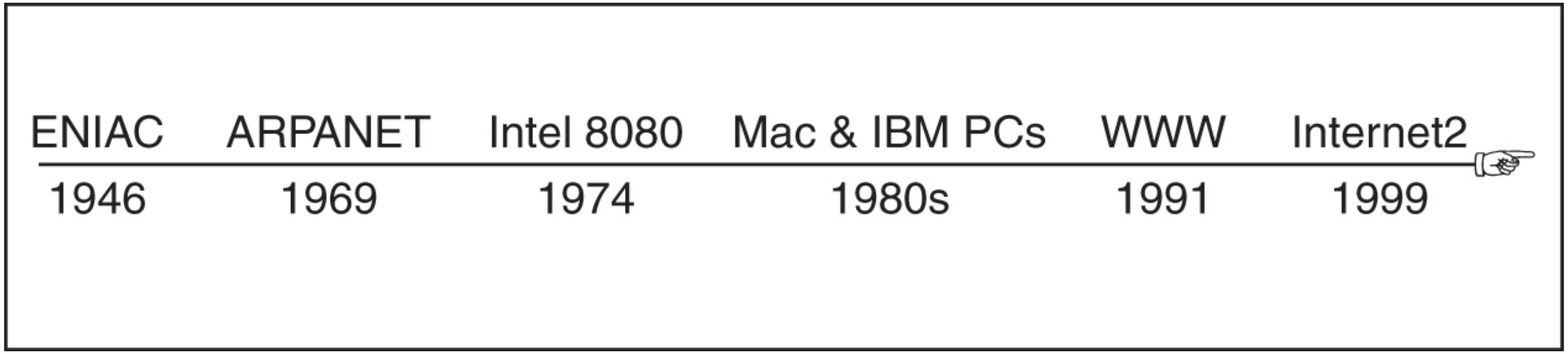
Computer Forensics

Andrej Brodnik

Computer network basics

chapters 21, 23, 24 and 25

- from history



ENIAC 1946

ARPANET 1969

Intel 8080 1974

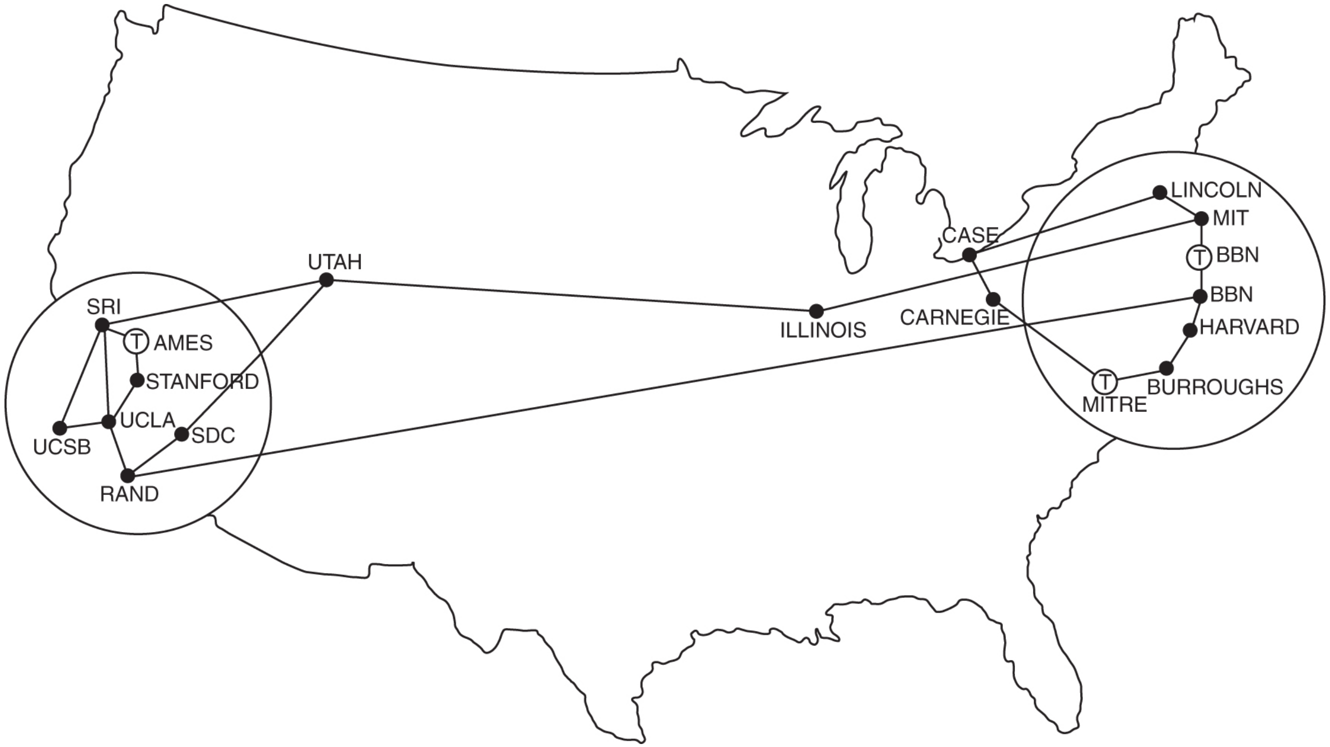
Mac & IBM PCs 1980s

WWW 1991

Internet2 1999

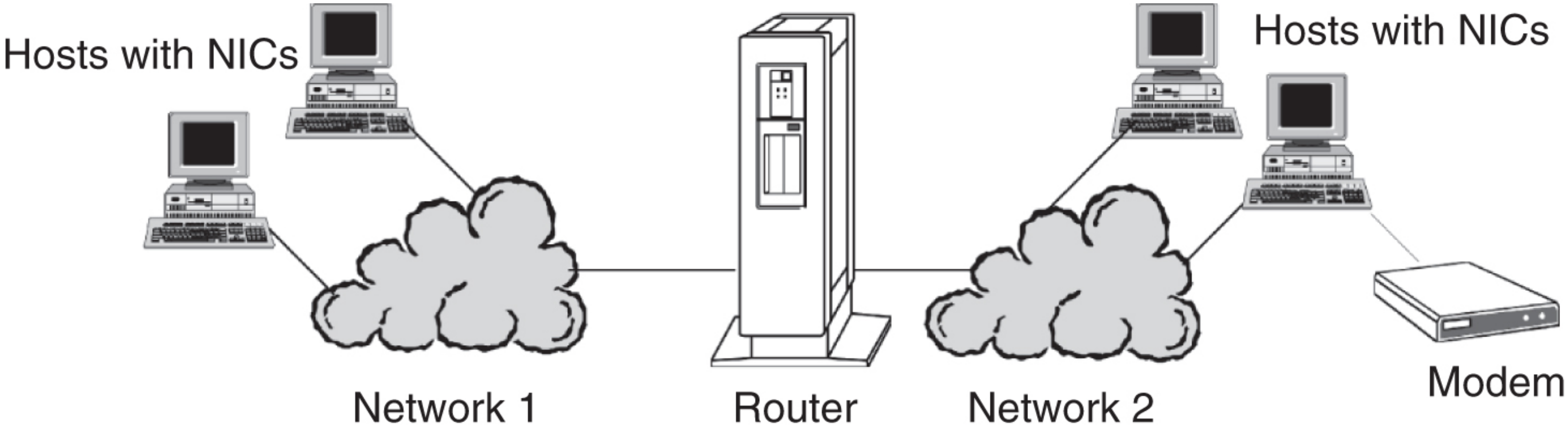
Computer network basics

- from history: ARPANET
- TCP/IP: 1973/74



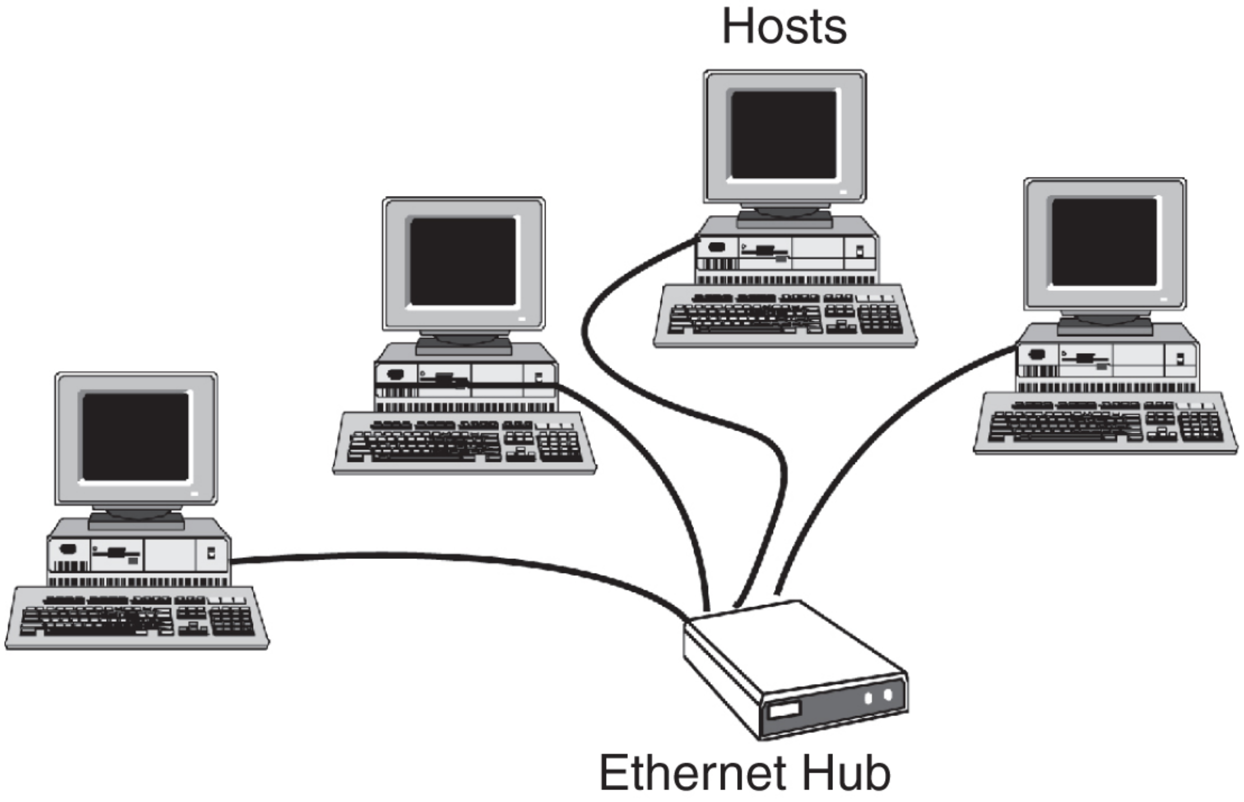
