

HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

BİLGİ TOPLAMA YÖNTEMLERİ VE KEŞİF:

Bilgi Toplama Terminolojisi:



Bilgi Toplamannın getirdiđi tehditler:



Bilgi toplama Metodolojisi:

- İnternet vasıtasıyla bilgi toplama
- Rekabet edilen firmalarla ilgili bilgi toplama:
 - Ürün – Sattıkları ürünün bizden farklılıkları neler? Bizi geçebilir mi?
 - Promosyon – Ürünlerinin satışı için sundukları cazip yöntemler neler?
 - Ürün pazarı – Ürünleri kimlere hitap ediyor. Kimler ilgi gösteriyor?
- Whois sorgulamalarıyla bilgi toplama
- DNS üzerinden bilgi toplama
- Websitelerini takip ederek bilgi toplama
- Eposta ile bilgi toplama
- Google Hacking

Hedef firma ile ilgili bilgi toplama adımları:

Google,Bing,Yahoo,Yandex vb. Çeşitli arama motorlarında aranabilir.

Örnek firma:”deneme.com”

Firmanın alanadı bulunduktan sonra iç alan adları link haritası ve alt alan adları listelenmelidir.

Hedef web sitesinin uptime bilgisi, sunucu çeşidi ile ilgili detaylı bilgiler listelenebilmektedir:
<http://news.netcraft.com/>

Hedef web sitesinin dns bilgisini,ip aralığını detaylı olarak listeleyen web sitesi:

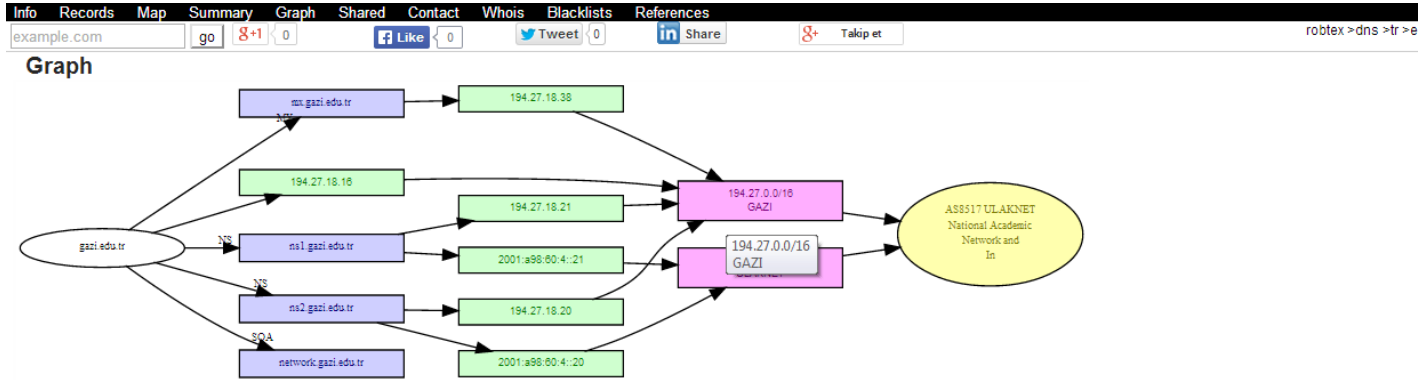
<http://bgp.he.net/>

Screenshot of the Hurricane Electric DNS lookup page for deneme.com. The page shows DNS information, website info, IP info, and whois data. The whois data includes Start of Authority, Nameservers, Mail Exchangers, and A Records.

Updated 02 Mar 2014 07:25 PST © 2014 Hurricane Electric

Robtex:

Örnek: <https://www.robtx.com/dns/gazi.edu.tr.html#graph>



Hedef web sitesinin iç urlleri ve dış bağlantıları listelenebilmektedir:

<http://www.webmaster-a.com/link-extractor-internal.php>

Alternatif:

<http://www.webmaster-toolkit.com/link-extractor.shtml>

Hedef şirket hakkında komplike aramalar gerçekleştirilmelidir. Şirket hakkında çalışan listesi, şirket eposta adresleri, linkedin gibi web siteleri üzerinden arařtırmalar gerekleřtirilerek toplanabilen bütn bilgiler toplanmalıdır.



