

Digitalna forenzika

Andrej Brodnik

Andrej Brodnik: Digitalna forenzika

Osnove računalniških omrežij

poglavja 21, 23, 24 in 25

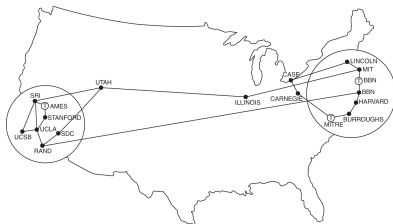
- iz zgodovine

ENIAC	ARPANET	Intel 8080	Mac & IBM PCs	WWW	Internet2
1946	1969	1974	1980s	1991	1999

Andrej Brodnik: Digitalna forenzika

Osnove računalniških omrežij

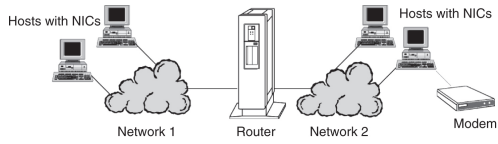
- iz zgodovine: ARPANET
- TCP/IP: 1973/74



Andrej Brodnik: Digitalna forenzika

Osnove računalniških omrežij

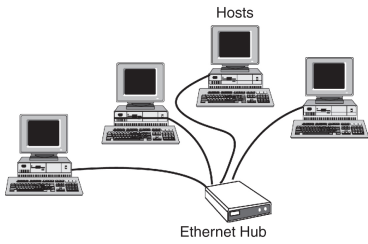
- mreža, omrežje in medmrežje



Andrej Brodnik, Digitalna forenzika

Mreža

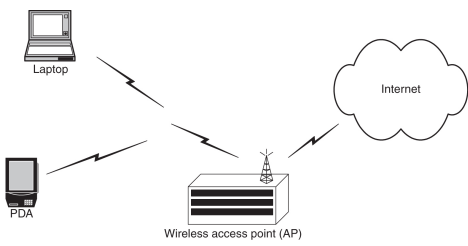
- ethernet mreža IEEE 802.3



Andrej Brodnik, Digitalna forenzika

Mreža

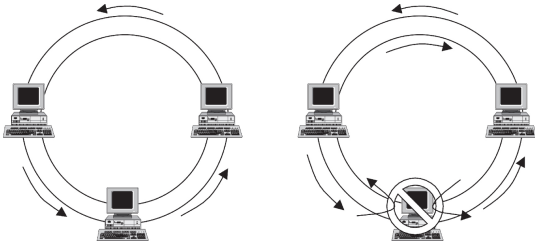
- ethernet mreža IEEE 802.11



Andrej Brodnik, Digitalna forenzika

Mreža

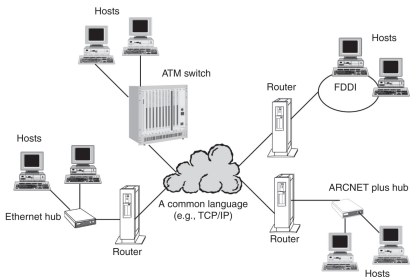
- FDDI mreža



Andrej Brodnik: Digitalna forenzika

Omrežje

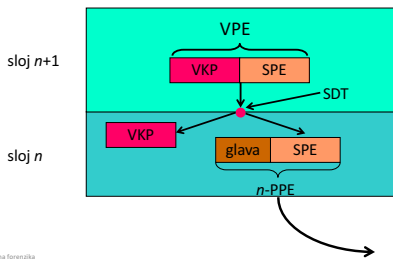
- omrežje in skupni jezik



Andrej Brodnik: Digitalna forenzika

Koncept omrežnih slojev

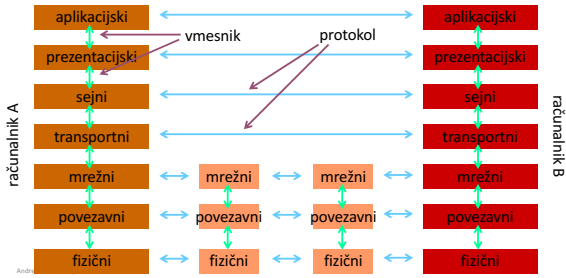
- vsak sloj je neodvisen od ostalih
- nudi storitve drugim slojem in uporablja storitve drugih slojev



