# 4. Culegerea de informaţii (recunoaşterea)

# Rol

- Primul pas în etapa de testare
- Nu poţi ataca ceea ce nu cunoşti
- Black-box / gray-box test
- Obţinerea a cât mai multor informaţii despre ţintă
- Activitate non-intruzivă pentru ţintă
- Se efectuează de obicei manual însă poate fi şi automatizată prin intermediul scripturilor

# Perspective asupra ţintei

- System view
  - tehnologii, dispozitive, sisteme de operare
- Functional / logical view
  - rolul fiecărui dispozitiv / sistem
- Physical view
  - sedii, locaţiile în care sunt dispuse echipamentele
- Temporal view
  - programul de lucru
- Social view
  - date despre angajaţi
- Lifecycle view
  - fazele unui proces de business
- Consequence view
  - daca producerea unui eveniment generează alt eveniment (e.g. accesul neautorizat în clădire duce la apariţia poliţiei / firmei de pază la faţa locului)

# De unde se pot obţine informaţii?

- Paginile de web ale companiei / angajaţilor
- Căutare pe Internet
  - Google, Yahoo
- Interogare baze de date publice
  - Whois
  - DNS
- Social networks
  - Facebook, LinkedIn
- Social engineering

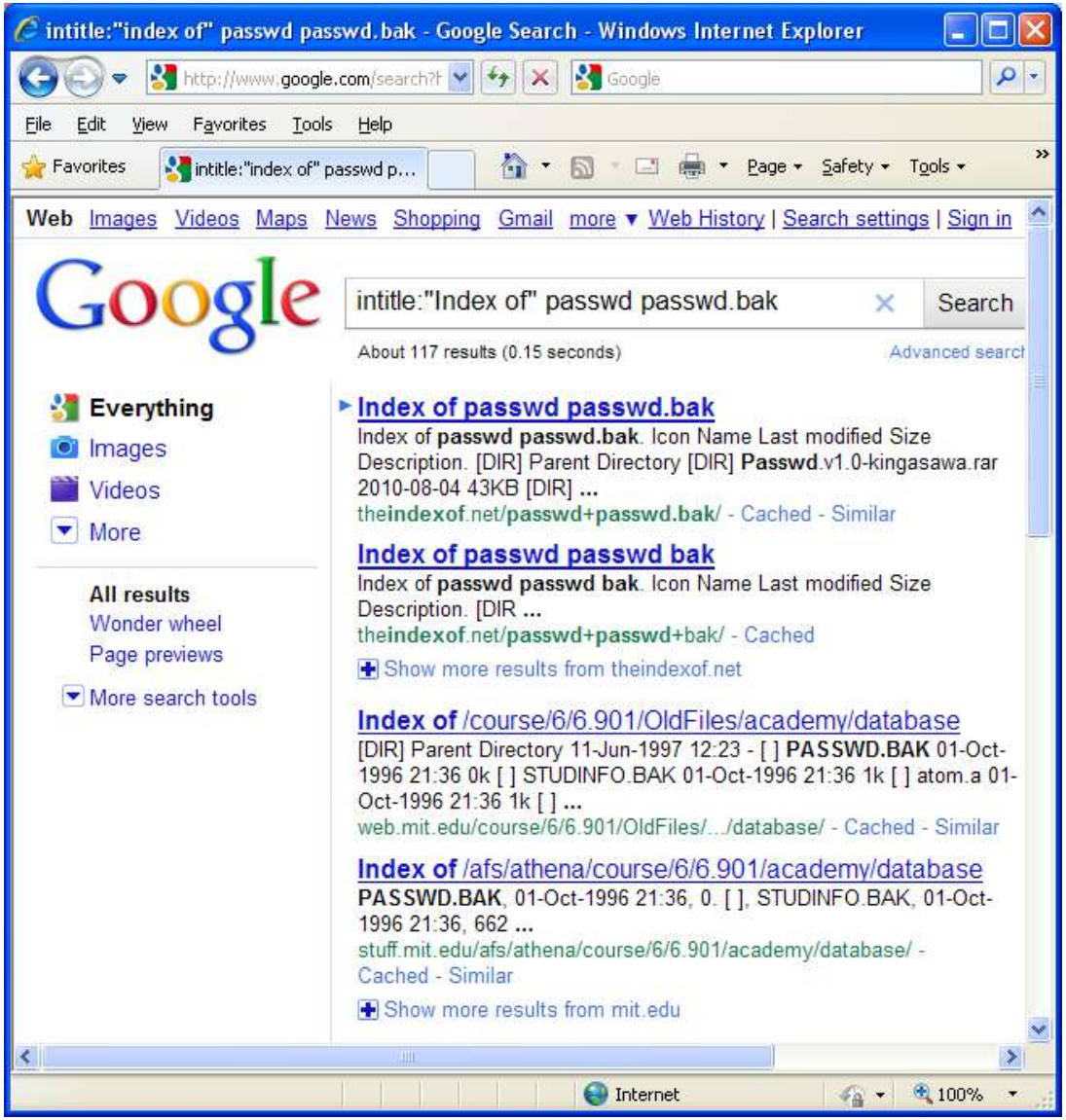
# Paginile de web ale companiei

- Vizitare pasivă a serverelor de Web
- Adrese, persoane de contact, numere de telefon, e-mail, evenimente, etc
- Mirror Web site
  - Wget, Teleport Pro
  - grep, findstr
- Outlook Web Access / Webmail
  - https://owa.abc.ro
  - https://outlook.abc.ro
  - https://webmail.abc.ro
- Virtual Private Network
  - http://vpn.abc.ro
  - http://www.abc.ro/vpn

