Nebrija Universidad MADRID

Hacking Ético

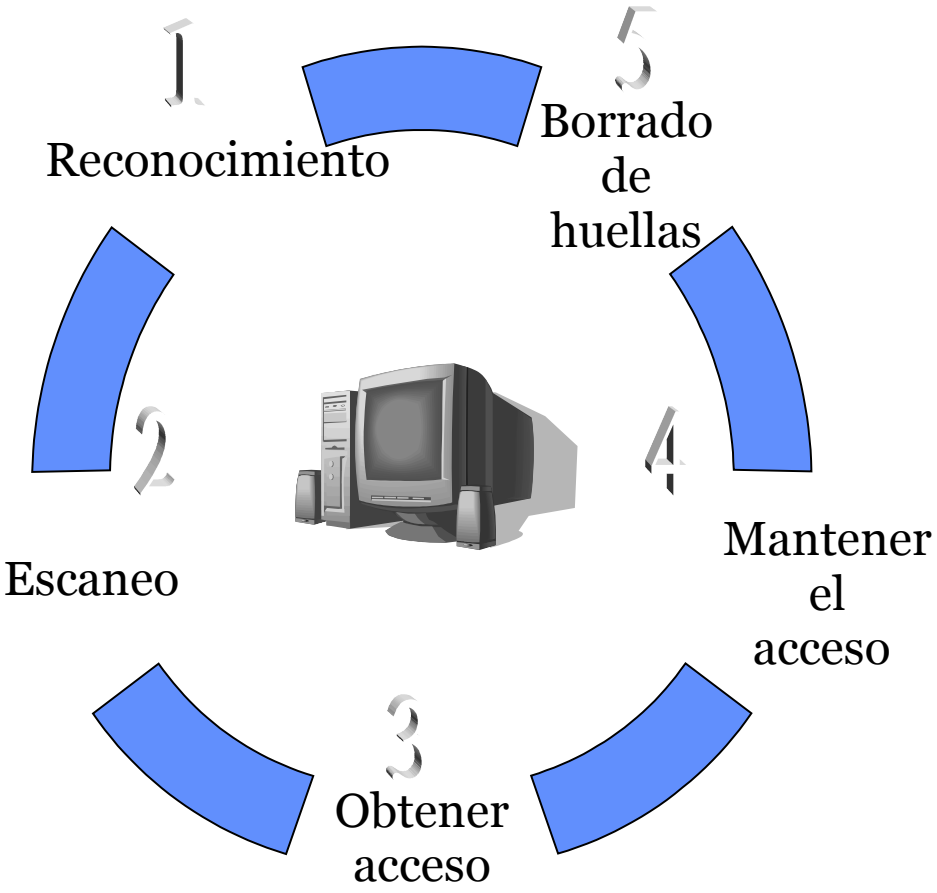
Módulo I

Fase 1: Obtención de información

Objetivos

- Visión general de la fase de reconocimiento
- Entender la metodología de obtención de información de los hackers
- Repaso de algunas herramientas

Obtención de información



Obtención de información

- Dos fases en el pre-ataque:
  - Footprinting (obtención de información)
  - Escaneo / Enumeración
- Obtención de los perfiles de seguridad de una organización haciendo uso de una metodología (*footprinting*).
- El resultado del *footprinting* es un perfil único de la organización en cuanto a sus redes (Internet / Intranet / Extranet / Wireless) y sistemas.

Fase 1 (pre ataque)- *Footprinting*

1.- Obtener información inicial
- whois
- nslookup

2.- Localizar el rango de red
- Traceroute

Metodología para la obtención de información

- Obtener información inicial
- Localizar el rango de la red

Footprinting

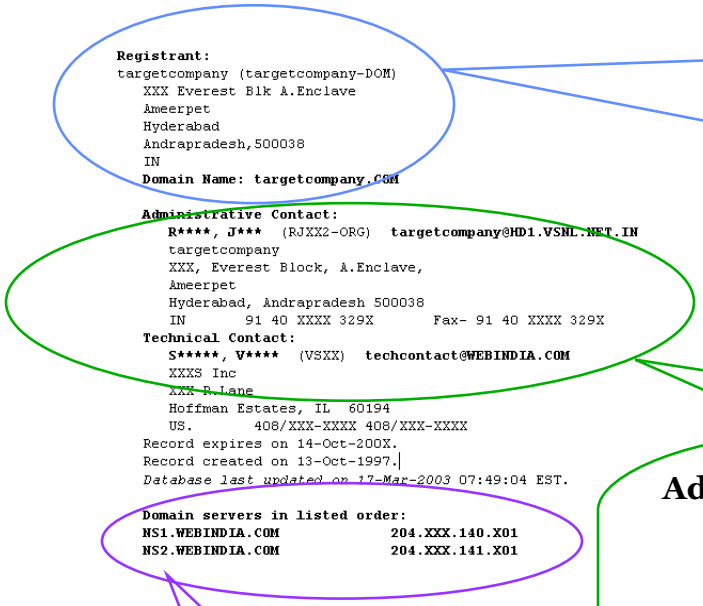
Footprinting

- Averiguar qué máquinas están activas
- Puertos abiertos / access points
- Detectar sistemas operativos
- Descubrir servicios escuchando en puertos
- Topología de la red

