğu güvensiz iletişim kanalları üzerinden akmaktadır.
- E-posta eğer SSL destekli kullanılmıyorsa aradaki iletişim kanallarından izlenebilir.
  - Sadece kullanıcı ile e-posta sunucu arasını şifreler
- E-posta eğer PKI altyapısıyla kullanılmıyorsa bir şekilde aradaki sistemler tarafından izlenir.

E-posta Takibi

- E-posta nasıl izlenebilir?
- E-postayı kontrol eden ağ çıkışında izlenebilir.
- E-posta'nın gönderildiği mail sunucu üzerinde izlenebilir.
- E-postanın gönderildiği hedef sistem ağında izlenebilir.
- E-posta'nın ulaştığı hedef mail sunucu üzerinde izlenebilir.
- ISP'lerde izlenebilir.
- Kısaca e-posta trafiğinin kullandığı yol üzerinde iyi/kötü niyetli birileri tarafından izlenebilir.

Neden E-posta Güvenliği?

- E-posta kullanılarak yapılabilecekler:
  - Facebook hesabına girme
  - Paypal hesabına girerek akçeli işler çevirme
  - E-posta sahibinin üzerine kayıtlı alan adlarını hackleme
  - E-posta sahibi üzerine kayıtlı alan adında kullanılan mail sunucu(@sirket.com.tr) trafiğini okuma
  - Başkasının adına e-posta gönderme
  - E-posta sahibinin gizli bilgilerini okuma
  - E-posta sahibinin finansal ve şirket bilgilerine erişim
  - E-posta sahibinin web arama geçmişini izleme
  - Gmail->Gdocs

E-Posta Temelleri

- Her tür ikili veri taşıyabilir
- TCP protokolü üzerinden çalışmaktadır
- IP spoofing yapılamaz!
- Başlık bilgileri analiz aşamasında oldukca önemlidir.
- Proxy sistemler üzerinden e-posta gönderilebilir
  - Yarı ip spoofing
- Sahte E-posta gönderimi mümkündür!

Genel Kavramlar

- Mail User Agent=E-posta istemcisi
  - Mozilla Thunderbird, Outlook
- MTA(Mail Transfer Agent)=SMTP protokolü üzerinden mail dağıtımı yapan sistemler
  - Qmail, postfix
- SMTP, POP, IMAP=Mail gönderim, alım protokolleri
- MIME=E-posta ile ASCII olmayan verileri taşımak için geliştirilen eklenti
  - Ses, resim vs gibi ikili dosyaları taşımak için kullanılır.

MIME Örneği

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="frontier"

This is a message with multiple parts in MIME format.
--frontier
Content-Type: text/plain

This is the body of the message.
--frontier
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+VGhpcyBpcyB0aGUg
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==
--frontier--
```

E-posta Sistemi Nasıl Çalışır?

- E-posta gerçek hayattaki posta servisi örnek alınarak oluşturulmuş bir servistir.
  - Mektup yazılır->Zarf içerisine konulur->Üzerine Gönderici-Alıcı bilgileri yazılır->Postahaneye bırakılır->Postacı alır->Üzerindeki adres bilgilerine göre hedefine ulaştırır.
- E-posta içeriği hazırlanır->Gönderici-Alıcı belirlenir->Gönder tuşuna basılır
  - MX kaydı sorgulanır, hedef mail sunucu bulunur ve iletişime geçilip, e-posta bırakılır.
- Aralarındaki fark birinde insan diğerinde yazılım kullanılmasıdır.

E-posta Gönderici Kontrolü

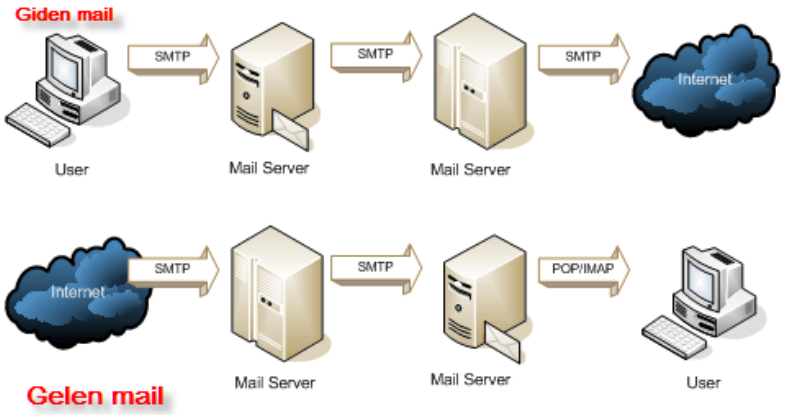
- Gerçek dünya:
  - İsimsiz, sahte isimli, adresli mektuplar
- Siber dünya:
  - Sahte adreslerden, sahte isimlerle gönderilen e-postalar
- Her iki sistemde de göndericinin kimliğine ulaşmak zordur.
- E-posta sistemi tüm özellikleriyle kandırılmaya müsait bir yapıdadır.

E-posta Protokolleri

- Sık kullanılan e-posta protokolleri
  - SMTP
    - Secure SMTP
  - POP
    - Secure POP
  - IMAP
    - Secure IMAP
  - MAPI
- Tüm protokoller TCP üzerinde çalışır.

SMTP

- Temel görevi e-posta dağıtımıdır.
  - Hem kullanıcı hem de diğer e-posta sunucularla iletişime geçen bileşen
- TCP port 25 kullanır
- Mail gönderim ve dağıtım için farklı fonksiyonlara sahiptir.



Smtp|SPAM

- SMTP üzerinden yetkili yetkisiz herkes e-posta gönderebilir.
- Yetkisiz gönderilen e-postalar SPAM amaçlı kullanılabilir.
- E-posta sunucu eğer önlem alınmamışsa(Relay'a açık olma durumu) sunucu üzerinden istenilen özelliklerde e-posta gönderilebilir.
  - X şahsı adına, Y şahsına, Z içerikli...

Relay Kavramı

- Relay: E-posta sunucu üzerinden kişilere e-posta gönderim izninin verilmesi
- E-posta sunucular, sadece yetkili kişilerin e-posta göndermesi için yapılandırılmalıdır.
- E-posta sunucularda SMTP-Auth fonksiyonu kullanılarak (varsa bu özellik) kullanıcıların e-posta gönderim yetkisi kontrol edilebilir.
- Kullanıcının e-posta göndermesiyle , smtp sunucunun e-posta bırakması farklı işlemlerdir.

SMTP-Submission Farkı

- SMTP Nasıl Çalışır, Submission SMTP'e ne ek getirir?
- SMTP sunucular kendilerine gelen bir mail üzerinde iki tür işlem yapabilirler.
  - 1)Gönderilen mail domaini sistemde tanımlı ise kabul ederler.
  - 2)Gönderilen mail domaini sistemde tanımlı değilse hata dönerler
- Bir de sistemin relaya açık olma durumu vardır ki onda da mailin nerden nereye gönerildiğine bakılmaksızın işlem yapılır.
-

SMTP Auth

- Sıkı yapılandırılmış bir mail sunucuda kayıtlı kullanıcılar mail gönderebilmek icin SMTP AUTH(kimlik dogrulama) yöntemini kullanır. Böylece kullanıcı kendisini sisteme tanıtarak istediği yere mail gönderebilir.

- SMTP portu üzerinde SMTP auth özelliği isteğe bağlı olarak aktif edilir.(helo/ehlo komutlarıyla) Dolayısı ile SMTP portu üzerinden hem normal kullanıcılar mail gönderme işlemi yapar hem de internetteki diğer smtp sunucuları bağlantı kurarak mail bırakır.

Uyarı!

- Eğer 25 smtp portu üzerinden zorunlu smtp auth yaptırılırsa internet üzerindeki mail sunuculardan mail almak imkansız hale gelir.

- SMTP’den ayrı bir porttan yine smtp protokolünü destekleyen fakat zorunlu smtp-auth isteyen bir servis çalıştırıyoruz(qmail, postfix, exim vs)
- Bu porttan bağlanan kullanıcı mail göndermeden önce mutlaka kendisini tanıtması gerekiyor.
- Böylece TTNet 25. portu kapatarak adsl abonelerinden yayılacak spamleri engelliyor.
- Normal kullanıcılar ayarlarını 587. port üzerinden yapacağı için mail gönderimlerinde problem çıkmıyor.

- Peki submission kullanmaya başlayınca sadece port mu değişecek?
  - Hayır!
- Submission portu SMTP portundan farklı olarak kendisine bağlanan her kullanıcıdan zorunlu smtp auth isteyecektir.
- Böylece 587 üzerinden sadece mail sunucularda tanımlı kullanıcılar mail gönderebilecek.
- Spam göndermek isteyen kişiler ilgili sistemde tanımlı değilse mesaj gönderemeyecekler.
- Yani sistemde iki tane smtp portu açılacak biri dışarıdan mail alımları için(yahoo, hotmail ve diğer mail sunucular)diğeri de ADSL abonelerinin mail göndermesi için auth gerektirecek bir port.

Önemli Sorular

- **Peki bu sistem dışardan gelecek spamları kesecek mi?**
- Hayır, zira dışarıdan gelen spamlar yine 25. porttan gelecekler. Ama amaç zaten dışarıdan gelen spamleri kesmek değil, TTNet den spam gönderilmesini engellemek.
- **Firewall'dan 587. portumu 25. porta yönlendirsem çözüm olur mu?**
- Evet kısa vadede bir çözüm olur fakat spamciler size 25. porttan değil de 587. porttan mail gönderirlerse birşey yapamazsınız.

POP

- Post Office Protocol
  - Ağ üzerinden e-posta alma protokolü
  - POP1, POP2 ve günümüzde kullanılan sürümü POP3 olmak üzere üç versiyonu bulunmaktadır
  - TCP port 110 kullanılır
- SMTP'den farkı:
  - SMTP e-posta dağıtımı için kullanılır
  - POP, e-postayı son kullanıcının alması için kullanılır
- Basit bir yapıya sahiptir

POP3 Komutları

- Telnet üzerinden POP3 destekli sunucuya bağlanıp e-postalar okunabilir.
- Temel komutlar
  - Yetkilendirme aşaması
    - User ahmet
    - Pass veli
  - List
  - Retr mail_numarası

