ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

# Module 2. Intelligence Gathering

## Penetration testing course

# OSINT

**Open-source intelligence (OSINT)** is intelligence collected from publicly available sources.

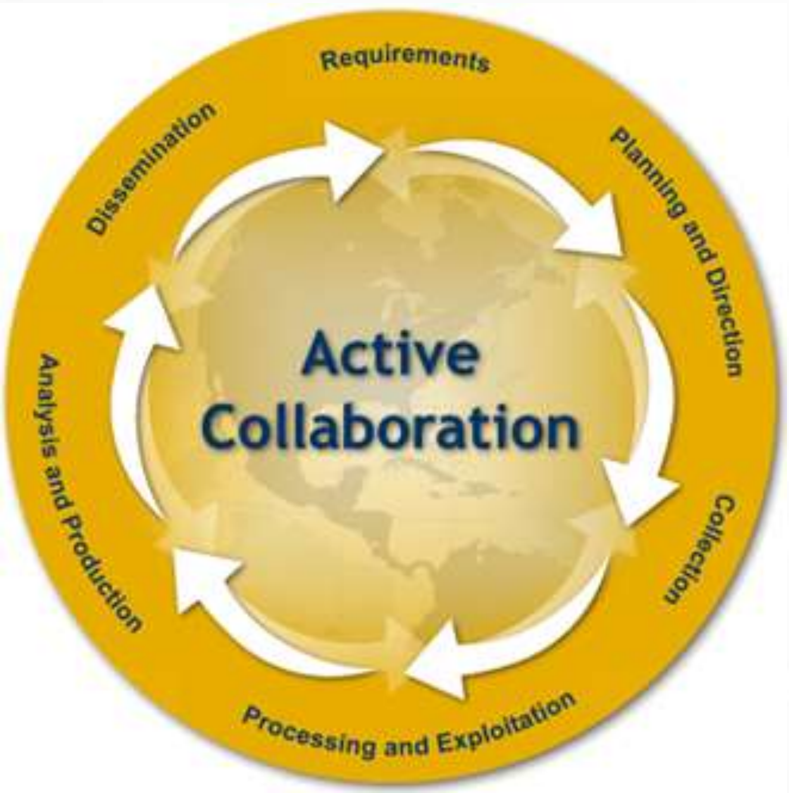
GLOSSARY

# Open sources

OSINT is drawn from publicly available material, including:

- The Internet
- Traditional mass media (e.g. television, radio, newspapers, magazines)
- Specialized journals, conference proceedings, and think tank studies
- Photos
- Geospatial information (e.g. maps and commercial imagery products)

# Intelligence lifecycle (1)



Source: fbi.gov

# Intelligence lifecycle (2)

- **Requirements** are identified information needs—what we must know.
- **Planning and Direction** is management of the entire effort, from identifying the need for information to delivering an intelligence product to a consumer. It involves implementation plans to satisfy requirements established.
- **Collection** is the gathering of raw information based on requirements.
- **Processing and Exploitation** involves converting the vast amount of information collected into a form usable by analysts.
- **Analysis and Production** is the conversion of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information's reliability, validity, and relevance is evaluated and weighed. The information is logically integrated, put in context, and used to produce intelligence. This includes both "raw" and finished intelligence. Raw intelligence is often referred to as "the dots"—individual pieces of information disseminated individually. Finished intelligence reports "connect the dots" by putting information in context and drawing conclusions about its implications.
- **Dissemination**—is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements.