Obtener información inicial

- *Incluiría*:
  - Nombres servidores DNS, algunas IPs
  - Localizaciones geográficas de la empresa.
  - Contactos (Teléfono / mail)
- *Fuentes de Información*:
  - Web de la empresa
  - Whois: http://www.internic.net/whois.html
  - Nslookup – posible transferencia de zona DNS
  - www.all-nettols.com
  - Infojobs / monster
  - Google:
    - allinurl:tsweb/defaul.htm

Whois



```
Registrant:
targetcompany (targetcompany-DOM)
   XXX Everest Blk A.Enclave
   Ameerpet
   Hyderabad
   Andrapradesh,500038
   IN
   Domain Name: targetcompany.COM

   Administrative Contact:
      R****, J***  (RJXX2-ORG)  targetcompany@HD1.VSNL.NET.IN
      targetcompany
      XXX, Everest Block, A.Enclave,
      Ameerpet
      Hyderabad, Andrapradesh 500038
      IN       91 40 XXXX 329X       Fax- 91 40 XXXX 329X
   Technical Contact:
      S*****, V****  (VSXX)  techcontact@WEBINDIA.COM
      XXXS Inc
      XXX R.Lane
      Hoffman Estates, IL  60194
      US.       408/XXX-XXXX 408/XXX-XXXX
   Record expires on 14-Oct-200X.
   Record created on 13-Oct-1997.
   Database last updated on 17-Mar-2003 07:49:04 EST.

   Domain servers in listed order:
   NS1.WEBINDIA.COM             204.XXX.140.X01
   NS2.WEBINDIA.COM             204.XXX.141.X01
```

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: **targetcompany.COM**

Administrative Contact:
Surname, Name (SNIDNo-ORG) t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

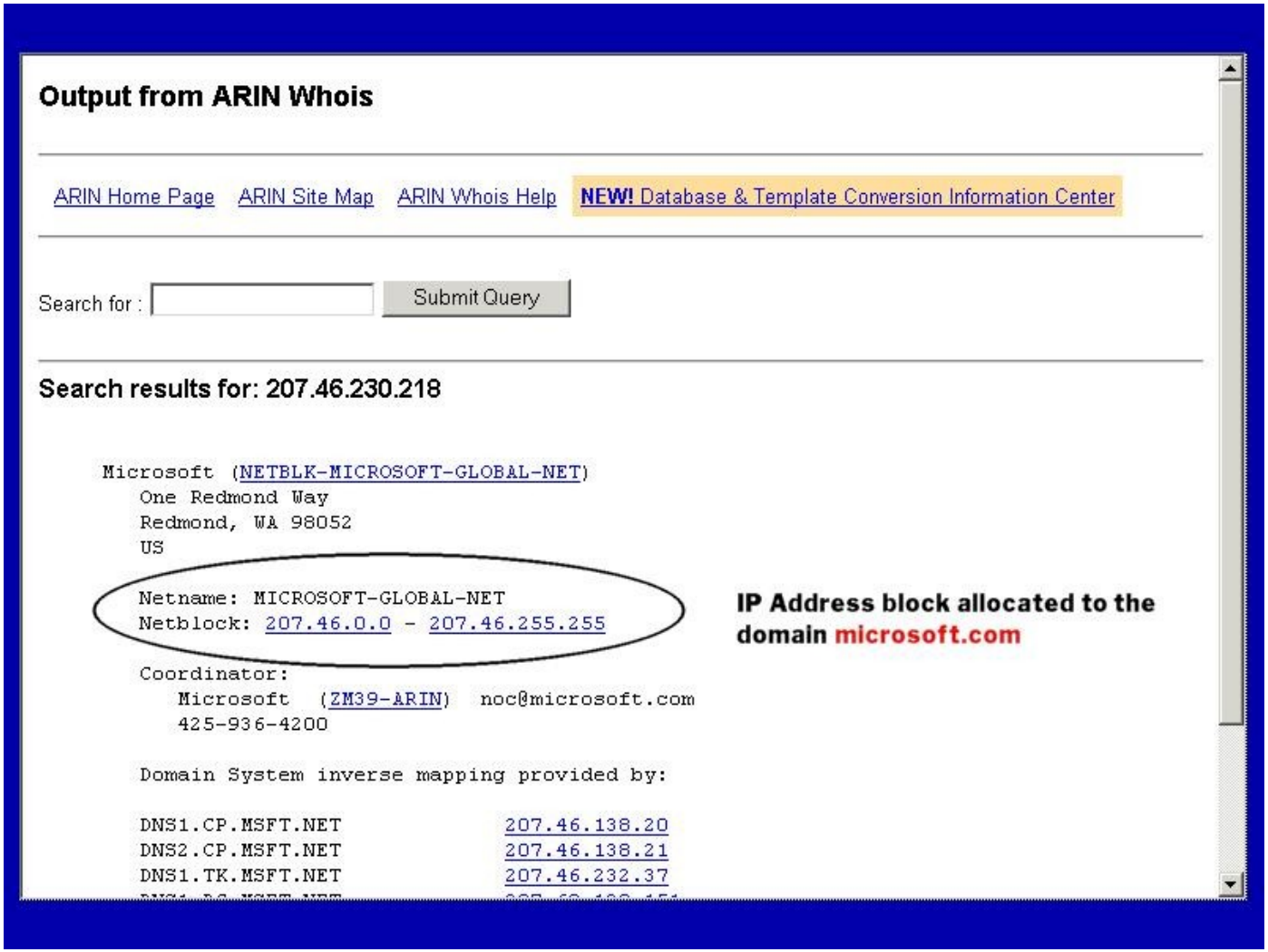
Technical Contact:
Surname, Name (SNIDNo-ORG) t**argetcompany@domain.com**
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

```
Domain servers in listed order:
    NS1.WEBHOST.COM              XXX.XXX.XXX.XXX
    NS2.WEBHOST.COM              XXX.XXX.XXX.XXX
```