Andrej Brodnik: Digitalna forenzika

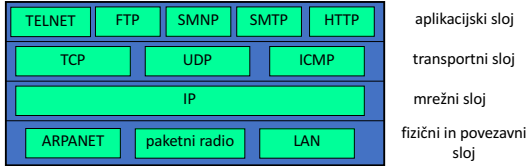
Referenčni modeli

- sloji referenčnega modela OSI: fizični, povezavni, mrežni, transportni, sejni, predstavitveni, aplikacijski.



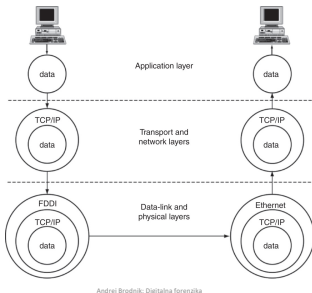
Referenčni model – TCP/IP

- referenčni model TCP/IP
 - je osnova Interneta in *de facto* standard
 - nima predstavnijskega in sejnega sloja
 - fizični in linijski sloj je združen v t.i. "host to network layer"
 - povezavna plast razdeljena na MAC in LLC (IEEE 802)



Vsebniki

- primer TCP/IP



Fizični in povezavni sloj

- fizični: fizični prenos signalov
- povezavni:
 - najpogostejši IEEE 802.11
 - združuje različne tehnologije
 - med najbolj znanimi IEEE 802.3, 11, 15, 16, ...
 - razdeljen na MAC in LLC
 - MAC – media access control: različen ed tehnologijami
 - LLC – link layer control: enak za vse tehnologije

Andrej Brodnik: Digitalna forenzika

Mrežni sloj

- IP (*internet protocol* – medmrežni protokol) skrbi za transparentno pošiljanje podatkov med mrežami
- dostava ni zagotovljena niti vrstni red dostave
- osnova je skupni naslovni prostor (IPv4, IPv6)
- povezava s povezavnim slojem je protokol ARP (orodje arp)
- *Izziv: preverite kateri računalniki so v vaši mreži. Kako lahko uporabimo protokol v forenzični preiskavi? Kako lahko s protokolom in še kakšnim orodjem sledimo dogodkom v naši mreži?*

Andrej Brodnik: Digitalna forenzika

Prenosni sloj

- prenosni ali transportni sloj
- TCP in UDP osnovna protokola: povezavni in brezpovezavni način delovanja
- TCP predstavlja tok podatkov med procesoma na različnih računalnikih

Andrej Brodnik: Digitalna forenzika

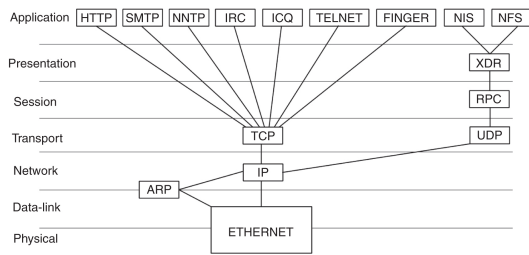
Aplikacijski sloj

- standardne aplikacije: pošta, splet, novice, IRC, ...
- nestandardne aplikacije: definira uporabnik

Andrej Brodnik: Digitalna forenzika

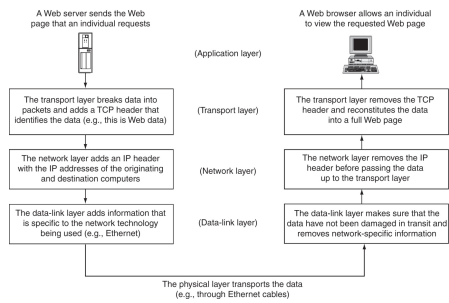
Primer TCP/IP

- primer taksonomije protokolov



Andrej Brodnik: Digitalna forenzika

Protokolni sklad TCP/IP



Andrej Brodnik: Digitalna forenzika

Nekaj osnovnih orodij

- osnovna orodja na voljo v operacijskem sistemu
 - arp:
- ```
Andy@svarun:~[122]#> arp -an
? (192.168.127.7) at 00:1f:5b:f2:e1:da on r10 expires in 1189
seconds [ethernet]
? (192.168.127.1) at 00:13:f7:39:d8:d1 on r10 permanent
[ethernet]
```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Nekaj osnovnih orodij ...