# Structured analytic techniques

- Structured analytic techniques (SATs) – set of methods used by intelligence officer or decision maker for conducting analysis

# The most famous SATs

**Diagnostic Techniques**

- Key Assumptions Check
- Quality of Information Check
- Indicators or Signposts of Change
- Analysis of Competing Hypotheses (ACH)

**Contrarian Techniques**

- Devil’s Advocacy
- Team A/Team B
- High-Impact/Low-Probability Analysis
- “What If?” Analysis

**Imaginative Thinking Techniques**

- Brainstorming
- Outside-In Thinking
- Red Team Analysis
- Alternative Futures Analysis

# Analysis of Competing Hypotheses

Analysis of competing hypotheses, sometimes abbreviated ACH, is a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions. It helps an analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

# Step-by-Step Outline of Analysis of Competing Hypotheses

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.
2. Make a list of significant evidence and arguments for and against each hypothesis.
3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments--that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.
4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.
5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.
6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.
7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.
8. Identify milestones for future observation that may indicate events are taking a different course than expected.

# ACH table example

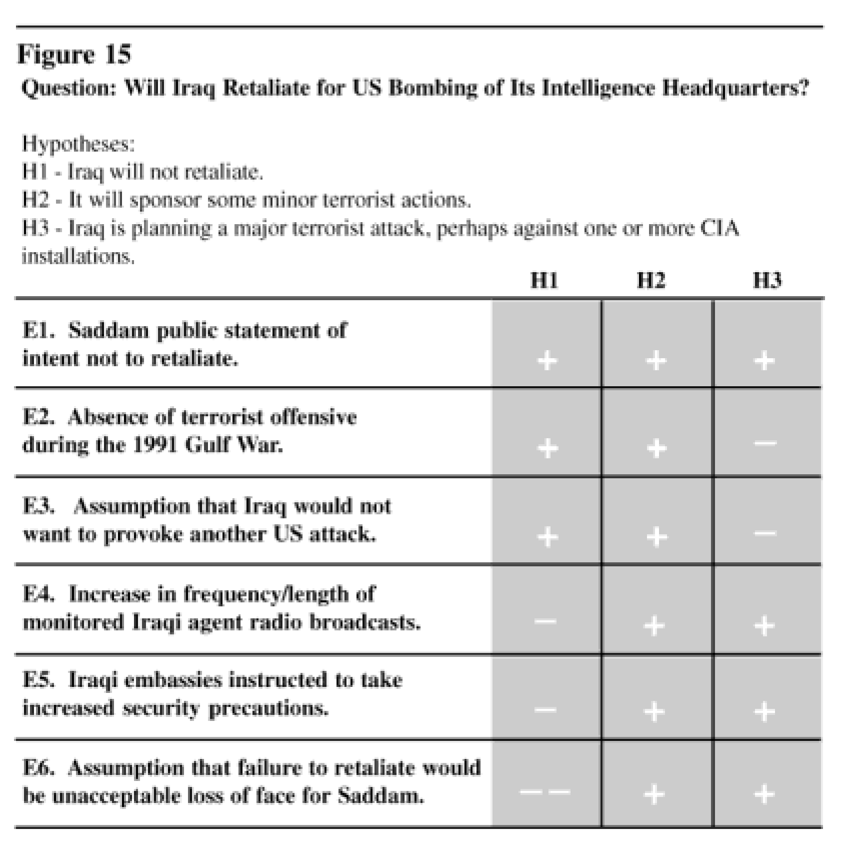


**Figure 15**

**Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?**

Hypotheses:
H1 - Iraq will not retaliate.
H2 - It will sponsor some minor terrorist actions.
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

| | H1 | H2 | H3 |
|---|---|---|---|
| **E1. Saddam public statement of intent not to retaliate.** | + | + | + |
| **E2. Absence of terrorist offensive during the 1991 Gulf War.** | + | + | – |
| **E3. Assumption that Iraq would not want to provoke another US attack.** | + | + | – |
| **E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.** | – | + | + |
| **E5. Iraqi embassies instructed to take increased security precautions.** | – | + | + |
| **E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.** | – – | + | + |