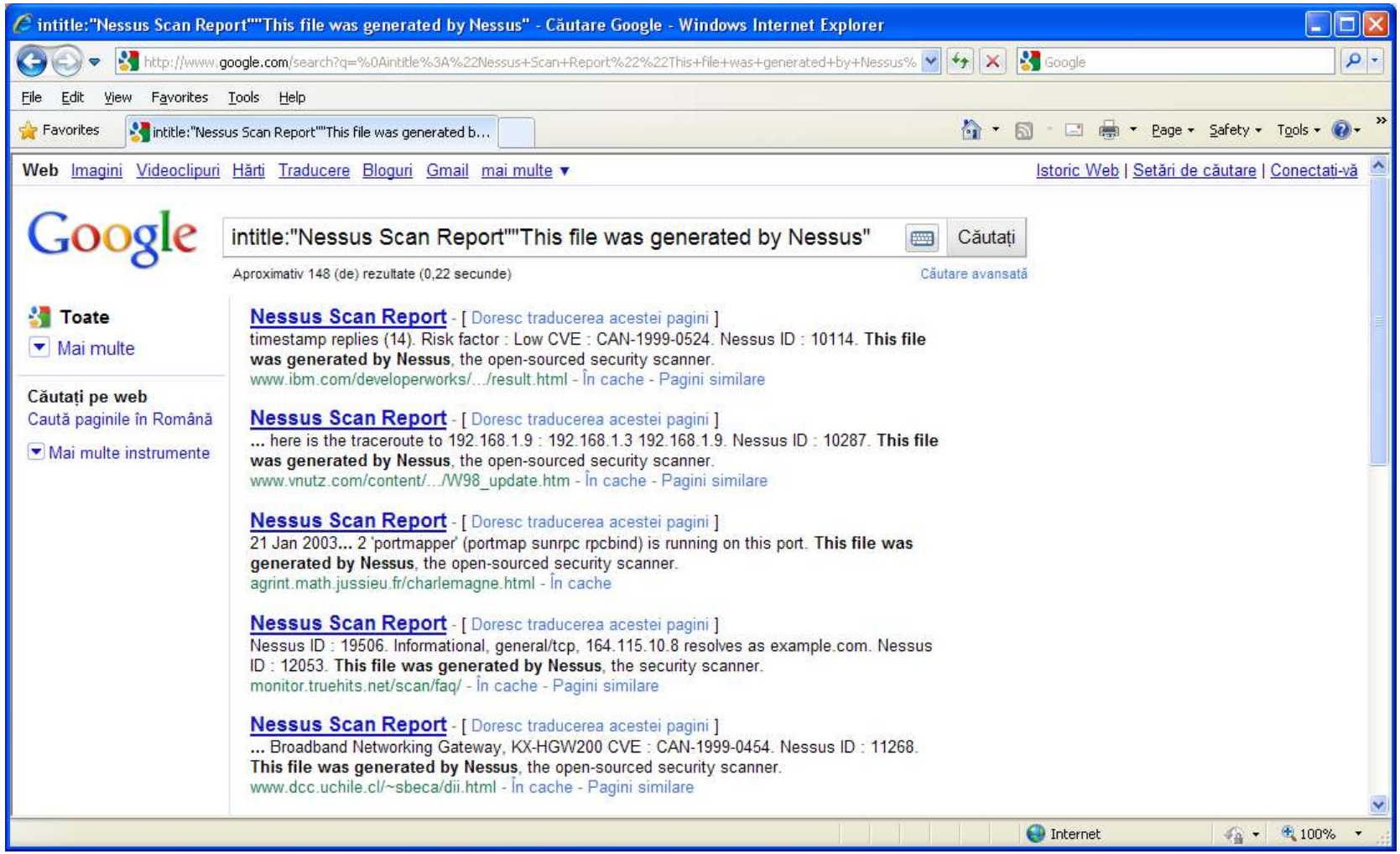
# Google Hacking

- Johnny Long, “Google Hacking for Penetration Testers”, Syngress, 2005
- Google search syntax
  - filetype:doc filetype:pdf filetype:xls
  - intext:, intitle:, inurl:
  - allintext:, allintitle:, allinurl:
  - site:gov site:mil site:abc.ro
  - related:www.abc.ro
  - ➢ http://www.googleguide.com/advanced_operators.html
- Google cache