Computer network basics

- network, internet



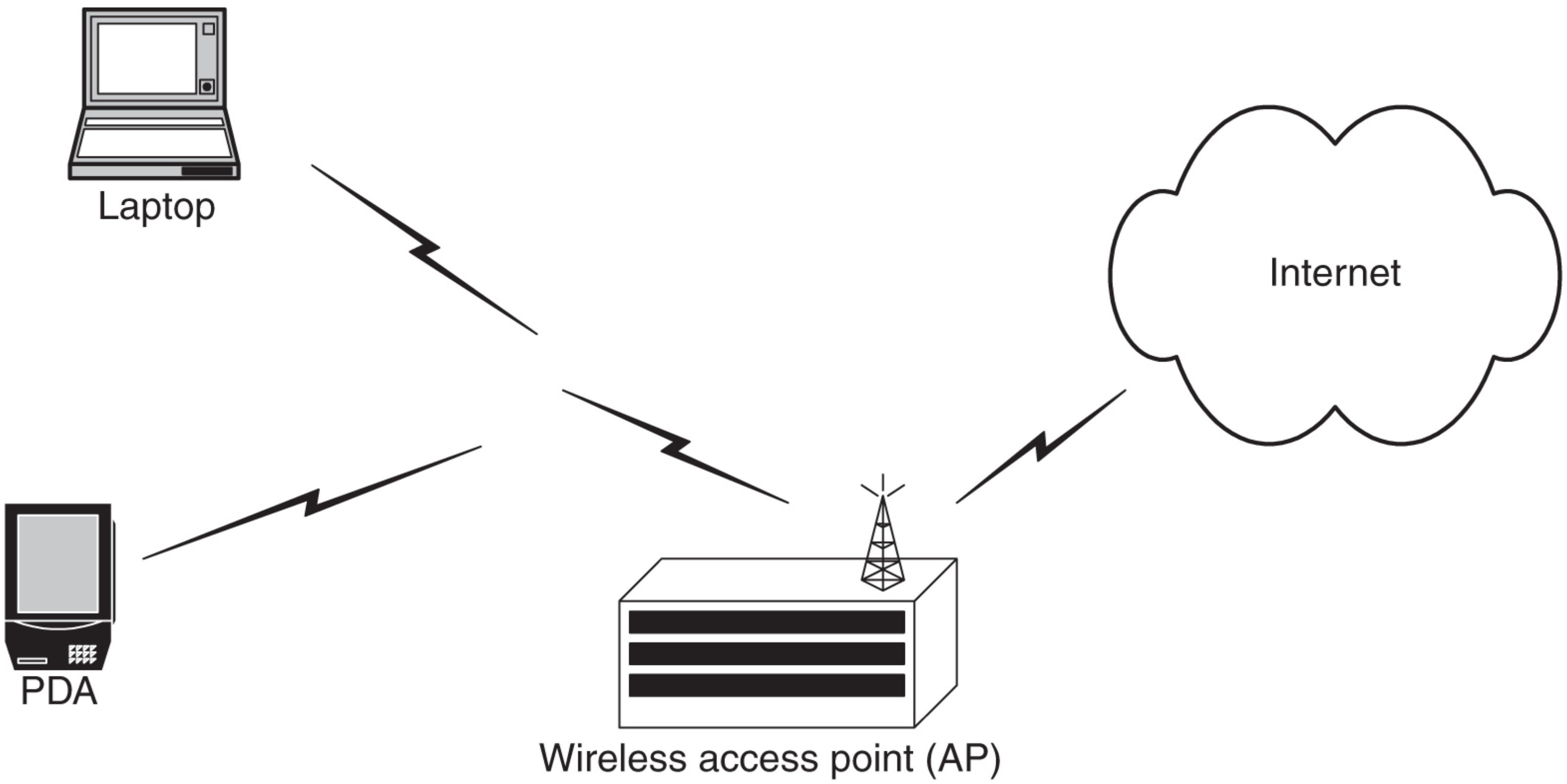
Network

- IEEE 802.3 Ethernet



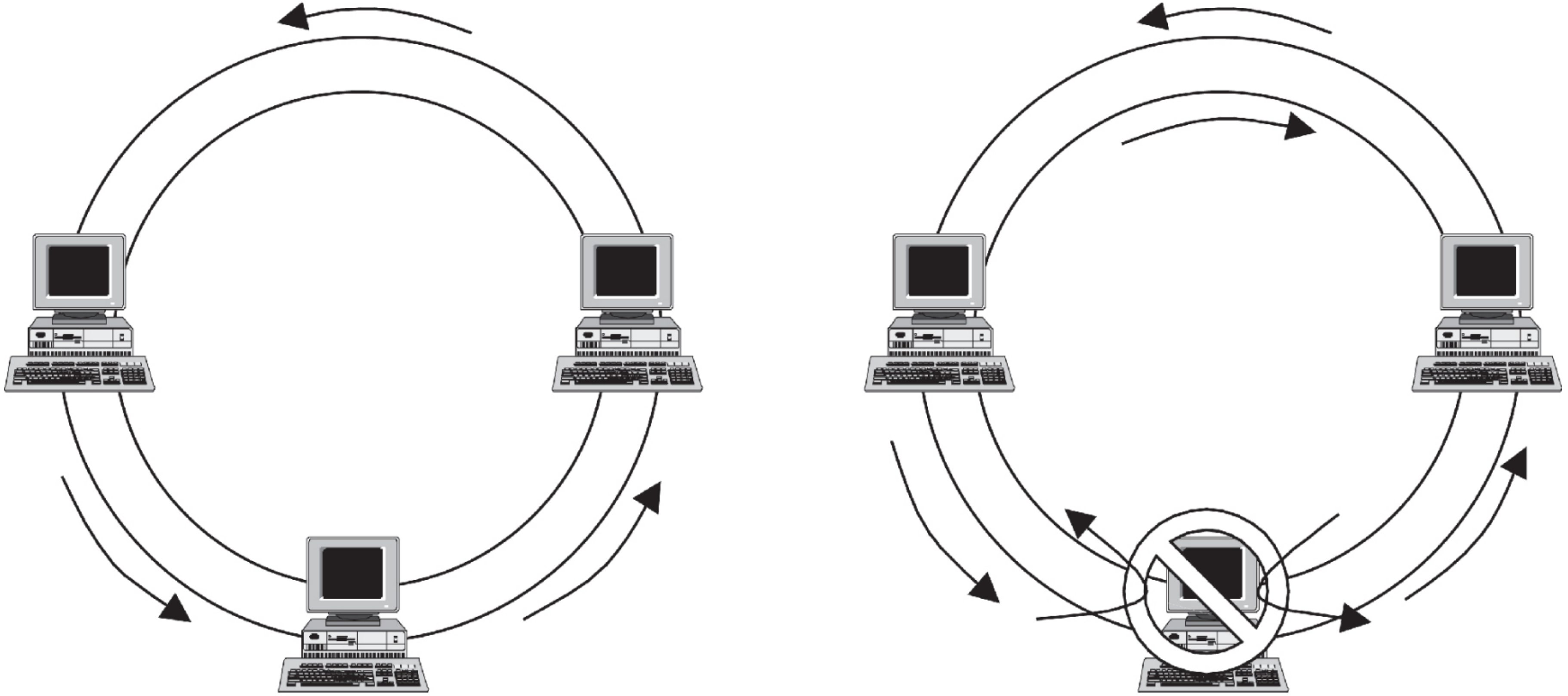
Network

- IEEE 802.11 Ethernet



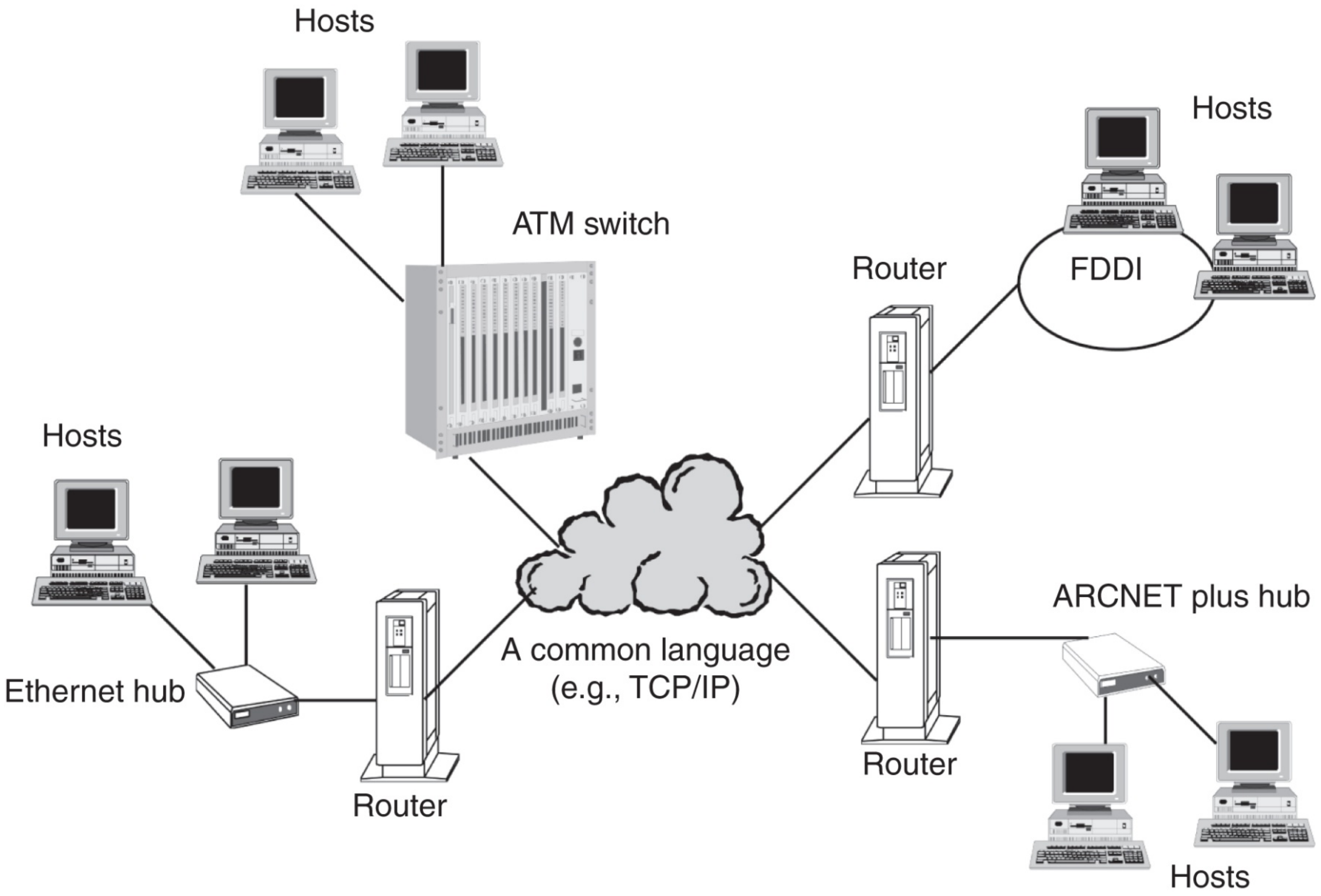
Network

- FDDI



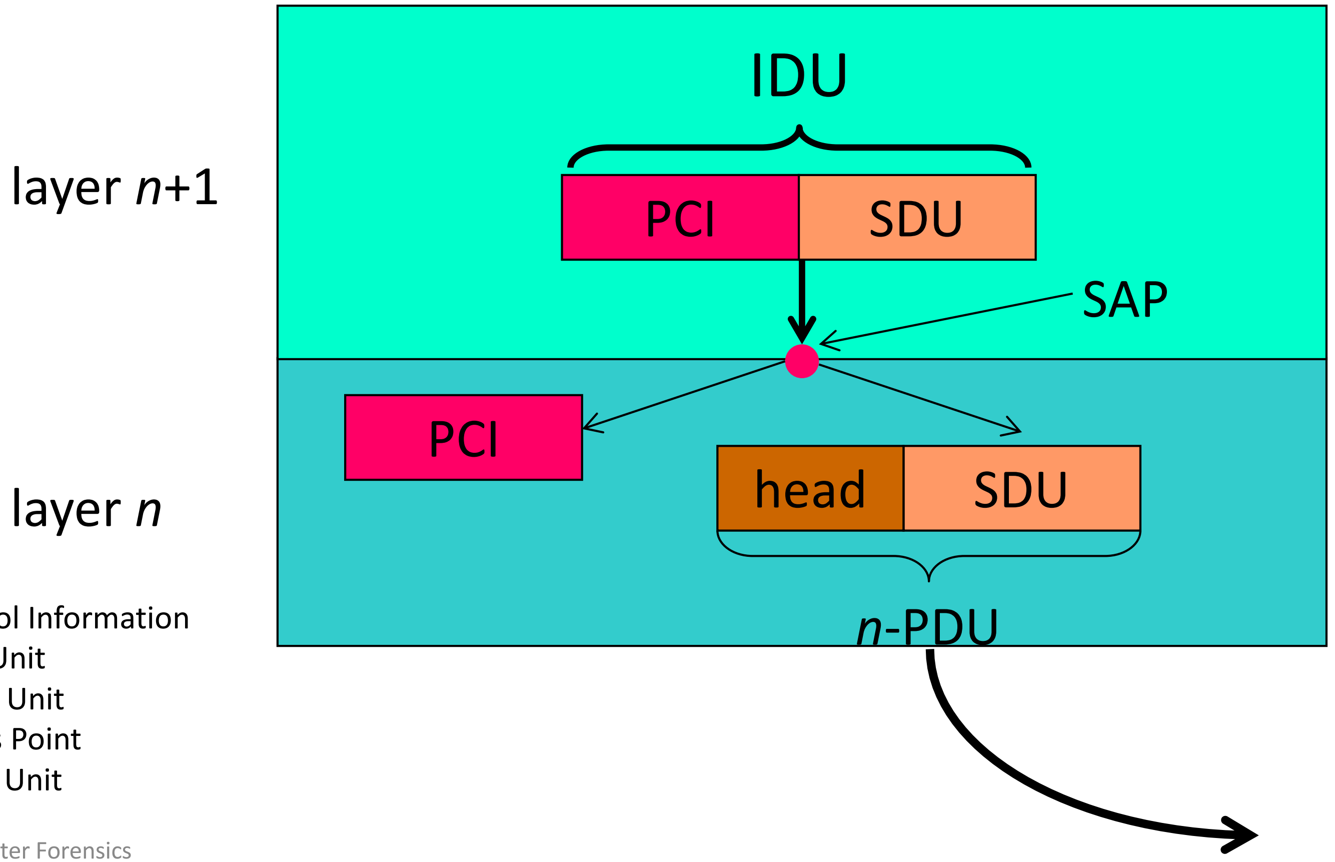
Network

- network of dissimilar networks and common language



Layer model

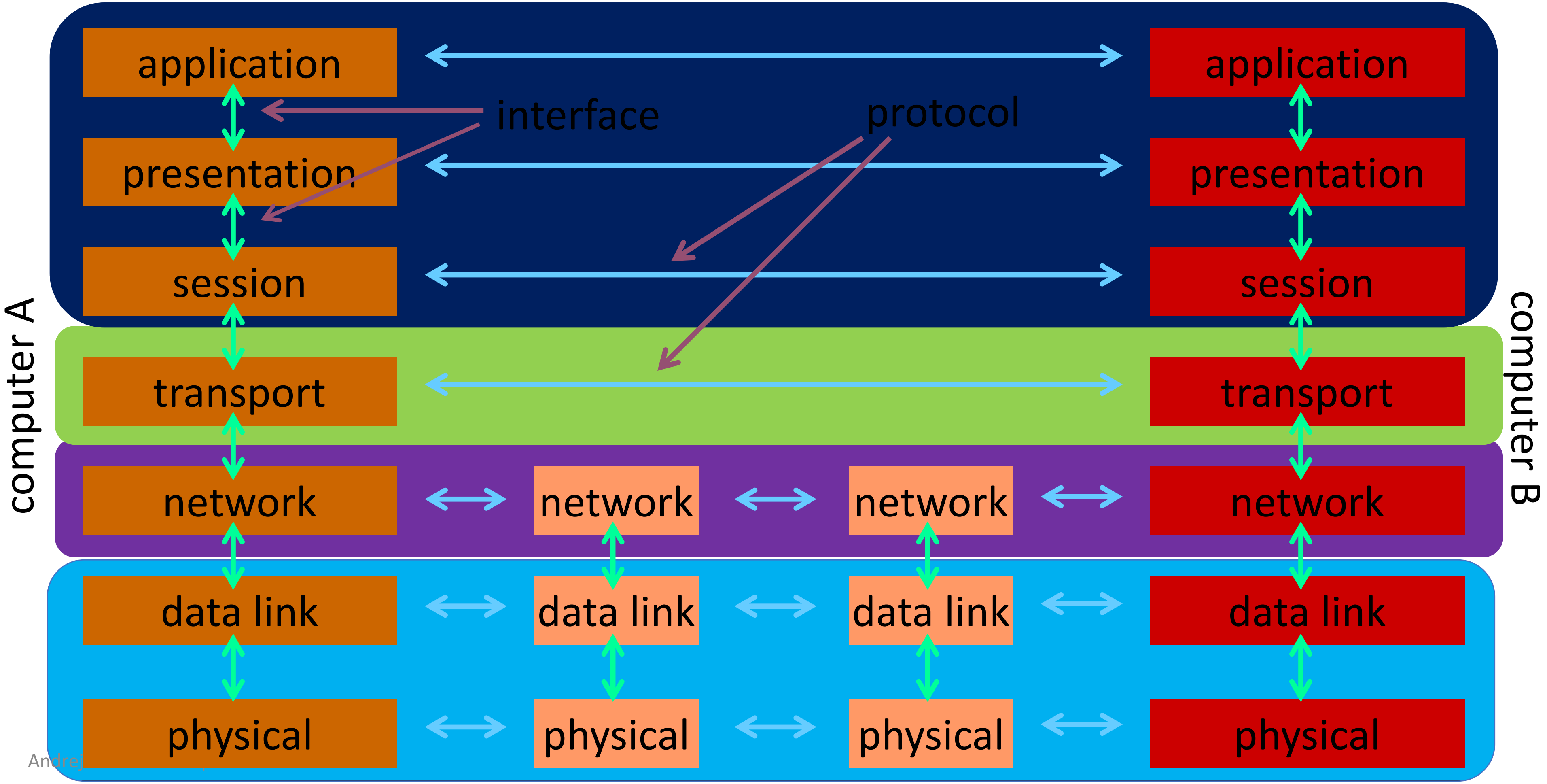
