Network Security (NetSec)

Summer 2015
Chapter 01: Fundamentals
Module 04: Reconnaissance

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

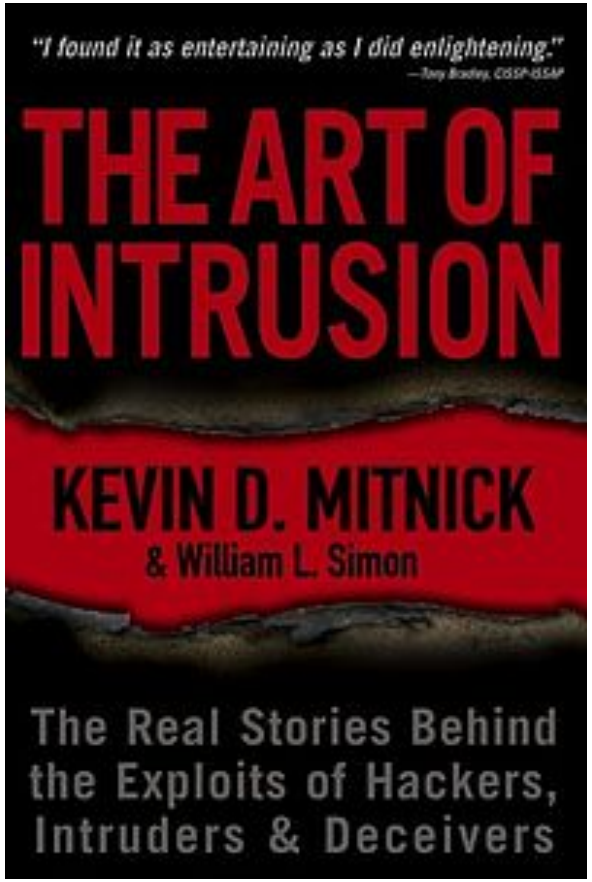
Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Learning Objectives

Some practical insights into reconnaissance (to prepare attacks on networks)

- Know basic means on how to identify and map networking infrastructure
- Identify which pieces of information are public and do hence not provide any stronghold/defense (in a sense of security by obscurity)
- Develop awareness of the attacker’ s moves; know the preparatory steps potential attackers are going to perform

To probe further


"I found it as entertaining as I did enlightening."
—Tony Bradley, CISSP-ISSAP
THE ART OF INTRUSION
KEVIN D. MITNICK
& William L. Simon
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Take an attacker’ s perspective before thinking about defenses!

Here: Reconnaissance

Overview of this Module

(1) "Casing the joint"

(2) The Robin Hood hacker

(3) Reconnaissance with public sources of information

(4) Reconnaissance with active scanning/probing
(in part in Appendix)

(5) Recommended readings

Chapter 01, Module 04

“Casing the Joint” - Definitions

“Casing the Joint” – informal for reconnoitering before a robbery

Random House Dictionary: **re·con·nais·sance**

- 1.the act of reconnoitering.
- 2.Military. a search made for useful military information in the field, esp. by examining the ground.
- 3.Surveying, Civil Engineering. a general examination or survey of a region, usually followed by a detailed survey.
- 4.Geology. an examination or survey of the general geological characteristics of a region.

Wordnet: **reconnaissance**

- the act of reconnoitring (especially to gain information about an enemy or potential enemy); "an exchange of fire occurred on a reconnaissance mission"

The Robin Hood Hacker

The Robin Hood Hacker

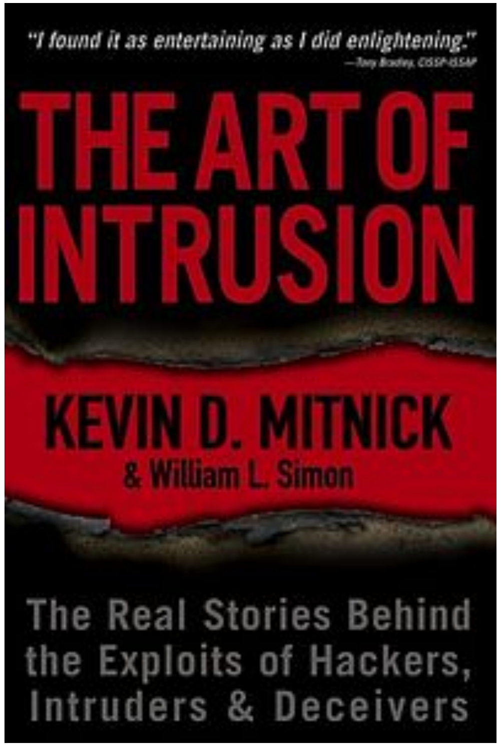
Who of you has heard about the "New York Times Hack"?
Who of you has heard about the "Robin Hood Hacker" behind it?

Here comes part of the story of Adrian Lamo …

- It gives some insights on what creative minds will do to hack a network …
- … and might teach you something about trust in humans.

- *"[Hacking] has always been for me less about technology and more about religion"*

– Adrian Lamo


"I found it as entertaining as I did enlightening."
—Tony Bradley, CISSP-ISSAP
THE ART OF INTRUSION
KEVIN D. MITNICK
& William L. Simon
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Source: Ch.5 from the above book

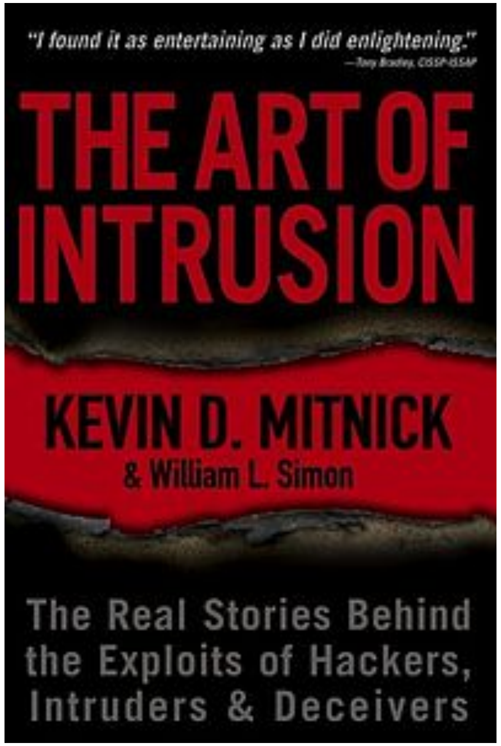
The Robin Hood Hacker

Some background

- The young Adrian Lamo is called Robin Hood hacker, since he does not hide his identity and he informs the owners of the hacked networks about the problems – he hacks out of curiosity, but for good
- Adrian hacked into Microsoft, Yahoo, MCI WorldCom, Excite@Home, Cingular, and other telcos

Hacking Excite@home

- Curiosity … a network managing all cable customers in the country surely is well protected
- From an open network in a students lounge, he accessed the webpage, finds a misconfigured proxy that gives access to one internal webserver


"I found it as entertaining as I did enlightening."
THE ART OF INTRUSION
KEVIN D. MITNICK
& William L. Simon
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

Source: Ch.5 from the above book

The Robin Hood Hacker

Hacking Excite@home contd.

- He posts message on this internal server on having problems to log in
- The response contains a URL pointing to the system for managing IT problems, this URL gives clues about other (similar) systems in the network that handle support related questions
- There is no authentication for the support systems – they are designed for "internal" access (anyone calling the system must have access since this is privileged info – security by obscurity)
- Netcraft.com to find out OS of server systems
- Network operation center offers helpdesk system … with plenty of details on customer account data, password, on handling trouble tickets, script for generating authentication cookies (allowing helpdesk members to login as the customer who is calling)
- He calls a guy with a particular strange ticket that has never been resolved by Excite@home support and is about stolen credit card details

The Robin Hood Hacker

Hacking Excite@home contd.

- Open proxy stops working
- He performs reverse DNS lookups and probes IP addresses, ends up finding dialup00.corp.home.net
- Dialup-users run Win98, have open network shares, etc.
- Changes startup script so remote users run software for Adrian
- Installs remote desktop management software (virus checkers do not alarm, since this is legitimate software)
- Learns what internal systems the dialup users access using netstat
- On the discovered servers, he finds
  - Database of > 3 million subscribers with details such as OS the users use, cable modem serial numbers, names, email addresses
  - Adrian nows a lead network engineer at Excite@home, tells him all details (meeting at 4:30 AM in the morning)
  - Finally wants to see proxy server in data-center … is asked: “how would you secure this server”, cuts ethernet wire with pocket knife … engineer says “that’s good enough”, attaches note “do not re-attach”

The Robin Hood Hacker

Hacking NY-Times

- Curiosity: have already access to washington post, wouldn't t be nice to be in the NYT network
- Website hosted with company, i.e. outside the network
- Using whois (arin.net) to get some basic server info
- Port scan of addresses belonging to NYT
- Various open proxies that allowed him in, but not of direct use
- Email of all NYT staffers from external website (that agrred on being reachable via the Internet) … sends mail and gets back answer
- IP addresses in mail headers as a starting point … manual scan of IP addresses, but only internal we servers without much info
- Finds old NYT Intranet site, decommissioned, but with link to production system … with material teaching staff on how to operate the system
- Search engine on this machine that allows free-form SQL queries

The Robin Hood Hacker

Hacking NY-Times (contd.)

- System used Lotus Nodes, full database access here meant all information of all employees, newsstand owners, etc … down to social security number, how much they earn, any complaints about service of NYT, etc.
- Yet Adrian does not know, which OS the system was running … "*I don't analyze networks this way*", "*its about the people and how they configure the network. Most people are very predictable*"
- Internal search engine in fact indexed the entire site, SQL query tool on server … by probing he finds database names, etc. containing
    - Complete username-password list at NYT
    - List of all persons held on terrorist charge in US
    - List of all op-ed (opposite the editorial page) writers, containing info of celebs such as robert redford
    - Adds his own number and contact detail as "computer hacking/ security and communicatoins intelligence"

The Robin Hood Hacker

Hacking NY-Times (contd.)

- …
- Discovers that he can use LexisNexis database system with access to legal and news information … is claimed to have performed 3000 searches … is undiscovered for some 3 months
- He decides to tell a friend (reporter) with details under agreement to not publish before he informs the NYT and told them how to fix problem
- NYT has no interest to learn this, has to be pressed to learn about the vulnerability … fixes it in the following 48 hours … call the FBI, after they learn that Adrian used LexisNexis … Adrian hides for five days, then “surrenders” at StarBucks
- Is sued with damages in the 300.000 USD range (calculated using the price of pay as you go searches with 12USD each, which would mean 270 queries per day for 3 months) …
- 65.000 USD charges + 6 months home confinement
- Btw. Is not fluent in any programming language …

Robin Hood turning Evil?

And now for something completely different

- The very same Adrian Lamo is also known as the person who turned in Bradley Manning with the report that Manning had leaked thousands of sensitive U.S. government documents, thus starting the wikileaks scandal … apparently, Manning trusted Lamo after having chatted with him extensively …

- If you are interested to learn more, the Internet is full of Information on this case … good starting points are wired.com (with a pro Lamo coverage) or for opposing views wikileaks.org and salon.com (condemning wired.com) …

Source: http://www.wikileaks.org/

Some Basic Reconnaissance

Reconnaissance based on Publicly Available Information

To be reachable, need to register domain names and to allow for resolving them (to allow for mapping “names” into “addresses”)

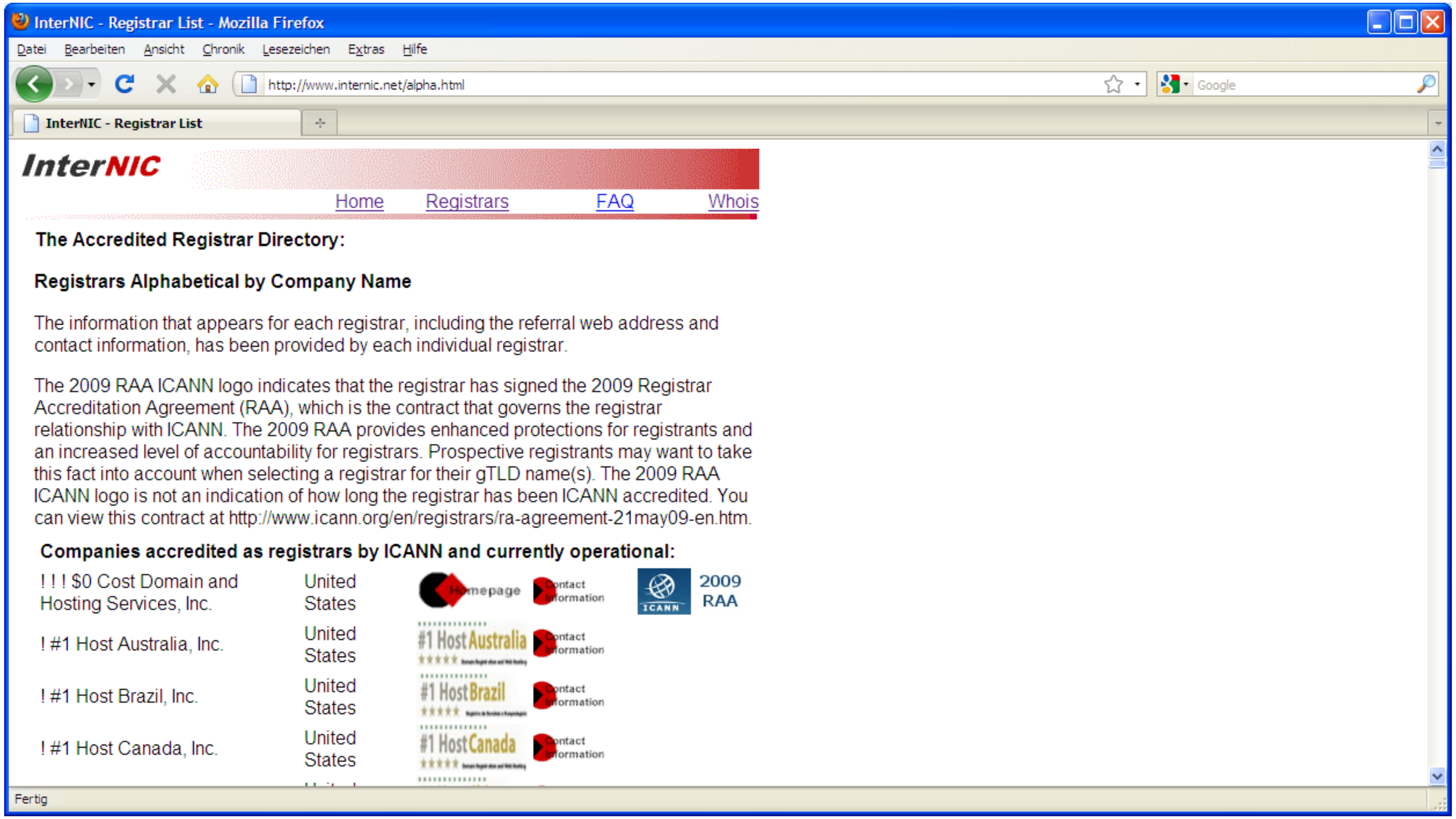
Here we are taking a closer look at

- Reconnaissance with whois
- Reconnaissance with DNS

A few words about a Registrar:

- Organization where you register a domain name
- Verifies uniqueness of name
- Enters domain name into various databases: whois & DNS
- List of registrars can be obtained from internic.net

Querying Databases: Target “tu-darmstadt.de”


InterNIC - Registrar List - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.internic.net/alpha.html
Google
InterNIC - Registrar List
InterNIC
Home Registrars FAQ Whois
Fertig

The Accredited Registrar Directory:

Registrars Alphabetical by Company Name

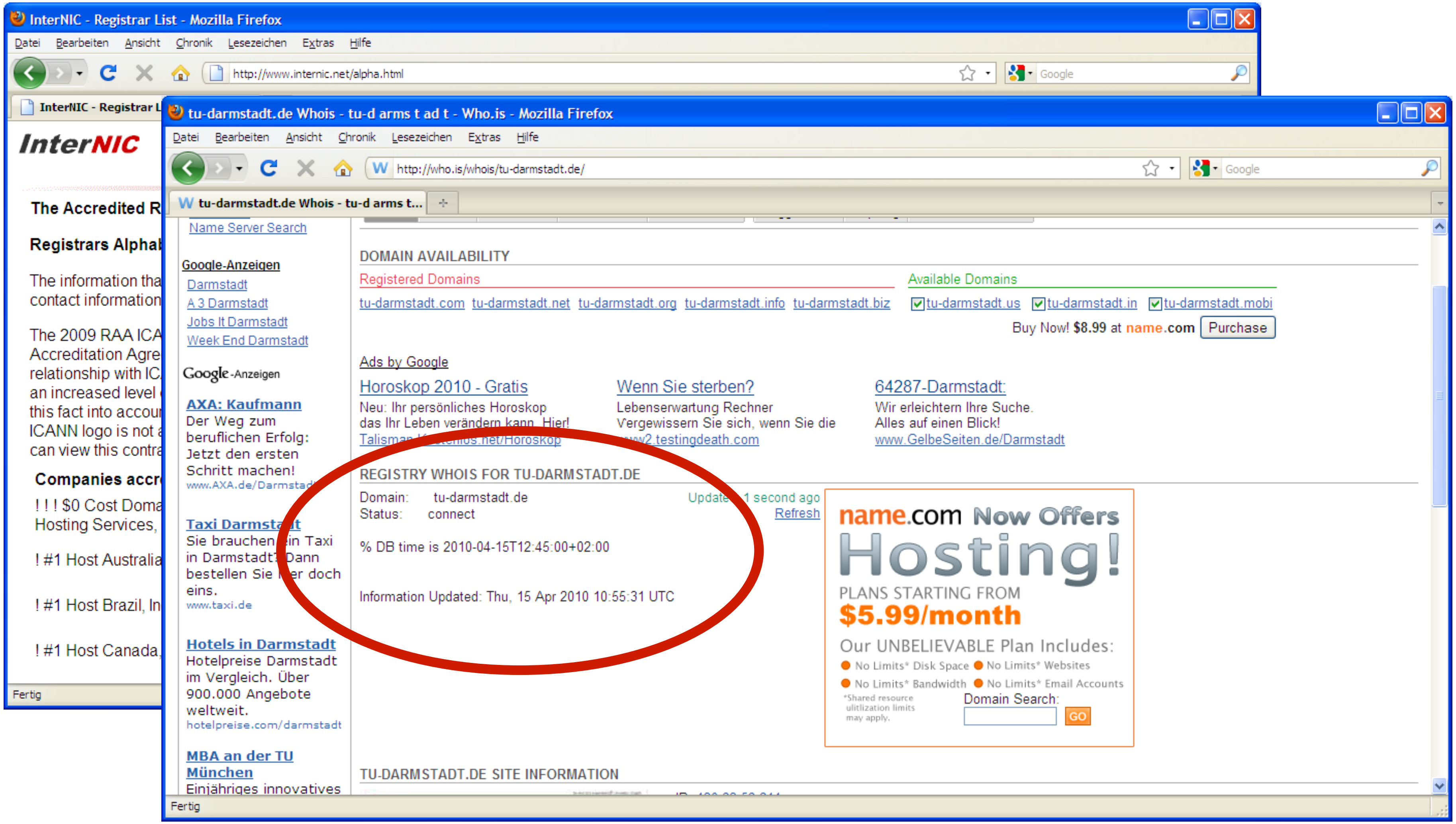
The information that appears for each registrar, including the referral web address and contact information, has been provided by each individual registrar.

The 2009 RAA ICANN logo indicates that the registrar has signed the 2009 Registrar Accreditation Agreement (RAA), which is the contract that governs the registrar relationship with ICANN. The 2009 RAA provides enhanced protections for registrants and an increased level of accountability for registrars. Prospective registrants may want to take this fact into account when selecting a registrar for their gTLD name(s). The 2009 RAA ICANN logo is not an indication of how long the registrar has been ICANN accredited. You can view this contract at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm.

Companies accredited as registrars by ICANN and currently operational:

! ! ! $0 Cost Domain and Hosting Services, Inc.	United States	Homepage	Contact Information	ICANN 2009 RAA
! #1 Host Australia, Inc.	United States	#1 Host Australia	Contact Information	
! #1 Host Brazil, Inc.	United States	#1 Host Brazil	Contact Information	
! #1 Host Canada, Inc.	United States	#1 Host Canada	Contact Information	

Querying Databases: Target “tu-darmstadt.de”


InterNIC - Registrar List - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.internic.net/alpha.html
Google
InterNIC - Registrar L
InterNIC
tu-darmstadt.de Whois - tu-d arms t ad t - Who.is - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://who.is/whois/tu-darmstadt.de/
Google
tu-darmstadt.de Whois - tu-d arms t...
Fertig

The Accredited R

Registrars Alphab

The information tha contact information

The 2009 RAA ICA Accreditation Agre relationship with IC an increased level this fact into accour ICANN logo is not a can view this contra

Companies accre

! ! ! $0 Cost Doma Hosting Services,

! #1 Host Australia

! #1 Host Brazil, In

! #1 Host Canada,

Fertig

Name Server Search

Google-Anzeigen

Darmstadt

A 3 Darmstadt

Jobs It Darmstadt

Week End Darmstadt

Google-Anzeigen

AXA: Kaufmann
Der Weg zum beruflichen Erfolg: Jetzt den ersten Schritt machen!
www.AXA.de/Darmstadt

Taxi Darmstadt
Sie brauchen ein Taxi in Darmstadt? Dann bestellen Sie hier doch eins.
www.taxi.de

Hotels in Darmstadt
Hotelpreise Darmstadt im Vergleich. Über 900.000 Angebote weltweit.
hotelpreise.com/darmstadt

MBA an der TU München
Einjähriges innovatives

DOMAIN AVAILABILITY

Registered Domains

tu-darmstadt.com tu-darmstadt.net tu-darmstadt.org tu-darmstadt.info tu-darmstadt.biz

Available Domains

☑ tu-darmstadt.us ☑ tu-darmstadt.in ☑ tu-darmstadt.mobi

Buy Now! $8.99 at name.com Purchase

Ads by Google

Horoskop 2010 - Gratis
Neu: Ihr persönliches Horoskop das Ihr Leben verändern kann. Hier!
Talisman-Kosmos.net/Horoskop

Wenn Sie sterben?
Lebenserwartung Rechner Vergewissern Sie sich, wenn Sie die
www2.testingdeath.com

64287-Darmstadt:
Wir erleichtern Ihre Suche. Alles auf einen Blick!
www.GelbeSeiten.de/Darmstadt

REGISTRY WHOIS FOR TU-DARMSTADT.DE

```
Domain:     tu-darmstadt.de
Status:    connect

% DB time is 2010-04-15T12:45:00+02:00

Information Updated: Thu, 15 Apr 2010 10:55:31 UTC
```

Updated 1 second ago
Refresh

TU-DARMSTADT.DE SITE INFORMATION

Whois Databases

Two steps

- First find target’s registrar, then whois target at registrar

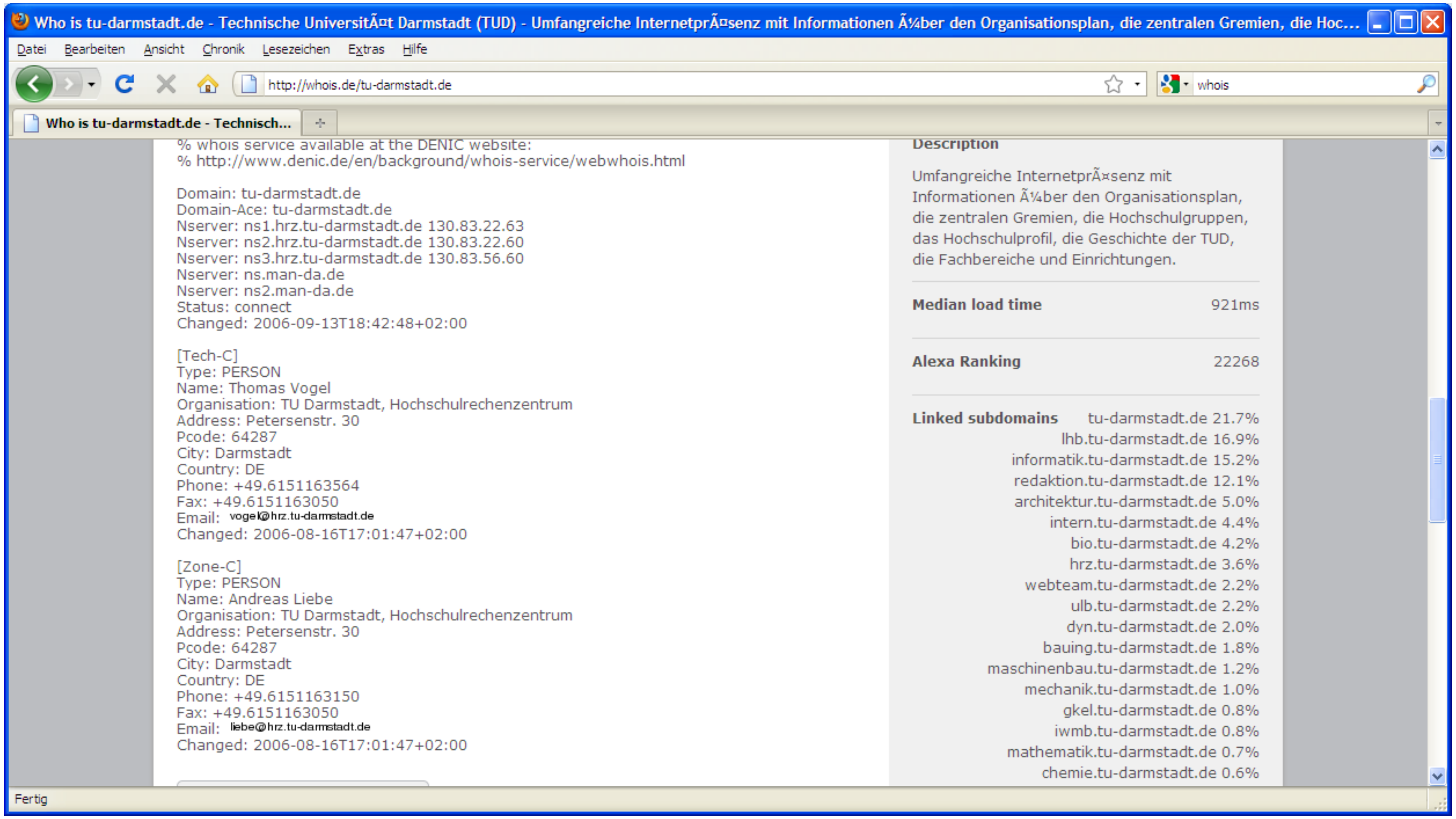
Input: domain name or company name

Output: registrar, whois server, dns server, names of people (administrator, billing contact), phone numbers, E-mail addresses

Some useful whois sites:

- www.internic.net
  - For com, net and org top-level domains
- whois.net, who.is, www.networksolutions.com/whois
  - For country-code top-level domains or arbitrary domains, e.g., jp, fr

Querying Databases: Target “tu-darmstadt.de”



Who is tu-darmstadt.de - Technische UniversitÃ¤t Darmstadt (TUD) - Umfangreiche InternetprÃ¤senz mit Informationen Ã¼ber den Organisationsplan, die zentralen Gremien, die Hoc...
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://whois.de/tu-darmstadt.de
whois
Who is tu-darmstadt.de - Technisch...
Fertig