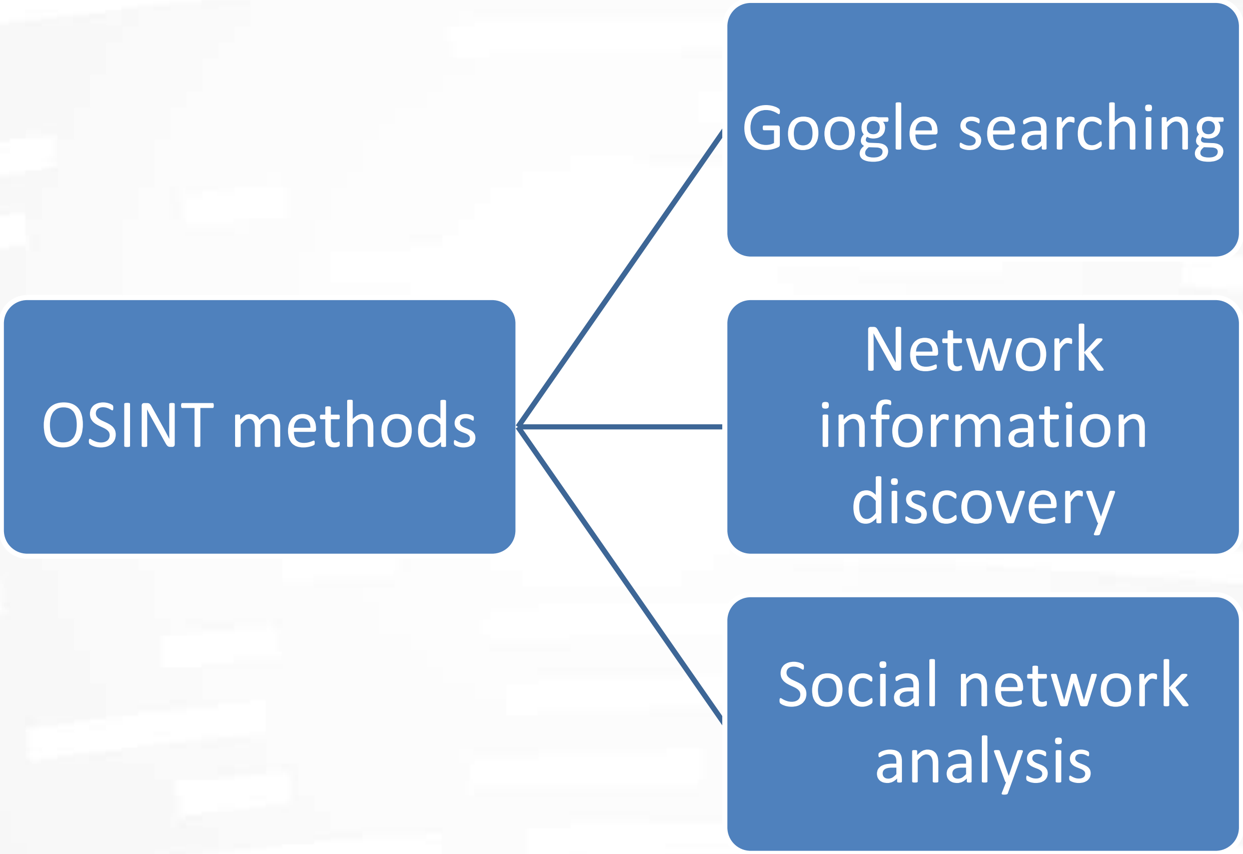
# Application of ACH for OSINT

- Use of ACH allows to limit amount of the information we have to collect to prove the selected hypothesis.

# Structured thinking

Structured thinking for penetration testers is more important than knowledge of Hacking tools and methods.