- netstat:
- ```
Andy@svarun:~[124]#> netstat -rn
Routing Table

Internet:
Destination Gateway      Flags  Refs  Use  Netif Expire
default    213.256.19.90 DGS#   0     0  tu00
10.0.0.1   link#11    URS#   0     0  tu00
10.0.0.2   link#11    URS#   0     0  tu00
127.0.0.1  link#10    U      0  168729  tu0
192.168.127.0/24 link#7    U      0  384148  r10
192.168.127.1 link#7    URS#   0  124062  tu0
192.168.127.2 link#7    URS#   0     0  tu0
213.256.19.90 link#11    URS#   0     0  tu00

Internet:
Destination Gateway      Flags  Netif Expire
:::96      :::         URS#   tu00
:::10.0.0.0/96 :::         URS#   tu00
fe80::10/64  :::         URS#   tu00
fe80::13:f7:f7:fe39:d8d1:r10 link#7     URS#   tu00
fe80::13:f7:f7:fe39:dac7:r11 link#8     URS#   tu00
fe80::100/64 link#10    URS#   tu00
fe80::100/64 link#10    URS#   tu00
ff01::r10/32 fe80::13:f7:f7:fe39:d8d1:r10 U          tu00
ff01::r10/32 fe80::13:f7:f7:fe39:dac7:r11 U          tu00
ff02::/16   :::         URS#   tu00
ff02::r10/32 fe80::13:f7:f7:fe39:d8d1:r10 U          tu00
ff02::r10/32 fe80::13:f7:f7:fe39:d8d1:r10 U          tu00
ff02::r10/32 fe80::13:f7:f7:fe39:d8d1:r11 U          tu00
```

Andrej Brodnik, Digitalna forenzika

Nekaj osnovnih orodij ...

- 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 *:1993 *:
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
...
```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Nekaj osnovnih orodij ...

```

• ifconfig:
Andy@svarun:~[131]# ifconfig
alo0: flags=8002<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
r10: 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:d8d1r10 prefixlen 64 scopeid 0x7
 inet 192.168.127.1 netmask 0xfffff00 broadcast
192.168.127.255
 nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
 media: Ethernet autoselect (100baseTX <full-duplex>)
 status: active
r11: 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:dac7r11 prefixlen 64 scopeid 0x8
 nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
 media: Ethernet autoselect (100baseTX <full-duplex>)
 status: active

```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Nekaj osnovnih orodij ...

```

• 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 0xffffffff0
 inet 193.77.156.167 --> 213.250.19.90 netmask 0xfffff00
 nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
 Opened by PID 85187

```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Nekaj osnovnih orodij ...