- each layer is independant from others
- It serves the layers above and is served by layers below



PCI = Protocol Control Information
SDU = Service Data Unit
PDU = Protocol Data Unit
SAP = Service Access Point
IDU = Interface Data Unit

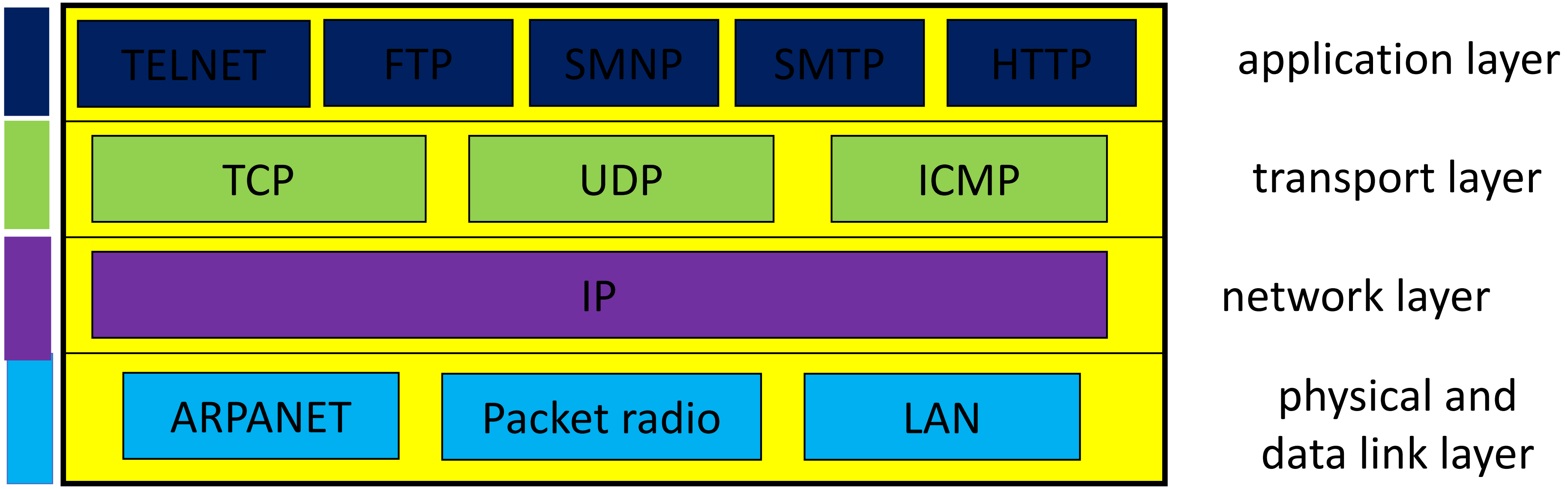
Reference models

- **layers of OSI reference model:** physical, data link, network, transport, session, presentation, application.