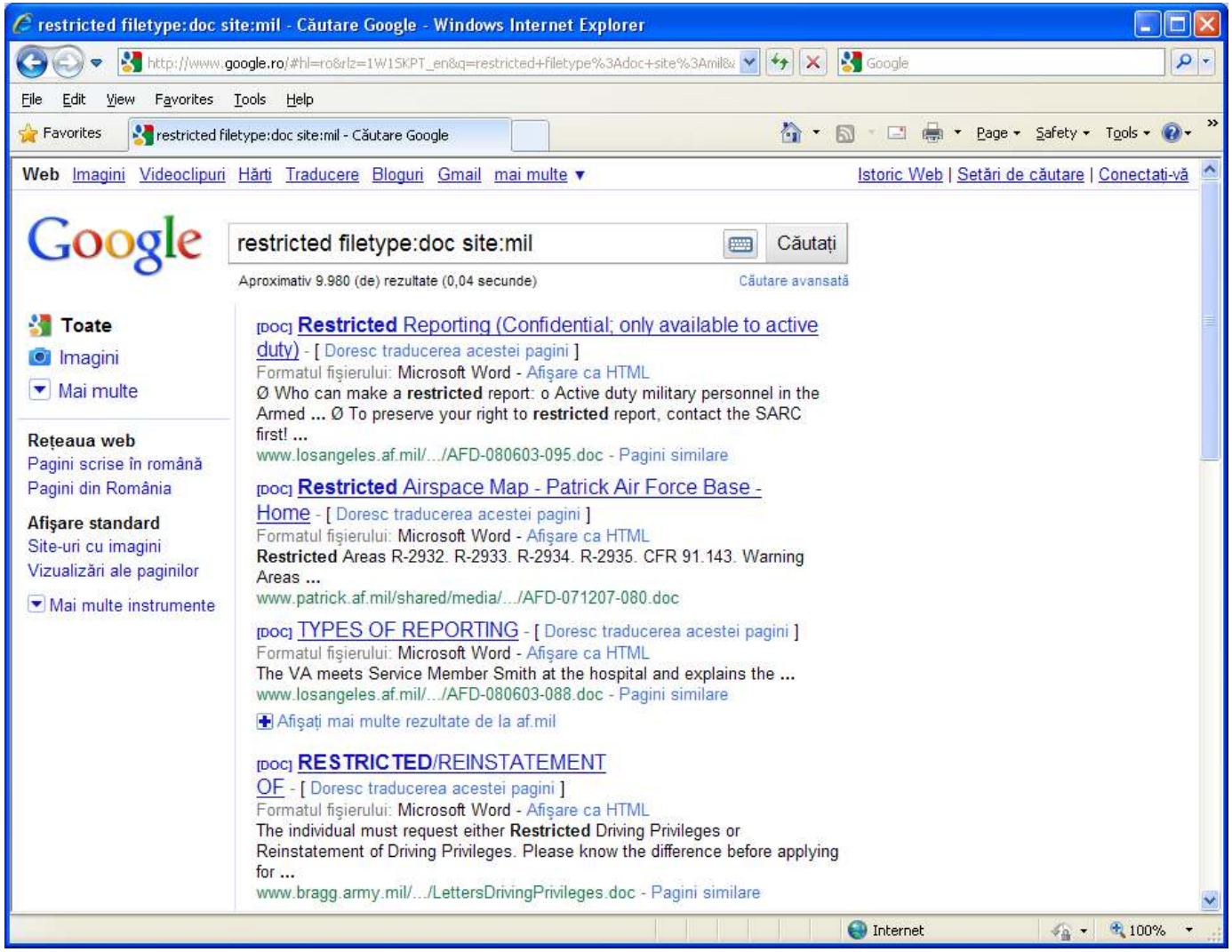
# Google Hacking (cont.)