```
root@bt:~# telnet mail.lifeoverip.net 110
Trying 91.93.119.80...
Connected to lifeoverip.net.
Escape character is '^]'.
+OK BGA is ready.
user test1@bga.com.tr
+OK
pass test1
+OK Logged in.
list
+OK 0 messages:
.
retr 1
-ERR There's no message 1.
quit
+OK Logging out.
Connection closed by foreign host.
root@bt:~#
```

Klasik POP islemleri

Sniffer POP3 Analizi

pop3.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.109	91.93.119.80	TCP	59390 > pop3 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV=1248432 TSER=0 WS=5
2	0.009822	91.93.119.80	192.168.1.109	TCP	pop3 > 59390 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=3 SACK_PERM=1 TSV=541
3	0.009871	192.168.1.109	91.93.119.80	TCP	59390 > pop3 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSV=1248435 TSER=54151999
4	0.018903	91.93.119.80	192.168.1.109	POP	S: +OK BGA is ready.
5	0.018920	192.168.1.109	91.93.119.80	TCP	59390 > pop3 [ACK] Seq=1 Ack=20 Win=5856 Len=0 TSV=1248438 TSER=54152008
6	6.510233	192.168.1.109	91.93.119.80	POP	C: USER test1@bga.com.tr
7	6.519884	91.93.119.80	192.168.1.109	POP	S: +OK
8	6.519898	192.168.1.109	91.93.119.80	TCP	59390 > pop3 [ACK] Seq=24 Ack=25 Win=5856 Len=0 TSV=1250388 TSER=54158508
9	8.516881	192.168.1.109	91.93.119.80	POP	C: PASS test"1
10	8.625833	91.93.119.80	192.168.1.109	TCP	pop3 > 59390 [ACK] Seq=25 Ack=37 Win=66240 Len=0 TSV=54160615 TSER=1250988
11	10.535913	91.93.119.80	192.168.1.109	POP	S: -ERR Authentication fail
12	10.535947	192.168.1.109	91.93.119.80	TCP	59390 > pop3 [ACK] Seq=37 Ack=54 Win=5856 Len=0 TSV=1251593 TSER=54162524
13	13.433547	192.168.1.109	91.93.119.80	POP	C: PASS test1
				P	pop3 > 59390 [ACK] Seq=54 Ack=49 Win=66224 Len=0 TSV=54165532 TSER=1252463
				P	S: -ERR No username given.
				P	59390 > pop3 [ACK] Seq=49 Ack=79 Win=5856 Len=0 TSV=1253094 TSER=54167527
				P	C: USER test1@bga.com.tr
				P	S: +OK
				P	59390 > pop3 [ACK] Seq=72 Ack=84 Win=5856 Len=0 TSV=1254751 TSER=54173050
				P	C: PASS test1
				P	S: +OK Logged in.
				P	59390 > pop3 [ACK] Seq=84 Ack=100 Win=5856 Len=0 TSV=1256016 TSER=54177264

(632 bits)
Dst: Cisco-Li_f1:33:2e (00:22:6b:f1:33:2e)
st: 91.93.119.80 (91.93.119.80)
Dst Port: pop3 (110), Seq: 24, Ack: 25, Len: 13

Wireshark: Capture Options

Capture

Interface: Local — Realtek RTL8168C/8111C PCI-E Gigabit Ethernet NIC: \Device\NPF

IP address: fe80::f08d:1392:82ac:8ba9, 192.168.1.100

Link-layer header type: Ethernet — Wireless Settings

☑ Capture packets in promiscuous mode — Remote Settings

☐ Capture packets in pcap-ng format (experimental) — Buffer size: 1 megabyte(s)

☐ Limit each packet to 1 bytes

Capture Filter: tcp port 110

pop3 için

Capture File(s)

File: Browse...

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

```
0000  00 22 6b f1 33 2e 08 00  27 31 96 22 08 00 45 10   ."k.3... '1."..E.
0010  00 41 29 83 40 00 40 06  7c 61 c0 a8 01 6d 5b 5d   .A).@.@. |a...m[]
0020  77 50 e7 fe 00 6e b8 c6  25 e6 f2 98 67 6e 80 18   wP...n.. %...gn..
0030  00 b7 94 f6 00 00 01 01  08 0a 00 13 16 ac 03 3a   ........ .......:
0040  64 ac 50 41 53 53 20 74  65 73 74 22 31 0d 0a      d.PASS t est"1..
```

IMAP

- Internet Mail Access Protocol
  - Pop3 benzeri mail alım protokolüdür
  - POP3'e oranla daha karmaşık bir yapıya sahiptir
  - TCP port 143 kullanır
- IMAP'in avantajları
  - E-postaları sunucu üzerinde saklayabilme
  - Paylaştırılmış e-posta kutusu kullanımı
  - Gelişmiş çevrimdışı çalışma imkanı
  - Filtreleme imkanı
    - Sadece seçilmiş e-postaların istemciye indirilmesi...

IMAP Komutları

- Telnet kullanarak IMAP destekli sunucuya bağlanarak e-postalar okunabilir.
- POP3'den farklı komut dizgisine sahiptir:


```
root@bt:~# telnet mail.lifeoverip.net 143
Trying 91.93.119.80...
Connected to lifeoverip.net.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS AUTH=PLAIN] BGA is ready.
a login test1@bga.com.tr test1
a OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE SORT SORT=DISPLAY THREAD=REFERENCES THRE
SELECT IDLE CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITI
T-STATUS] Logged in
B select INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1298279418] UIDs valid
* OK [UIDNEXT 1] Predicted next UID
* OK [HIGHESTMODSEQ 1] Highest
B OK [READ-WRITE] Select completed.
a logout
* BYE Logging out
a OK Logout completed.
Connection closed by foreign host.
root@bt:~#
```

Sniffer IMAP Analizi

imap.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.109	91.93.119.80	TCP	35003 > imap [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV=1325063 TSER=0 WS=5
2	0.008596	91.93.119.80	192.168.1.109	TCP	imap > 35003 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=3 SACK_PERM=1 TSV=1822
3	0.008619	192.168.1.109	91.93.119.80	TCP	35003 > imap [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSV=1325066 TSER=1822271160
4	0.019376	91.93.119.80	192.168.1.109	IMAP	Response: * OK [CAPABILITY IMAP4re
5	0.019402	192.168.1.109	91.93.119.80	TCP	35003 > imap [ACK] Seq=1 Ack=107 Win=5856 Len=0 TSV=1325069 TSER=1822271168
6	10.350490	192.168.1.109	91.93.119.80	IMAP	Request: a login test1@bga.com.tr
7	10.363584	91.93.119.80	192.168.1.109	IMAP	Response: a OK [CAPABILITY IMAP4re
8	10.363624	192.168.1.109	91.93.119.80	TCP	35003 > imap [ACK] Seq=33 Ack=392 Win=6912 Len=0 TSV=1328172 TSER=1822281513
9	24.031546	192.168.1.109	91.93.119.80	IMAP	Request: B select INBOX
10	24.042962	91.93.119.80	192.168.1.109	IMAP	Response: * FLAGS (\Answered \Flag
11	24.042991	192.168.1.109	91.93.119.80	TCP	35003 > imap [ACK] Seq=49 Ack=702 Win=8000 Len=0 TSV=1332276 TSER=1822295190
12	36.073804	192.168.1.109	91.93.119.80	IMAP	Request: a logout
13	36.088744	91.93.119.80	192.168.1.109	IMAP	Response: * BYE Logging out
14	36.088789	192.168.1.109	91.93.119.80	TCP	35003 > imap [ACK] Seq=59 Ack=721 Win=8000 Len=0 TSV=1335890 TSER=1822307231
15	36.088830	91.93.119.80	192.168.1.109	IMAP	Response: a OK Logout completed.
16	36.089125	192.168.1.109	91.93.119.80	TCP	35003 > imap [FIN, ACK] Seq=59 Ack=746 Win=8000 Len=0 TSV=1335890 TSER=1822307231
17	36.104752	91.93.119.80	192.168.1.109	TCP	imap > 35003 [ACK] Seq=746 Ack=60 Win=66232 Len=0 TSV=1822307246 TSER=1335890

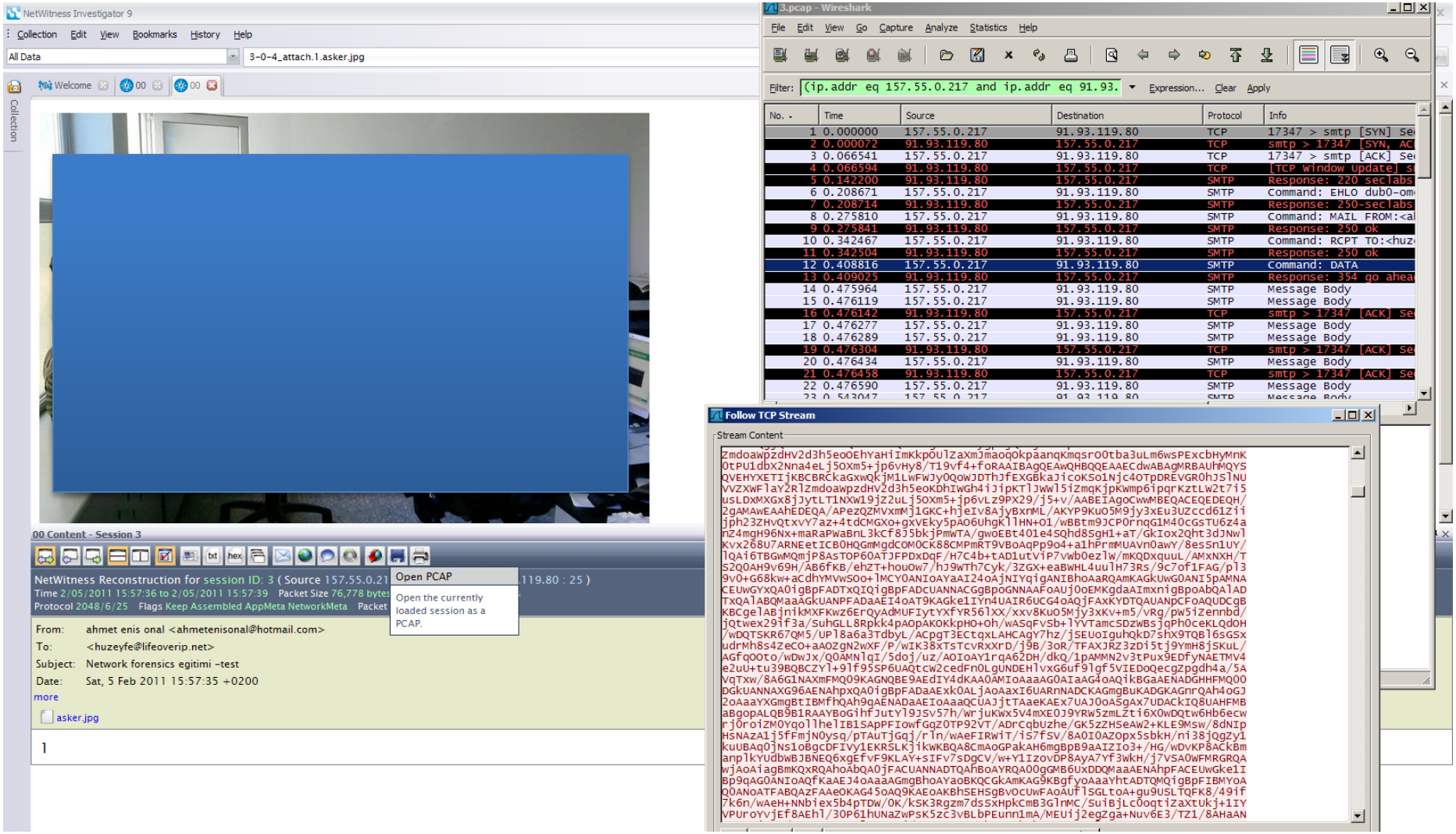
```
⊞ Frame 9: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
⊞ Ethernet II, Src: CadmusCo_31:96:22 (08:00:27:31:96:22), Dst: Cisco-Li_f1:33:2e (00:22:6b:f1:33:2e)
⊞ Internet Protocol, Src: 192.168.1.109 (192.168.1.109), Dst: 91.93.119.80 (91.93.119.80)
⊞ Transmission Control Protocol, Src Port: 35003 (35003), Dst Port: imap (143), Seq: 33, Ack: 392, Len: 16
⊟ Internet Message Access Protocol
  ⊟ B select INBOX\r\n
      Request Tag: B
      Request: select INBOX
```

```
0000  00 22 6b f1 33 2e 08 00  27 31 96 22 08 00 45 10   ."k.3... '1."..E.
0010  00 44 fb 73 40 00 40 06  aa 6d c0 a8 01 6d 5b 5d   .D.s@.@. .m...m[]
0020  77 50 88 bb 00 8f a7 0b  c3 8a a3 c3 69 61 80 18   wP...... ....ia..
0030  00 d8 94 f9 00 00 01 01  08 0a 00 14 54 31 6c 9d   ........ ....T1l.
0040  cf 29 42 20 73 65 6c 65  63 74 20 49 4e 42 4f 58   .)B sele ct INBOX
0050  0d 0a                                              ..
```

E-posta Güvenliği Bileşenleri

- Güvenliğin bağlı olduğu bileşenler:
  - Gizlilik
  - Bütünlük
  - Erişebilirlik
- Her üç bileşen için çeşitli ek protokoller geliştirilmiştir.
- E-posta'nın %100 güvenilir olması için e-postayı alan ve gönderenin aynı algoritma ve yöntemleri kullanması gerekir.

E-posta Güvenliği(!)



Güvenli E-Posta Protokolleri

- Klasik e-posta protokolleri SSL desteklemez ve aradaki sistemler tarafından rahatlıkla okunup/değiştirilebilir.
- E-posta protokollerinin SSL destekli halleri
  - Secure SMTP
  - Secure POP
  - Secure IMAP
- Internetin temelini oluşturan SMTP cleartext çalışacak şekilde düşünüldüğü için kısa vadede SSL destekli yapıya geçilmesi mümkün görünmemektedir.

E-posta ve DNS İlişkisi

- E-posta sisteminin sağlıklı çalışabilmesi çeşitli etkenlere bağlıdır.
- Bu etkenlerin başında DNS gelir.
  - DNS olmadan E-posta servisi sağlıklı çalışamaz!
- DNS'in E-posta servisi ile olan ilişkisi:
  - Bir e-postanın hangi adrese teslim edileceği DNS(MX kayıtları) ile belirlenir
  - DNS çalışmazsa e-postalar teslim edilemez.
- DNS ile ilişkisi olan E-posta protokolü SMTP'dir.

E-posta DNS İlişkisi|Örnek

- Ahmet, arkadaşı Enis'e e-posta göndermek için adresini istemiştir.
  - Enis'in adresi: enis@lifeoverip.net
  - Ahmet'in adresi: ahmet@bga.com.tr
- Ahmet, Enis'e mail gönderebilmesi için öncelikli olarak Enis'e gönderilecek maillerin hangi IP adresine(hosta) gönderileceğini bulması gerekir.
- Bu bilgi lifeoverip.net MX kaydında yatar

MX Kayıt Tipi

- Bir domaine ait e-postaların hangi adrese teslim edileceği bilgisini tutan DNS kaydı
- Internet üzerinden anonim bir şekilde ulaşılabilir.
- E-posta sistemlerini yedekleme amaçlı birden fazla MX kaydı girilebilir.
- Düşük sayıya sahip olan MX kaydı daha öncelikli demektir.

MX Kaydı Sorgulama | Linux

```
root@bt:/var/www# dig MX gmail.com

; <<>> DiG 9.5.0-P2.1 <<>> MX gmail.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25004
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 9

;; QUESTION SECTION:
;gmail.com.                     IN      MX

;; ANSWER SECTION:
gmail.com.              1352    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.              1352    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.              1352    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              1352    IN      MX      10 alt1.gmail-smtp-in.l.google.com.
gmail.com.              1352    IN      MX      20 alt2.gmail-smtp-in.l.google.com.