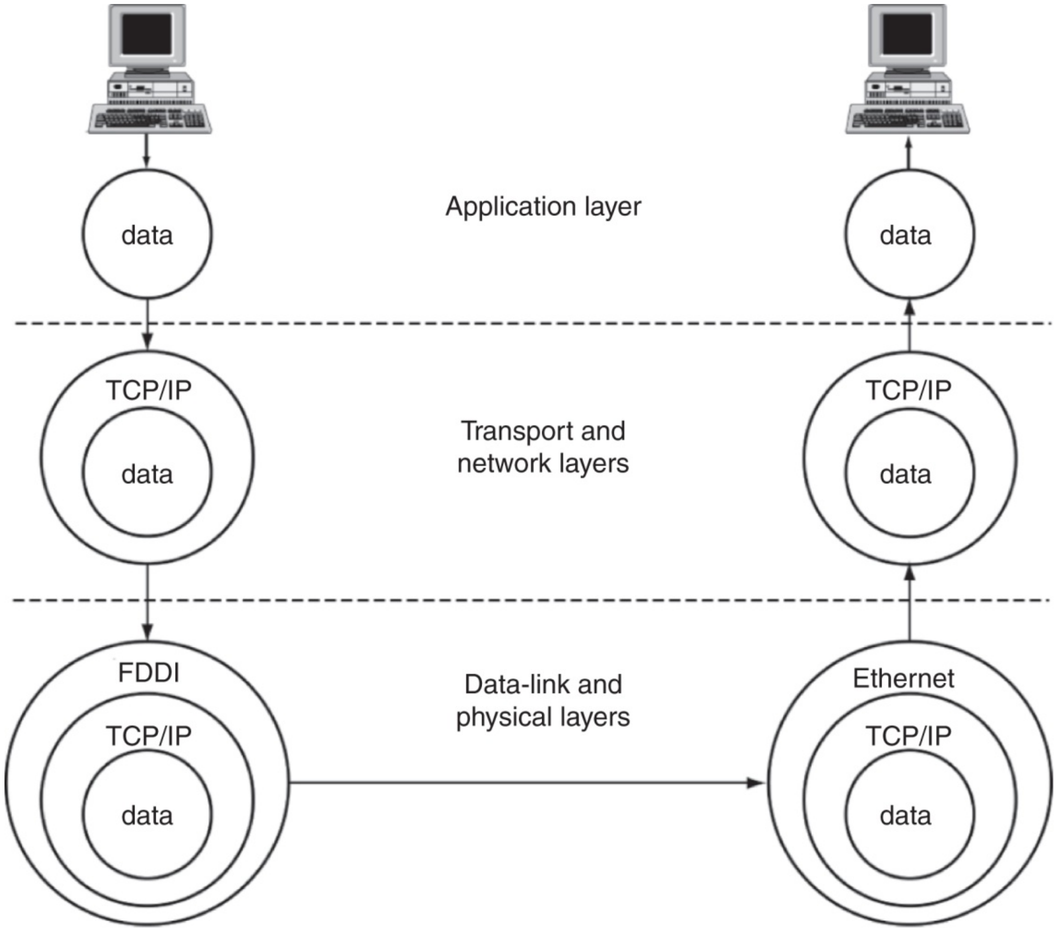
Reference model – TCP/IP

- TCP/IP reference model
  - is the foundation of the internet and *de facto* standard
  - no presentation or session layers
  - physical and data link layers are combined in so called “Host-to-network” layer
  - data link layer is composed of MAC and LLC (IEEE 802)



Containers

- TCP/IP example



Physical and data link layers

- physical: transmission of physical signals
- data link:
  - IEEE 802.11 is the most common
  - encompases different technologies
    - among the most well known are IEEE 802.3, 11, 15, 16, ...
  - composed of MAC and LLC sublayers
    - MAC – *media access control*: unique for a particular technology
    - LLC – *link layer control*: equal for all technologies

Network layer

- IP (*internet protocol*) is used for transparently relaying packets across networks
- best-effort and out-of-order delivery
- shared address space (IPv4, IPv6)
- connected to the data link layer through ARP (arp tool)
- *Challenge:* determine which computers are in your network. How would the protocol be used in a forensic investigation? How would the protocol (possibly with additional tools) be used in finding out what is happening in our network?

Transport layer

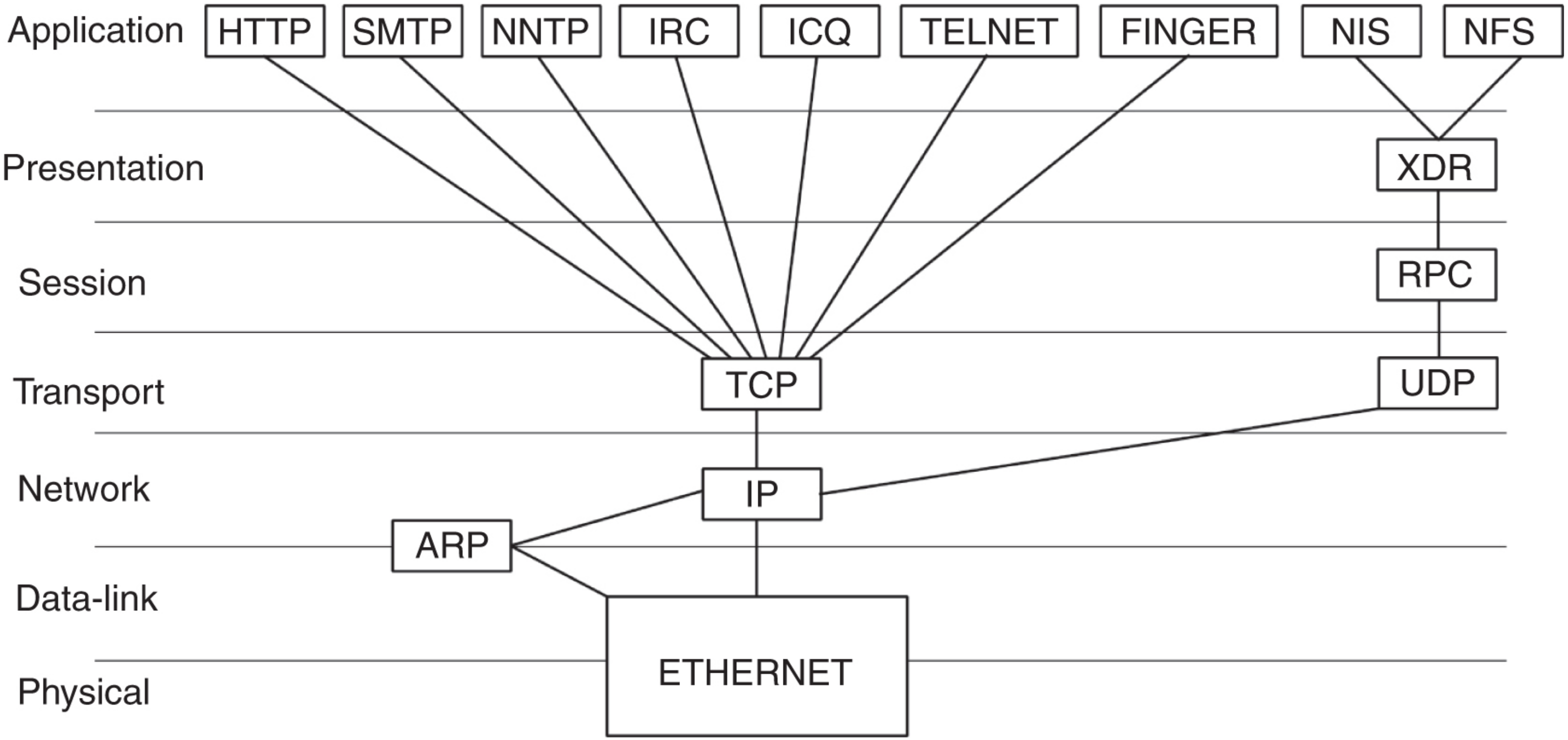
- fundamental protocols TCP and UDP: connection-oriented and connectionless communication
- TCP represents a stream of data between two processes on different computers