```

• tcpdump / pcap:
Andy@svarun:~[129]# svarun# tcpdump -i r10 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on r10, 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, len 10867427, 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 192736, ack 1, win 1040, options [nop,nop,TS val
2243986208 ecr 1042431634], length 544
...

```

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

---

---



Nekaj osnovnih orodij ...

- *Izziv:* uporabite osnovna orodja in si oglejte okolico svojega sistema.
- *Izziv:* pregledajte svoj sistem in preverite, katere vse storitve nudi okolici?
- *Izziv:* orodje tcpdump omogoča hranjenje zajetih podatkov in kasnejšo raziskavo. Slednjo lahko naredimo z orodjem wireshark. Preverite kako to gre.
- *Izziv:* izvedite korektno forenzičen zajem omrežnih podatkov na vašem sistemu ter ga objavite na forumu. Kolega naj naredi forenzično analizo le-teh.

Andrija Brodnik, Digitalna forenzika

---

---

---

---

---

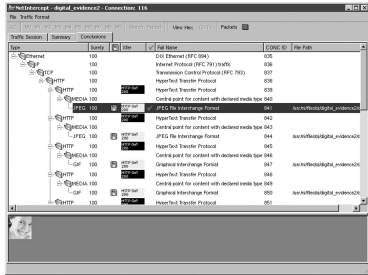
---

---

---

Profesionalna in druga orodja

- Nixsun forenzična orodja <http://www.nixsun.com/sandstorm.php>: netintercept




---

---

---

---

---

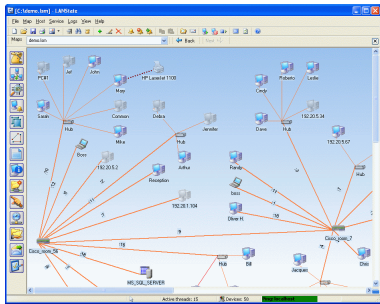
---

---

---

Profesionalna in druga orodja

- protokoli za upravljanje z omrežji: snmp, rmon, ...




---

---

---

---

---

---

---

---

## Protokol SNMP

- snmp v2 in v3
- nepovezavni način prenosa podatkov: UDP
- dve vrsti ukazov:
  - prenos podatkov na zahtevo in
  - prenos ob dogodku
- podatki o stanju omrežja se hranijo v MDB in v dnevniških zapisih
- **Izziv: poiščite orodja za preiskovanje omrežja s protokolom snmp in preiščite svojo okolico.**

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Vse je v številkah

- [www.fri.uni-lj.si](http://www.fri.uni-lj.si) = 212.235.188.25
- storitev DNS preslikuje med črkovnim nizom in številko
  - namesto DNS storitve lahko uporabimo preslikovalno tabelo v datoteki `/etc/hosts`
- strežnik DNS sprašuje druge strežnike DNS, če česa ne ve
  - datoteka `/etc/namedb/named.root`
- orodji *dig* in *nslookup*

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## Strežnik DNS

```

• datoteka /etc/namedb/named.root (izvleček):
; 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
;
B.ROOT-SERVERS.NET. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 192.228.79.201
;
; FORMERLY C.PSI.NET
;
C.ROOT-SERVERS.NET. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
D.ROOT-SERVERS.NET. 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
;
E.ROOT-SERVERS.NET. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
;
; FORMERLY NS.ISC.ORG

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Strežnik DNS

- Izziv: poiščite z ustreznim orodjem svoj strežnik DNS storitve in pregledajte, kaj vse hrani.
- Izziv: s kolegi se dogovorite in vzpostavite ločeno omrežje tako, da si postavite svoje korenenske strežnike.
- Izziv: recimo, da smo zajeli naslednji paket na omrežju:  
 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  
 komentirajte vsebino in kdo komu pošilja.

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Vse je v številkah

- DNS storitev uporablja vrata številka 53
- nimamo storitve, ki bi preslikovala med imenom DNS in 53
  - imamo preslikovalno tabelo v datoteki /etc/services
- sistem poveže aplikacijo s procesom (programom) ob zagonu

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Imena aplikacij

```

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

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Imena aplikacij

• sockstat

```

Andy@svanun:~[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
...

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Imena aplikacij

- Izziv: kako se v resnici imenuje DNS storitev v omenjeni tabeli?
- Izziv: dodajte/spremenite kakšen vnos v omenjeni tabeli. Ali se kaj spremeni pri sockstat, netstat, tcpdump?
- Izziv: kako operacijski sistem poveže aplikacijo z vrati za storitev? Kako se to naredi na Windows, na FreeBSD in kako na Linux?