;; AUTHORITY SECTION:
gmail.com.              194967  IN      NS      ns1.google.com.
gmail.com.              194967  IN      NS      ns2.google.com.
gmail.com.              194967  IN      NS      ns3.google.com.
gmail.com.              194967  IN      NS      ns4.google.com.
```

MX Kaydı Sorgulama | Windows

C:\Windows\system32\cmd.exe - nslookup

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\seclabs>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> set q=mx
> gmail.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
>
```

E-posta Adli Bilişim Analizi

- Disk üzerinde kaydedilmiş e-posta analizi
- Ağ üzerinden kayıt alınmış paketler içerisinden e-posta analizi
- Gönderilen, alınan e-posta başlık bilgilerinden gönderici/alıcı ve ara sistem tespiti
- “E-posta, bundan sonra SMTP yerine kullanılacaktır.”

E-posta Başlık Bilgisi

- Her e-posta bir adet başlık bir adet gövde kısmından oluşur
- Sosyal hayattaki Mektup+Zarf ilişkisine benzer
  - Zarf=başlık bilgileri
- Bir E-posta'nın tüm kimliğini barındırır
  - Kim, kime göndermiş
  - Hangi IP adresinden gönderilmiş(hangi ülke, hangi ile)
    - Şirket iç IP adresi
  - Hangi E-posta sunucuları dolaşmış
  - Hangi E-posta istemci yazılımı kullanılarak gönderilmiş
  - Hangi saat,saniyede gönderilmiş...

Başlık Bilgisi Örnek

E-posta başlık bilgileri

Konu: Re: [Fedora-ambassadors-list] Meeting Reminder: Thursday, Jeanuary 19, 2006, 14:00 UTC
Kimden: [redacted]
Gönderen: fedora-ambassadors-list-bounces@redhat.com
Cevapla: fedora-ambassadors-list@redhat.com
Tarih: 18.01.2006 22:55
Kime: fedora-ambassadors-list@redhat.com

X-Account-Key: account6
X-UIDL: 1137624669.26541.cc.kou.edu.tr,S=3363
X-Mozilla-Status: 0000
X-Mozilla-Status2: 00000000
Return-Path: <fedora-ambassadors-list-bounces@redhat.com>
Received: (qmail 26538 invoked by uid 1009); 18 Jan 2006 22:51:09 -0000
X-Mail-Scanner: Scanned by qSheff 1.0-r4 (http://www.enderunix.org/qsheff/)
Received: from hormel.redhat.com (209.132.177.30) by cc.kou.edu.tr with SMTP; 18 Jan 2006 22:51:07 -0000
Received: from listman.util.phx.redhat.com (listman.util.phx.redhat.com [10.8.4.110]) by hormel.redhat.com (Postfix) with ESMTP id 089C2733FE; Wed, 18 Jan 2006 15:55:47 -0500 (EST)
Received: from int-mx1.corp.redhat.com (int-mx1.corp.redhat.com [172.16.52.254]) by listman.util.phx.redhat.com (8.13.1/8.13.1) with ESMTP id k0IKtjKn031212 for <fedora-ambassadors-
Received: from mx1.redhat.com (mx1.redhat.com [172.16.48.31]) by int-mx1.corp.redhat.com (8.11.6/8.11.6) with ESMTP id k0IKtj130366 for <fedora-ambassadors-list@redhat.com>; Wed
Received: from www.fedoranews.org (www.fedoranews.org [64.34.165.170]) by mx1.redhat.com (8.12.11/8.12.11) with ESMTP id k0IKtjDH025410 for <fedora-ambassadors-list@redhat.com
Received: from fedoranews.org (localhost.localdomain [127.0.0.1]) by www.fedoranews.org (8.12.10/8.12.10) with ESMTP id k0IKti0T010351 for <fedora-ambassadors-list@redhat.com>; Wec
Message-Id: <20060118205423.M74373@fedora.redhat.com>
In-Reply-To: <13dbfe4f0601181245w3072cbfcqe7940a90d4cd5377@mail.gmail.com>
References: <7f617d270601181241i4129f36du87596dbc896f2958@mail.gmail.com> <13dbfe4f0601181245w3072cbfcqe7940a90d4cd5377@mail.gmail.com>
X-Mailer: Open WebMail 2.51 20050627
X-OriginatingIP: 128.149.158.197 ([redacted])
MIME-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
X-RedHat-Spam-Score: 0
X-loop: fedora-ambassadors-list@redhat.com
X-BeenThere: fedora-ambassadors-list@redhat.com
X-Mailman-Version: 2.1.5
Precedence: junk
List-Id: fedora-ambassadors-list.redhat.com
List-Unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-ambassadors-list>, <mailto:fedora-ambassadors-list-request@redhat.com?subject=unsubscribe>
List-Archive: <https://www.redhat.com/mailman/private/fedora-ambassadors-list>
List-Post: <mailto:fedora-ambassadors-list@redhat.com>

sunucuda hangi spam/virus programı tarafından kontrol edildigi

Hangi sunucuclardan gectigi

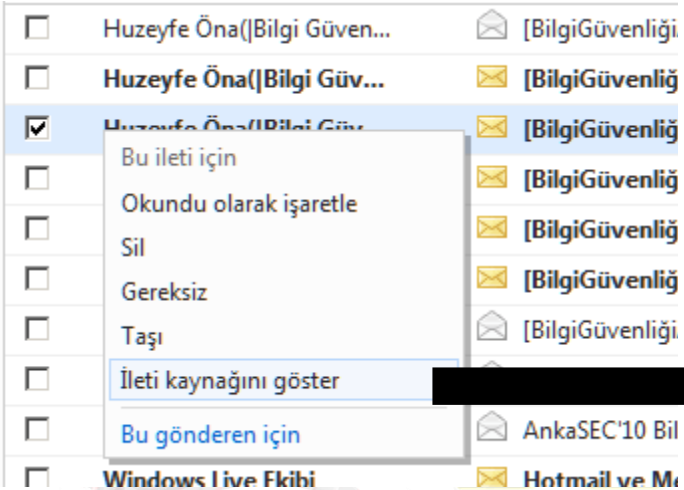
Kullanılan Mail Istemci Programı

Mail atılan Orjinal Adres

Başlık Bilgilerine Nereden Ulaşılır?

- Kullanılan programa göre başlık bilgilerine ulaşım yolu değişecektir.
- Hemen her sistem özet mod haricinde tüm başlık bilgilerini gösterecek detay moda sahiptir.