Application layer

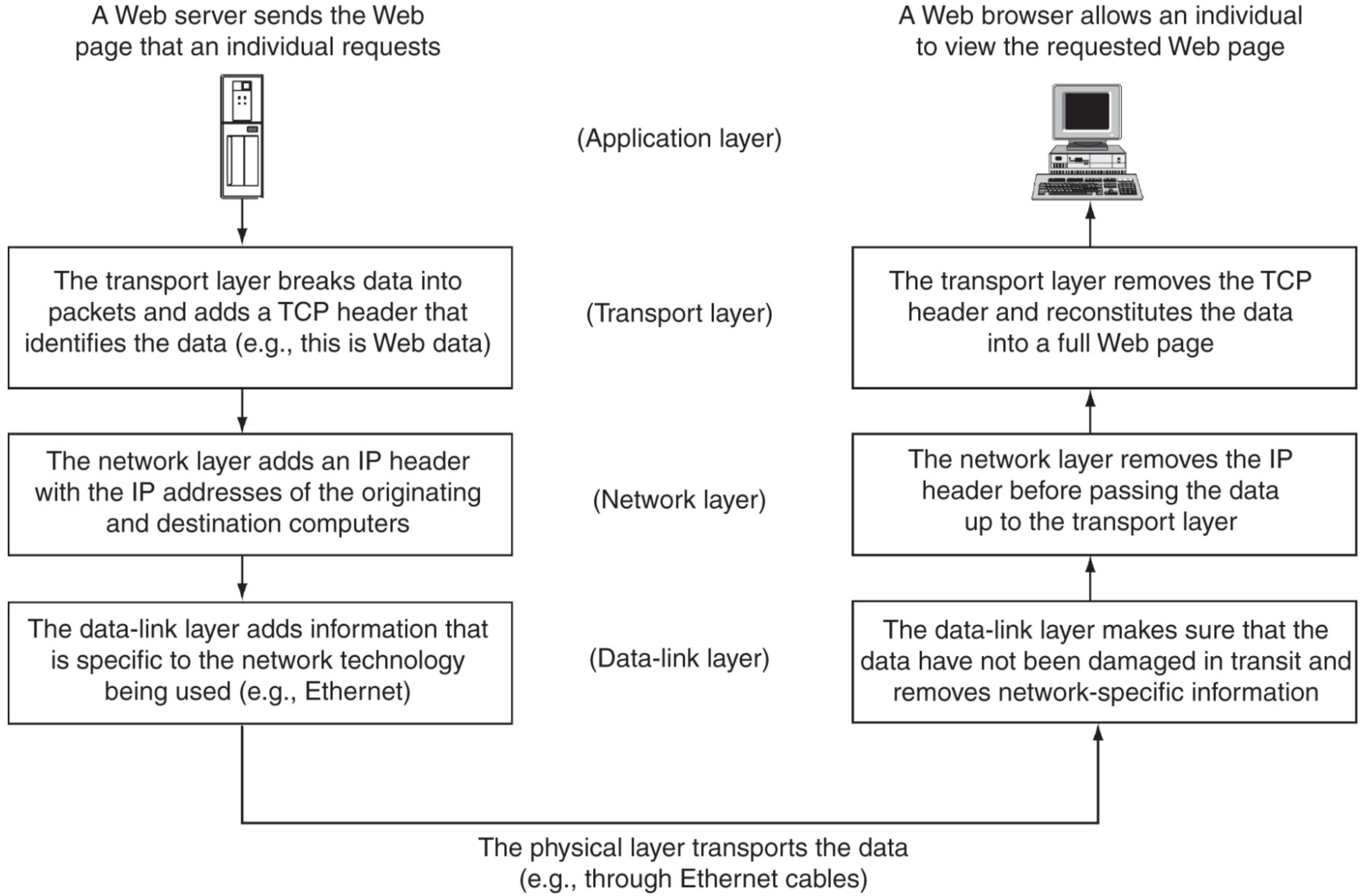
- standard applications: mail, web, news, IRC, ...
- non-standard applications: defined by the user

TCP/IP example

- example of protocol taxonomy



Protocol stack TCP/IP



A Web server sends the Web page that an individual requests

A Web browser allows an individual to view the requested Web page

(Application layer)

The transport layer breaks data into packets and adds a TCP header that identifies the data (e.g., this is Web data)

(Transport layer)

The transport layer removes the TCP header and reconstitutes the data into a full Web page

The network layer adds an IP header with the IP addresses of the originating and destination computers

(Network layer)

The network layer removes the IP header before passing the data up to the transport layer

The data-link layer adds information that is specific to the network technology being used (e.g., Ethernet)

(Data-link layer)

The data-link layer makes sure that the data have not been damaged in transit and removes network-specific information

The physical layer transports the data (e.g., through Ethernet cables)

Some fundamental tools

- basic tools made available by the operating system
  - arp:

```
Andy@svarun:~[122]%> arp -an
? (192.168.127.7) at 00:1f:5b:f2:e1:da on rl0 expires in 1189
  seconds [ethernet]
? (192.168.127.1) at 00:13:f7:39:d8:d1 on rl0 permanent
  [ethernet]
```

Some fundamental tools ...

- netstat:

```
Andy@svarun:~[124]%> netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif Expire
default            213.250.19.90      UGS            0 15915184   tun0
10.0.0.1           link#11            UHS            0        0    lo0
10.0.0.2           link#11            UHS            0        0   tun0
127.0.0.1          link#10            UH             0   168729    lo0
192.168.127.0/24   link#7             U              0  3843148    rl0
192.168.127.1      link#7             UHS            0   134062    lo0
193.77.156.167     link#11            UHS            0        0    lo0
213.250.19.90      link#11            UHS            0        0   tun0

Internet6:
Destination                       Gateway                       Flags      Netif Expire
::/96                             ::1                           UGRS        lo0
::1                               ::1                           UH          lo0
::ffff:0.0.0.0/96                 ::1                           UGRS        lo0
fe80::/10                         ::1                           UGRS        lo0
fe80::%rl0/64                     link#7                        U           rl0
fe80::213:f7ff:fe39:d8d1%rl0      link#7                        UHS         lo0
fe80::%rl1/64                     link#8                        U           rl1
fe80::213:f7ff:fe39:dac7%rl1      link#8                        UHS         lo0
fe80::%lo0/64                     link#10                       U           lo0
fe80::1%lo0                       link#10                       UHS         lo0
ff01::%rl0/32                     fe80::213:f7ff:fe39:d8d1%rl0  U           rl0
ff01::%rl1/32                     fe80::213:f7ff:fe39:dac7%rl1  U           rl1
ff01::%lo0/32                     ::1                           U           lo0
ff02::/16                         ::1                           UGRS        lo0
ff02::%rl0/32                     fe80::213:f7ff:fe39:d8d1%rl0  U           rl0
ff02::%rl1/32                     fe80::213:f7ff:fe39:dac7%rl1  U           rl1
ff02::%lo0/32                     ::1                           U           lo0
```

Some fundamental tools …

- sockstat:

```
Andy@svarun:~[128]%> sockstat
USER     COMMAND    PID   FD PROTO  LOCAL ADDRESS         FOREIGN
  ADDRESS
....     imap       97205 0  stream -> ??
dovecot  imap-login 97204 3  stream -> ??
dovecot  imap-login 97204 4  tcp4   *:143                 *:*
dovecot  imap-login 97204 5  tcp4   *:993                 *:*
dovecot  imap-login 97204 11 stream -> /var/run/dovecot/login/default
bind     named      1750  513 udp4  127.0.0.1:53          *:*
bind     named      1750  514 udp4  10.0.0.1:53           *:*
root     syslogd    1649  4  dgram  /var/run/log
root     syslogd    1649  5  dgram  /var/run/logpriv
...
```

Some fundamental tools …

- ifconfig:

```
Andy@svarun:~[131]%> ifconfig
alc0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500

  options=c3198<VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4,WOL_MCAST,WOL_
  MAGIC,VLAN_HWTSO,LINKSTATE>
          ether 54:04:a6:94:54:0b
          nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
          media: Ethernet autoselect
rl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu
  1500
          options=3808<VLAN_MTU,WOL_UCAST,WOL_MCAST,WOL_MAGIC>
          ether 00:13:f7:39:d8:d1
          inet6 fe80::213:f7ff:fe39:d8d1%rl0 prefixlen 64 scopeid 0x7
          inet 192.168.127.1 netmask 0xffffff00 broadcast
  192.168.127.255
          nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
          media: Ethernet autoselect (100baseTX <full-duplex>)
          status: active
rl1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu
  1500
          options=3808<VLAN_MTU,WOL_UCAST,WOL_MCAST,WOL_MAGIC>
          ether 00:13:f7:39:da:c7
          inet6 fe80::213:f7ff:fe39:dac7%rl1 prefixlen 64 scopeid 0x8
          nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
          media: Ethernet autoselect (100baseTX <full-duplex>)
          status: active
```

Some fundamental tools ...

- ifconfig:

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0xa
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
ipfw0: flags=8801<UP,SIMPLEX,MULTICAST> metric 0 mtu 65536
        nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu
 1492
        options=80000<LINKSTATE>
        inet 10.0.0.1 --> 10.0.0.2 netmask 0xffffff00
        inet 193.77.156.167 --> 213.250.19.90 netmask 0xffffff00
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        Opened by PID 85187
```

Some fundamental tools …

- tcpdump / pcap:

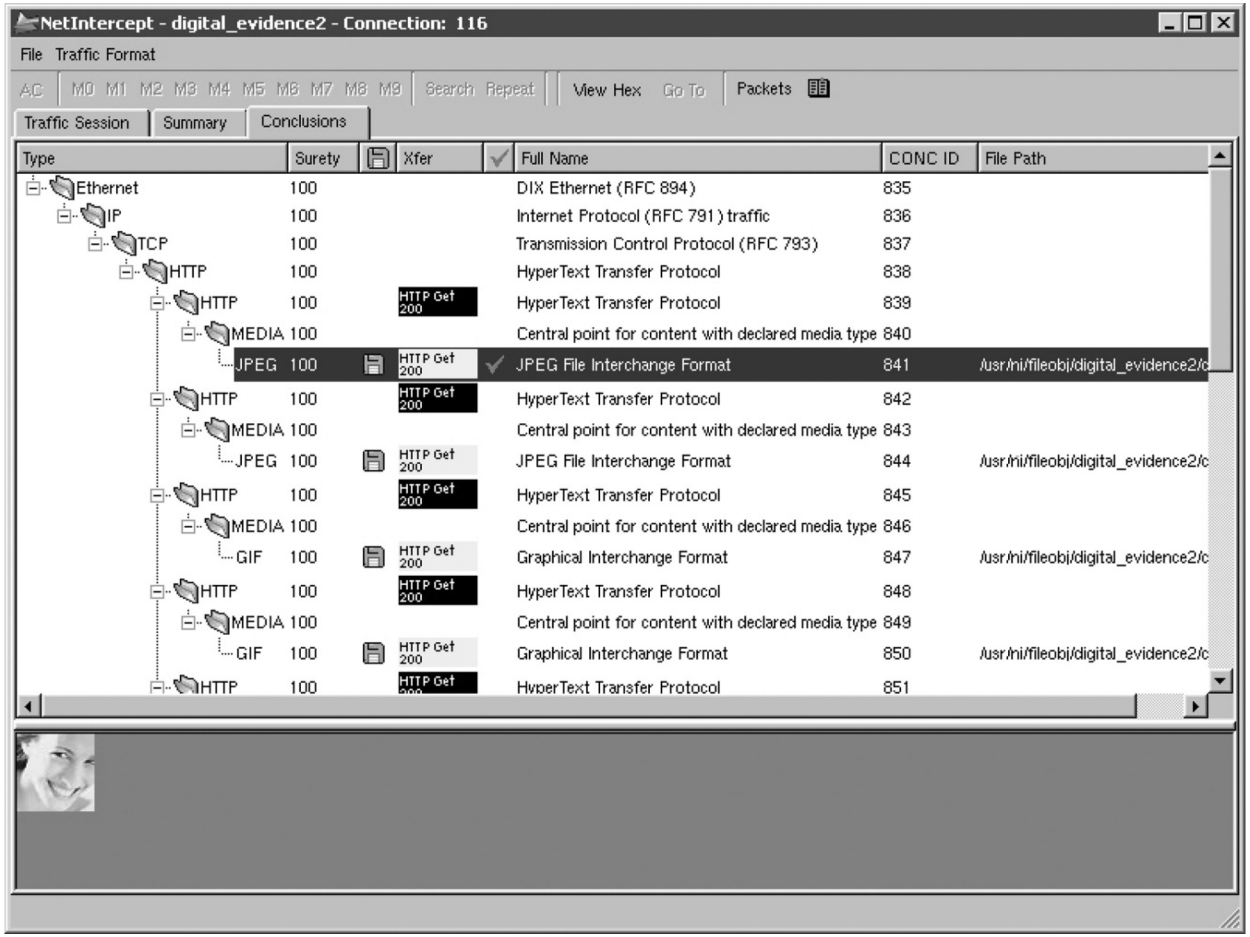
```
Andy@svarun:~[129]%> svarun# tcpdump -i rl0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol
  decode
listening on rl0, link-type EN10MB (Ethernet), capture size 65535
  bytes
08:10:33.878428 IP 193.77.156.167.22 > 192.168.127.7.53945: Flags
  [P.], seq 1108677235:1108677427, ack 2653943873, win 1040, options
  [nop,nop,TS val 2243985208 ecr 1042431634], length 192
08:10:33.878574 IP 192.168.127.7.53945 > 193.77.156.167.22: Flags [.],
  ack 192, win 33208, options [nop,nop,TS val 1042431634 ecr
  2243985208], length 0
08:10:34.379667 IP 192.168.127.7.47895 > 195.221.158.190.56534: UDP,
  length 137
08:10:34.429933 IP 192.168.127.7.47895 > 111.221.74.19.40012: UDP,
  length 32
08:10:34.441387 IP 195.221.158.190 > 192.168.127.7: ICMP
  195.221.158.190 udp port 56534 unreachable, length 156
08:10:34.712616 IP 111.221.74.19.40012 > 192.168.127.7.47895: UDP,
  length 434
08:10:34.878466 IP 193.77.156.167.22 > 192.168.127.7.53945: Flags
  [P.], seq 192:736, ack 1, win 1040, options [nop,nop,TS val
  2243986208 ecr 1042431634], length 544
...
```

Some fundamental tools ...

- *Challenge:* use basic tools to explore your neighborhood.
- *Challenge:* examine your system and determine which services it offers to the devices in the neighborhood?
- *Challenge:* the tcpdump tool allows for storage of captured data for later usage. The analysis of this data can be done using the wireshark tool. Try to perform this procedure.
- *Challenge:* in a forensically sound manner capture the data in your network and post the results on the forum. A colleague should then perform the analysis.

Professional and other tools

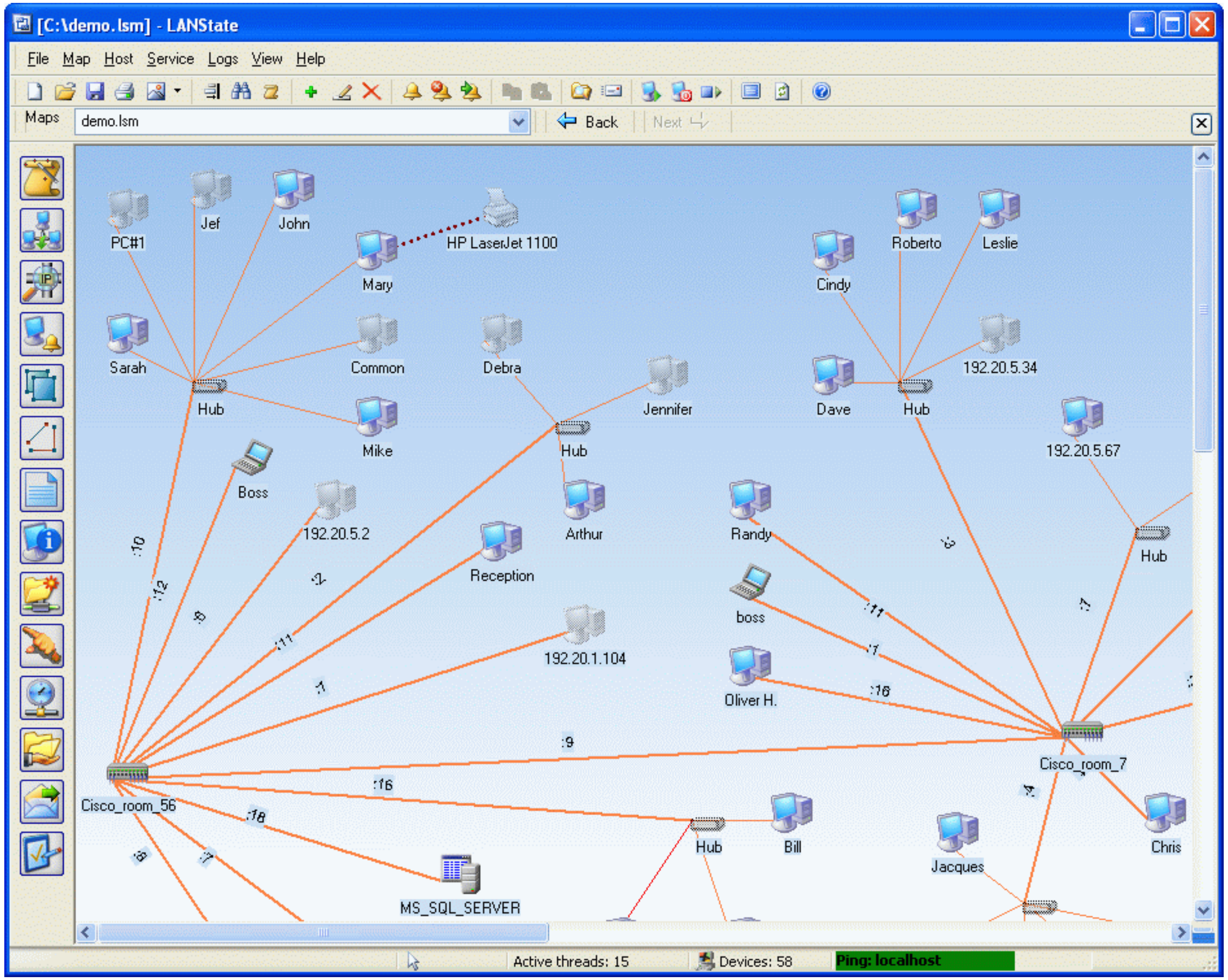
- Niksun forensics tools http://www.niksun.com/sandstorm.php: netintercept



Type	Surety	🖫	Xfer	✓	Full Name	CONC ID	File Path
Ethernet	100				DIX Ethernet (RFC 894)	835	
IP	100				Internet Protocol (RFC 791) traffic	836	
TCP	100				Transmission Control Protocol (RFC 793)	837	
HTTP	100				HyperText Transfer Protocol	838	
HTTP	100		HTTP Get 200		HyperText Transfer Protocol	839	
MEDIA	100				Central point for content with declared media type	840	
JPEG	100	🖫	HTTP Get 200	✓	JPEG File Interchange Format	841	/usr/ni/fileobj/digital_evidence2/c
HTTP	100		HTTP Get 200		HyperText Transfer Protocol	842	
MEDIA	100				Central point for content with declared media type	843	
JPEG	100	🖫	HTTP Get 200		JPEG File Interchange Format	844	/usr/ni/fileobj/digital_evidence2/c
HTTP	100		HTTP Get 200		HyperText Transfer Protocol	845	
MEDIA	100				Central point for content with declared media type	846	
GIF	100	🖫	HTTP Get 200		Graphical Interchange Format	847	/usr/ni/fileobj/digital_evidence2/c
HTTP	100		HTTP Get 200		HyperText Transfer Protocol	848	
MEDIA	100				Central point for content with declared media type	849	
GIF	100	🖫	HTTP Get 200		Graphical Interchange Format	850	/usr/ni/fileobj/digital_evidence2/c
HTTP	100		HTTP Get		HyperText Transfer Protocol	851	

Professional and other tools

- network management protocols: snmp, rmon, …



[C:\demo.lsm] - LANState

Active threads: 15

Devices: 58

Ping: localhost

Protocol SNMP

- snmp v2 and v3
- connectionless data transfer: UDP
- two types of commands:
  - on-demand data transfer and
  - event based data transfer
- the status of the network is stored in the MDB and in the log files
- *Challenge:* find tools for network exploration that employ the snmp protocol and explore your neighborhood.

Strength in numbers

- www.fri.uni-lj.si = 212.235.188.25
- DNS service maps strings to numbers
  - a mapping table in /etc/hosts can alternatively be used
- a DNS server inquires other DNS servers if there is a string it can’t map
  - file /etc/namedb/named.root
- tools *dig* and *nslookup*

DNS server

- file /etc/namedb/named.root (excerpt):

```
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
```

DNS server

- *Challenge:* with an appropriate tool find your DNS server and examine its records.
- *Challenge:* with your colleagues set up an isolated network with its own root name servers.
- *Challenge*: assume that the following packet was captured on the network:

```
09:13:01.839003 IP (tos 0x10, ttl 64, id 13571,
 offset 0, flags [DF], proto TCP (6), length 180)
    www.brodnik.org.ssh >
 AndyMac.gotska.brodnik.org.53945: Flags [P.], cksum
 0xf181 (correct), seq 1108696419:1108696547, ack
 2653946897, win 1040, options [nop,nop,TS val
 2247733168 ecr 1042469077], length 128
```

comment on the contents and determine the sender and the recipient.

Strength in numbers

- DNS service uses port 53
- there is no service that would map DNS to 53
    - there is however a mappign table in /etc/services
- the system binds the application to the process (program) at startup

Application names

```
#
# Network services, Internet style
#
# WELL KNOWN PORT NUMBERS
#
rtmp                1/ddp     #Routing Table Maintenance
 Protocol
tcpmux              1/udp      # TCP Port Service
 Multiplexer
tcpmux              1/tcp      # TCP Port Service
 Multiplexer

                              ...
domain             53/tcp     #Domain Name Server
domain             53/udp     #Domain Name Server
imap              143/tcp     imap2 imap4  #Interim Mail
 Access Protocol v2
imap              143/udp     imap2 imap4  #Interim Mail
 Access Protocol v2
imaps             993/tcp     # imap4 protocol over TLS/SSL
imaps             993/udp
                              ...
```

Application names

- sockstat