ARIN

- ARIN permite hacer búsquedas whois
- Podemos obtener el rango de red
- Y dirigir nuestros esfuerzos en ese rango

Screenshot: ARIN Whois Output



Nslookup

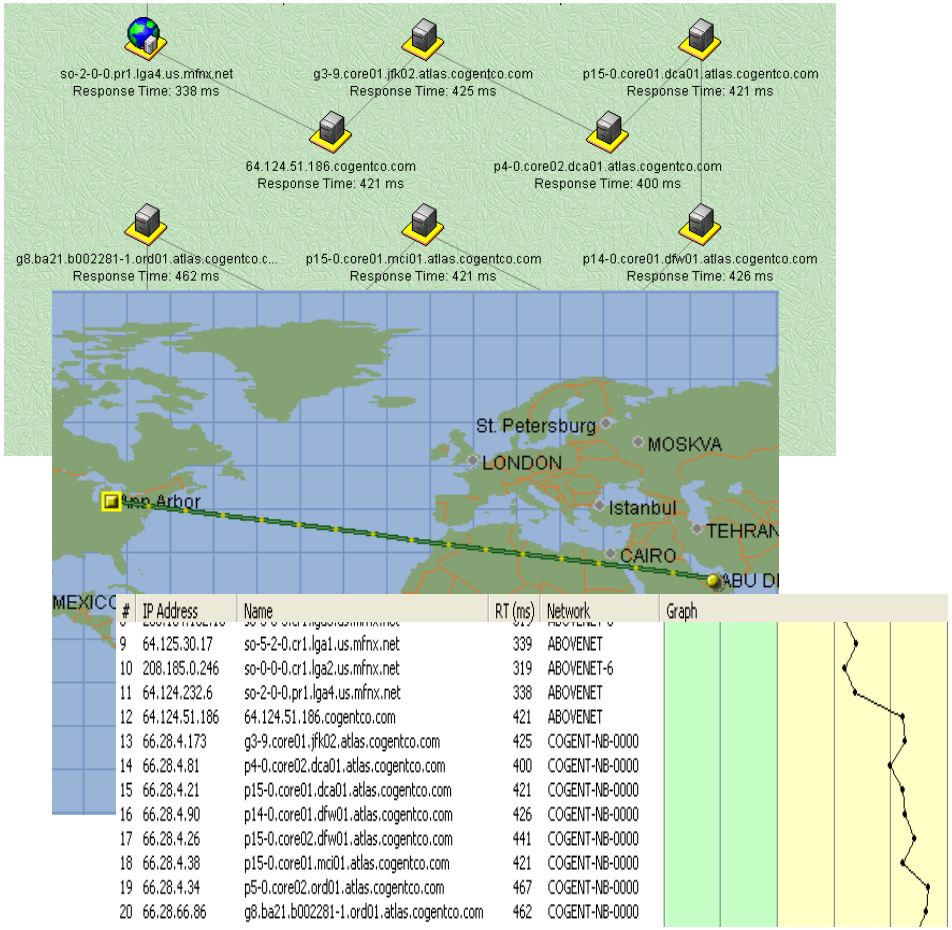
- Nslookup – resolución DNS.