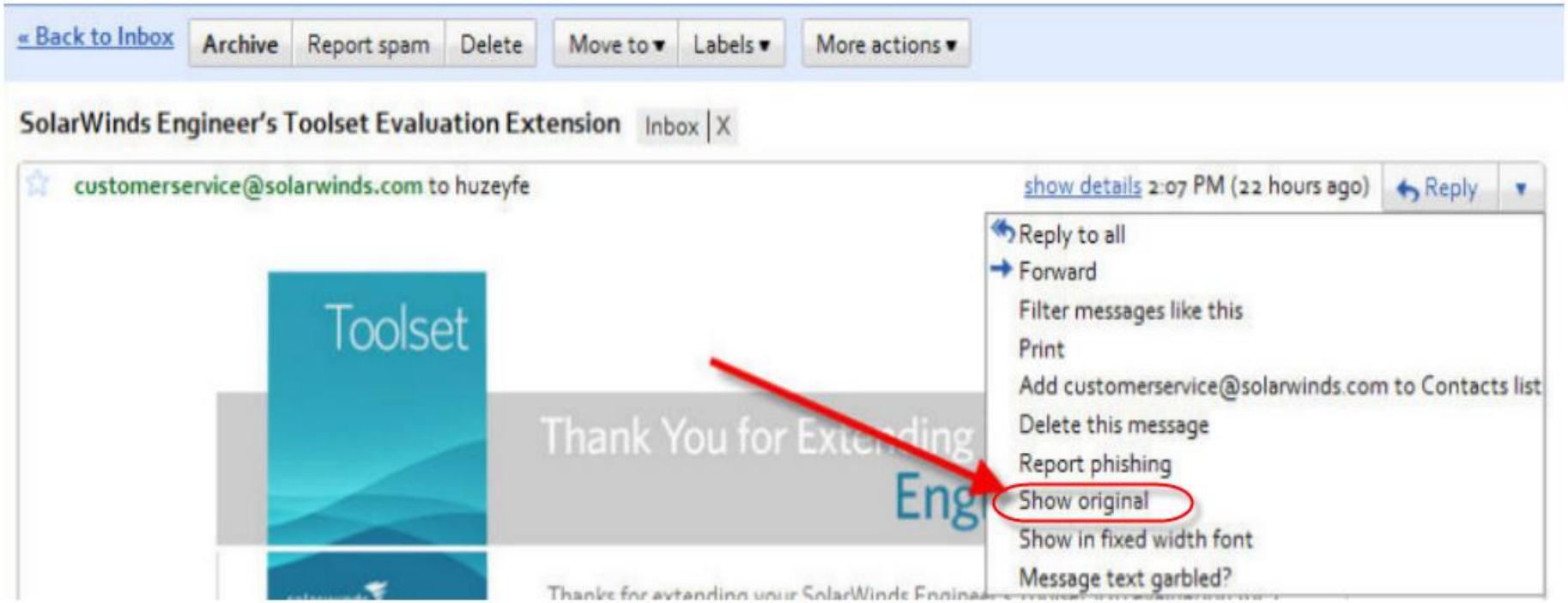
Hotmail ve Başlık Bilgileri




```
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtTQ0w9Mg==
X-Message-Status: n
X-SID-PRA: duyuru@bga.com.tr
X-AUTH-Result: NONE
X-Message-Info: JGTYoYF78jF7A5zAdQhKlNeW5V8D5fOFM9GkBw1gd5Kg7uj9cO0qgePCbS9nWUENak/JSHolG
Received: from seclabs.bga.com.tr ([91.93.119.87]) by col0-mc4-f21.Col0.hotmail.com with
        Fri, 4 Feb 2011 00:54:19 -0800
Received: (qmail 8810 invoked by uid 1011); 4 Feb 2011 08:53:45 -0000
Mailing-List: contact duyuru-help@bga.com.tr; run by ezmlm
Sender: <duyuru@bga.com.tr>
Precedence: bulk
X-No-Archive: yes
List-Post: <mailto:duyuru@bga.com.tr>
List-Help: <mailto:duyuru-help@bga.com.tr>
List-Unsubscribe: <mailto:duyuru-unsubscribe@bga.com.tr>
List-Subscribe: <mailto:duyuru-subscribe@bga.com.tr>
Delivered-To: mailing list duyuru@bga.com.tr
Delivered-To: moderator for duyuru@bga.com.tr
Received: (qmail 8698 invoked by uid 1011); 4 Feb 2011 08:45:35 -0000
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on seclabs.bga.com.tr
X-Spam-Level: ***
X-Spam-ASN: AS15169 209.85.212.0/24
X-Spam-Status: No, score=3.2 required=6.0 tests=AWL=-0.074,BAYES_99=4,
        DKIM_SIGNED=0.1,DKIM_VALID=-0.1,HTML_MESSAGE=0.001,RCVD_IN_DNSWL_LOW=-0.7
        seclabs.bga.com.tr 1215; Body=1 Fuz1=1 Fuz2=1 Reported 0 times.
        <dns:44.212.85.209.list.dnswl.org> [127.0.5.1] autolearn=no version=3.3.1
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=gamma;
        h=domainkey-signature:mime-version:sender:in-reply-to:references:from
         :date:x-google-sender-auth:message-id:subject:to:content-type;
        bh=Xmq9hFoDrNqZxeel04Yu3ZispLm24AL0JtMRD7sDp54=;
        b=WlXbvQV20fvb8ptU7FXwTHljY1/HQis4rqrtP5KYWJ5p3z7+ZvbmvTJAdYzgziTOrA
         3VXk9is4FZRNgVKBdOCGwSXmy3GBmdj1xR18OA3LJUW9wRQ6l3QntQLPNmNbb6+ITPGm
         lZS5nTUrM3r+mB8bwRAVG/6yn/jHN/eti5wmA=
DomainKey-Signature: a=rsa-sha1; c=nofws;
        d=gmail.com; s=gamma;
        h=mime-version:sender:in-reply-to:references:from:date
         :x-google-sender-auth:message-id:subject:to:content-type;
        b=aPWbyYDozLrwfzp65uBwRJ5bVOtpGGc7Vd/NUpZJvGcmlqAvpTqcQrtsKCeGyXVp5N
         rCwoHYCMdPwkEg6TE77MjuCoctQWf2In9X/+bJBfufewWKs4jDHH0lYi46wx+YcV1vTT
         Joy9uZnwsVosPtfXCIEcr3XJ6JgS6DP8ucsOg=
MIME-Version: 1.0
```

Gmail ve Başlık Bilgileri

- Show details→Show original adımları takip edilerek detay başlık bilgileri analiz edilebilir.

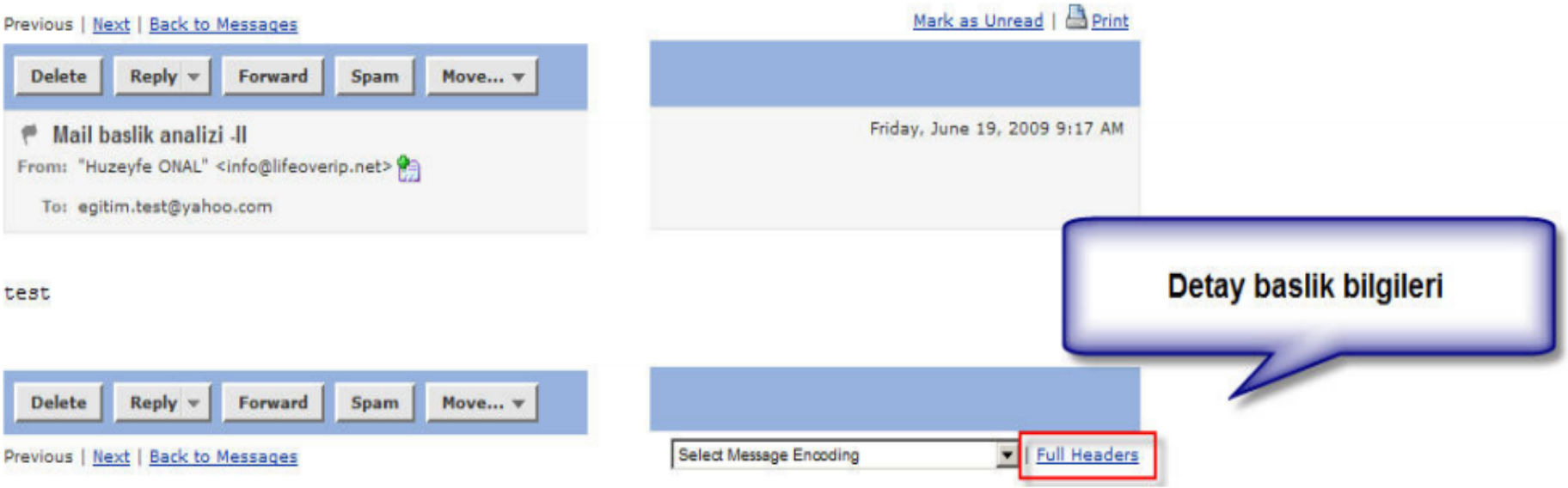


Gmail “Show Original” Özelliği

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

Yahoo! Ve Başlık Bilgileri

- Yahoo webmail, Full Headers linki kullanarak gelen e-postalara ait detay başlık bilgilerinin analizine izin verir.