# Google Hacking (cont.)



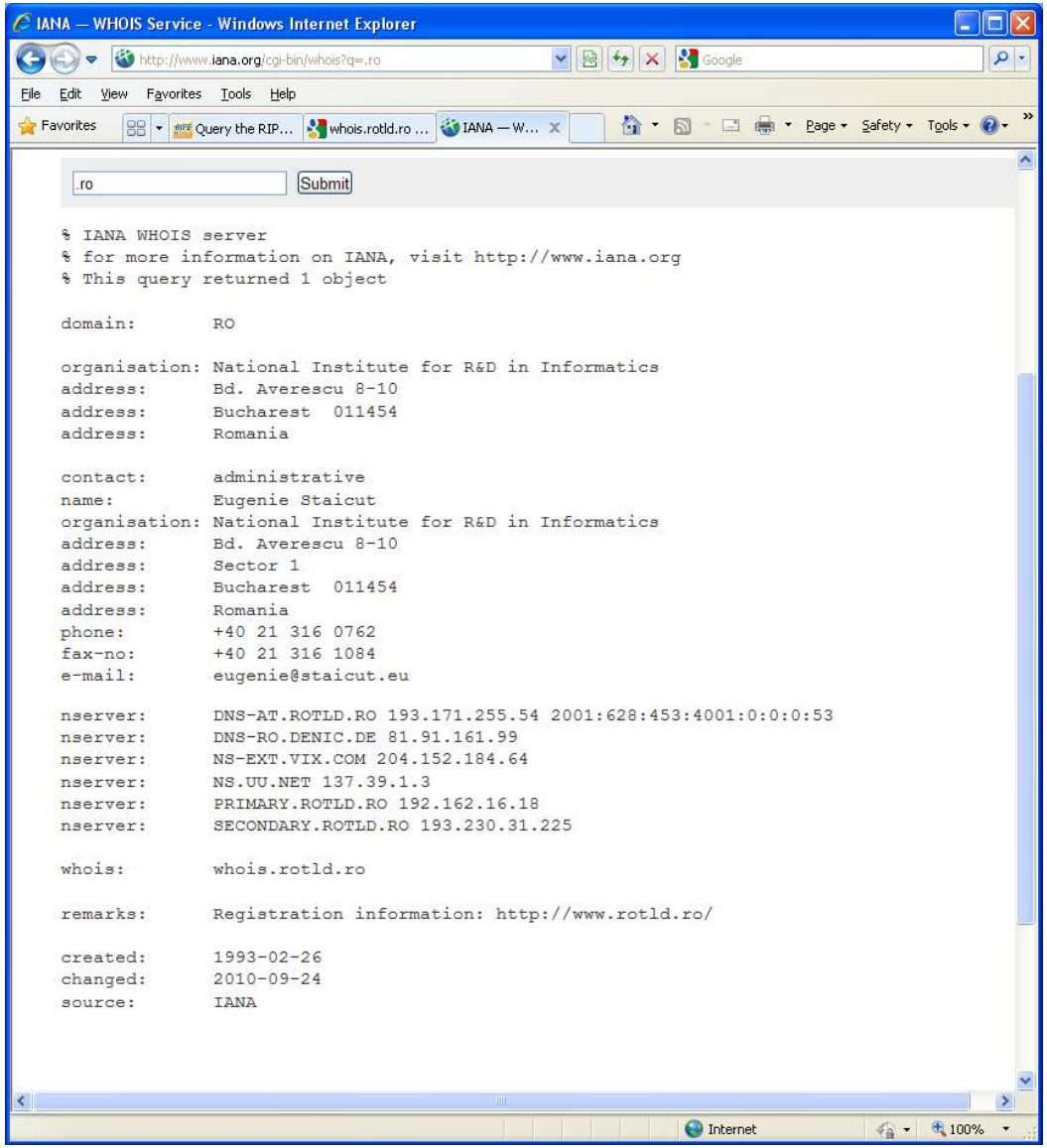
# Google Hacking (cont.)