# Open source data collection for penetration testers



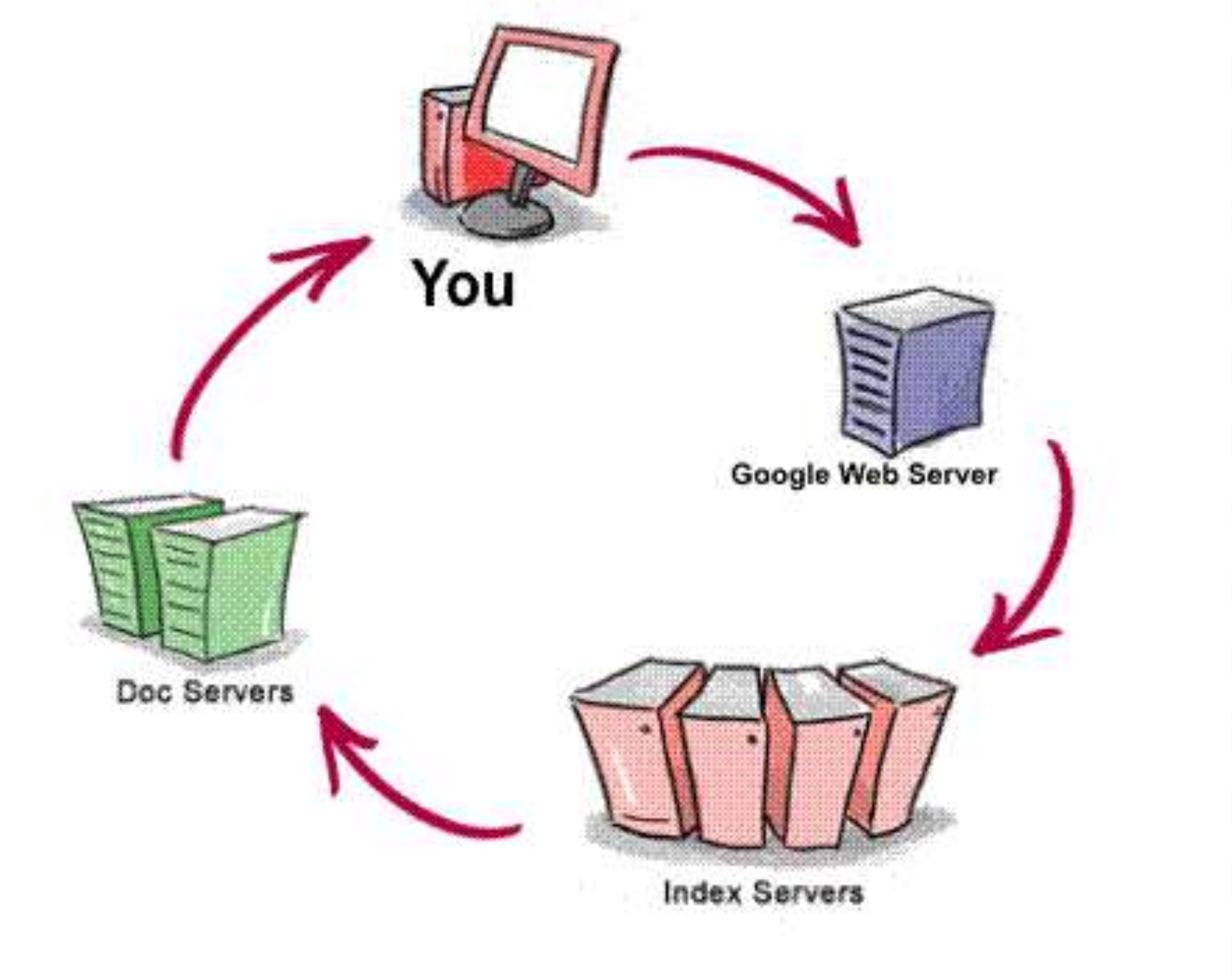
OSINT methods

Google searching

Network information discovery

Social network analysis

# What happens when you are googling?

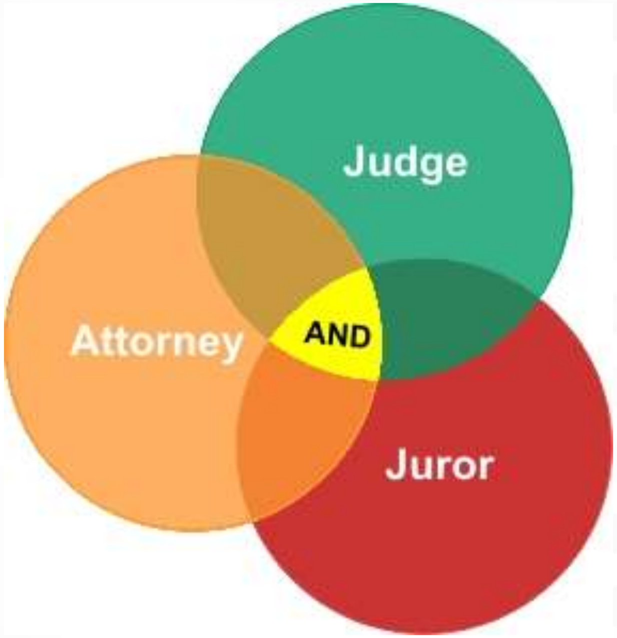


# Google Cache

- Cached reveals the page as Google found it
  - may differ from the current page
  - Cached exists if a page is full-text indexed
    - Not fully searchable
  - no Cached if a page owner requests not to be cached

# Boolean search

- AND



# Stemming

- Google stems “when appropriate”
  - Includes plural, singular, past, present tense of words in search

Search: school librarian

Result: library, librarian, library’s, librarian’s

Single word searches aren’t stemmed

# What Google doesn’t search

- Common or Stop words are ignored
  - No official list from Google
  - Auto-phrasing
  - Searches containing only stop words

Example: he, here, her, a

# Advanced operators (1)

**+** Inclusion operator

- Force searches on stop words
- Turns off stemming

Use **quotation marks** for phrases ("searching phrase")

- Forces searches on stop words
- Turns off stemming

# Advanced operators (2)

OR search

- Search for two terms at once

Search: “penetration testing” OR “ethical hacking”

- exclusion operator

- Exclude results with the specific word

Search: bmv 3 series -advertisement

# Advanced operators (3)

***** full-word wild card, word substitution

- Ideal for partly remembered quotes
- Searching for answers to questions
- Proximity searches