Nslookup y DNS

- Nslookup – resolución DNS.
- Dominios y zonas.
- Fichero de zona
- Registros de recursos (RR)
- Registros de recursos: SOA, NS, A, CNAME, MX
- Transferencia de zona entre servidores DNS – ya lo haremos.

Determinar el rango de red

- *Incluiría:*
  - Encontrar el rango de Ips
  - Encontrar la máscara de subred
- *Fuentes de información:*
  - ARIN (American Registry of Internet Numbers)
  - Traceroute
- **Hacking Tool:**
  - NeoTrace / Geotrace
  - VisualRoute /Xroute (xt)
  - Whatroute

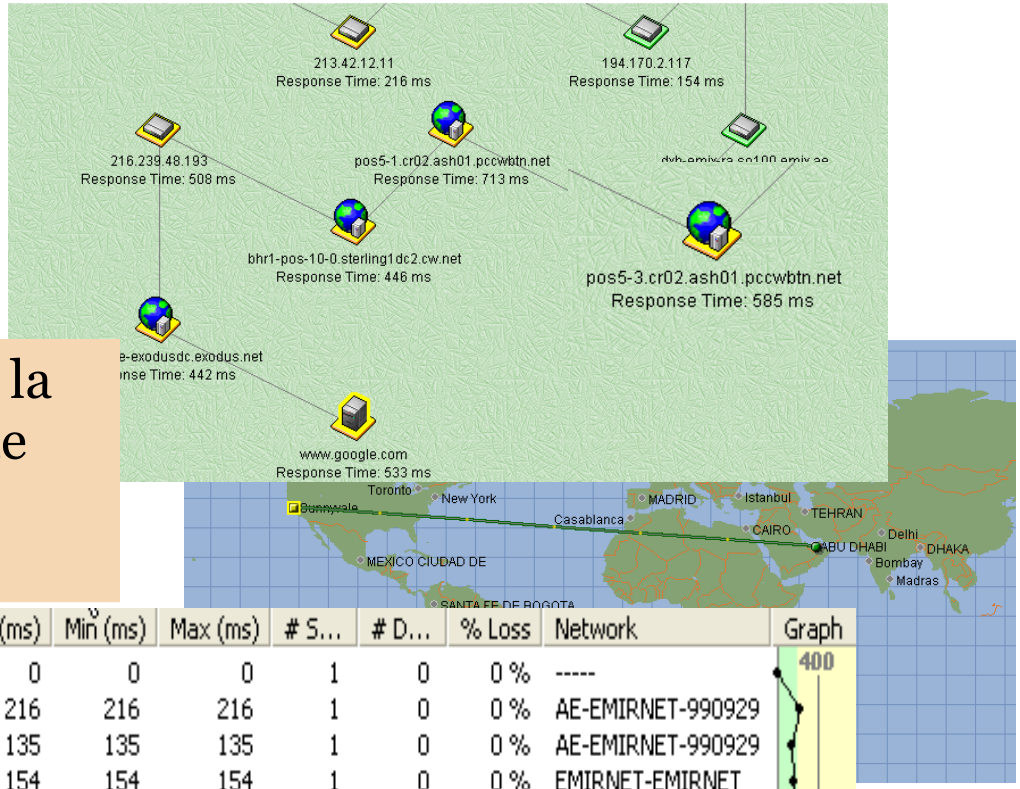


Traceroute

- Traceroute se basa en el parámetro de IP TTL (Time To Live).
- Saltos de routers.
- Cada router en un salto disminuye el TTL. Cuando el TTL se hace cero, devuelve un mensaje "TTL exceeded" (usando ICMP) al origen.