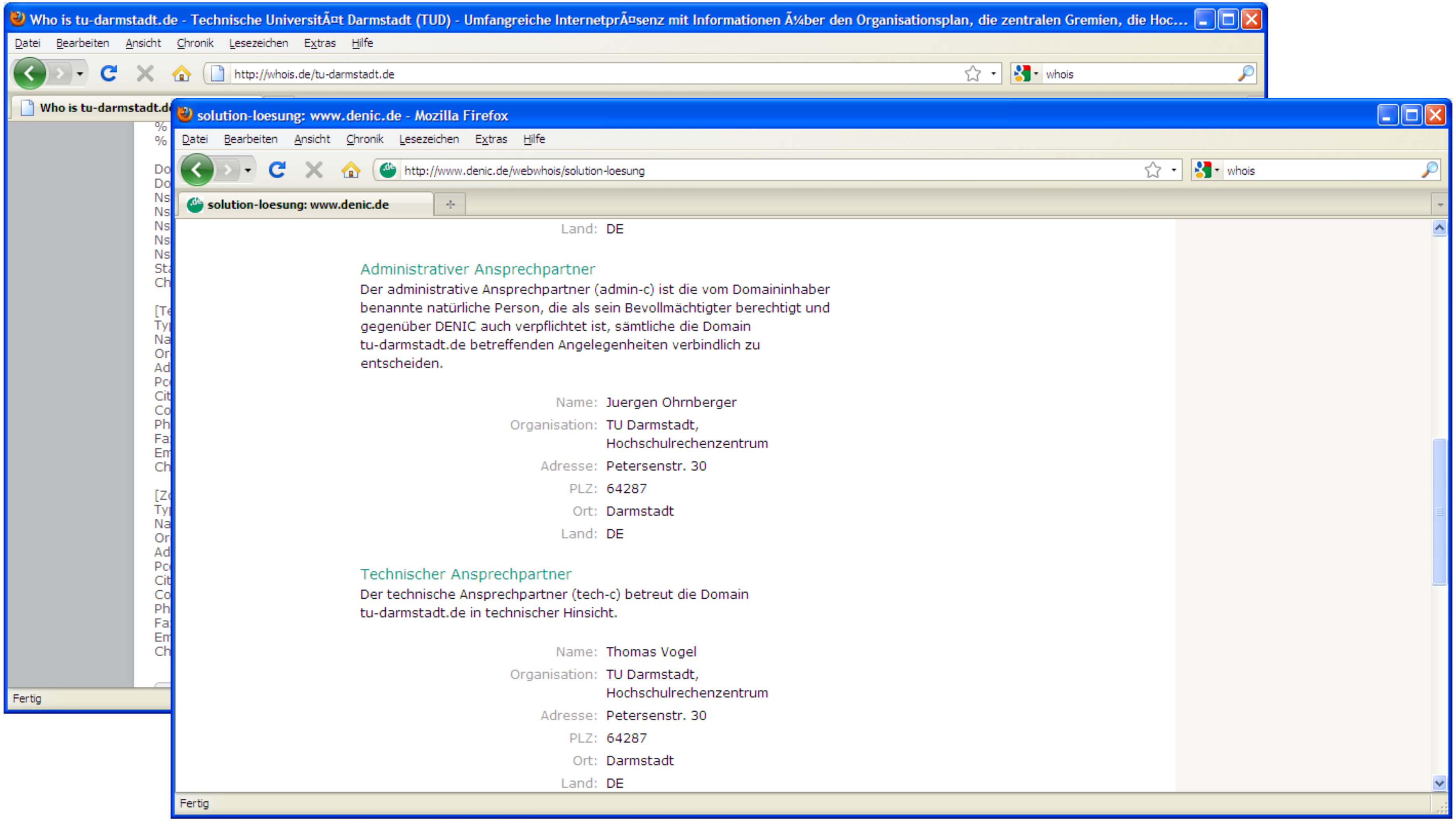
```
% whois service available at the DENIC website:
% http://www.denic.de/en/background/whois-service/webwhois.html

Domain: tu-darmstadt.de
Domain-Ace: tu-darmstadt.de
Nserver: ns1.hrz.tu-darmstadt.de 130.83.22.63
Nserver: ns2.hrz.tu-darmstadt.de 130.83.22.60
Nserver: ns3.hrz.tu-darmstadt.de 130.83.56.60
Nserver: ns.man-da.de
Nserver: ns2.man-da.de
Status: connect
Changed: 2006-09-13T18:42:48+02:00

[Tech-C]
Type: PERSON
Name: Thomas Vogel
Organisation: TU Darmstadt, Hochschulrechenzentrum
Address: Petersenstr. 30
Pcode: 64287
City: Darmstadt
Country: DE
Phone: +49.6151163564
Fax: +49.6151163050
Email: vogel@hrz.tu-darmstadt.de
Changed: 2006-08-16T17:01:47+02:00

[Zone-C]
Type: PERSON
Name: Andreas Liebe
Organisation: TU Darmstadt, Hochschulrechenzentrum
Address: Petersenstr. 30
Pcode: 64287
City: Darmstadt
Country: DE
Phone: +49.6151163150
Fax: +49.6151163050
Email: liebe@hrz.tu-darmstadt.de
Changed: 2006-08-16T17:01:47+02:00
```

Description

Umfangreiche InternetprÃ¤senz mit Informationen Ã¼ber den Organisationsplan, die zentralen Gremien, die Hochschulgruppen, das Hochschulprofil, die Geschichte der TUD, die Fachbereiche und Einrichtungen.

Median load time	921ms
Alexa Ranking	22268
Linked subdomains	tu-darmstadt.de 21.7%
	lhb.tu-darmstadt.de 16.9%
	informatik.tu-darmstadt.de 15.2%
	redaktion.tu-darmstadt.de 12.1%
	architektur.tu-darmstadt.de 5.0%
	intern.tu-darmstadt.de 4.4%
	bio.tu-darmstadt.de 4.2%
	hrz.tu-darmstadt.de 3.6%
	webteam.tu-darmstadt.de 2.2%
	ulb.tu-darmstadt.de 2.2%
	dyn.tu-darmstadt.de 2.0%
	bauing.tu-darmstadt.de 1.8%
	maschinenbau.tu-darmstadt.de 1.2%
	mechanik.tu-darmstadt.de 1.0%
	gkel.tu-darmstadt.de 0.8%
	iwmb.tu-darmstadt.de 0.8%
	mathematik.tu-darmstadt.de 0.7%
	chemie.tu-darmstadt.de 0.6%

Querying Databases: Target "tu-darmstadt.de"



Who is tu-darmstadt.de - Technische UniversitÃ¤t Darmstadt (TUD) - Umfangreiche InternetprÃ¤senz mit Informationen Ã¼ber den Organisationsplan, die zentralen Gremien, die Hoc...
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://whois.de/tu-darmstadt.de
whois
Who is tu-darmstadt.de
Fertig
solution-loesung: www.denic.de - Mozilla Firefox
http://www.denic.de/webwhois/solution-loesung
solution-loesung: www.denic.de

Land: DE

Administrativer Ansprechpartner

Der administrative Ansprechpartner (admin-c) ist die vom Domaininhaber benannte natürliche Person, die als sein Bevollmächtigter berechtigt und gegenüber DENIC auch verpflichtet ist, sämtliche die Domain tu-darmstadt.de betreffenden Angelegenheiten verbindlich zu entscheiden.

Name:	Juergen Ohrnberger
Organisation:	TU Darmstadt, Hochschulrechenzentrum
Adresse:	Petersenstr. 30
PLZ:	64287
Ort:	Darmstadt
Land:	DE

Technischer Ansprechpartner

Der technische Ansprechpartner (tech-c) betreut die Domain tu-darmstadt.de in technischer Hinsicht.

Name:	Thomas Vogel
Organisation:	TU Darmstadt, Hochschulrechenzentrum
Adresse:	Petersenstr. 30
PLZ:	64287
Ort:	Darmstadt
Land:	DE

Reconnaissance: IP Ranges

IANA: Internet Assigned Numbers Authority

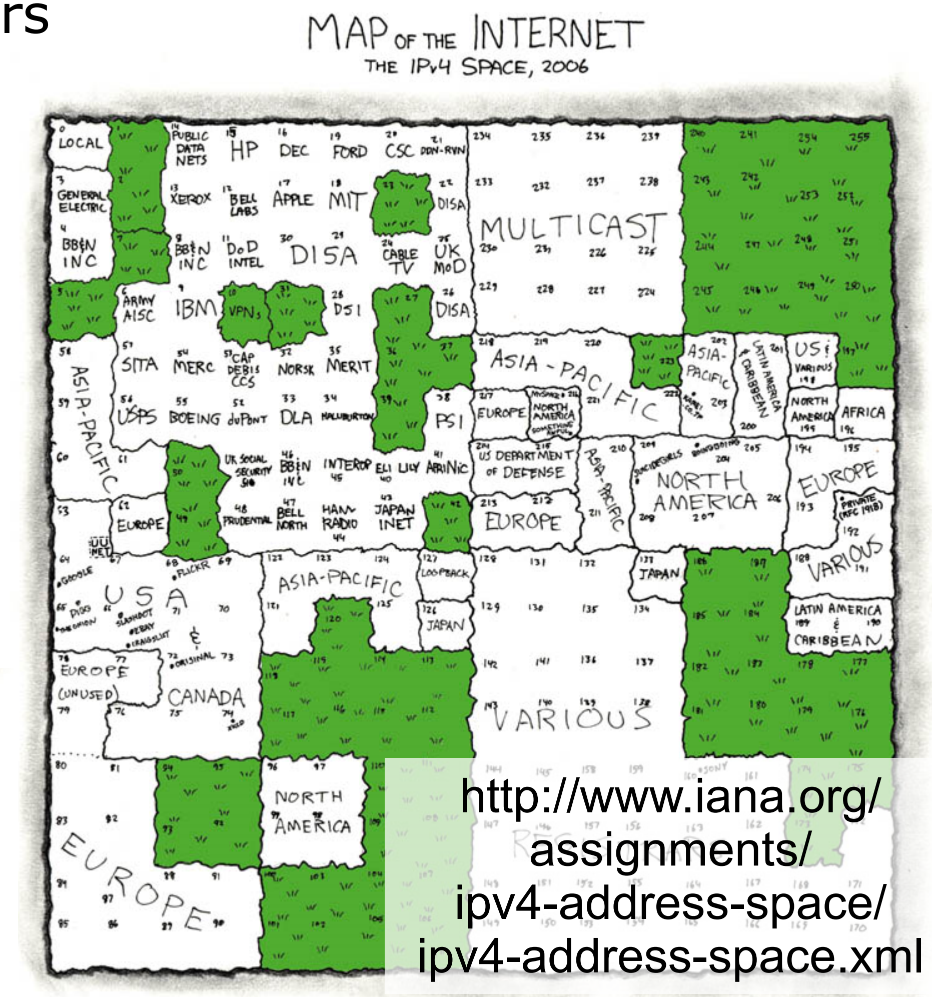
ARIN: American Registry for Internet Numbers

- Maintains whois database that includes IP address ranges in US

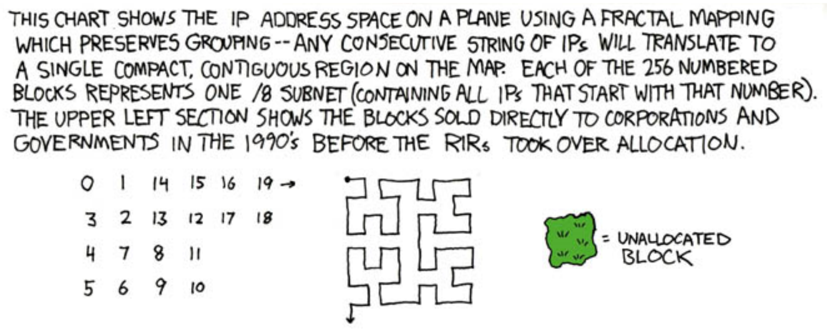
RIPE: Europe

APNIC: Asia

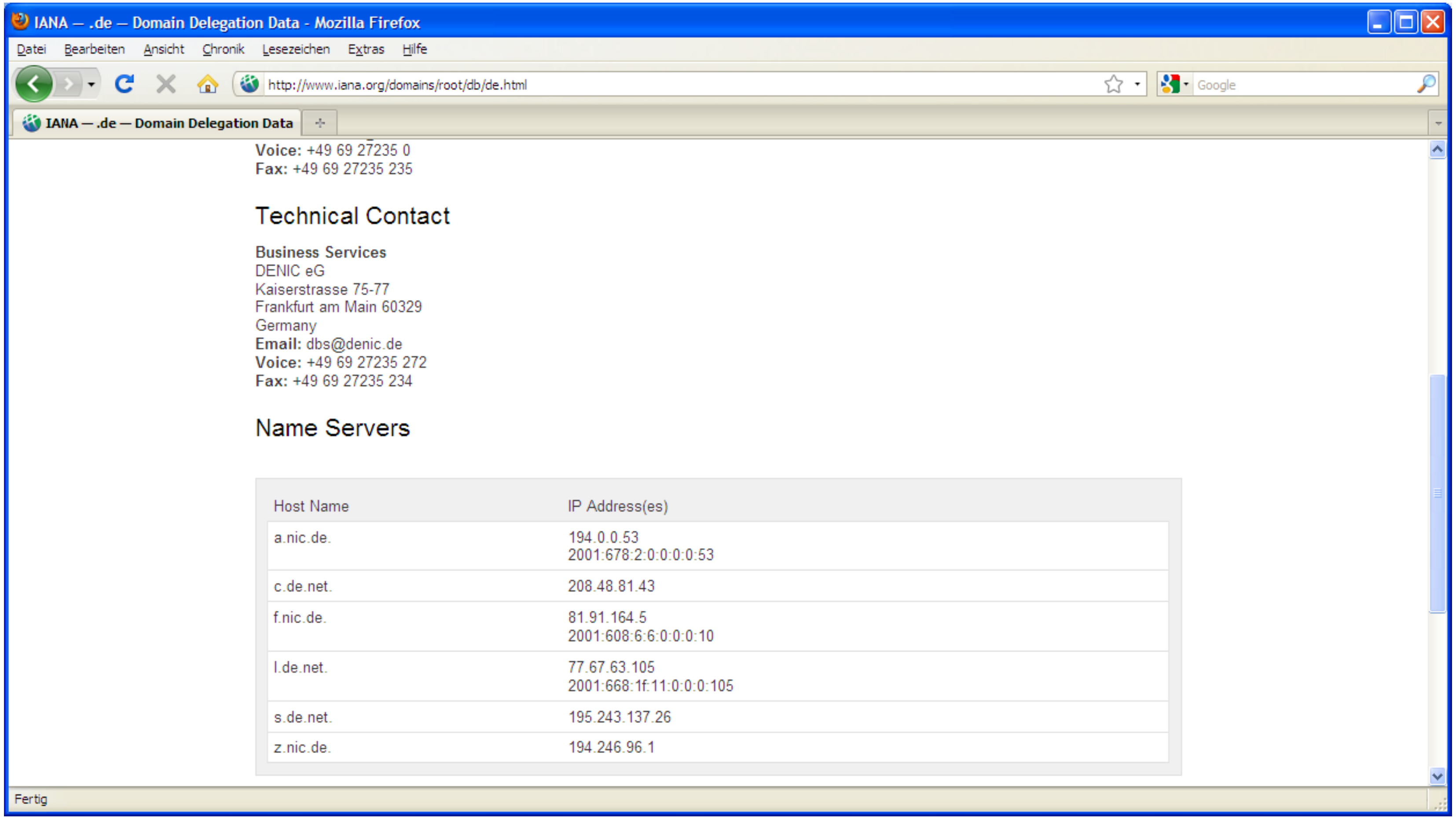
[Source: http://xkcd.com/195/]



http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml


THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

IANA Databases
Query at RIPE.NET



IANA — .de — Domain Delegation Data - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.iana.org/domains/root/db/de.html
Google
IANA — .de — Domain Delegation Data
Fertig