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Imena protokolov

• izvleček:

```

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 # ICMP for IPv6
etherip 97 ETHERIP # Ethernet-within-IP Encapsulation

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Imena ...

- Izziv: kateri protokol ima številko 50 in za kaj se uporablja?
- Izziv: Kakšni so formati vseh treh etc datotek – hosts, protocols, services?
- Izziv: kaj je to cifs / smb? V kateri datoteki bi iskali njegovo definicijo?

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### In od kje pridejo številke

- svetovni dogovor o številkah
- številke hrani in oglašča IANA – *The Internet Assigned Numbers Authority*, [www.iana.org](http://www.iana.org)
  - korenski DNS strežniki: [www.iana.org/domains/root/db/arpa.html](http://www.iana.org/domains/root/db/arpa.html)
  - vrata: [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)
  - protokoli: [www.iana.org/protocols/](http://www.iana.org/protocols/)
- Izziv: napišite program, ki tvori samodejno datoteko services iz podatkov na IANA strežniku
- Izziv: kakšni podatki so na [www.iana.org/domains/root/db/si.html](http://www.iana.org/domains/root/db/si.html)?

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

### Iščemo naprej

- do sedaj razumemo:
  - kaj je IP naslov in kako se preslikuje z imenom (FQN – *fully qualified name*) (*hosts, DNS*)
  - kaj je ime protokola, ki ga uporabljamo (*protocols*)
  - kaj je storitev, ki jo želimo na oddaljenem računalniku in kako se imenuje (*services*)
  - katera aplikacija ponuja določeno storitev (*sockstat, netstat*)

Andrej Brodnik: Digitalna forenzika

---

---

---

---

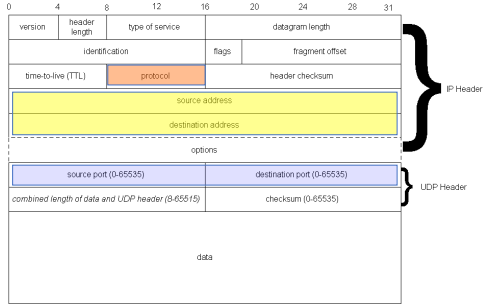
---

---

---

---

### Iščemo naprej




---

---

---

---

---

---

---

---

### Iščemo naprej

- In kdo je dejanski ponudnik storitve?
- ponudnika poznamo po IP naslovu, oziroma iz njega izhajajočem FQN
  - lahko tudi neposredno na aplikacijski plasti

---

---

---

---

---

---

---

---

### Storitev WHOIS

- storitev
  - nicname 43/tcp whois
  - nicname 43/udp whois
- potrebujemo strežnik storitve whois
  - whois.iana.org, whois.arnes.si
  - orodja telnet, whois

---

---

---

---

---

---

---

---

### Storitev WHOIS

```

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 defined by ARNES.si Registry is
% provided for information purposes only. REGISTRARS 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 cause advertising in any possible way
% to be sent to you or to any other person;
%
% o cause nuisance in any possible way to the registrants
% by sending together 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).

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Storitev WHOIS

```

Andy@svarun-[172]# whois uni-lj.si
...
domain: uni-lj.si
registrar: Arnes
registrar-url: http://www.arnes.si/storitev/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: C29085
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

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### Storitev WHOIS

```

Andy@svarun-[173]# whois ul.si
...
domain: ul.si
registrar: Arnes
registrar-url: http://www.arnes.si/storitev/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: C29085
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

```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

Storitev WHOIS

| DOMAIN        |                                                                                |
|---------------|--------------------------------------------------------------------------------|
| name          | uni-lj.si                                                                      |
| registrar     | Arnes                                                                          |
| registrar-uri | 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                                                                          |

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

Storitev WHOIS

| 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                |

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

Storitev WHOIS

| TECH    |                         |
|---------|-------------------------|
| nic-hdl | O167923                 |
| email   | anton.jagodic@uni-lj.si |
| address | SI                      |
| source  | ARNES                   |

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---



### Storitev WHOIS

- *Izziv:* iskanje podatkov o domeni gov.si ne bo težko. Kaj pa o kakšni drugi, tuji domeni?
- *Izziv:* google.si ne bo težko, kaj pa google.com?
- *Izziv:* rkc.si – človek si ne bi mislil.
- *Izziv:* našli smo naslednje pakete, ki jih komentirajte upoštevaje vire informacij, ki smo jih spoznali danes:

```
14:59:26.608728 IP xx.domain.nethop.net.52497 >
valh4.lell.net.ssh: . ack 340 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)
```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---