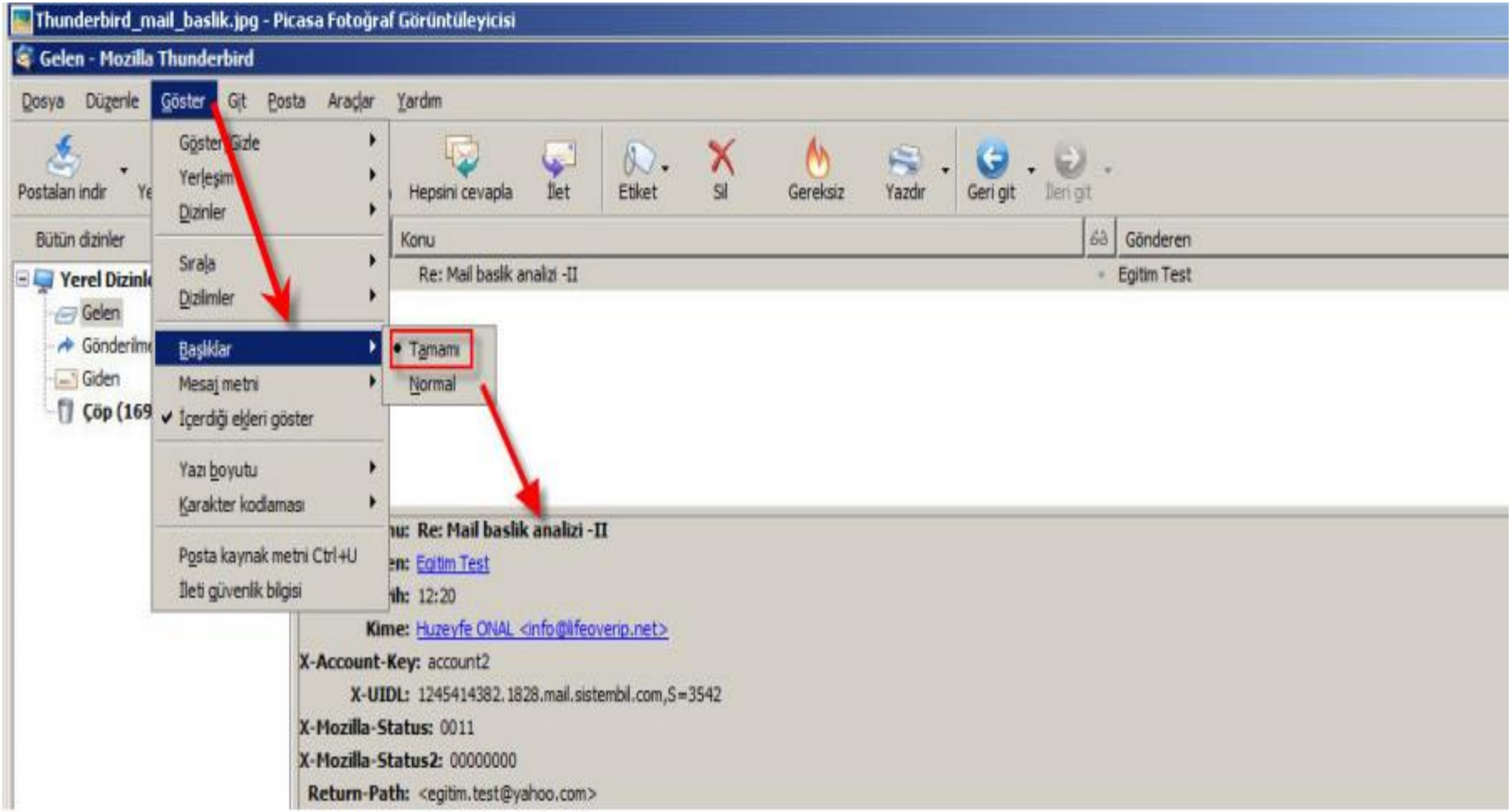


Yahoo Full Headers Özelliği

- Yahoo Full Headers aracılığıyla gözüken başlık bilgileri

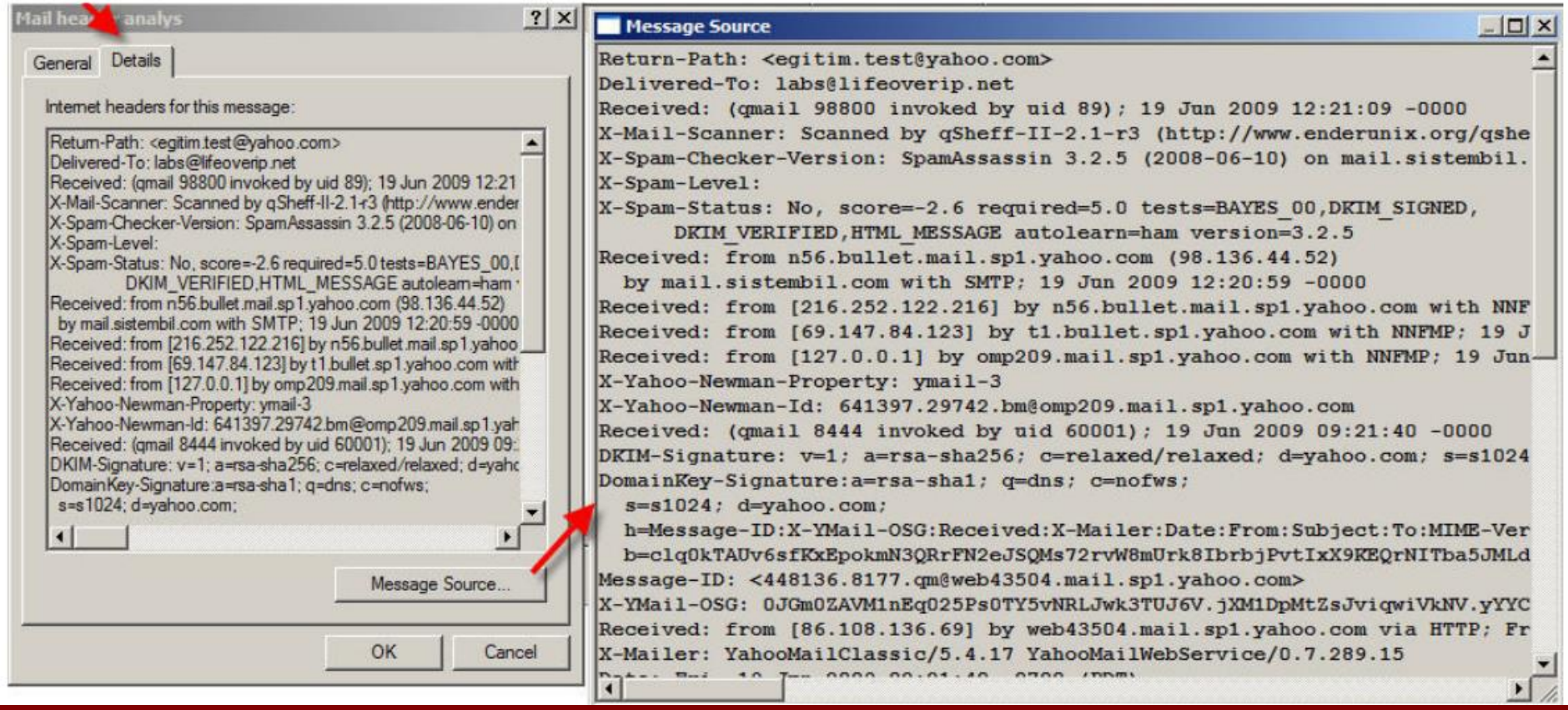
From Huzeyfe ONAL Fri Jun 19 02:17:05 2009
Return-Path: <info@lifeoverip.net>
Received: from 91.93.119.80 (HELO mail.sistembil.com) (91.93.119.80) by mta146.mail.re4.yahoo.com with SMTP;
Received: from unknown (HELO ?10.20.4.1?) (info@lifeoverip.net@86.108.1.9) by mail.sistembil.com with SMTP; 19 Jun 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