Voice: +49 69 27235 0
Fax: +49 69 27235 235

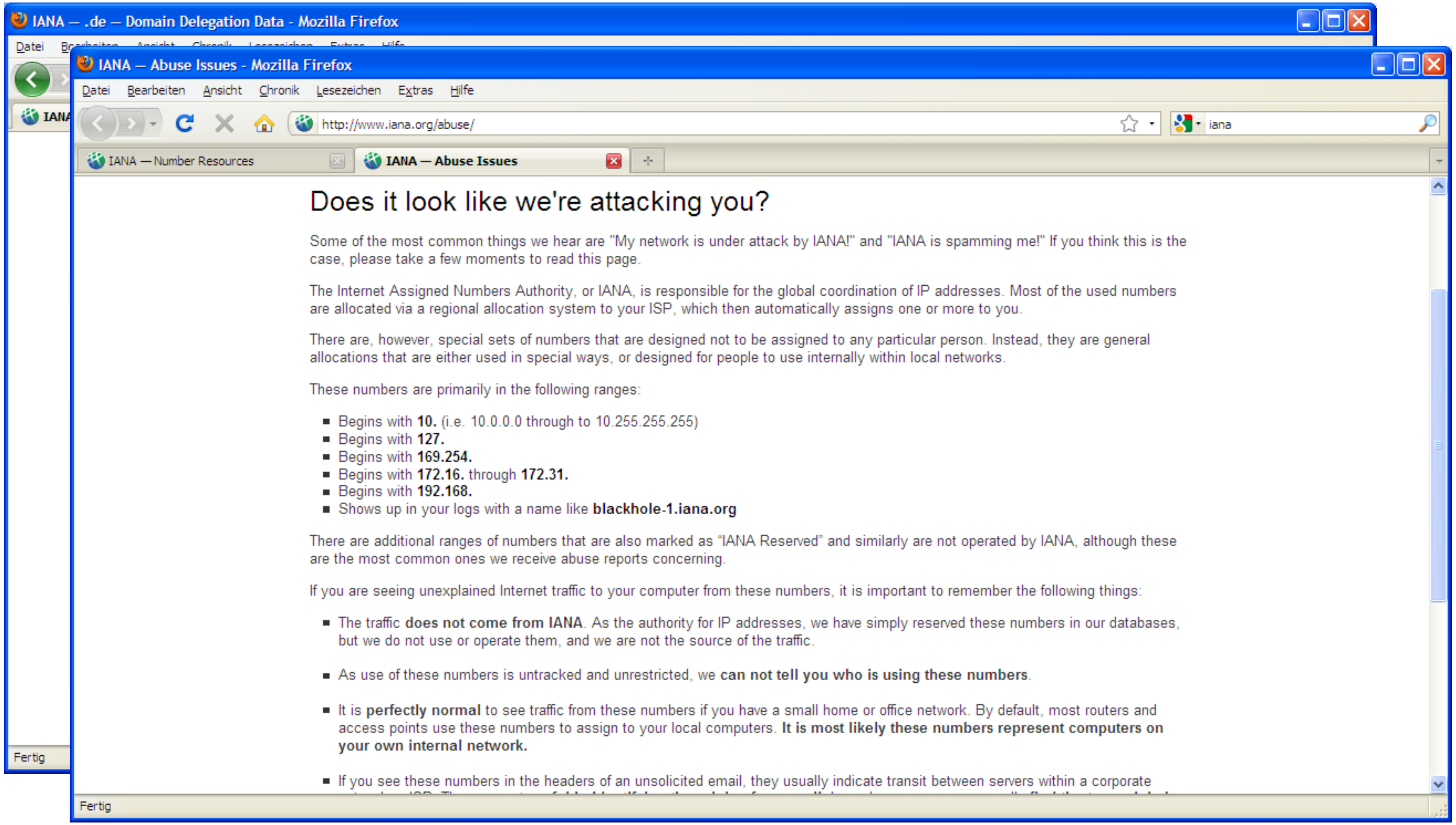
Technical Contact

Business Services
DENIC eG
Kaiserstrasse 75-77
Frankfurt am Main 60329
Germany
Email: dbs@denic.de
Voice: +49 69 27235 272
Fax: +49 69 27235 234

Name Servers

Host Name	IP Address(es)
a.nic.de.	194.0.0.53 2001:678:2:0:0:0:0:53
c.de.net.	208.48.81.43
f.nic.de.	81.91.164.5 2001:608:6:6:0:0:0:10
l.de.net.	77.67.63.105 2001:668:1f:11:0:0:0:105
s.de.net.	195.243.137.26
z.nic.de.	194.246.96.1

IANA Databases
Query at RIPE.NET


IANA — .de — Domain Delegation Data - Mozilla Firefox
IANA — Abuse Issues - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.iana.org/abuse/
iana
IANA — Number Resources
IANA — Abuse Issues
Fertig

Does it look like we're attacking you?

Some of the most common things we hear are "My network is under attack by IANA!" and "IANA is spamming me!" If you think this is the case, please take a few moments to read this page.

The Internet Assigned Numbers Authority, or IANA, is responsible for the global coordination of IP addresses. Most of the used numbers are allocated via a regional allocation system to your ISP, which then automatically assigns one or more to you.

There are, however, special sets of numbers that are designed not to be assigned to any particular person. Instead, they are general allocations that are either used in special ways, or designed for people to use internally within local networks.

These numbers are primarily in the following ranges:

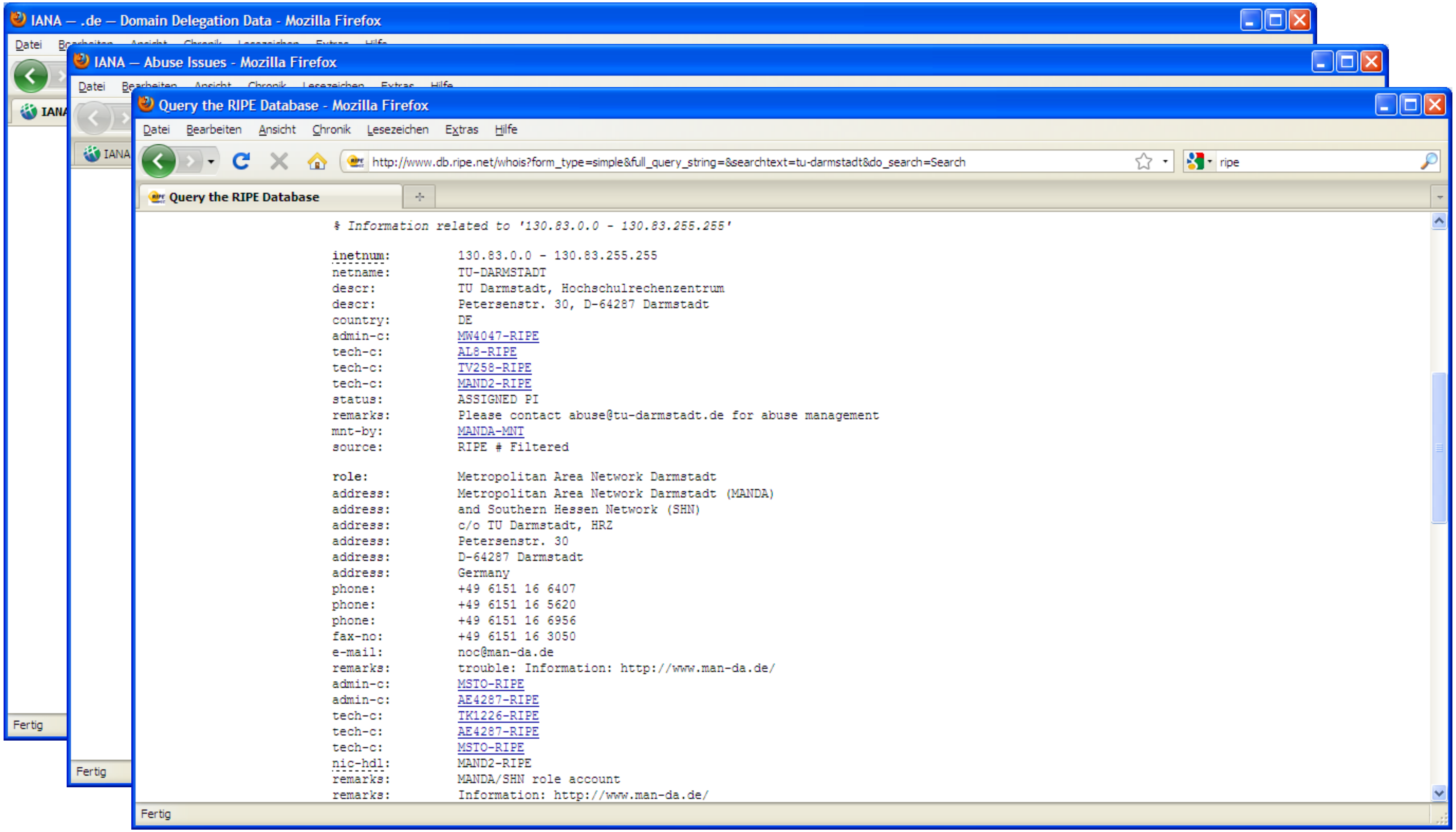
- Begins with **10.** (i.e. 10.0.0.0 through to 10.255.255.255)
- Begins with **127.**
- Begins with **169.254.**
- Begins with **172.16.** through **172.31.**
- Begins with **192.168.**
- Shows up in your logs with a name like **blackhole-1.iana.org**

There are additional ranges of numbers that are also marked as "IANA Reserved" and similarly are not operated by IANA, although these are the most common ones we receive abuse reports concerning.

If you are seeing unexplained Internet traffic to your computer from these numbers, it is important to remember the following things:

- The traffic **does not come from IANA**. As the authority for IP addresses, we have simply reserved these numbers in our databases, but we do not use or operate them, and we are not the source of the traffic.
- As use of these numbers is untracked and unrestricted, we **can not tell you who is using these numbers**.
- It is **perfectly normal** to see traffic from these numbers if you have a small home or office network. By default, most routers and access points use these numbers to assign to your local computers. **It is most likely these numbers represent computers on your own internal network.**
- If you see these numbers in the headers of an unsolicited email, they usually indicate transit between servers within a corporate

IANA Databases
Query at RIPE.NET


IANA — .de — Domain Delegation Data - Mozilla Firefox
IANA — Abuse Issues - Mozilla Firefox
Query the RIPE Database - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Query the RIPE Database
ripe
Fertig

http://www.db.ripe.net/whois?form_type=simple&full_query_string=&searchtext=tu-darmstadt&do_search=Search

```
% Information related to '130.83.0.0 - 130.83.255.255'

inetnum:        130.83.0.0 - 130.83.255.255
netname:        TU-DARMSTADT
descr:          TU Darmstadt, Hochschulrechenzentrum
descr:          Petersenstr. 30, D-64287 Darmstadt
country:        DE
admin-c:        MW4047-RIPE
tech-c:         AL8-RIPE
tech-c:         TV258-RIPE
tech-c:         MAND2-RIPE
status:         ASSIGNED PI
remarks:        Please contact abuse@tu-darmstadt.de for abuse management
mnt-by:         MANDA-MNT
source:         RIPE # Filtered

role:           Metropolitan Area Network Darmstadt
address:        Metropolitan Area Network Darmstadt (MANDA)
address:        and Southern Hessen Network (SHN)
address:        c/o TU Darmstadt, HRZ
address:        Petersenstr. 30
address:        D-64287 Darmstadt
address:        Germany
phone:          +49 6151 16 6407
phone:          +49 6151 16 5620
phone:          +49 6151 16 6956
fax-no:         +49 6151 16 3050
e-mail:         noc@man-da.de
remarks:        trouble: Information: http://www.man-da.de/
admin-c:        MSTO-RIPE
admin-c:        AE4287-RIPE
tech-c:         TK1226-RIPE
tech-c:         AE4287-RIPE
tech-c:         MSTO-RIPE
nic-hdl:        MAND2-RIPE
remarks:        MANDA/SHN role account
remarks:        Information: http://www.man-da.de/
```

Why are Whois Databases Publicly Available?