**~** synonym operator

- ~guide searches for: tutorial, manual, help, map, tips

# Advanced operators (4)

**site:**

- limits search for particular domain name

books site:cia.gov

**filetype:**

- search for a particular type of document

tax return **filetype:**pdf

# Malicious use of Google

Google Hacking Database

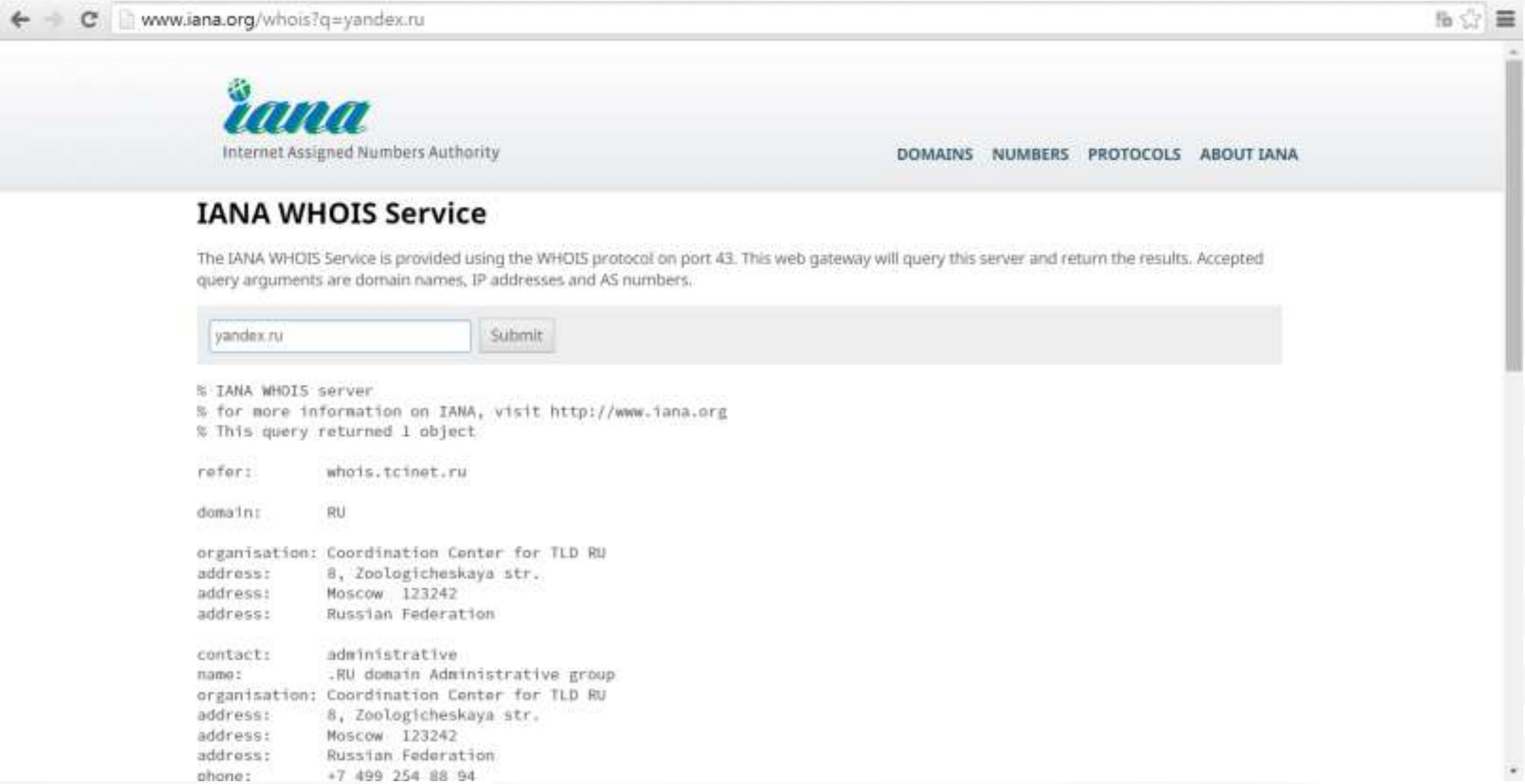
www.**hackers**forcharity.org/ghdb/

Contains a lot of requests for searching for passwords, vulnerable sites, interesting log-files, etc.

# Whois service

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.

# Whois example

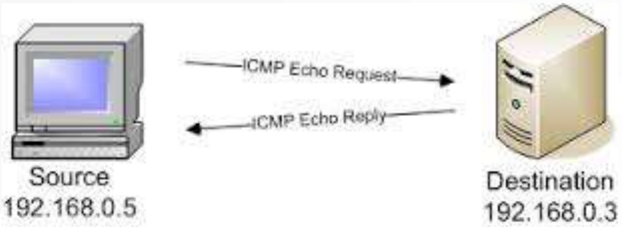

www.iana.org/whois?q=yandex.ru
iana
Internet Assigned Numbers Authority
DOMAINS
NUMBERS
PROTOCOLS
ABOUT IANA
yandex.ru
Submit