Firma Bilgilerini dkmek iin kullanılabilecek aralar:

<http://www.webextractor.com>

Aynı IP adresinde yer alan adresleri listelemek iin bing kullanılabilir:

Derste yaptığımız rnek:

www.bing.com

ping sahibinden.com

ıkan ip sonucu: 85.111.30.111

Bing sorgusu:ip:85.111.30.111.

Sorgu ile ip zerindeki adresler listelenir.

People Search Online Servisleri:

people.yahoo.com

123people.com

wink.com

peoplefinders.com

pipl.com:Derste kullandığımız web sitesi.Sosyal ağlar dahil olmak üzere kişi bilgilerini dōkebilmektedir.

Google Alerts(Otomatik arama uyarıları oluřturup eposta adresinize gōnderir)

Linkedin

Twitter

Kariyer.net vb. Iř ilan siteleri



Rekabet edilen firmalarla ilgili bilgi toplama:

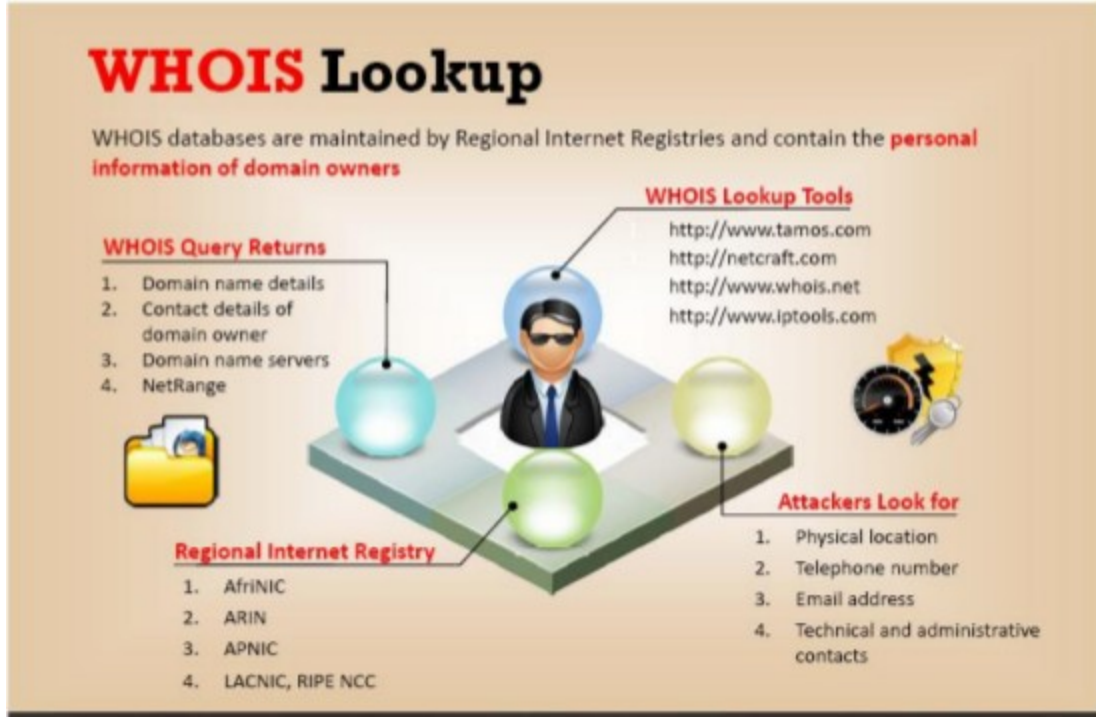
Hedef firmaların yaptığı anlaşmalar ve gōncel bilgileriyle ilgili dōkōm cıkaran web siteleri:

Derste incelenen web siteleri:

www.dnb.com

www.sec.gov/edgar.shtml

Whois Sorgulama:



Debian tabanlı ubuntu kali gibi işletim sisteminde whois komutu mevcuttur.