Troubleshooting is one reason, security another:

- If you’re under attack, can analyze source address of packets
- Can use whois database to obtain info about the domain from where the attack is coming
- Can inform admin that their systems are source of an attack

Reconnaissance: DNS Database

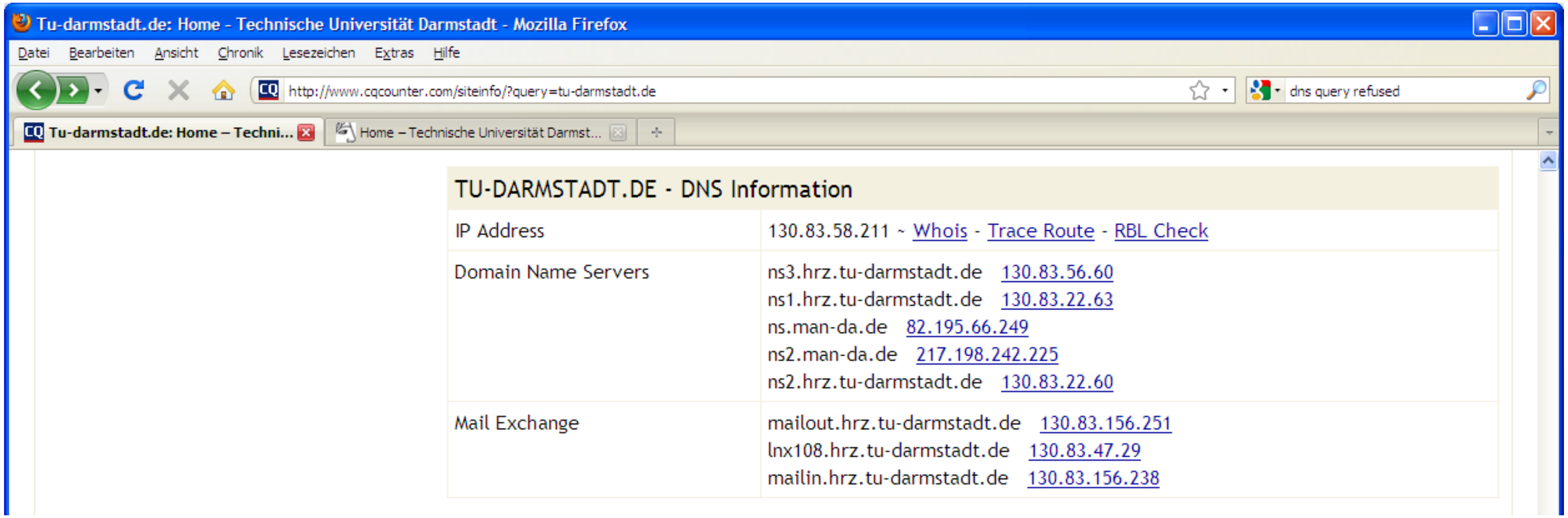
Let’s quickly review DNS

- Distributed database implemented in hierarchy of many DNS servers

Authoritative name server

- For a given domain (e.g., tu-darmstadt.de), provides server name to IP address mappings for servers (web, email, ftp, etc) in domain

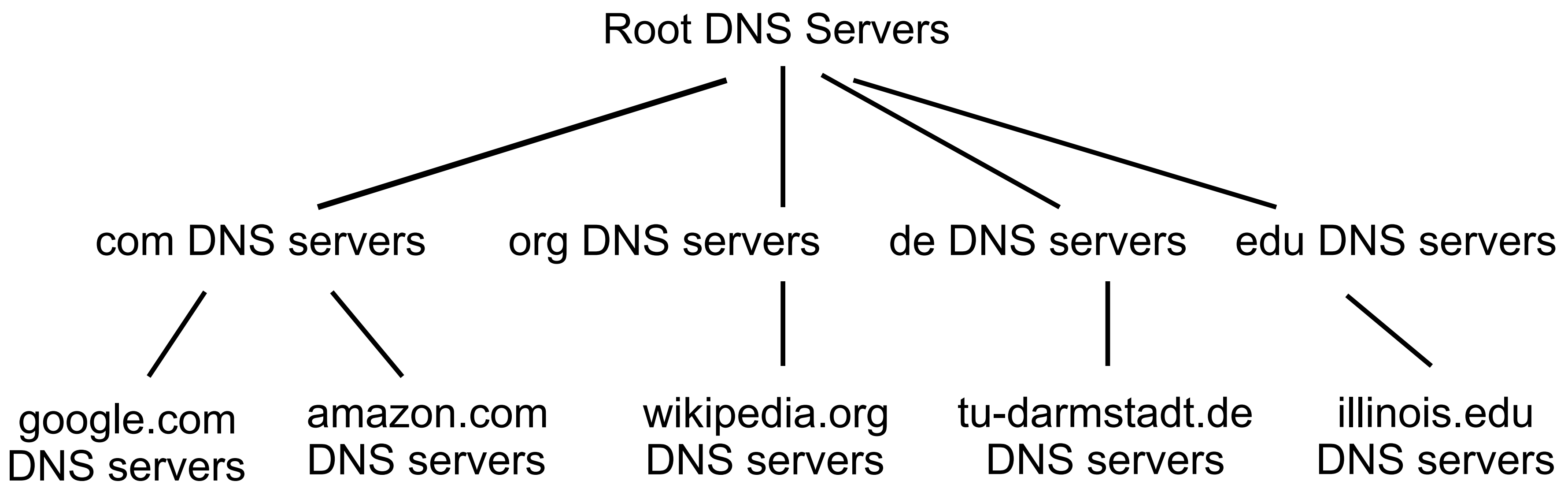
Primary and secondary name server for reliability


Tu-darmstadt.de: Home - Technische Universität Darmstadt - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.cqcounter.com/siteinfo/?query=tu-darmstadt.de
dns query refused
Tu-darmstadt.de: Home – Techni...
Home – Technische Universität Darmst...

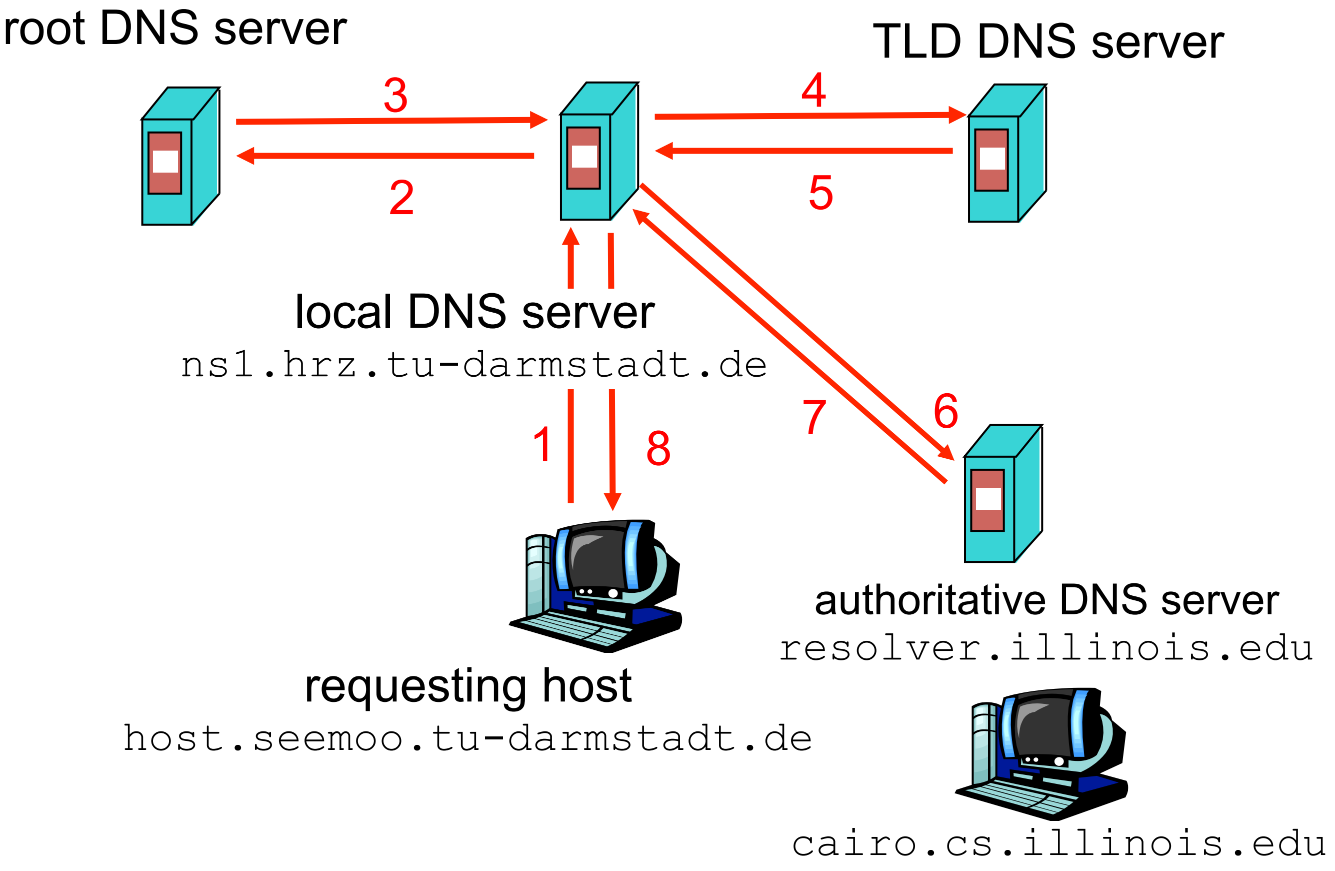
TU-DARMSTADT.DE - DNS Information

IP Address	130.83.58.211 ~ Whois - Trace Route - RBL Check
Domain Name Servers	ns3.hrz.tu-darmstadt.de 130.83.56.60 ns1.hrz.tu-darmstadt.de 130.83.22.63 ns.man-da.de 82.195.66.249 ns2.man-da.de 217.198.242.225 ns2.hrz.tu-darmstadt.de 130.83.22.60
Mail Exchange	mailout.hrz.tu-darmstadt.de 130.83.156.251 lnx108.hrz.tu-darmstadt.de 130.83.47.29 mailin.hrz.tu-darmstadt.de 130.83.156.238

DNS Hierarchy



DNS: Queries


root DNS server
TLD DNS server
3
2
4
5
local DNS server
ns1.hrz.tu-darmstadt.de
1
8
7
6
authoritative DNS server
resolver.illinois.edu
requesting host
host.seemoo.tu-darmstadt.de
cairo.cs.illinois.edu

DNS Records

DNS: distributed db storing resource records (RR)

RR format: `(name, value, type, ttl)`

Which RRs do you know?

Type=NS

- `name` is domain (e.g. foo.com)
- `value` is IP address of authoritative name server for this domain

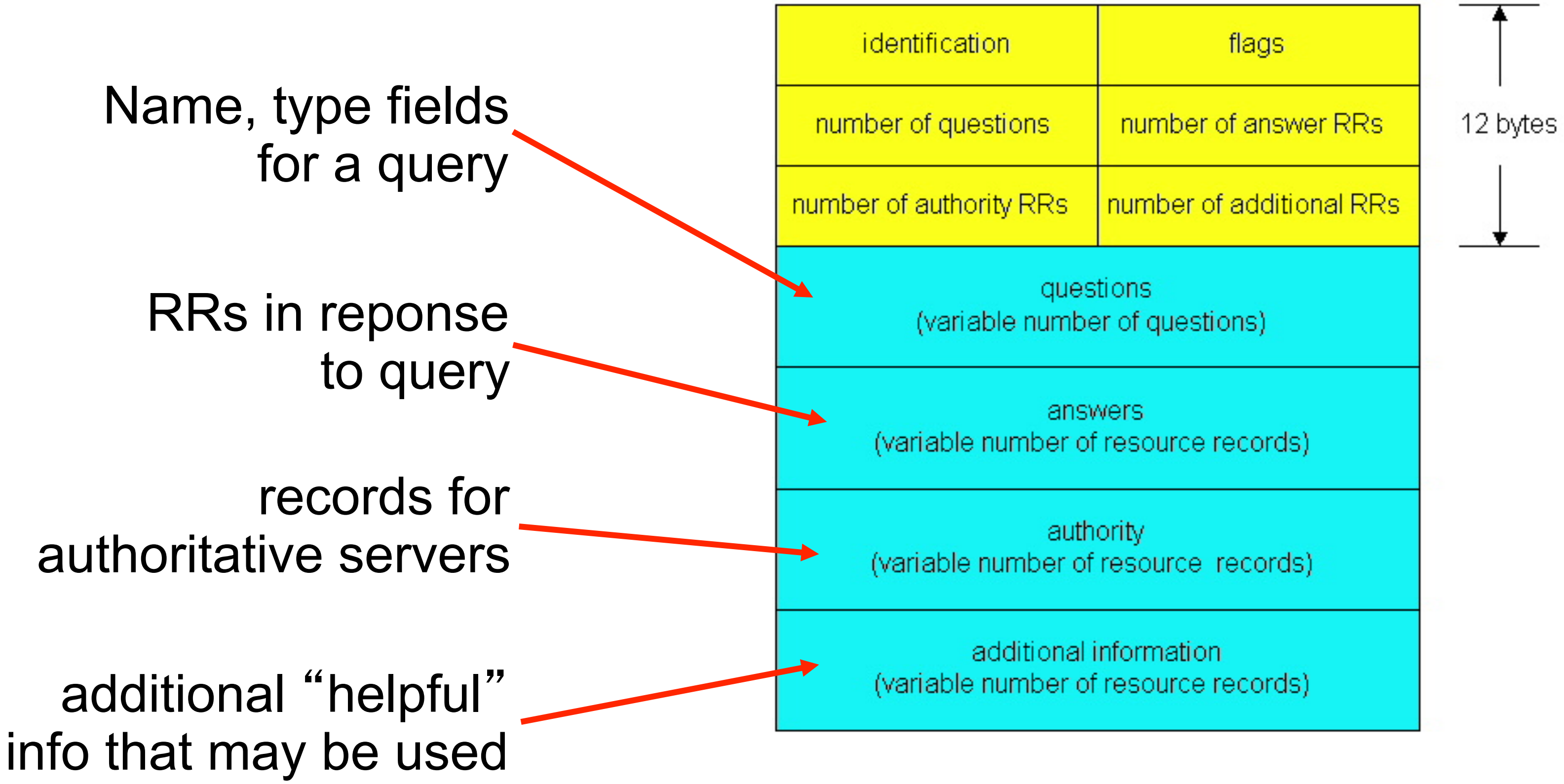
Type=A

- `name` is hostname
- `value` is IP address

Type=MX

- `value` is name of mailserver associated with name

DNS Protocol, Messages



Name, type fields for a query

RRs in reponse to query

records for authoritative servers

additional "helpful" info that may be used

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs
questions (variable number of questions)	
answers (variable number of resource records)	
authority (variable number of resource records)	
additional information (variable number of resource records)	

12 bytes

Query and reply messages sent over UDP on port 53

DNS Contd.