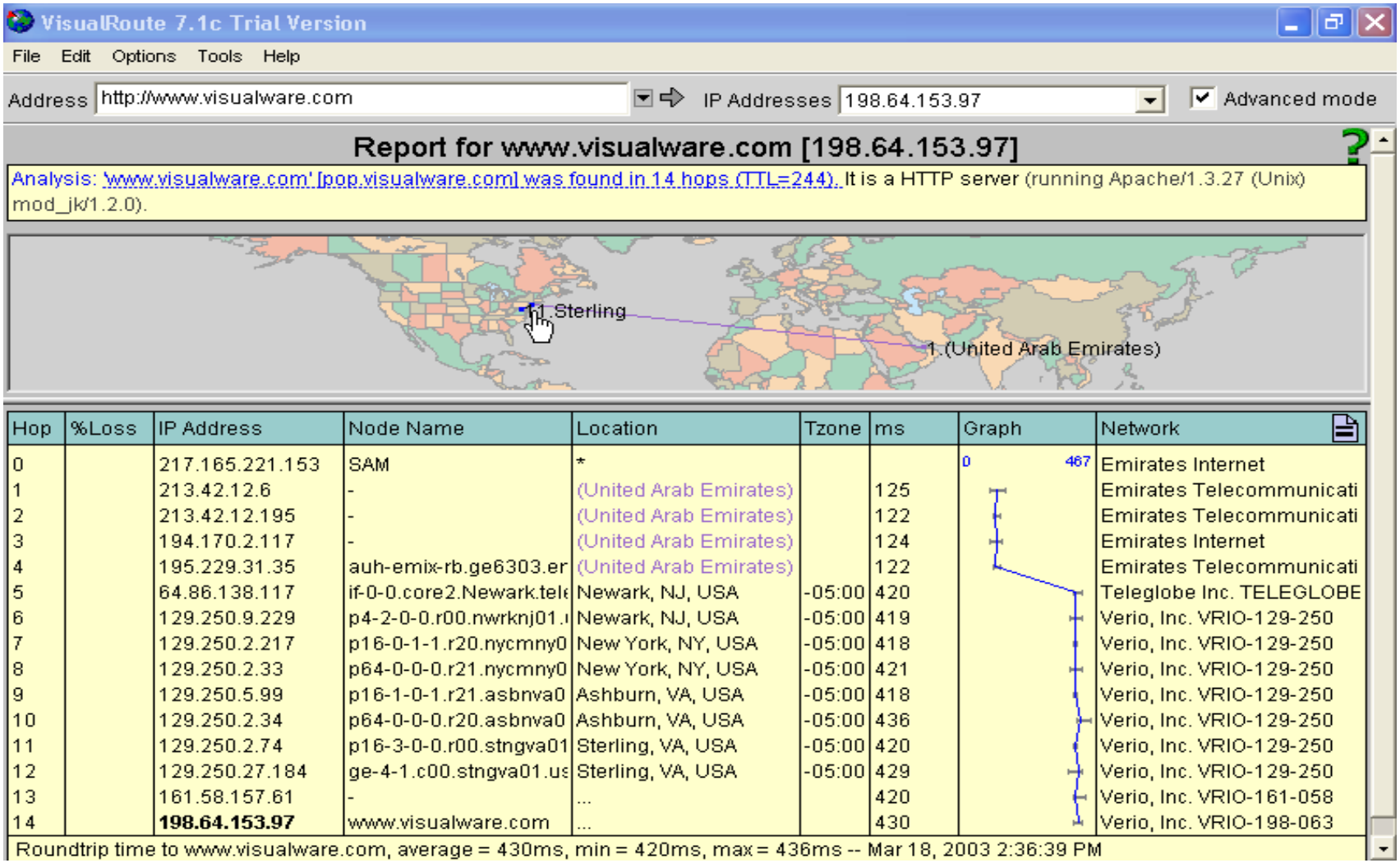
Tool: NeoTrace (Now McAfee Visual Trace) – Geotrace (GNU)

NeoTrace muestra la salida de traceroute visualmente en un mapa.