Yüklenmesi halinde kullanılabilir.

yüklemek için:`apt-get install whois`

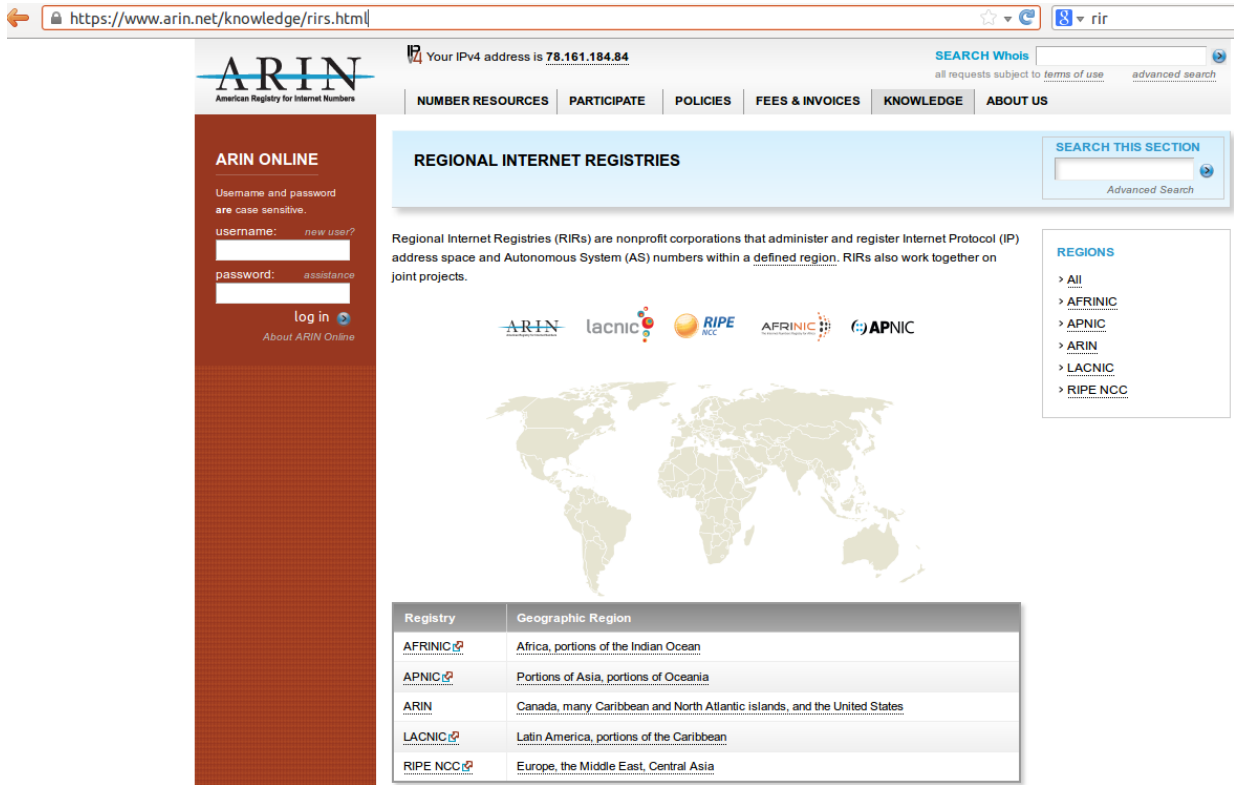
Whois sorgulama siteleri:

domaintools.com

who.is

Bölgesel alanadı ve ip sorgulama hizmetleri:

Adres: <https://www.arin.net/knowledge/rirs.html>



The screenshot shows the ARIN website's "Regional Internet Registries" page. The page features a search bar at the top right, a navigation menu, and a list of RIRs. The ARIN logo is prominently displayed at the top left. The page content includes a search bar, a navigation menu, and a list of RIRs with their geographic regions.

REGIONAL INTERNET REGISTRIES

Regional Internet Registries (RIRs) are nonprofit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region. RIRs also work together on joint projects.