Thunderbird Başlık Bilgisi Okuma



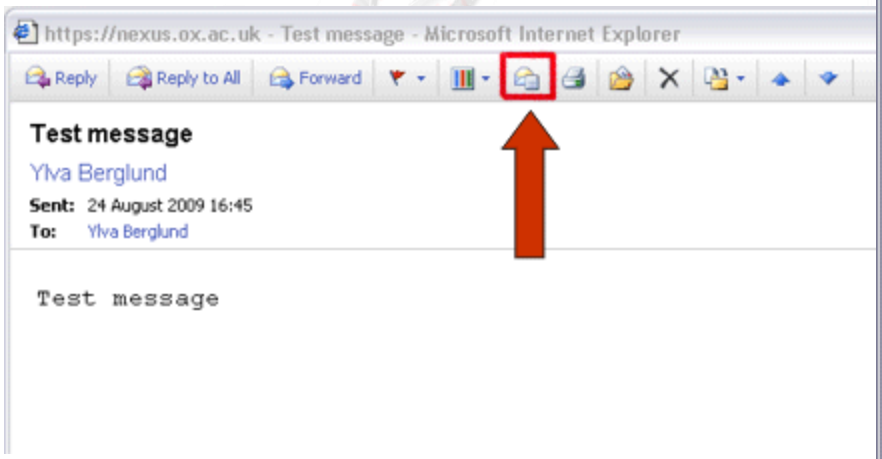
Outlook Express Başlık Bilgisi Okuma

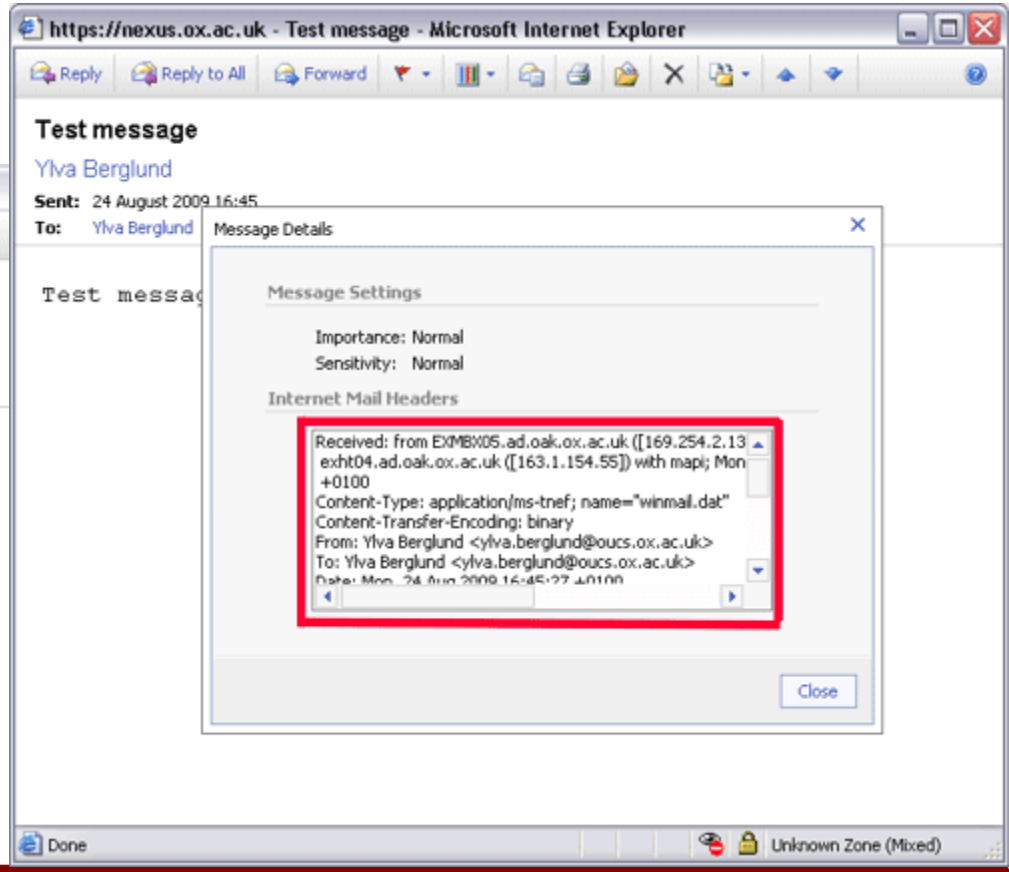
- Başlık bilgisi incelenmek istenen E-postaya sağ tıklanarak özellikler sekmesine gelinir.



OWA Başlık Bilgileri

- Message Details-->Internet Mail Headers





Başlık Bilgisi Yorumlama/Analiz

- E-posta başlıklarında geçen bilgiler son kullanıcının anlayamayacağı kadar teknik detay içerir.
- E-posta başlık bilgilerinden ilgili e-postaya ait tüm detaylar –eğer ara sunucular eksiltmediyse- edinilebilir.
- Bu bilgilerin ne işe yaradığını bilmeyen birisi onlien başlık analiz servislerini kullanarak başlık bilgisi analizi gerçekleştirebilir.

Online Başlık Bilgisi Analiz Hizmetleri

Email Header Analyzer, RFC822 Parser - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

Most Visited Getting Started Latest Headlines

Email Header Analyzer, RFC822 Parser

Email Header Analyzer

Paste Header:

```
Delivered-To:
huzeyfe.onal@gmail.com
Received: by 10.86.35.8
with SMTP id
i8cs106219fgi;
        Fri, 24 Jul 2009
```

Analyze Header

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-	mx.google.com; spf=neutral (google.com: 91.93.119.80 is neither permitted nor denied by best guess record for domain of

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

From: Başlık Bilgisi

- E-postayı kimin gönderdiğini gösteren başlık bilgisidir.
- Rahatlıkla değiştirilebilir olduğu için güvenilmez başlık bilgisidir!
- “From:” bilgisi ile “From” bilgisi birbirinden farklıdır.
  - From bazı e-posta yazılımları tarafından eklenen standart dışı bir başlık bilgisidir.

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

“To:” Başlık Bilgisi

- E-postanın kime gönderildiği bilgisini taşır

To:”Huzeyfe ONAL” <honal@bga.com.tr>

- CC: (Carbon Copy)
  - Birden fazla kişiye e-posta gönderirken CC: kısmına ek bilgilendirme amaşlı kişiler yazılır
  - E-postayı alan tüm kullanıcılar kimlere gönderildiğini görebilir
- BCC: (Blind Carbon Copy)
  - E-posta alıcıları birbirlerinin adreslerini görmezler, sadece gönderici kimlere gittiğini bilir.

Analiz

- "To:" kısmında <u>başka adres</u> yer alan bir e-postanın size gelmiş olması neyi ifade eder?

Reply-To: Başlık Bilgisi

- Gelen e-postaya dönecek cevabın hangi adrese gönderileceğini belirtir.
- Değiştirilebilir başlık bilgisidir, analiz çalışmalarında güvenilmez!
- Bazı sahtekarlık saldırılarında kullanılır!

To:masum@banka.com
Mail From:bankasahibi@banka.com
Reply-To:bankasahibi@bannka.com

“Return-Path:” Başlık Bilgisi

- Reply-to: benzeri bir başlık bilgisidir,
- Amacı dönecek hata mesajlarının hangi adrese gitmesi gerektiğini belirlemektir.

“Received:” Başlık Bilgisi

- E-postanın hangi adresten gönderildiği bilgisini tutan başlık bilgisidir.
- Kullanıcı ile MTA(Mail Transfer Agent), MTA-MTA arasındaki iletişimin geriye yönelik takibi için kullanılır.
- Postayı teslim alan her MTA bir adet(ya da daha fazla) Received başlığı ekler.
- Received satırları aşağıdan yukarı takip edilerek mesajın dolaştığı sistemler belirlenebilir.
- Adli bilişim analizi açısından en önemli başlık bilgisidir.

“Received:” Formatı

- Received başlık bilgisi kendi içerisinde ek bilgiler barındıran bir başlık bilgisidir.
- Received başlık formatı :

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

by recipient host (MTA Bilgisi)

with protocol id message ID

for recipient;

timestamp

Received:-1

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.

Received: Analizi

- Received başlık alanı da diğer başlık alanları gibi rahatlıkla değiştirilebilir bir formata sahiptir.
- Fakat son Received başlığı değiştirilemez, e-postayı alan sunucu tarafından eklenir.

Delivered-To: huzeyfe.onal@gmail.com
Received: by 10.114.156.1 with SMTP id d1mr1825769wae.1179636286474;
Sat, 19 May 2007 21:44:46 -0700 (PDT)
Return-Path: <owner-advocacy+M1030@openbsd.org>
Received: from shear.ucar.edu (lists.openbsd.org [192.43.244.163])
by mx.google.com with ESMTP id a8si2499671poa.2007.05.19.21.44.42;
Sat, 19 May 2007 21:44:46 -0700 (PDT) sender)
Received: from openbsd.org (localhost.ucar.edu [127.0.0.1])
by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4heF4002161;
Sat, 19 May 2007 22:43:40 -0600 (MDT)
Received: from mail4out.barnet.com.au (mail4.barnet.com.au [202.83.178.125])
by shear.ucar.edu (8.14.1/8.13.6) with ESMTP id l4K4gwhT025317
Received: by mail4out.barnet.com.au (Postfix, from userid 1001) id 8AF9F37D73E;
Sun, 20 May 2007 14:42:52 +1000 (EST)
Received: from mail4auth.barnet.com.au (mail4.barnet.com.au [202.83.178.125])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
Received: from mail1.test (mail1.test.org [10.251.1.18])
by mail4auth.barnet.com.au (Postfix) with ESMTP id 2E9F937D731
for <advocacy@openbsd.org>; Sun, 20 May 2007 14:42:52 +1000 (EST)
Received: by mail1.test (Postfix, from userid 1001) id 0DE621A3; Sun, 20 May 2007 14:42:52 +1000
(EST

E-posta Göndericisinin IP Adresini Bulma

- ....
- Received başlığı kullanılır.