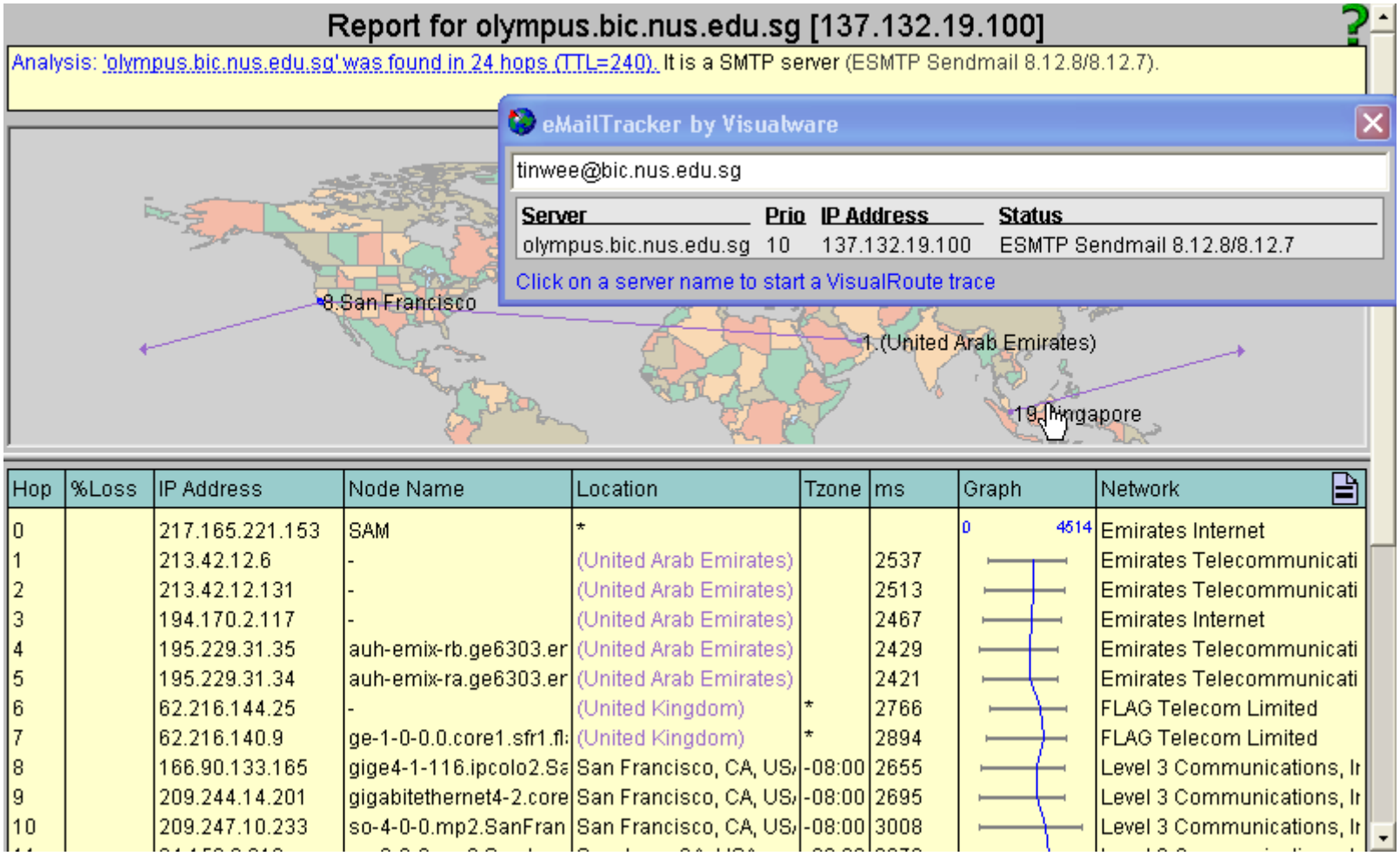


#	IP Address	Name	RT (ms)	Ave (ms)	Min (ms)	Max (ms)	# S...	# D...	% Loss	Network	Graph
1	217.165.236.73	SAM	0	0	0	0	1	0	0 %	-----	400
2	213.42.12.11	-----	216	216	216	216	1	0	0 %	AE-EMIRNET-990929	
3	213.42.12.130	-----	135	135	135	135	1	0	0 %	AE-EMIRNET-990929	
4	194.170.2.117	-----	154	154	154	154	1	0	0 %	EMIRNET-EMIRNET	
5	195.229.31.66	dxb-emix-rb.ge130.emix.ae	159	159	159	159	1	0	0 %	AE-EMIRNET-971125	
6	195.229.0.234	dxb-emix-ra.so100.emix.ae	139	139	139	139	1	0	0 %	EMIRNET-EMIRNET	
7	166.63.210.62	bcr2.thamesside.cw.net	442	442	442	442	1	0	0 %	CW-NETCS2	
8	63.216.0.42	pos5-1.cr02.ash01.pccwbtn.net	713	713	713	713	1	0	0 %	CAIS-CIDR7	
9	206.24.238.166	bhr1-pos-10-0.sterling1dc2.cw.net	446	446	446	446	1	0	0 %	CW-05BLK	
10	216.239.48.193	-----	508	508	508	508	1	0	0 %	GOOGLE	
11	216.109.88.218	218-google-exodusdc.exodus.net	442	442	442	442	1	0	0 %	DC3-8	
12	216.239.39.99	www.google.com	533	533	533	533	1	0	0 %	GOOGLE	