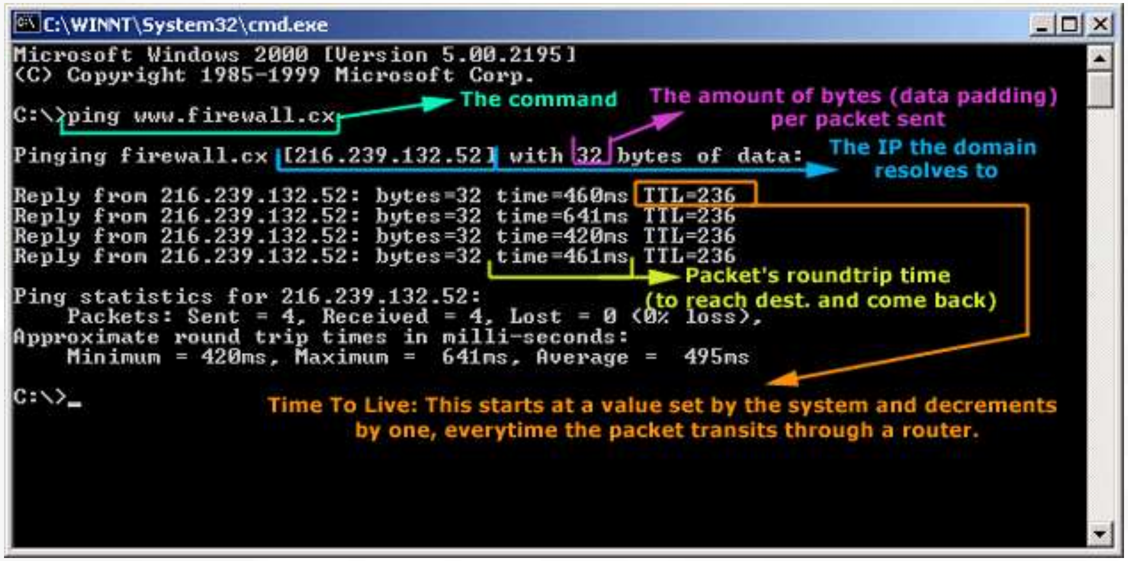
## IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this server and return the results. Accepted query arguments are domain names, IP addresses and AS numbers.

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.tcinet.ru

domain:       RU

organisation: Coordination Center for TLD RU
address:      8, Zoologicheskaya str.
address:      Moscow  123242
address:      Russian Federation

contact:      administrative
name:         .RU domain Administrative group
organisation: Coordination Center for TLD RU
address:      8, Zoologicheskaya str.
address:      Moscow  123242
address:      Russian Federation
phone:        +7 499 254 88 94
```

# Ping





```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ping www.firewall.cx

Pinging firewall.cx [216.239.132.52] with 32 bytes of data:

Reply from 216.239.132.52: bytes=32 time=460ms TTL=236
Reply from 216.239.132.52: bytes=32 time=641ms TTL=236
Reply from 216.239.132.52: bytes=32 time=420ms TTL=236
Reply from 216.239.132.52: bytes=32 time=461ms TTL=236

Ping statistics for 216.239.132.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 420ms, Maximum =  641ms, Average =  495ms