DNS: Caching and Updating Records

- Once (any) DNS server learns mapping, it caches mapping
  - Cache entries timeout (disappear) after some time
  - Cache poisoning is well-known attack

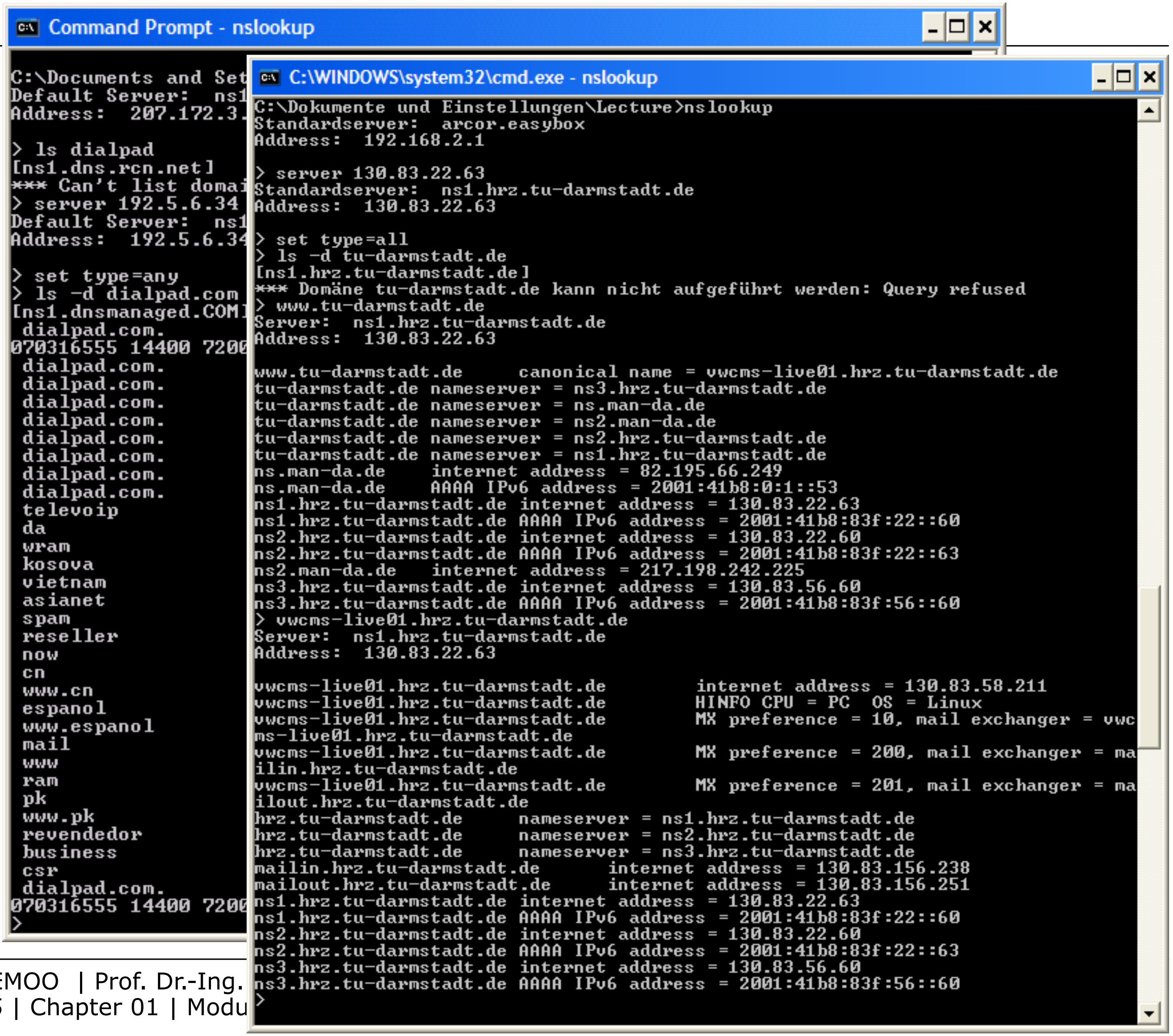
Interrogating DNS Servers

- Attacker first gets primary or secondary authoritative server for target organization using whois
- Attacker can then query the DNS by sending DNS query messages.
- Tools (often available in Unix and Windows machines; also available at web sites):
  - `nslookup`
  - `host`
  - `dig` (domain information groper)

nslookup

Available in most unix & Windows Machines

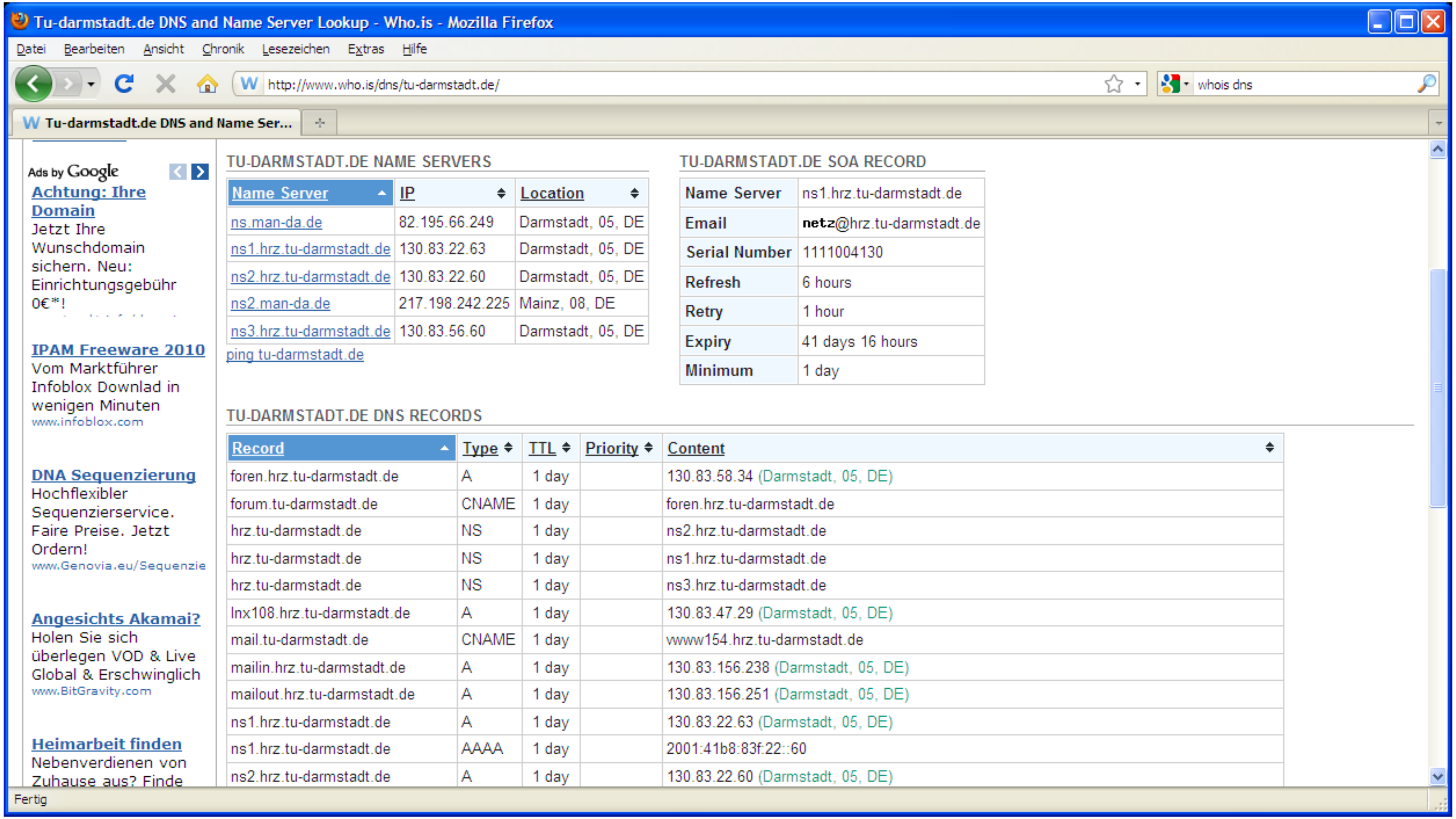
- Get DNS server IP address from whois
- set type=any "get all" …
- however, today best practice is to disable zone-transfers


Command Prompt - nslookup
C:\WINDOWS\system32\cmd.exe - nslookup

```
C:\Documents and Set
Default Server:  ns1
Address:  207.172.3.

> ls dialpad
[ns1.dns.rcn.net]
*** Can't list domai
> server 192.5.6.34
Default Server:  ns1
Address:  192.5.6.34

> set type=any
> ls -d dialpad.com
[ns1.dnsmanaged.COM]
 dialpad.com.
070316555 14400 7200
 dialpad.com.
 dialpad.com.
 dialpad.com.
 dialpad.com.
 dialpad.com.
 dialpad.com.
 dialpad.com.
 dialpad.com.
 televoip
 da
 wram
 kosova
 vietnam
 asianet
 spam
 reseller
 now
 cn
 www.cn
 espanol
 www.espanol
 mail
 www
 ram
 pk
 www.pk
 revendedor
 business
 csr
 dialpad.com.
070316555 14400 7200
>
```

```
C:\Dokumente und Einstellungen\Lecture>nslookup
Standardserver:  arcor.easybox
Address:  192.168.2.1

> server 130.83.22.63
Standardserver:  ns1.hrz.tu-darmstadt.de
Address:  130.83.22.63

> set type=all
> ls -d tu-darmstadt.de
[ns1.hrz.tu-darmstadt.de]
*** Domäne tu-darmstadt.de kann nicht aufgeführt werden: Query refused
> www.tu-darmstadt.de
Server:  ns1.hrz.tu-darmstadt.de
Address:  130.83.22.63

www.tu-darmstadt.de     canonical name = vwcms-live01.hrz.tu-darmstadt.de
tu-darmstadt.de nameserver = ns3.hrz.tu-darmstadt.de
tu-darmstadt.de nameserver = ns.man-da.de
tu-darmstadt.de nameserver = ns2.man-da.de
tu-darmstadt.de nameserver = ns2.hrz.tu-darmstadt.de
tu-darmstadt.de nameserver = ns1.hrz.tu-darmstadt.de
ns.man-da.de    internet address = 82.195.66.249
ns.man-da.de    AAAA IPv6 address = 2001:41b8:0:1::53
ns1.hrz.tu-darmstadt.de internet address = 130.83.22.63
ns1.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:22::60
ns2.hrz.tu-darmstadt.de internet address = 130.83.22.60
ns2.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:22::63
ns2.man-da.de   internet address = 217.198.242.225
ns3.hrz.tu-darmstadt.de internet address = 130.83.56.60
ns3.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:56::60
> vwcms-live01.hrz.tu-darmstadt.de
Server:  ns1.hrz.tu-darmstadt.de
Address:  130.83.22.63

vwcms-live01.hrz.tu-darmstadt.de        internet address = 130.83.58.211
vwcms-live01.hrz.tu-darmstadt.de        HINFO CPU = PC  OS = Linux
vwcms-live01.hrz.tu-darmstadt.de        MX preference = 10, mail exchanger = vwc
ms-live01.hrz.tu-darmstadt.de
vwcms-live01.hrz.tu-darmstadt.de        MX preference = 200, mail exchanger = ma
ilin.hrz.tu-darmstadt.de
vwcms-live01.hrz.tu-darmstadt.de        MX preference = 201, mail exchanger = ma
ilout.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de     nameserver = ns1.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de     nameserver = ns2.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de     nameserver = ns3.hrz.tu-darmstadt.de
mailin.hrz.tu-darmstadt.de      internet address = 130.83.156.238
mailout.hrz.tu-darmstadt.de     internet address = 130.83.156.251
ns1.hrz.tu-darmstadt.de internet address = 130.83.22.63
ns1.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:22::60
ns2.hrz.tu-darmstadt.de internet address = 130.83.22.60
ns2.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:22::63
ns3.hrz.tu-darmstadt.de internet address = 130.83.56.60
ns3.hrz.tu-darmstadt.de AAAA IPv6 address = 2001:41b8:83f:56::60
>
```

`nslookup` via web


Tu-darmstadt.de DNS and Name Server Lookup - Who.is - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://www.who.is/dns/tu-darmstadt.de/
whois dns
Tu-darmstadt.de DNS and Name Ser...
Fertig

TU-DARMSTADT.DE NAME SERVERS

Name Server	IP	Location
ns.man-da.de	82.195.66.249	Darmstadt, 05, DE
ns1.hrz.tu-darmstadt.de	130.83.22.63	Darmstadt, 05, DE
ns2.hrz.tu-darmstadt.de	130.83.22.60	Darmstadt, 05, DE
ns2.man-da.de	217.198.242.225	Mainz, 08, DE
ns3.hrz.tu-darmstadt.de	130.83.56.60	Darmstadt, 05, DE

ping tu-darmstadt.de

TU-DARMSTADT.DE SOA RECORD

Name Server	ns1.hrz.tu-darmstadt.de
Email	**netz**@hrz.tu-darmstadt.de
Serial Number	1111004130
Refresh	6 hours
Retry	1 hour
Expiry	41 days 16 hours
Minimum	1 day