```
Andy@svarun:~[128]%> sockstat
USER     COMMAND    PID   FD PROTO  LOCAL ADDRESS         FOREIGN
  ADDRESS
....     imap       97205 0  stream -> ??
dovecot  imap-login 97204 3  stream -> ??
dovecot  imap-login 97204 4  tcp4   *:143                 *:*
dovecot  imap-login 97204 5  tcp4   *:993                 *:*
dovecot  imap-login 97204 11 stream -> /var/run/dovecot/login/default
bind     named      1750  513 udp4  127.0.0.1:53          *:*
bind     named      1750  514 udp4  10.0.0.1:53           *:*
root     syslogd    1649  4  dgram  /var/run/log
root     syslogd    1649  5  dgram  /var/run/logpriv
...
```

Application names

- *Challenge:* what is the actual name of the DNS service in the said table?
- *Challenge:* add/modify an entry in the table. Do you notice any changes when running sockstat, netstat, tcpdump?
- *Challenge:* how does the operating system bind an application to a service port? How is this done on Windows, FreeBSD and on Linux?

Protocol names

- excerpt:

```
ip      0       IP              # internet protocol,
 pseudo protocol number
icmp    1       ICMP            # internet control
 message protocol
igmp    2       IGMP            # internet group
 management protocol
ggp     3       GGP             # gateway-gateway
 protocol
tcp     6       TCP             # transmission control
 protocol
udp     17      UDP             # user datagram protocol
ddp     37      DDP             # Datagram Delivery
 Protocol
ipv6    41      IPV6            # ipv6
mobile  55      MOBILE          # IP Mobility
ipv6-icmp       58      IPV6-ICMP       icmp6   # ICMP
 for IPv6
etherip 97      ETHERIP         # Ethernet-within-IP
 Encapsulation
```

Names …

- *Challenge:* which protocol is denoted by the number 50 ans what is it used for?
- *Challenges:* what are the formats of all three etc files – hosts, protocols, services?
- *Challenge*: what is cifs/smb? In which folder would you look for its definition?

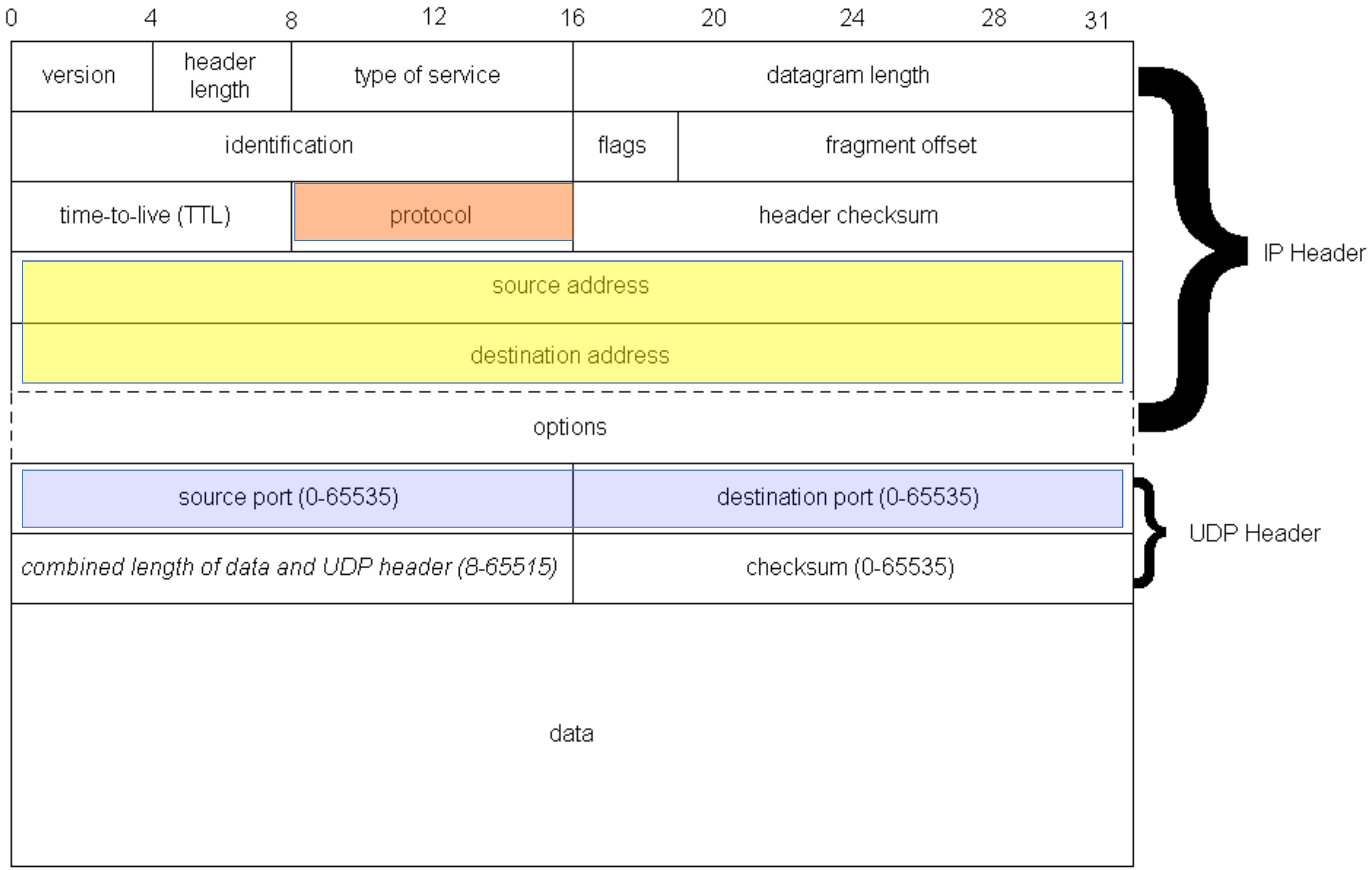
Where are the numbers from?

- global number assignment agreement
- numbers stored and allocated by IANA – *The Internet Assigned Numbers Authority*, www.iana.org
  - root DNS servers: www.iana.org/domains/root/db/arpa.html
  - *ports: www.iana.org/assignments/port-numbers*
  - *protocols: www.iana.org/protocols/*
- *Challenge:* write a program which can produce a services file from the available information on the IANA server
- *Challenge:* what information does the following webpage contain: www.iana.org/domains/root/db/si.html?

Going further

- so far, we understand the following:
  - what is an IP address and how is it mapped from a name (FQN – *fully qualified name*) (*hosts*, *DNS*)
  - what is the name of the protocol we are using (*protocols*)
  - what service do we want from a remote computer and what is its name (*services*)
  - what application offers a particular service (*sockstat*, *netstat*)

Going further



0 4 8 12 16 20 24 28 31

version | header length | type of service | datagram length

identification | flags | fragment offset

time-to-live (TTL) | protocol | header checksum

source address

destination address

options

IP Header

source port (0-65535) | destination port (0-65535)

combined length of data and UDP header (8-65515) | checksum (0-65535)

UDP Header

data

Going further

- who is the service provider?

- we can identify the provider by its IP or by the FQN bound to it
    - or directly through the application layer

WHOIS service

- service

```
    nicname            43/tcp    whois
    nicname            43/udp    whois
```

- we need a whois server
  - whois.iana.org, whois.arnes.si
  - tools: telnet, whois

WHOIS service

```
Andy@svarun:~[171]%> whois fri.uni-lj.si
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% This is ARNES whois database
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Rights restricted by copyright.
% See http://www.arnes.si/domene/whois-legal.html
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% The WHOIS service offered by Arnes, .si Registry, is
% provided for information purposes only. It allows persons
% to check whether a specific domain name is still available
% or not and to obtain information related to the registration
% records of existing domain names.
%
% This WHOIS service accepts and displays only ASCII characters.
%
% Arnes cannot be held liable should the stored information
% prove to be wrong, incomplete or inaccurate in any sense.
%
% By submitting a query you agree not to use the information
% made available to:
%      o Allow, enable or otherwise support the transmission
%        of unsolicited, commercial advertising or other solicitations
%        whether via email or otherwise;
%      o Target advertising in any possible way;
%      o Cause nuisance in any possible way to the registrants
%        by sending (whether by automated, electronic processes
%        capable of enabling high volumes or other possible
%        means) messages to them;
%      o copy, extract and/or publish contents of the WHOIS database.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% No entries found for the selected source(s).
```

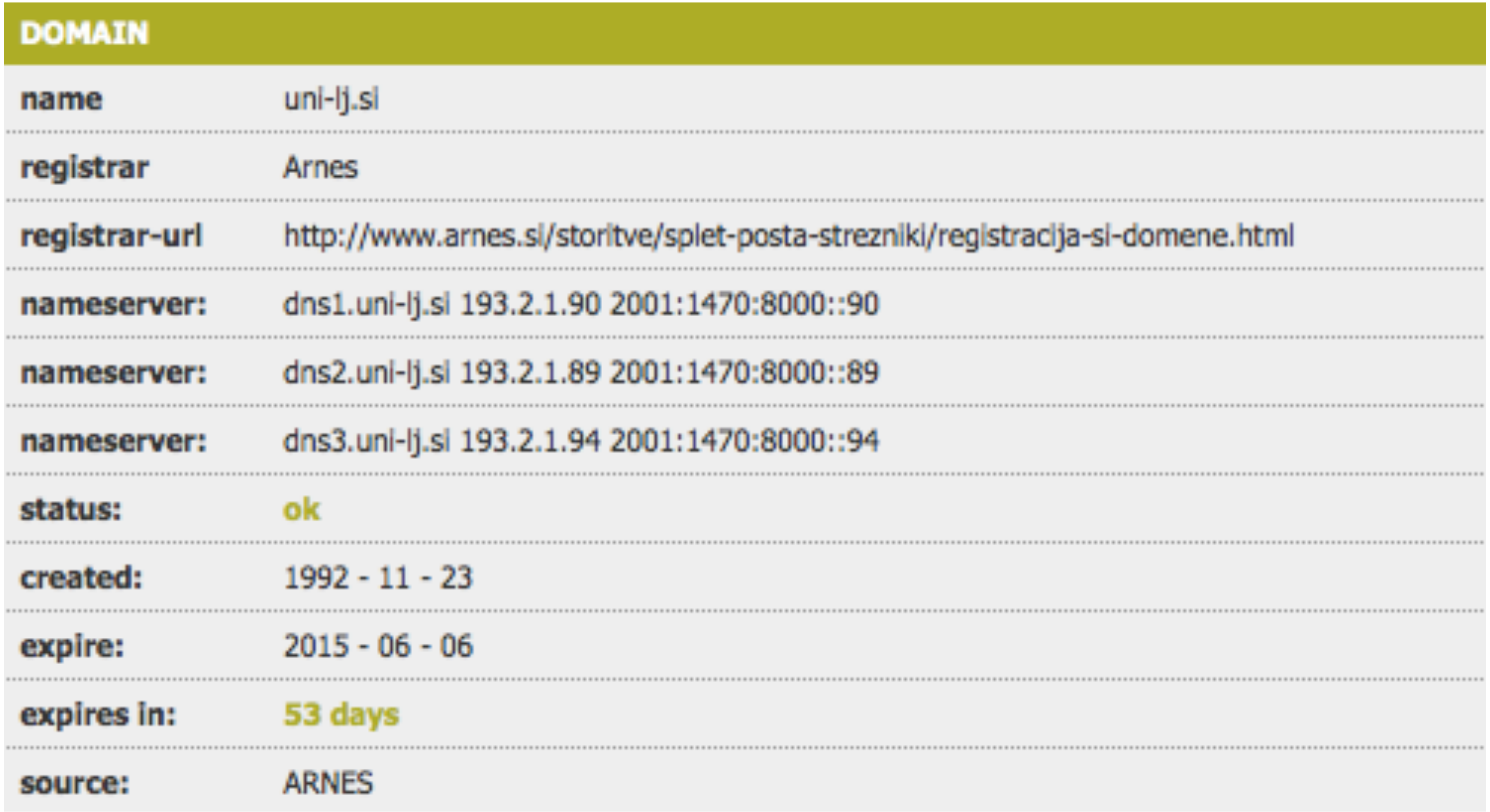
WHOIS service