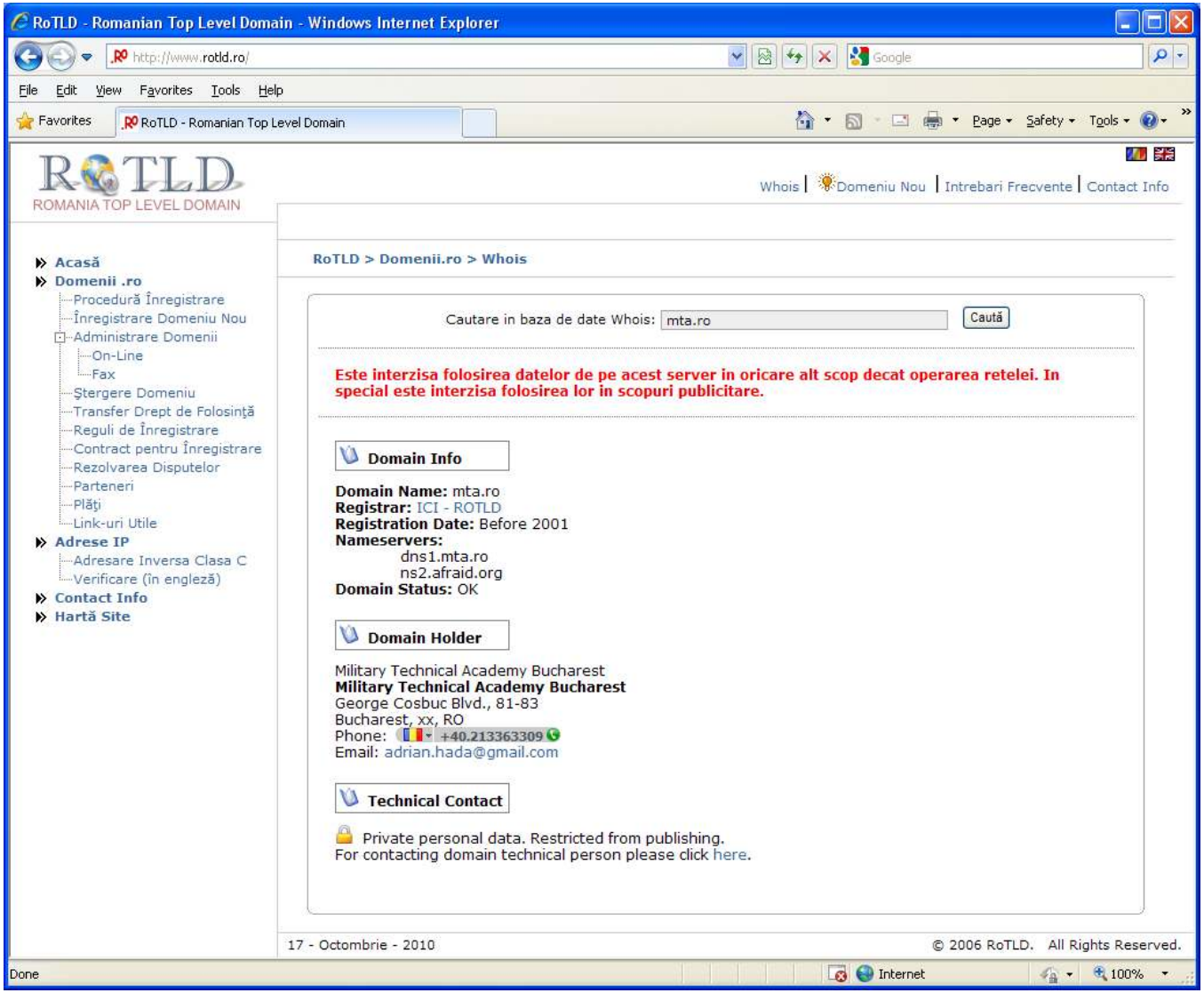
# Whois

- Gestiunea numelor de domeniu, adreselor IP, protocoalelor şi numerelor de porturi în Internet:
  - Internet Assigned Numbers Authority (IANA)
    - http://www.iana.org
  - Internet Corporation for Assigned Names and Numbers (ICANN)
    - http://www.icann.org
- Alocarea Adreselor IP - Regional Internet Registries (RIR)
  - African Network Information Centre (AfriNIC) pentru Africa
  - American Registry for Internet Numbers (ARIN) pentru SUA şi Canada
  - Asia-Pacific Network Information Centre (APNIC) pentru Asia şi Australia
  - Latin America and Caribbean Network Information Centre (LACNIC) pentru America Latină
  - RIPE NCC pentru Europe, Orientul Mijlociu şi Asia Centrală