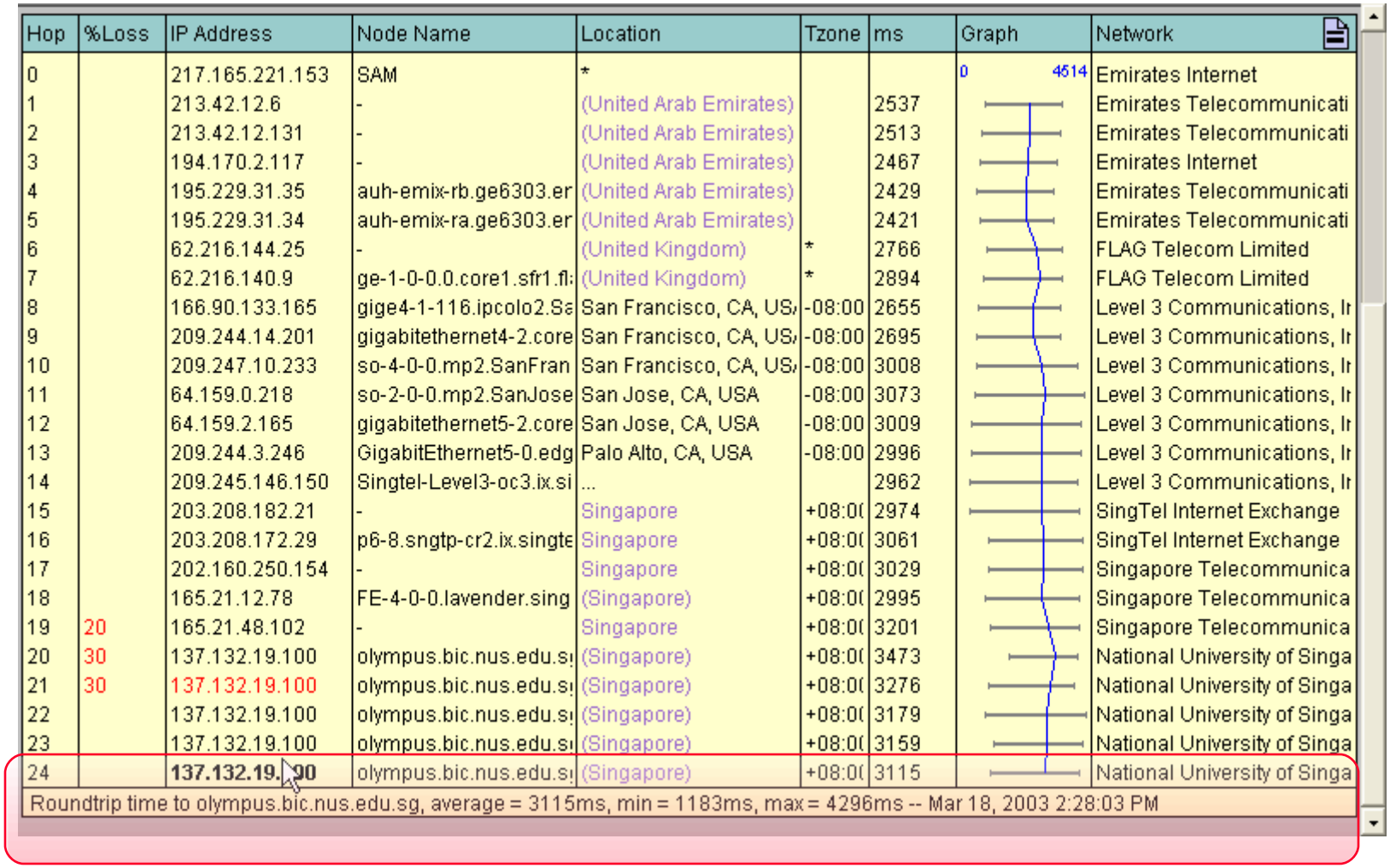
Tool: VisualRoute Trace



Tool: VisualRoute Mail Tracker



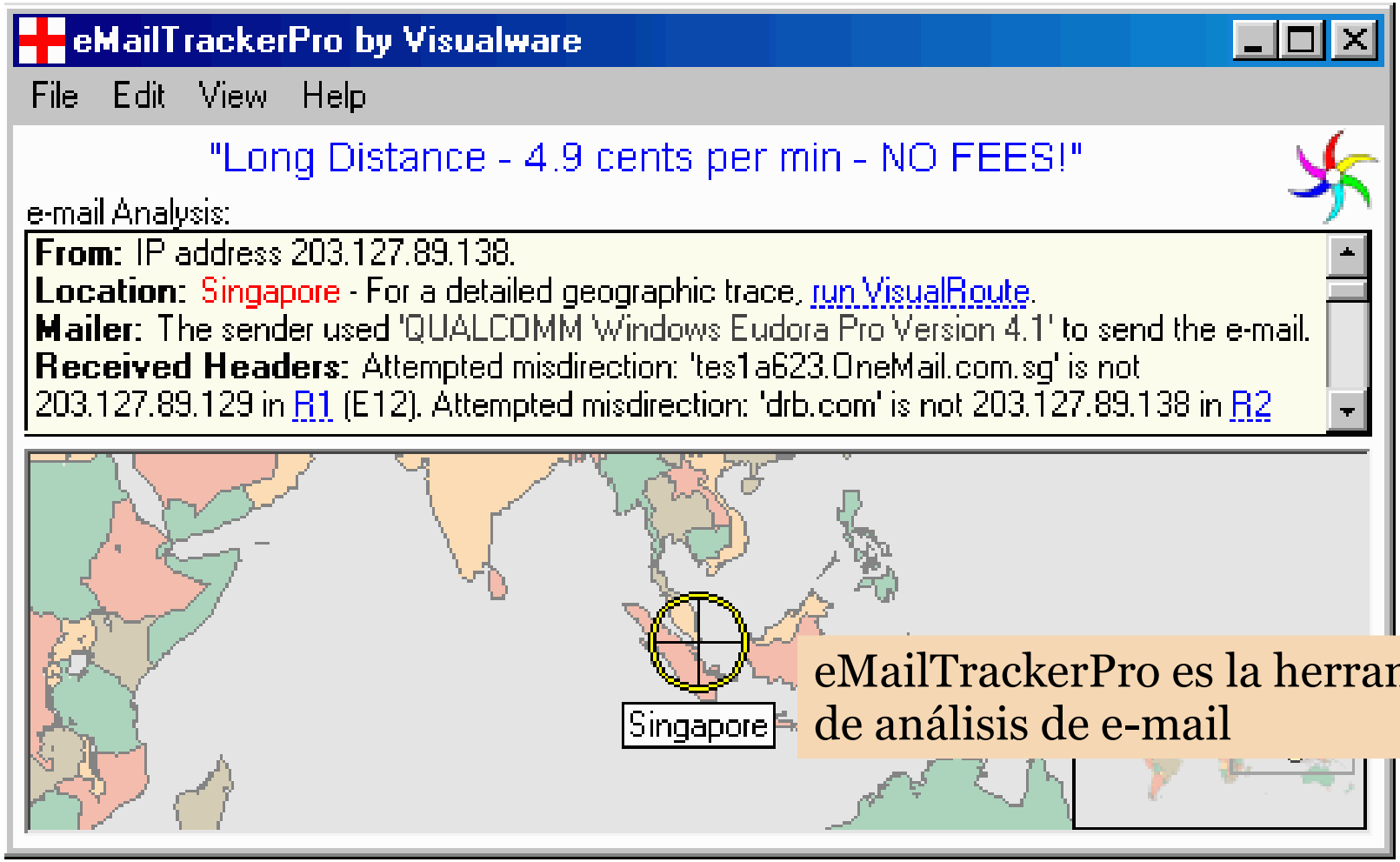
Screenshot: VisualRoute Mail Tracker



Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0 4514	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fl	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US/	-08:00	2655		Level 3 Communications, Ir
9		209.244.14.201	gigabitethernet4-2.core	San Francisco, CA, US/	-08:00	2695		Level 3 Communications, Ir
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US/	-08:00	3008		Level 3 Communications, Ir
11		64.159.0.218	so-2-0-0.mp2.SanJose	San Jose, CA, USA	-08:00	3073		Level 3 Communications, Ir
12		64.159.2.165	gigabitethernet5-2.core	San Jose, CA, USA	-08:00	3009		Level 3 Communications, Ir
13		209.244.3.246	GigabitEthernet5-0.edg	Palo Alto, CA, USA	-08:00	2996		Level 3 Communications, Ir
14		209.245.146.150	Singtel-Level3-oc3.ix.si	...		2962		Level 3 Communications, Ir
15		203.208.182.21	-	Singapore	+08:0(	2974		SingTel Internet Exchange
16		203.208.172.29	p6-8.sngtp-cr2.ix.singte	Singapore	+08:0(	3061		SingTel Internet Exchange
17		202.160.250.154	-	Singapore	+08:0(	3029		Singapore Telecommunica
18		165.21.12.78	FE-4-0-0.lavender.sing	(Singapore)	+08:0(	2995		Singapore Telecommunica
19	20	165.21.48.102	-	Singapore	+08:0(	3201		Singapore Telecommunica