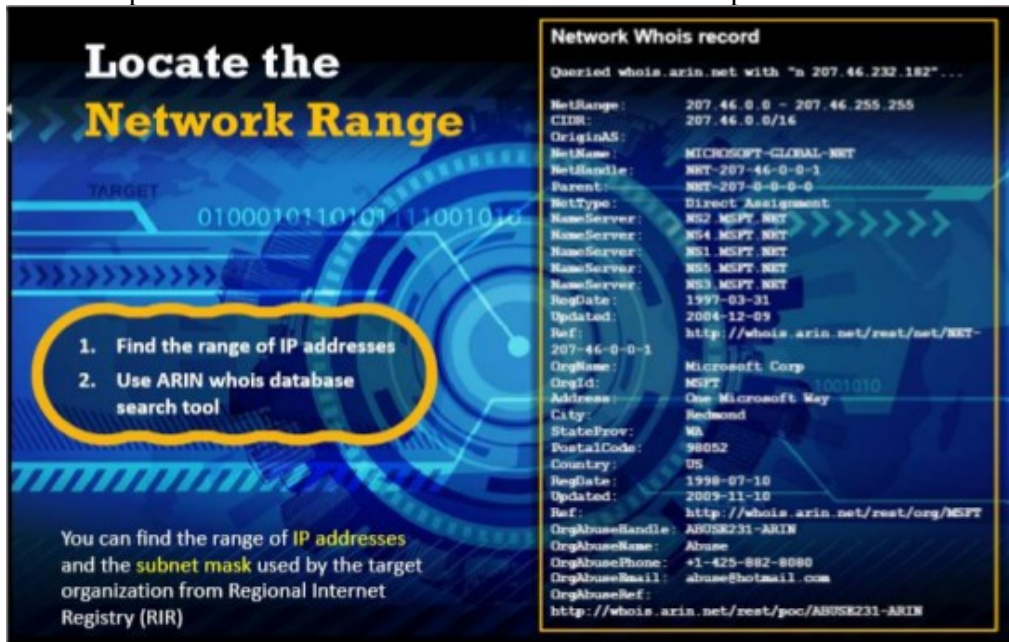
REGIONS

- > All
- > AFRINIC
- > APNIC
- > ARIN
- > LACNIC
- > RIPE NCC

Registry	Geographic Region
AFRINIC	Africa, portions of the Indian Ocean
APNIC	Portions of Asia, portions of Oceania
ARIN	Canada, many Caribbean and North Atlantic islands, and the United States
LACNIC	Latin America, portions of the Caribbean
RIPE NCC	Europe, the Middle East, Central Asia

Hedef ip adresinin Ağ subnet aralığını çıkartma:

Örnek: <http://whois.arin.net/rest/net/NET-208-109-0-0-1/pft>



Locate the Network Range

TARGET: 010001011010111001010

1. Find the range of IP addresses
2. Use ARIN whois database search tool

You can find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR)