```
Andy@svarun:~[172]%> whois uni-lj.si
                                      ...

domain:              uni-lj.si
registrar:    Arnes
registrar-url:       http://www.arnes.si/storitve/splet-posta-
  strezniki/registracija-si-domene.html
nameserver:   dns1.uni-lj.si (193.2.1.90,2001:1470:8000::90)
nameserver:   dns2.uni-lj.si (193.2.1.89,2001:1470:8000::89)
nameserver:   dns3.uni-lj.si (193.2.1.94,2001:1470:8000::94)
registrant:   G39085
status:              ok
created:      1992-11-23
expire:              2015-06-06
source:              ARNES

Domain holder:
NOT DISCLOSED

Tech:
NOT DISCLOSED

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% For more information, please visit http://www.registry.si/whois.html
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

WHOIS service

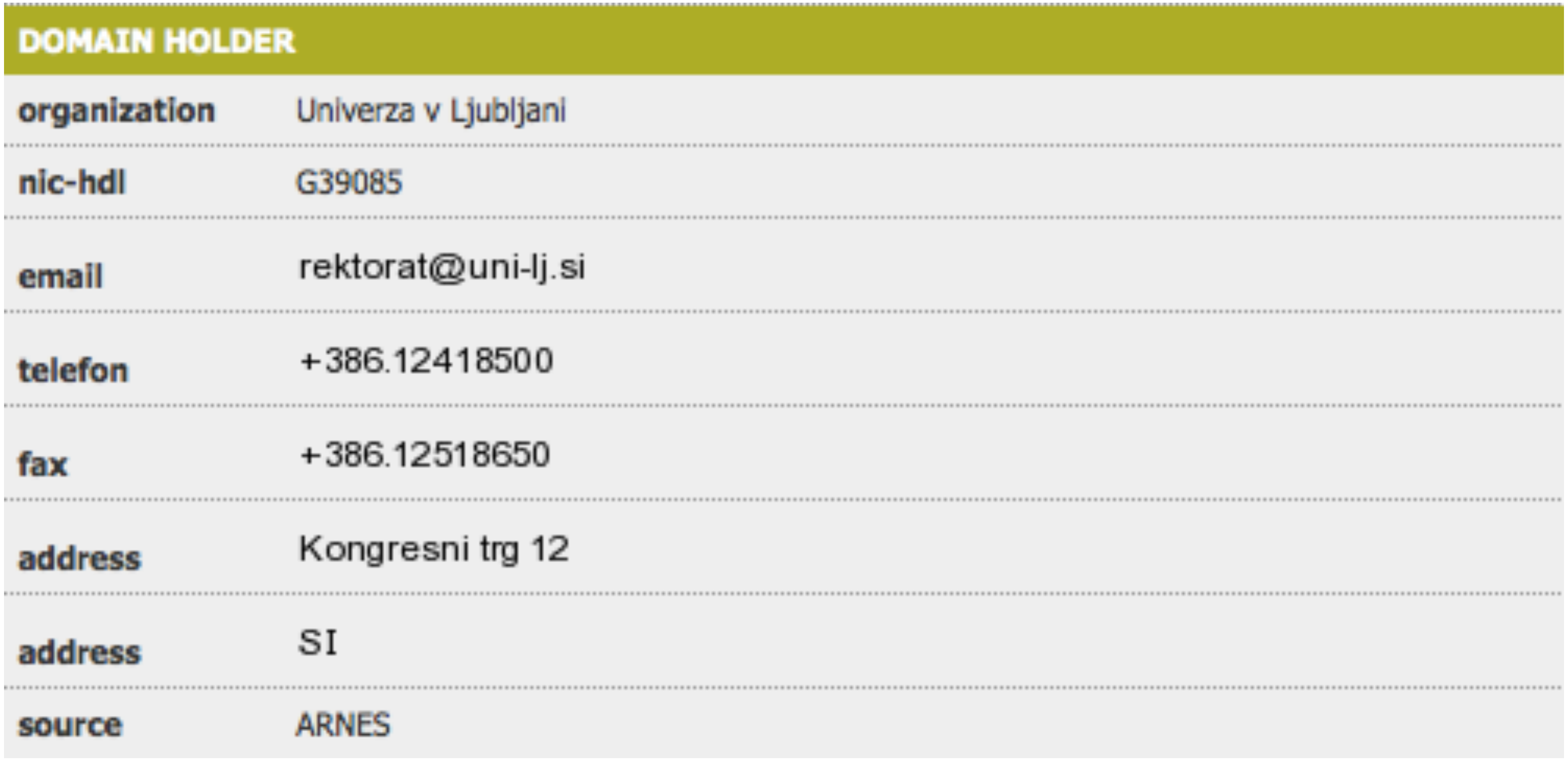
```
Andy@svarun:~[173]%> whois ul.si
                                        ...

domain:        ul.si
registrar:     Arnes
registrar-url: http://www.arnes.si/storitve/splet-posta-strezniki/registracija-si-
  domene.html
nameserver:    dns1.uni-lj.si (193.2.1.90,2001:1470:8000::90)
nameserver:    dns2.uni-lj.si (193.2.1.89,2001:1470:8000::89)
nameserver:    dns3.uni-lj.si (193.2.1.94,2001:1470:8000::94)
registrant:    G39085
status:        ok
created:       2010-10-20
expire:        2015-10-20
source:        ARNES

Domain holder:
NOT DISCLOSED

Tech:
NOT DISCLOSED

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% For more information, please visit http://www.registry.si/whois.html
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

WHOIS service



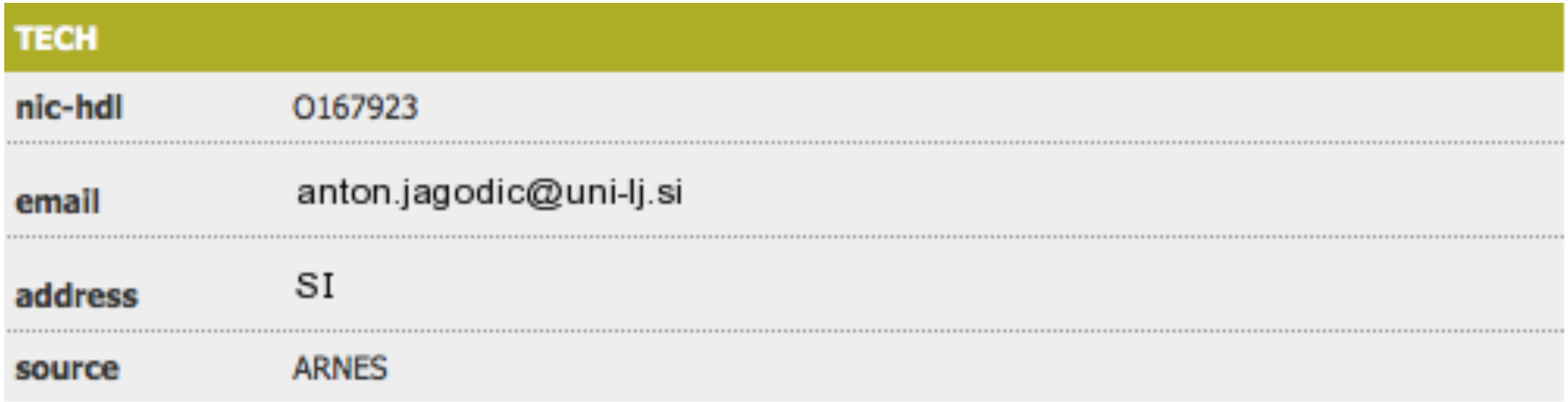
DOMAIN	
name	uni-lj.si
registrar	Arnes
registrar-url	http://www.arnes.si/storitve/splet-posta-strezniki/registracija-si-domene.html
nameserver:	dns1.uni-lj.si 193.2.1.90 2001:1470:8000::90
nameserver:	dns2.uni-lj.si 193.2.1.89 2001:1470:8000::89
nameserver:	dns3.uni-lj.si 193.2.1.94 2001:1470:8000::94
status:	ok
created:	1992 - 11 - 23
expire:	2015 - 06 - 06
expires in:	53 days
source:	ARNES

WHOIS service



DOMAIN HOLDER	
organization	Univerza v Ljubljani
nic-hdl	G39085
email	rektorat@uni-lj.si
telefon	+386.12418500
fax	+386.12518650
address	Kongresni trg 12
address	SI
source	ARNES

WHOIS service



TECH	
nic-hdl	0167923
email	anton.jagodic@uni-lj.si
address	SI
source	ARNES

WHOIS service

- *Challenge:* looking up information about the gov.si domain should not be difficult. What about other, foreign domains?
- *Challenge:* google.si is no challenge, what about google.com?
- *Challenge:* rkc.si – one would not have thought.
- *Challenge:* keeping in mind the sources of information we have talked about today, examine and comment on the following packets:

```
14:59:26.608728 IP xx.domain.netbcp.net.52497 >
  valh4.lell.net.ssh: . ack 540 win 16554
14:59:26.610602 IP resolver.lell.net.domain >
  valh4.lell.net.24151: 4278 1/0/0 (73)
14:59:26.611262 IP valh4.lell.net.38527 >
  resolver.lell.net.domain: 26364+ PTR? 244.207.104.10.in-
  addr.arpa. (45)
```