C:\>_
```

The command

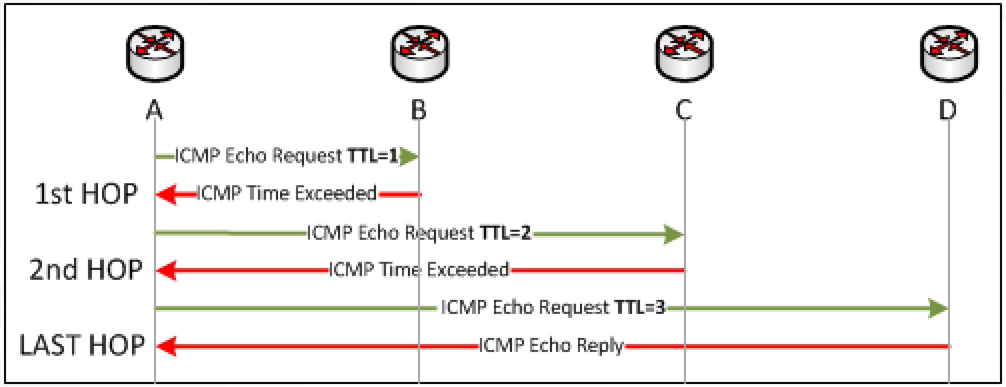
The amount of bytes (data padding) per packet sent

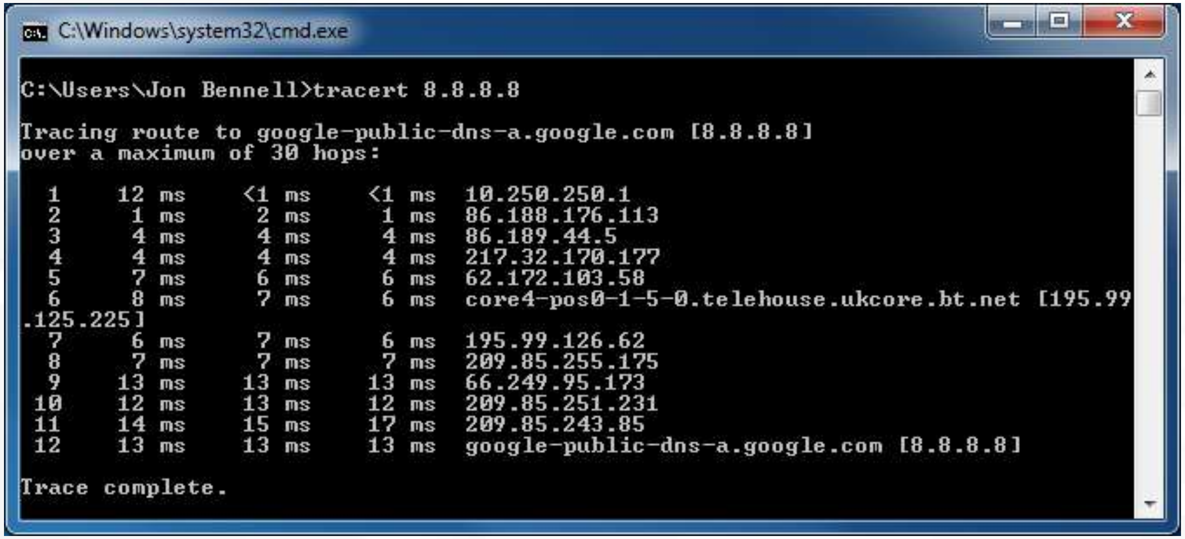
The IP the domain resolves to

Packet's roundtrip time (to reach dest. and come back)

Time To Live: This starts at a value set by the system and decrements by one, everytime the packet transits through a router.

# Tracert or traceroute





```
C:\Users\Jon Bennell>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1    12 ms    <1 ms    <1 ms  10.250.250.1
  2     1 ms     2 ms     1 ms  86.188.176.113
  3     4 ms     4 ms     4 ms  86.189.44.5
  4     4 ms     4 ms     4 ms  217.32.170.177
  5     7 ms     6 ms     6 ms  62.172.103.58
  6     8 ms     7 ms     6 ms  core4-pos0-1-5-0.telehouse.ukcore.bt.net [195.99
.125.225]
  7     6 ms     7 ms     6 ms  195.99.126.62
  8     7 ms     7 ms     7 ms  209.85.255.175
  9    13 ms    13 ms    13 ms  66.249.95.173
 10    12 ms    13 ms    12 ms  209.85.251.231
 11    14 ms    15 ms    17 ms  209.85.243.85
 12    13 ms    13 ms    13 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

# Maltego

- Maltego: open source intelligence & forensics application offering extraordinary data mining and intelligence gathering capabilities
- Results are well represented in a variety of easy to understand views
- In concert with its graphing libraries, Maltego identifies key relationships between data sets and identifies previously unknown relationships between them

# A few words about social network analysis