Network Whois record

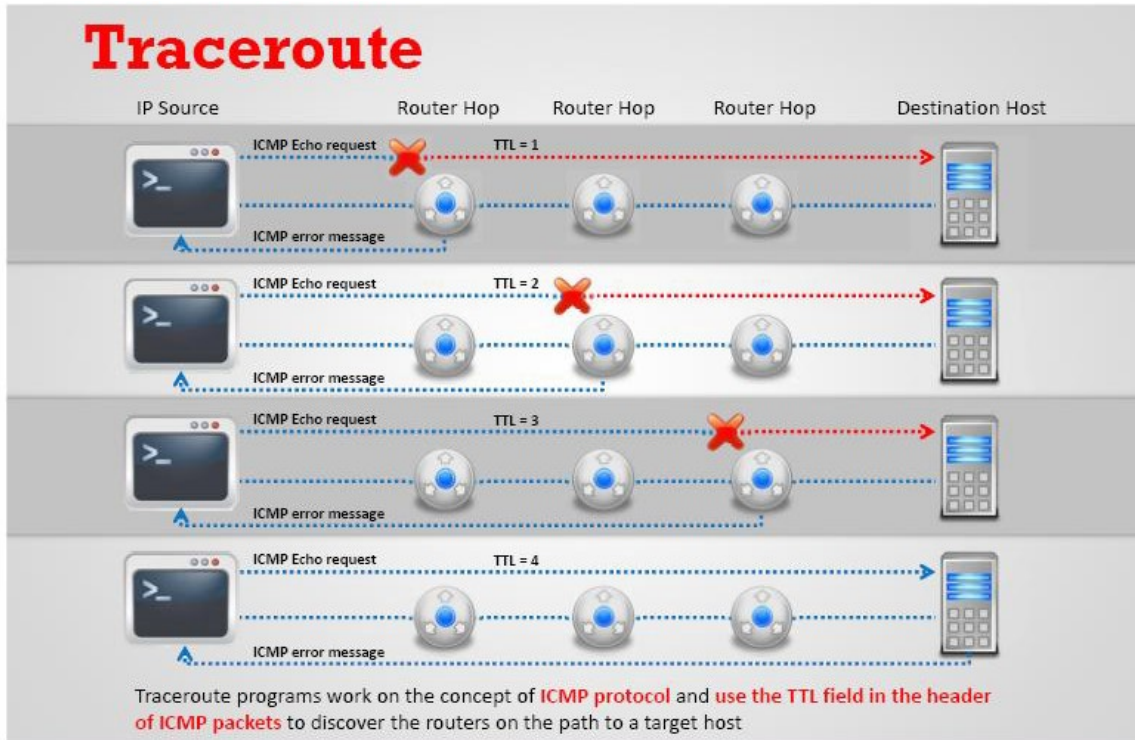
Queried whois.arin.net with "n 207.46.232.182" ...

```
NetRange: 207.46.0.0 - 207.46.255.255
CIDR: 207.46.0.0/16
OriginAS:
NetName: MICROSOFT-GLOBAL-NET
NetHandle: NET-207-46-0-0-1
Parent: NET-207-0-0-0-0
NetType: Direct Assignment
NameServer: NS2.MSFT.NET
NameServer: NS4.MSFT.NET
NameServer: NS1.MSFT.NET
NameServer: NS5.MSFT.NET
NameServer: NS3.MSFT.NET
RegDate: 1997-03-31
Updated: 2004-12-09
Ref: http://whois.arin.net/rest/net/NET-207-46-0-0-1
OrgName: Microsoft Corp
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1998-07-10
Updated: 2009-11-10
Ref: http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle: ABUSE231-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@hotmail.com
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

Traceroute:

Traceroute IP başlığındaki TTL (time-to-live) alanını ve ICMP protokolünü kullanır.

TTL, IP başlığında 8 bitlik alana sahiptir. İlk değeri gönderen tarafından atanır ve bu değer , üzerinden geçtiği her hopta router tarafından azaltılır. TTL alanının amacı sonsuz yönlendirme olmasını engellemektir. Bir yönlendirici TTL alanı 0 ya da 1 olan bir veri paketi almış ise paketi başka bir yere yönlendirmez ve kaynak hostuna ICMP “zaman aşımı” mesajı gönderir. ICMP mesajına sahip olan veri paketi router’ın ip adresini kaynak adresi olarak alır. Traceroute bu sistemi kullanır. Traceroute hedef hosta TTL alan değeri 1 olan veri paketi gönderir. Veri paketini alan router, TTL değerini düşüremediği için hedefe giden yoldaki diğer router’a yönlendirme yapmaz ve geriye icmp “zaman aşımı” mesajını gönderir. Böylece ilk yönlendiricinin IP adresini bulur. Traceroute diğer adımda hedef hosta TTL değeri 2 olan veri paketi gönderir ve yoldaki ikinci router’ın IP adresini bulur. Bu yolla hedef hosta ulaşıncaya kadarki yönlendiriciler tanımlanır.



Traceroute komutuyla hackerlar hedefin ağ topolojisi çıkartabilir gönderilen paketin geçtiği yolları tespit edebilir, firewall cihazlarını tespit edebilir

Traceroute Tools

 VisualRoute Trace http://visualroute.visualware.com	 GEOspider http://www.oreware.com
 vTrace http://vtrace.pl	 Magic NetTrace http://www.tialsoft.com
 3d Visual Trace Route http://www.3dtracroute.com	 Visual IP Trace http://www.visualiptrace.com
 Trout http://www.foundstone.com	 Patrice Zwenger Traceroute http://patrice-zwenger.co.cc

Online Görsel Traceroute web sitesi:

<http://traceroute.monitis.com/>

Örnek:

Linux terminalinde :traceroute komutu kullanılmalıdır.

Windows'da ise cmd.exe üzerinde tracert komutu kullanılmalıdır.

Örnek:

linux örnek:traceroute deneme.com

windows örnek:tracert deneme.com

DNS TOOLS:

DNS Data Extraction Siteleri:

<http://network-tools.com>

<http://intodns.com/>

DNS bilgisi toplama ARAÇLARI:

NSLOOKUP:

İsim sunucularını interaktif olarak sorgulamamızı sağlayan araç.

Windows ve linux'da da kullanılabilen aktif bilgi toplama aracı.

Basit Kullanımı:

cmd.exe açıldıktan sonra sırasıyla

**Windows için komutları verildiği takdir de:
nslookup.exe**

set type=any

deneme.com

dns bilgisi dökülmektedir.