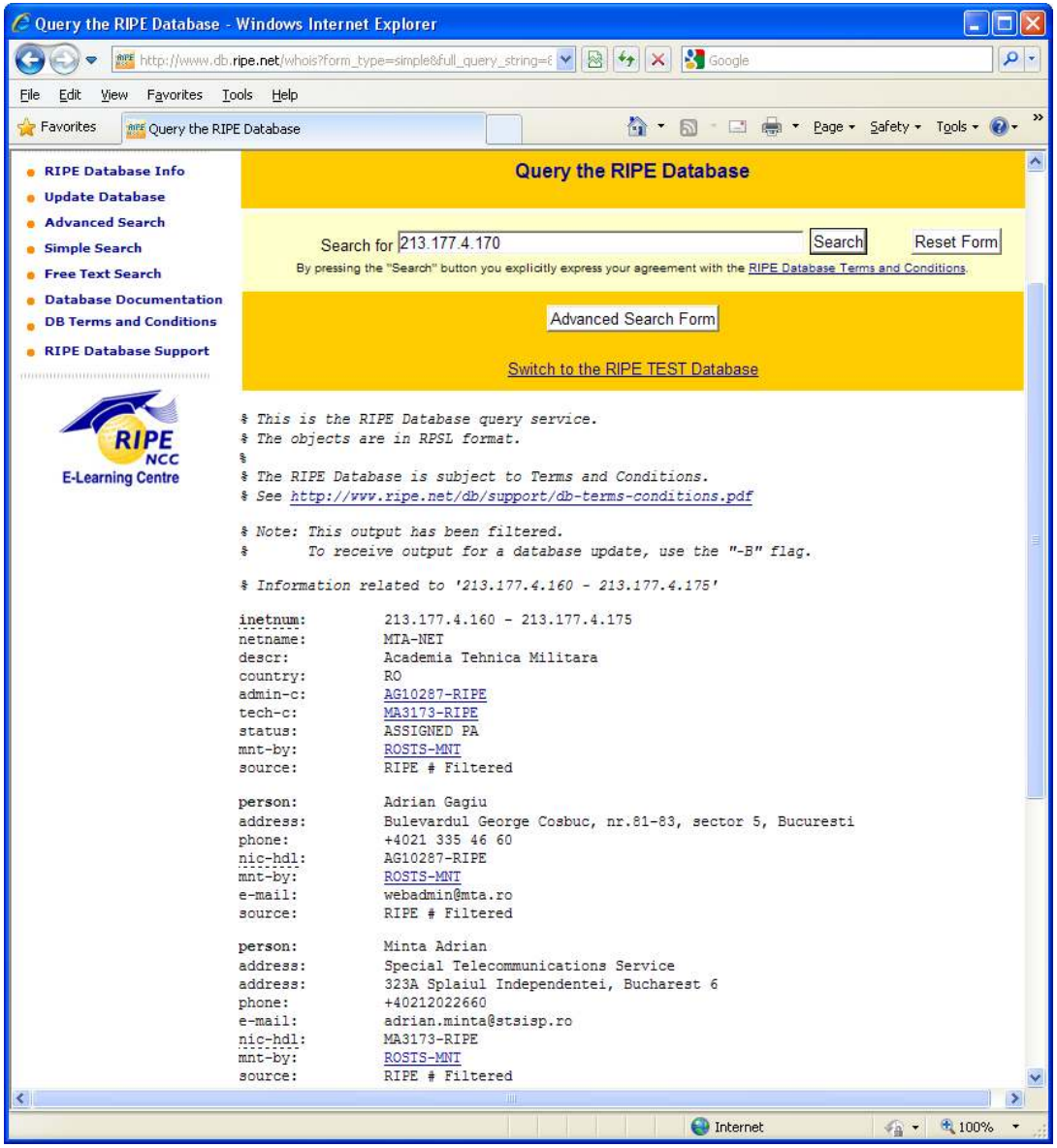
# IANA Search



# ROTLD Search



# RIPE Search



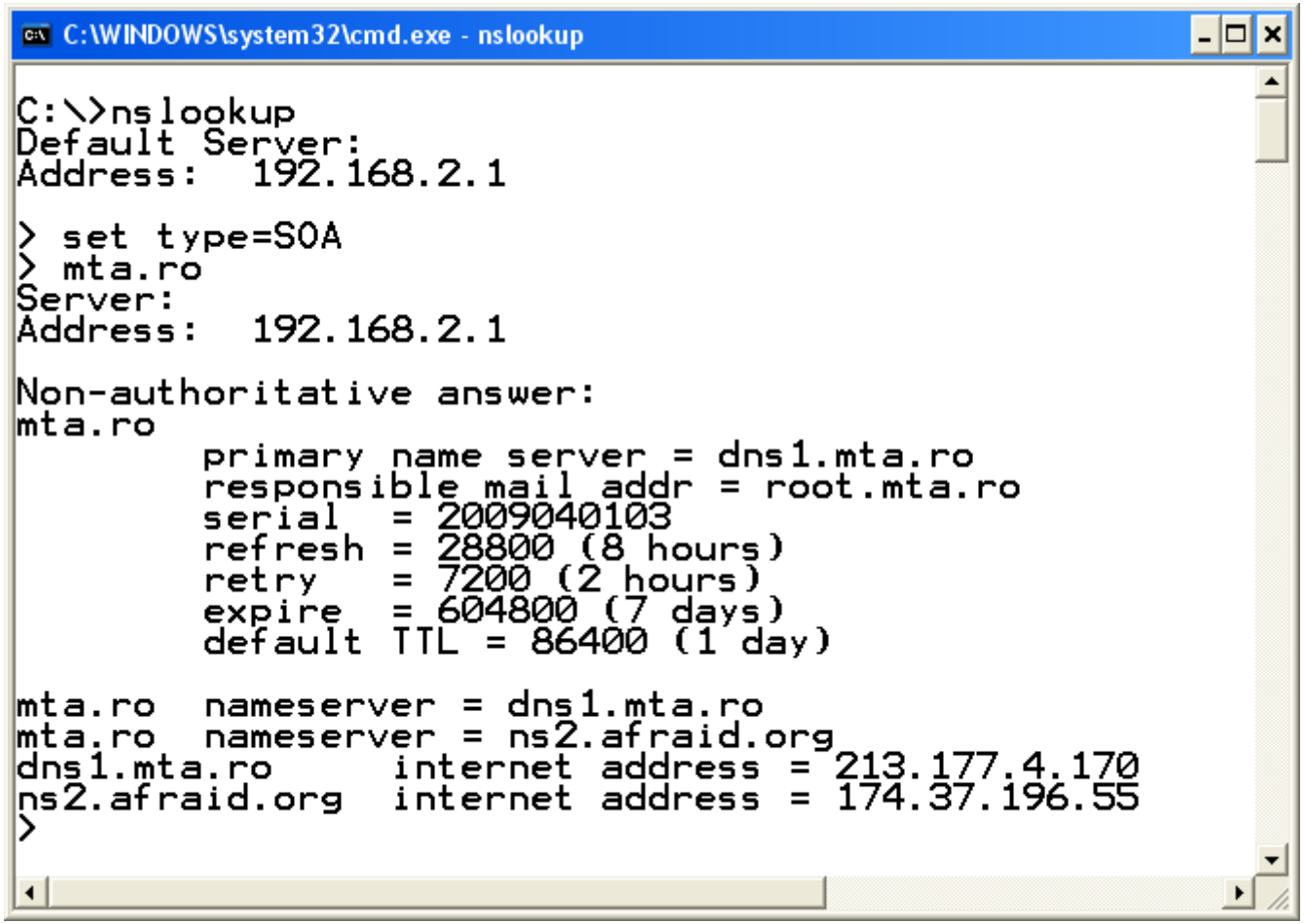
# Interogări DNS

- nslookup, dig, host
- Tipuri de înregistrări

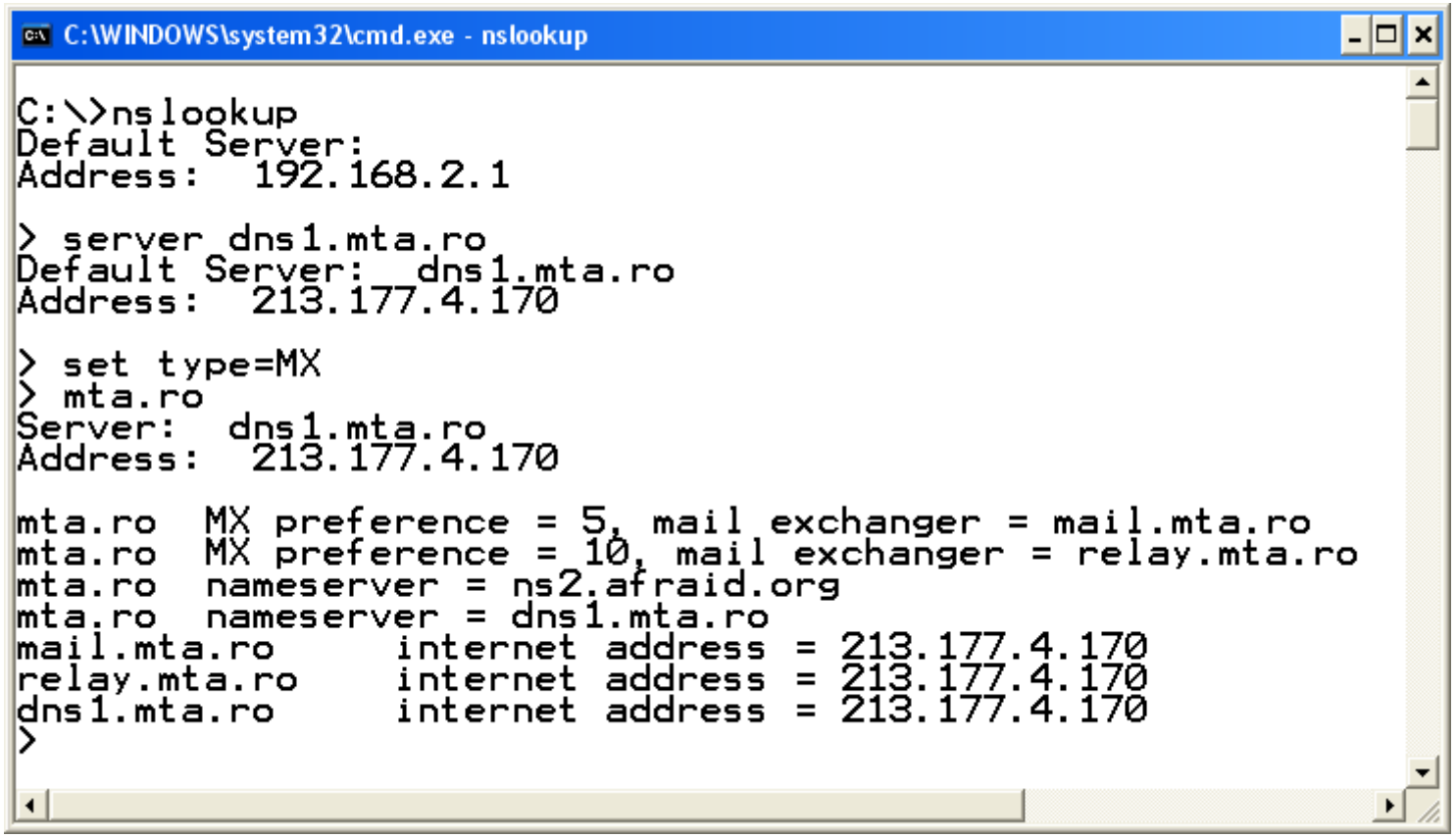
| | |
|---|---|
| SOA | Indicates authority for the domain |
| NS | Host's or domain's name server(s) |
| MX | Host's or domain's mail exchanger(s) |
| A | A host's IP address |