20	30	137.132.19.100	olympus.bic.nus.edu.s	(Singapore)	+08:0(	3473		National University of Singa
21	30	137.132.19.100	olympus.bic.nus.edu.s	(Singapore)	+08:0(	3276		National University of Singa
22		137.132.19.100	olympus.bic.nus.edu.s	(Singapore)	+08:0(	3179		National University of Singa
23		137.132.19.100	olympus.bic.nus.edu.s	(Singapore)	+08:0(	3159		National University of Singa
24		**137.132.19.90**	olympus.bic.nus.edu.s	(Singapore)	+08:0(	3115		National University of Singa

Roundtrip time to olympus.bic.nus.edu.sg, average = 3115ms, min = 1183ms, max = 4296ms -- Mar 18, 2003 2:28:03 PM

Tool: eMailTrackerPro



eMailTrackerPro es la herramienta de análisis de e-mail

Ejemplo

- wikipedia.org
  - whois (www.betterwhois.org)
    - nombres servidores DNS
    - ...
  - nslookup – sacar la IP del servidor DNS
  - traceroute – obtener el nombre del servidor web
  - nslookup – obtener la IP del servidor web

Resumen

- Siete fases en el proceso de obtención de información.
- Footprinting – deberíamos obtener como resultado un perfil del objetivo.
- Whois y ARIN pueden darnos información pública de un dominio muy valiosa.
- Traceroute y mail tracking pueden ser usados para identificar Ips de la red (que podría venir bien para hacer luego IP spoofing)
- Nslookup puede revelar usuarios específicos y permitirnos realizar una transferencia de zona.
- En el siguiente módulo veremos más fases.