help yazarak diğer komutların listesinde görülebilir.

DIG:

dig aracı ile dns ile ilgili aktif bilgi toplama gerçekleştirilir.

Komut adımları sırasıyla:

dig sahibinden.com

dig NS sahibinden.com

dns01.sahibinden.com adresi recursive sorgulara cevap vermektedir.Bu dns poisoning saldırılarının gerçekleştirilmesine olanak sağlar!

dig deneme.com @dns01.sahibinden.com

Aynı işlemi pasif olarak detaylı olarak raporlayan ve bilgi veren web sitesi görülebilir:

“<http://www.dnsstuff.com/tools#dnsReport?type=domain&&value=sahibinden.com>”

DNS Data Extraction Siteleri:

<http://network-tools.com>

<http://intodns.com/>

<http://www.dnsstuff.com/>

PENTEST-TOOLS:

Alan adı ile ilgili isim sağlayıcı bilgilerini verir.Zone transfer yapmak mümkündür.Alt alan adlarını mail sunucu bilgilerini dns kayıtlarını sorgulamak mümkündür.

Adres:<https://pentest-tools.com/reconnaissance/dns-search-online>

Aynı işlemi dig ile şu şekilde yapmak mümkündür:

dig AXFR example.com @ns1.exampledns.com.

GOOGLE HACKING:

Google Hacking Database:

Adres:<http://www.exploit-db.com/google-dorks/>

Google arama operatörleri için:

Bütün arama operatörleri aşağıdaki adreste yer almaktadır:

http://www.googleguide.com/using_advanced_operators.html

Google arama ipuçları:

intitle index of "parent directory"

Sayfa başlığında “yönetim” paneli olan siteleri listeler
allintitle:yönetim

Web sayfalarındaki alt klasörleri, urleri arar.
inurl:

Web sitesinin altındaki bütün herşeyi arar:

site:sahibinden.com/*.php: **Web sitesinde yer alan bütün php dosyalarını listeler**
site:*.sahibinden.com: **Web sitesindeki bütün herşeyi listeler.**

Web sitelerindeki dosya uzantılarına göre arama yapar.
filetype:pdf : **Örnek olarak pdf dosyalarını verdim.**

Kullanılabilecek hazır araçlar:

Goolag Scanner

Adres:www.soldierx.com

Açık sistemleri ve dışarıya açık ağlardaki açıklıkları aramak için kullanılan arama motoru:
Shodan

Site kapanmış bile olsa arşiv bilgisini bulmak mümkündür.

Archive.org bilgi toplama araçları içerisinde en sık kullanılan web sitesidir.Crawl ettiği web sitelerinin geçmiş bilgilerini saklayarak yıllar öncesindeki bilgilere bile ulaşılabilir.

Websitewatcher tool:site sayfa kayıt tarihi çekme

Dirbuster nedir?

Dirbuster web sitesine deneme yanılma yöntemi dahil olmak üzere wordlist ekleyerek de bütün url'leri listeler.

Bütün araçları barındıran online footprinting websitesi :

www.dirk-loss.de/onlinetools.htm

Otomatize bilgi toplama aracı Harvester:

Adres:<https://code.google.com/p/theharvester/>

Kali işletim sisteminde mevcuttur.

Eposta ile ilgili bilgi toplama:

Gelen epostaların kaynağını görüntüleyerek detaylı bilgi edinilebilir.

Eposta maillistelerine üye olunarak bilgi toplamak mümkündür.

Email Tracker Pro:www.emailtrackerpro.com

Eposta bildirim ve bilgi takibi:

<http://www.readnotify.com/>

<http://www.getnotify.com/>

Ücretli eposta bildirim ve bilgi takibi:

<http://www.didtheyreadit.com/>

Faydalanılabilecek Kaynaklar:

<http://www.slideshare.net/leminhvuong/module-2-foot-printing>

http://ptgmedia.pearsoncmg.com/images/9780789735317/samplechapter/0789735318_CH03.pdf