| PTR | Host's domain name, host identified by its IP address |
| SRV | Service location record |
| HINFO | Host information record |
| TXT | Generic text record |
| CNAME | Host's canonical name (aliases) |
| RP | Responsible person |

  - $dig mta.ro SOA
- Transfer de zone
  - $dig @server domain AXFR
  - de regulă, această operaţie este restricţionată în mod corespunzător

# Interogări DNS (cont.)



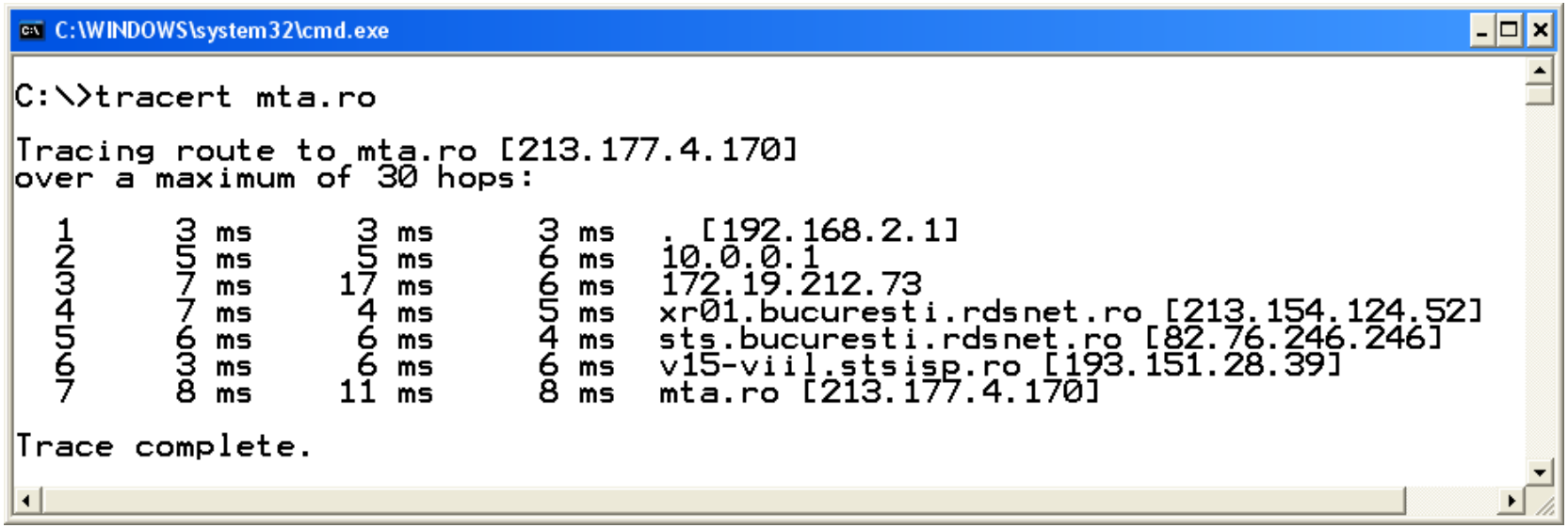
# Interogări DNS (cont.)