TU-DARMSTADT.DE DNS RECORDS

Record	Type	TTL	Priority	Content
foren.hrz.tu-darmstadt.de	A	1 day		130.83.58.34 (Darmstadt, 05, DE)
forum.tu-darmstadt.de	CNAME	1 day		foren.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de	NS	1 day		ns2.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de	NS	1 day		ns1.hrz.tu-darmstadt.de
hrz.tu-darmstadt.de	NS	1 day		ns3.hrz.tu-darmstadt.de
lnx108.hrz.tu-darmstadt.de	A	1 day		130.83.47.29 (Darmstadt, 05, DE)
mail.tu-darmstadt.de	CNAME	1 day		www154.hrz.tu-darmstadt.de
mailin.hrz.tu-darmstadt.de	A	1 day		130.83.156.238 (Darmstadt, 05, DE)
mailout.hrz.tu-darmstadt.de	A	1 day		130.83.156.251 (Darmstadt, 05, DE)
ns1.hrz.tu-darmstadt.de	A	1 day		130.83.22.63 (Darmstadt, 05, DE)
ns1.hrz.tu-darmstadt.de	AAAA	1 day		2001:41b8:83f:22::60
ns2.hrz.tu-darmstadt.de	A	1 day		130.83.22.60 (Darmstadt, 05, DE)

Reconnaissance via Google

Google sees lots of content that is not properly protected

- Sample query:
  - "intitle:Cisco Systems, Inc. VPN 3000 Concentrator“
    - Online devices that might be open to anyone, if not properly configured
  - „allinurl:auth_user_file.txt“
  - Search Operators
    - site: search for references to the specified site
    - link: find sites containing search term as a link
    - cache: display the cached version of pages found
    - intitle: find sites containing terms in the title of a page
    - inurl: find sites containing terms in the URL of a page
    - filetype: search specific document type
  - Look for webcams, printer, etc. – maybe outdated security patches
- Source: http://www.au.af.mil/au/awc/awcgate/nist/ljutic_fissea_22mar05.pdf

Reconnaissance
Intermediate Summary

So far: Obtaining information from public databases:

- whois databases
  - Tool: web sites
- DNS database & server OS for web servers
  - Tool: nslookup, web sites (netcraft.com), Google

Defense

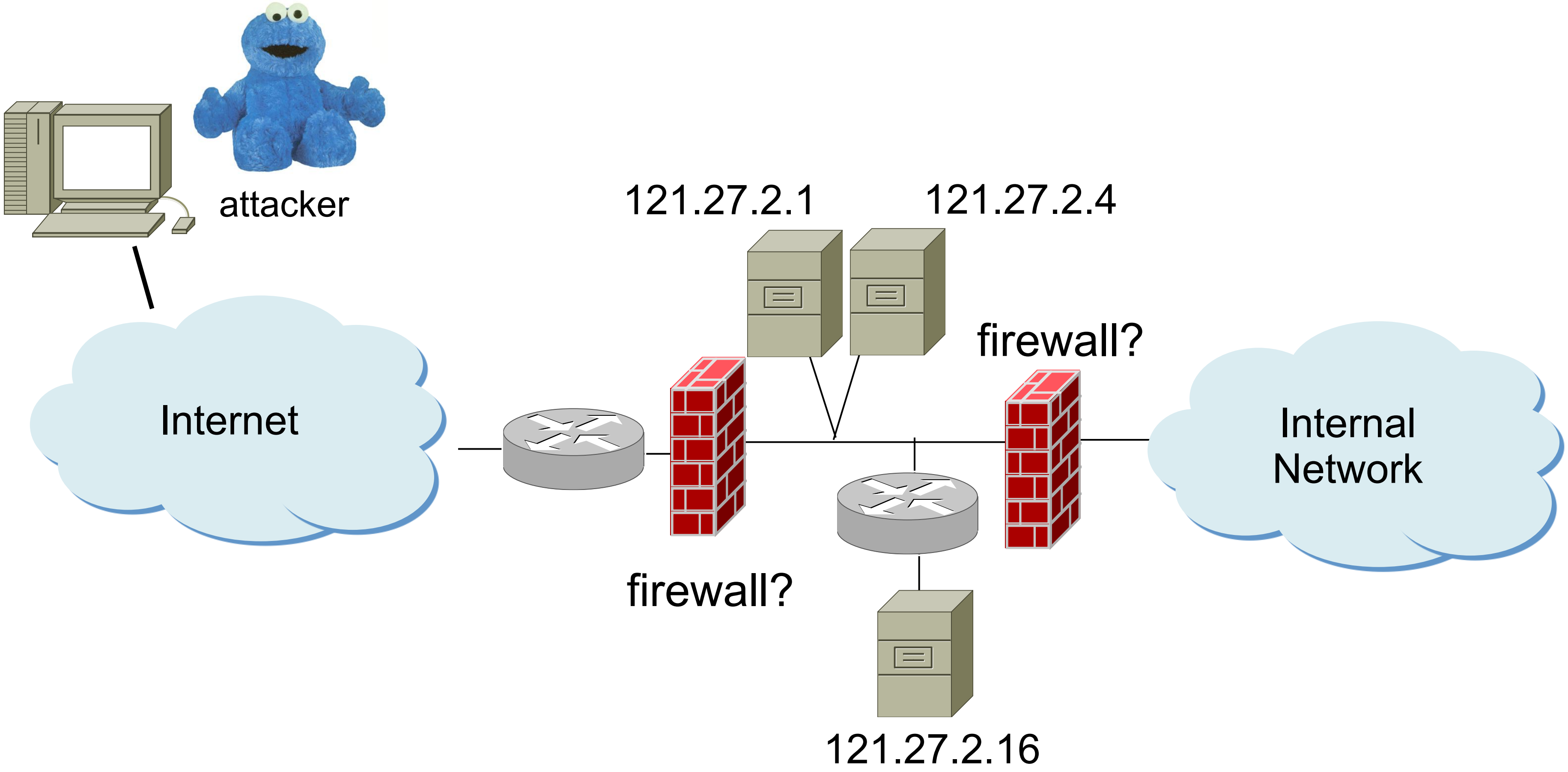
- Keep to a minimum what you put in the public database: only what is necessary

Whats up next: active scans

- Network mapping
- Port scanning (e.g. using nmap)
- Sniffing (e.g. using wireshark)

Network Mapping Tools

Goal: Learn about a remote network



Network Mapping

Attacker uses ping sweeps to determine live hosts

Attacker uses port scans to determine live services

Attacker often uses traceroute/pathping to determine path to each host discovered during ping sweep

- Traceroute: How it works
  - Source sends UDP packets to target
    - Each to an unlikely port
    - 3 packets with the same TTL, then increments TTL
  - When router decrements TTL to 0, sends back to source ICMP packet
    - type 11, code 0, TTL expired
  - When target receives packet, sends back to source ICMP packet
    - type 3, code 0, destination port unreachable
- Overlay results from traceroute to create an approximate network diagram

Ping Sweep

Ping

- Recall ICMP messages are directly encapsulated in IP datagrams (protocol 1)
- To ping a host:
  - Send ICMP Echo Request (ICMP type 8)
  - Host responds with ICMP Echo Reply (type 0)
- So let's ping the entire IP address range
  - Use automated tool for this ping sweep
- If firewall blocks ping packets:
  - Try sweeping with TCP SYN packets to port 80
  - Or try sending UDP packets to possible ports

Port Scanning

Now that we have a map with some hosts, let's find out what ports are open on a target host

- 65,535 TCP ports; 65,535 UDP ports
  - Web server: TCP port 80
  - DNS server: UDP port 53
  - Mail server: TCP port 25
- Port scanning tools can scan:
  - List of ports
  - Range of ports
  - All possible TCP and UDP ports
- Attacker may scan a limited set of ports, to avoid detection

Traceroute/Pathping

traceroute: gaia.cs.umass.edu to www.eurecom.fr

Three delay measements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

trans-oceanic link

* means no reponse (probe lost, router not replying)

Nmap (1) – see also Appendix

Extremely popular

- usually run over linux
- rich feature set, exploiting raw sockets
- need root to use all features

Ping sweeping

- over any range of IP addresses
- with ICMP, SYN, ACK
- OS determination

Port scanning

- Over any range of ports
- Almost any type of TCP, UDP packet

Source IP address spoofing

- Decoy scanning

Packet fragmentation

Timing Options

nmap MAN page details use and is excellent source of information

Nmap (2)

Input

```
nmap [Scan Type] [Options] <target hosts>
```

- Default for port scanning: ports 1-1024 plus ports listed in nmap service file

Output

- open ports: syn/ack returned; port is open
- unfiltered ports: RST returned: port is closed but not blocked by firewall
- filtered ports: nothing returned; port is blocked by firewall

See Appendix for further examples

Network Mapping Defenses

Filter using firewalls and packet-filtering capabilities of routers

- Block incoming ICMP packets, except to the hosts that you want to be pingable
- Filter Time Exceeded ICMP messages leaving your network

Close all unused ports

Scan your own systems to verify that unneeded ports are closed

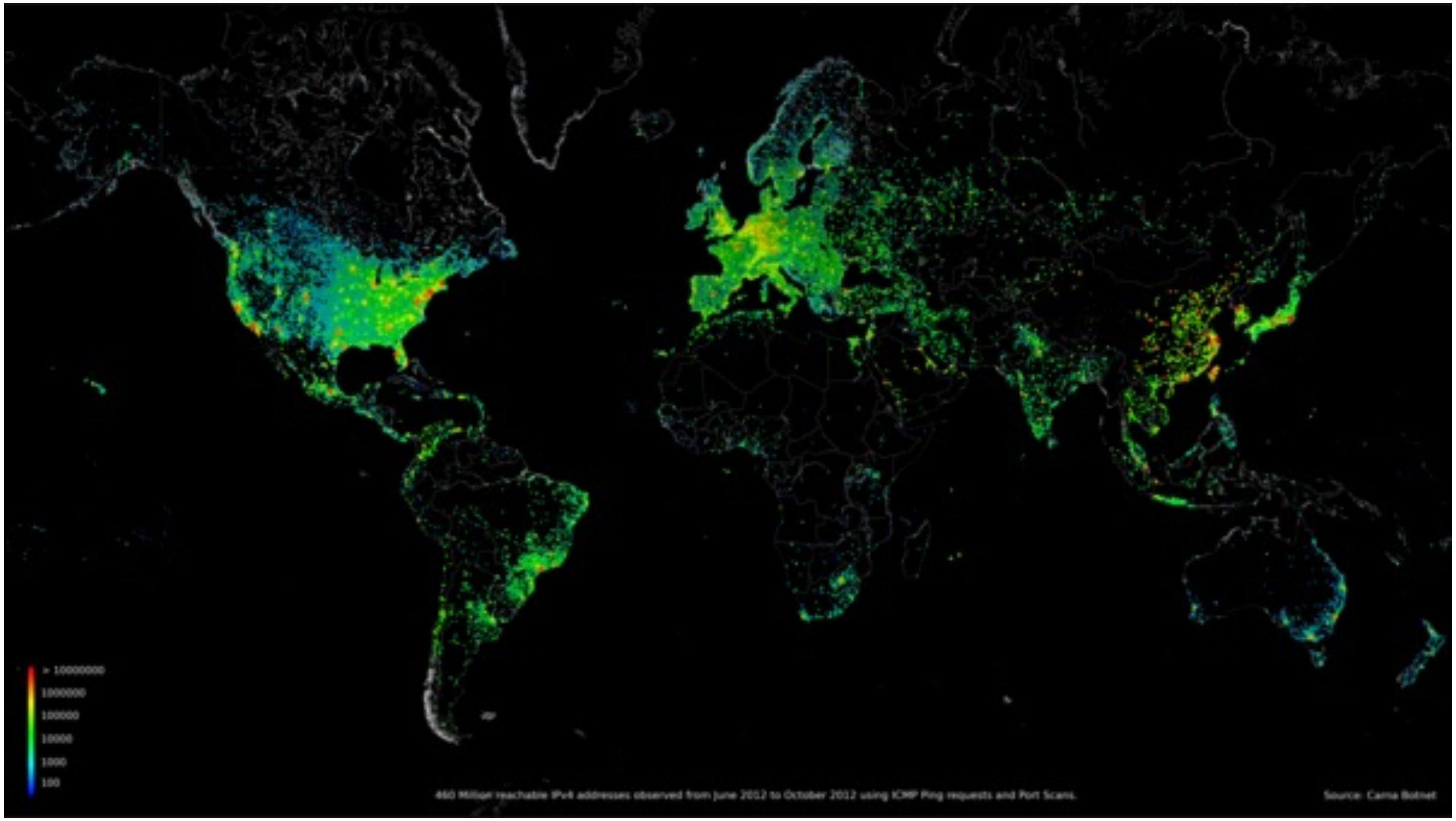
Intrusion Detection Systems

But be aware: makes network troubleshooting also harder

A Cool Project to Map the Internet

Have you heard of the Carna botnet?