Webmail Hizmetleri ve Gönderici IP Adresi Bulma

- Webmail kullanılarak gönderilen e-postalarda gönderici MTA webmailin çalıştığı sistem olduğu için genellikle received alanlarından bilgi edinilemez.
  - Edinilecek IP adresi maili gönderenin değil, webmail sisteminin IP adresi olacaktır.
  - İstisnaları vardır
- Sık kullanılan webmail hizmetleri ve başlık analizleri
  - Hotmail, Yahoo.com, Gmail.com, Hushmail.com, Klasik webmail servisi, Facebook mesaj gönderim servisi, Outlook Web Access(OWA)

Hotmail’den Gönderilen E-posta

- Hotmail mail göndericinin IP adresini X-Originating-IP: başlık bilgisinde gönderir.
- Bu bilgi eğer e-postayı gönderen proxy hizmeti kullanmadıysa gerçek ip adresidir.

Hotmail E-posta Gönderici Bulma

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]

Gönderici orjinal IP adresi

Yahoo’dan Gönderilen E-posta

- Yahoo webmail kullanılarak gönderilen e-postalarda gönderici IP adresi başlık bilgileri arasından bulunabilir.

Yahoo! Mail Gönderen IP Adresi

```
 Wh2s-
Received: from [193.140.86.3] by web29507.mail.ird.yahoo.com via HTTP; Tue, 11 Jan 2011 15:15:45 GMT
X-Mailer: YahooMailClassic/11.4.20 YahooMailWebService/0.8.107.285259
Date: Tue, 11 Jan 2011 15:15:45 +0000 (GMT)
From: Gokhan ALKAN <gokhan.alkan@yahoo.com.tr>
Subject: Webci eleman gerek
To: Huzeyfe Onal <huzeyfe@lifeoverip.net>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-39252945-1294758945=:45135"
```

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

Gmail'den Gönderilen E-posta

- Gmail bilinçli bir şekilde göndericiye ait başlık bilgilerini gizlemektedir.
- Gmail başlık bilgilerinden göndericiye ait edinilebilecek tek bilgi gönderici e-posta adresidir.
- Gmail'i web üzerinden kullanmayanlar için e-posta başlık bilgileri alınabilir.

```
        P7tXStNqdJfBCtF9az0X6BNikBJ+12AuNMQK4=
MIME-Version: 1.0
Received: by 10.204.63.211 with SMTP id c19mr12707572bki.21.1296891186673;
 Fri, 04 Feb 2011 23:33:06 -0800 (PST)
Received: by 10.204.127.164 with HTTP; Fri, 4 Feb 2011 23:33:06 -0800 (PST)
Date: Sat, 5 Feb 2011 09:33:06 +0200
Message-ID: <AANLkTineOdyQpufj6PYh57WWrN=6mNkDWgMwibWSZN2q@mail.gmail.com>
Subject: bgayi parmakliyorlar sanki
From: =?ISO-8859-1?Q?G=F6khan_Alkan?= <cigalkan@gmail.com>
To: ekip <ekip@bga.com.tr>
Content-Type: multipart/alternative; boundary=001636e1ecff7e7a1d049b840292
```

Facebook Başlık Bilgileri

- Facebook'da listenizdeki birinden gönderilen maillerde e-posta başlığı detaylı incelenirse mesajı göndericinin IP adresi yer alıyor.
- **X-Facebook: from zuckmail** ([ODYu...LjE42OQ==]) by www.facebook.com with HTTP (ZuckMail);
- Facebook mesaj gönderimlerinde Zuckmail kullanıyor ve bu mail yazılımı maili gönderirken HTTP üzerinden aldığı başlık bilgilerini(kullanıcı IP adresi)de gönderilen maile ekliyor.

Facebook Mail Başlık Bilgileri

Tüm Başlıklar Görüntüleniyor - Mesajı

Return-Path: <notification+kr4mkmmxmqxx@facebookmail.com>
Delivered-To: toc@lifeoverip.net
Received: (qmail 57615 invoked by uid 89); 30 Mar 2010 10:43:42 -0000
X-Mail-Scanner: Scanned by qSheff-II-2.1-r3 (http://www.enderunix.org/qsheff/)
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on mail.sistembil.com
X-Spam-Level:
X-Spam-Status: No, score=-2.1 required=5.0 tests=BAYES_00,FROM_LOCAL_NOVOWEL,
HTML_MESSAGE autolearn=no version=3.2.5
Received: from outmail006.snc1.tfbnw.net (HELO mx-out.facebook.com) (69.63.178.165)
by mail.sistembil.com with SMTP; 30 Mar 2010 10:42:58 -0000
Return-Path: <notification+kr4mkmmxmqxx@facebookmail.com>
DKIM-Signature: v=1; a=rsa-sha1; d=facebookmail.com; s=q1-2009b; c=relaxed/relaxed;
q=dns/txt; i=@facebookmail.com; t=1269946038;
h=From:Subject:Date:To:MIME-Version:Content-Type;
bh=m4Y1IoV80PMqWgQMicW9EEgBX9M=;
b=lrBsgC4f9GalNHK/GtUQDC4uyd5mmm0bMLKu0CzArxVtIHB5NzzX+BBMxDZoNVSa
8VyD0ctp3E7HzRnibBCAyg==;
Received: from [10.18.255.123] ([10.18.255.123:43718])
by mta003.snc1.facebook.com (envelope-from <notification+kr4mkmmxmqxx@facebookmail.com>)
(ecelerity 2.2.2.45 r(34067)) with ECSTREAM
id B5/7F-30454-6B6D1BB4; Tue, 30 Mar 2010 03:47:18 -0700
X-Facebook: from zuckmail ([ODY[redacted]A4LjEzNi42OQ==])
by www.facebook.com with HTTP (ZuckMail);
Date: Tue, 30 Mar 2010 03:47:18 -0700
To: Hayhuy Deneme <toc@lifeoverip.net>
From: Facebook <notification+kr4mkmmxmqxx@facebookmail.com>
Reply-to: noreply <noreply@facebookmail.com>
Subject: Huzeyfe Onal sent you a message on Facebook...
Message-ID: <474875fd6f6a4570832348c9f8dc4c28@www.facebook.com>
X-Priority: 3
X-Mailer: ZuckMail [version 1.00]
X-Facebook-Notify: msg; from=532386892; t=1189838801188; mailid=21bd3e4G5af348e52c46G914G0
Errors-To: notification+kr4mkmmxmqxx@facebookmail.com
X-FACEBOOK-PRIORITY: 0
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="b1_474875fd6f6a4570832348c9f8dc4c28"

base64 encoded istemci IP adresi

“ Date:” Başlık Bilgisi

- Mailin ilk kaynakta oluşturulma zamanının gösterir.

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

“User-Agent:” Başlık Bilgisi

- Gönderilen e-postanın hangi istemci yazılımı kullanılarak gönderildiğini gösterir.
- Değiştirilebilir bir başlık alanı olduğu için güvenilmez’

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 program ve MTA(Mail sunucu) harici ara yazılımların(Antispam-GW, virüs gateway vs)ekledikleri başlıkların standart başlıklar ile karışmaması için X- başlıkları kullanılır.


```
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
```

Sahte E-posta Başlıkları Oluşturma

- E-posta başlık bilgileri istemci/MTA yazılımları tarafından eklenebileceği gibi gönderici tarafından da eklenebilir.
- SMTP üzerinden başlık bilgilerini değiştirmek için ek bir programa ihtiyaç duyulmaz
  - telnet istemcisi kullanılarak SMTP komutlarına istenen başlık bilgileri parametre olarak verilebilir.
- Telnet kullanılarak başlık bilgisi değiştirilirken dikkat edilmesi gereken husus başlık bilgilerinin "data" komutundan sonra verilmesi gerektiğidir.

Sahte E-posta Başlığı Oluşturma

```
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?
```

Telnet kullanarak sahte e-posta başlık bilgileri oluşturma

Kullanıcı tarafından girilen veri alanları

Sahte E-posta Başlık Analizi

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?

E-posta Takip Programları

- Amaç:gönderilen e-postanın kimler tarafından okunduğunun, kimlere iletildiğinin bilgisini alma
  - E-postanızı kaç kişi okudu?
  - Hangi şirketlerden okundu?
  - E-postanız başkasına iletildi mi?

BGA İletişim

www.bga.com.tr

blog.bga.com.tr

twitter.com/bgasecurity

facebook.com/BGAkademisi

bilgi@bga.com.tr

egitim@bga.com.tr