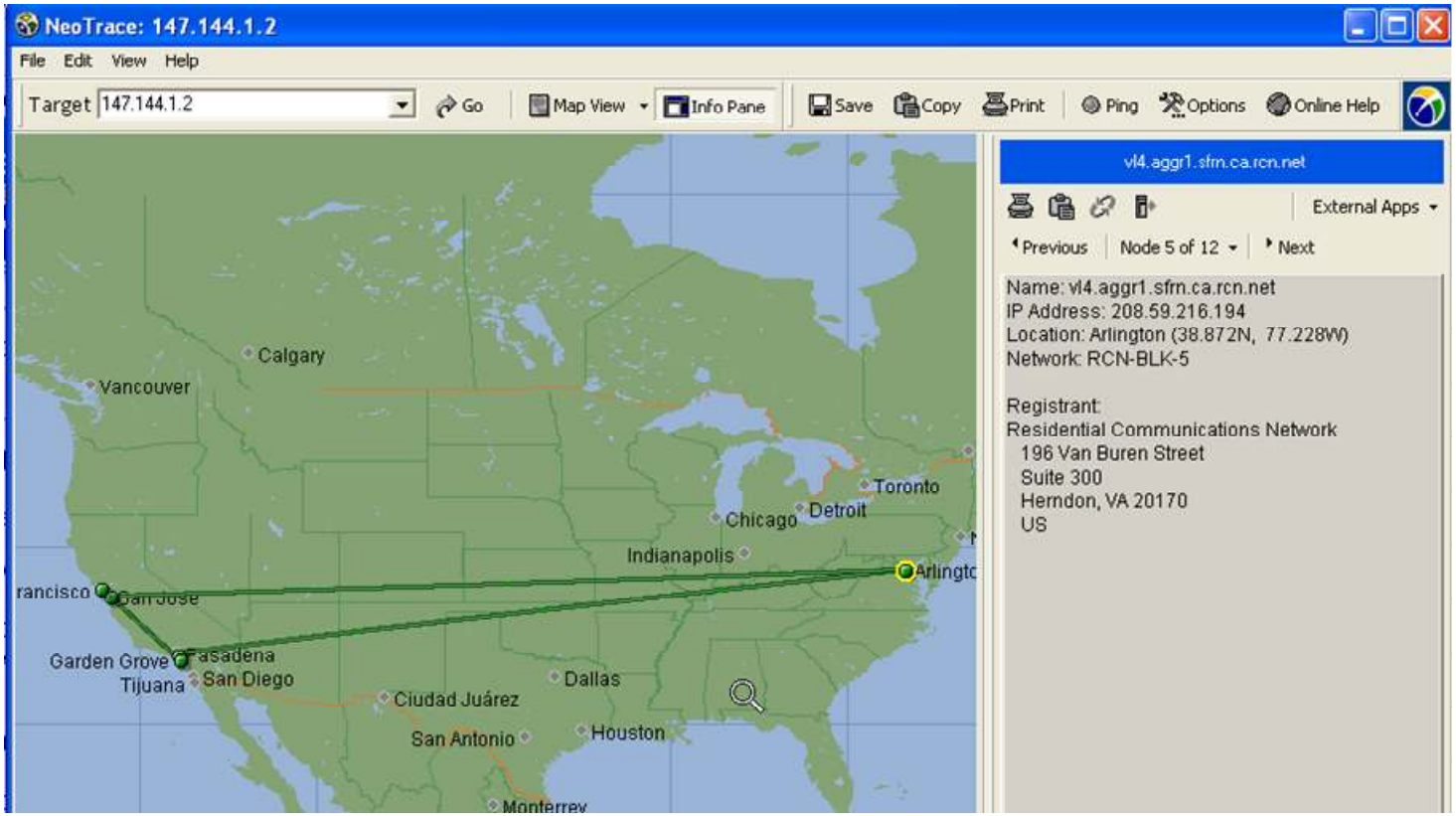
# Recunoaştere la nivel de reţea

- Traceroute
  - descoperire rute, localizare firewall, routere, etc
- tracert (Windows)
  - foloseşte ICMP
- traceroute (Linux)
  - foloseşte UDP
- NeoTrace, VisualRoute, VisualLookout
  - interfaţă grafică

# tracert



# NeoTrace



# Unelte online

- whois.net
- www.dnsstuff.com
- www.netcraft.com
- www.samspade.com