- Recommended: http://internetcensus2012.bitbucket.org/paper.html


> 10000000
1000000
100000
10000
1000
100
460 Million reachable IPv4 addresses observed from June 2012 to October 2012 using ICMP Ping requests and Port Scans.
Source: Carna Botnet

Summary

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Keith Ross

Recommended reading

- Manuals of popular unix tools
  - ping
  - traceroute
  - Nmap

Additional reading

- There are various online resources on “ethical hacking”
- Always a good starting point is the ccc (chaos computer club) … but do not expect to find “handbooks for hacking” at their site

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de

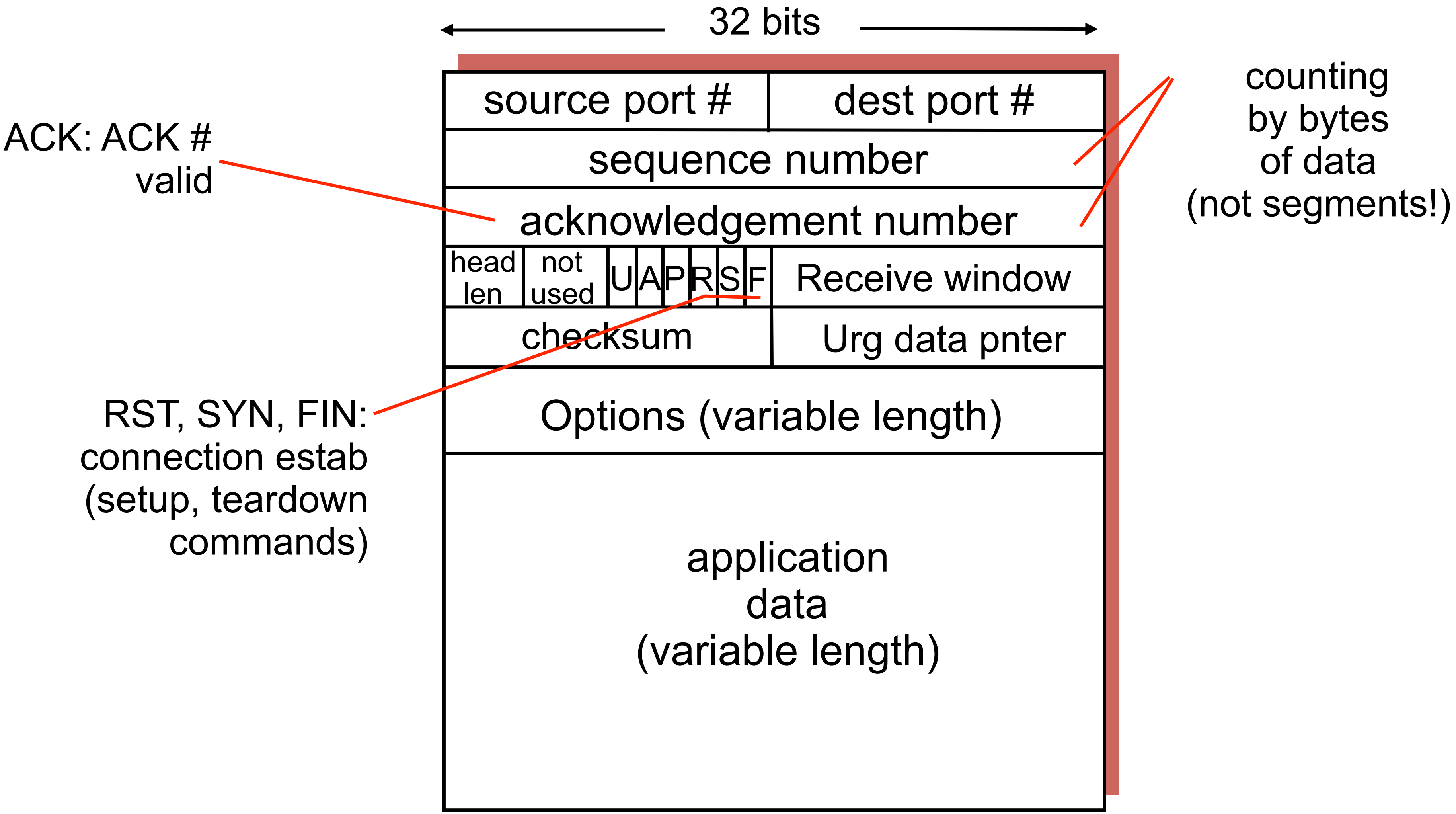
Appendix: Nmap Examples

Some details on TCP

Some nmap examples

Please note: Appendices are in general not relevant for the exam

Excursus:
TCP Segment Structure



32 bits

source port # | dest port #

sequence number

acknowledgement number

head len | not used | U | A | P | R | S | F | Receive window

checksum | Urg data pnter

Options (variable length)

application data (variable length)

ACK: ACK # valid

RST, SYN, FIN: connection estab (setup, teardown commands)

counting by bytes of data (not segments!)

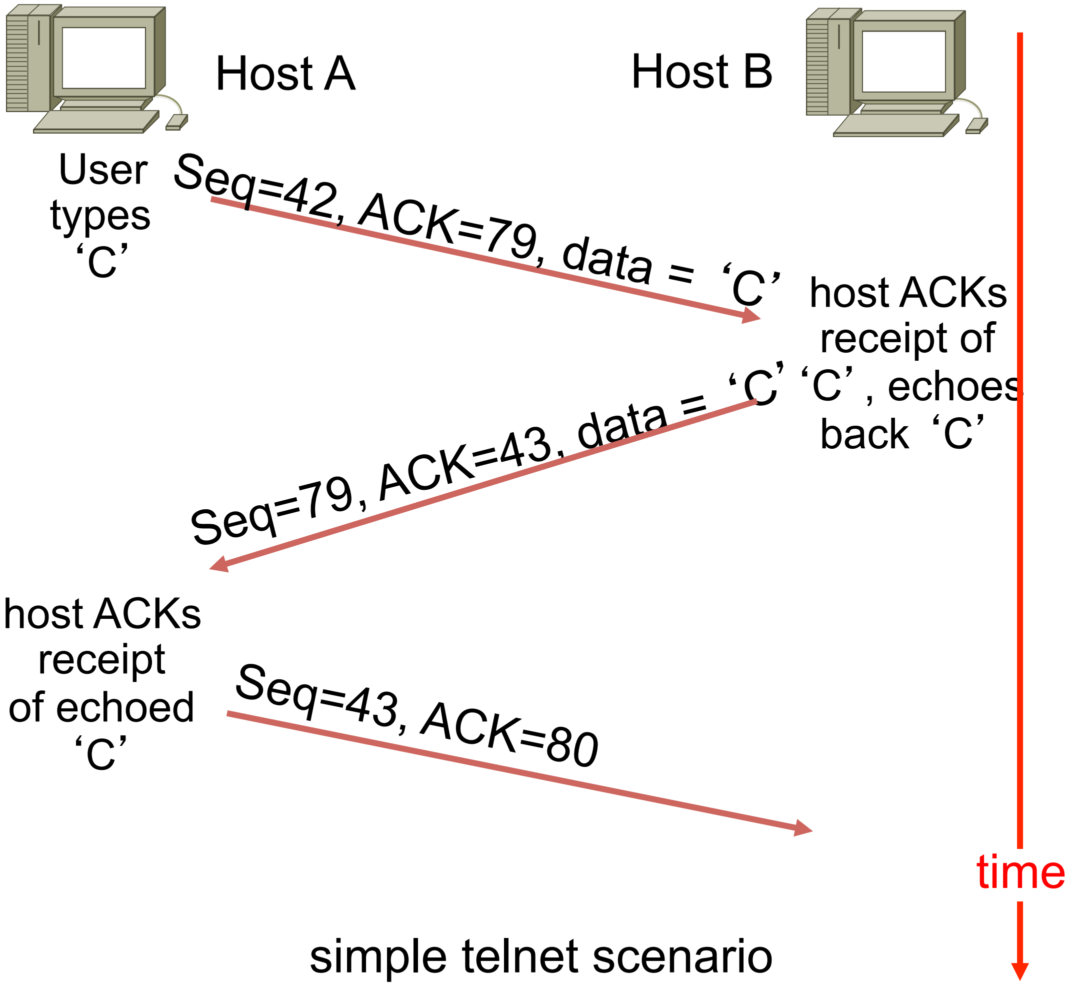
Excursus:
TCP seq. #’s and ACKs

Seq. #’s:

- byte stream “number” of first byte in segment’s data

ACKs:

- seq # of next byte expected from other side


Host A
Host B
User types ‘C’
Seq=42, ACK=79, data = ‘C’
host ACKs receipt of ‘C’, echoes back ‘C’
Seq=79, ACK=43, data = ‘C’
host ACKs receipt of echoed ‘C’
Seq=43, ACK=80
time

simple telnet scenario

Excursus:
TCP Connection Establishment

Three way handshake:

Step 1: client host sends TCP SYN segment to server

- SYN=1, ACK=0
- specifies initial seq #
- no data

Step 2: server host receives SYN, replies with SYN-ACK segment

- SYN=1, ACK=1
- server host allocates buffers
- specifies server initial seq. #

Step 3: client receives SYN-ACK, replies with ACK segment, which may contain data

- SYN=0, ACK=1

TCP: Reset packet

If machine receives a TCP packet it is not expecting, it responds with TCP packet with RST bit set.

- For example when no process is listening on destination port

For UDP, machine returns ICMP “port unreachable” instead

Nmap (3): ping sweep

```
nmap -sP -v 116.27.38/24
```

Sends ICMP echo request (ping) to 256 addresses

Can change options so that pings with SYNs, ACKs…

- `-sP = ping`
- `-v = verbose`

Nmap (4): polite port scan

```
nmap -sT -v target.com
```

Attempts to complete 3-way handshake with each target port

Sends SYN, waits for SYNACK, sends ACK, then sends FIN to close connection

If target port is closed, no SYNACK returned

- Instead RST packet is typically returned

TCP connect scans are easy to detect

- Target (e.g. Web server) may log completed connections
- Gives away attacker's IP address

Nmap (5) : TCP SYN port scan

```
nmap -sS -v target.com
```

Stealthier than polite scan

Send SYN, receive SYNACK, send RST

- Send RST segment to avoid an accidental DoS attack

Stealthier: hosts do not record connection

- But routers with logging enabled will record the SYN packet

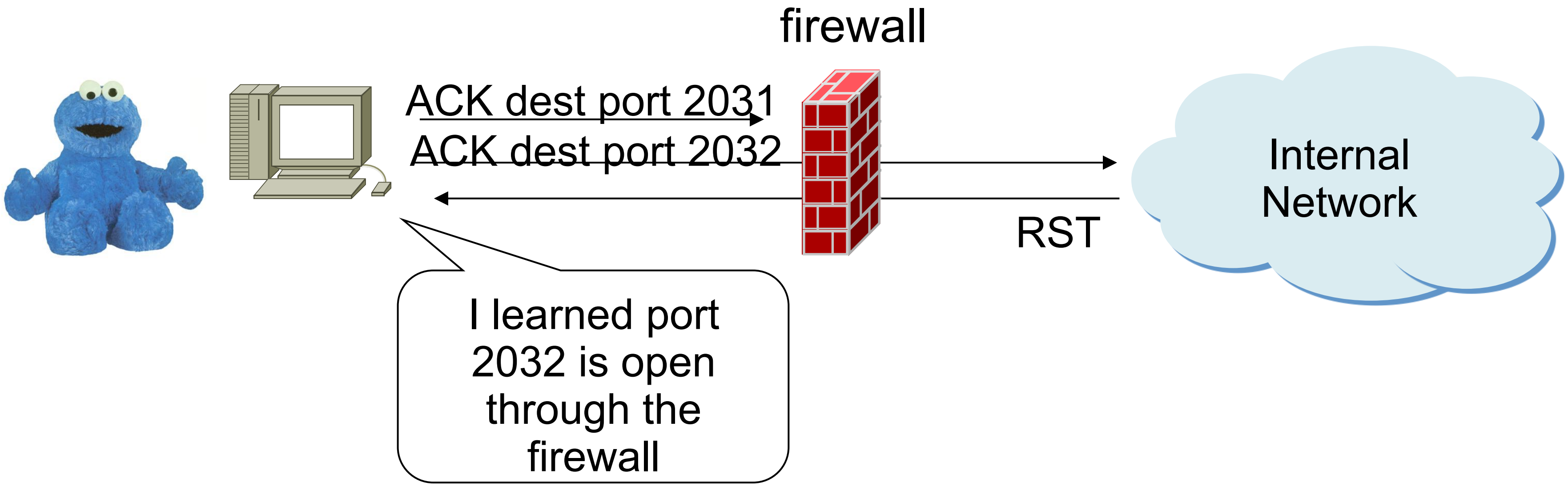
Faster: don’t need to send FIN packet

Nmap (6): TCP ACK scans

Many filters (in firewalls and routers) only let internal systems hosts initiate TCP connections

- Drop packets for which ACK=0 (ie SYN packet): no sessions initiated externally

To learn what ports are open through firewall, try an ACK scan (segments with ACK=1)



Nmap (7): UDP port scans

UDP doesn't have SYN, ACK, RST packets

nmap simply sends UDP packet to target port

- ICMP Port Unreachable: interpret port closed
- Nothing comes back: interpret port open
  - False positives common

Nmap (8): Obscure Source

Attacker can enter list of decoy source IP addresses into Nmap

For each packet it sends, Nmap also sends packets from decoy source IP addresses

- For 4 decoy sources, send five packets

Attacker's actual address must appear in at least one packet, to get a result

If there are 30 decoys, victim network will have to investigate 31 different sources!

Nmap (9): TCP Stack Fingerprinting

In addition to determining open ports, attacker wants to know OS on targeted machine:

- exploit machine's known vulnerabilities
- sophisticated hacker may set up lab environment similar to target network

TCP implementations in different OSes respond differently to (illegal) combinations of TCP flag bits

Nmap (10): Fingerprinting

Nmap sends

- SYN to open port
- NULL to open port (no flag bits set)
- SYN/FIN/URG/PSH to open port
- SYN to closed port
- ACK to closed port
- FIN/PSH/URG to closed port
- UDP to closed port

Nmap includes a database of OS fingerprints for hundreds of platforms

- See nmap.org for further details

Nmap (11): examples

```
nmap -v target.com
```

- Scans all TCP default ports on target.com; verbose mode

```
nmap -sS -O target.com/24
```

- First pings addresses in target network to find hosts that are up. Then scans default ports at these hosts; stealth mode (doesn’t complete the connections); tries to determine OS running on each scanned host

```
nmap -sX -p 22,53,110,143 198.116.*.1-147
```

- Sends an Xmas tree scan to the first half of each of the 255 possible subnets in the 198.116/16. Testing whether the systems run ssh, DNS, pop3, or imap

```
nmap -v -p 80 *.*.2.3-5
```

- finds all web servers on machines with IP addresses ending in .2.3, .2.4, or .2.5