2. PRAKTIKA: SARRERA WIRESHARK

PROTOKOLO AZTERTZAILEA

2020 – 2021 KURTSOA

Konputagailu Sareen Oinarriak

Irakaslea: Gaizka Saldaña

SISTEMEN INGENIARITZA ETA AUTOMATIKA SAILA

PRAKTIKAREN HELBURUA

Praktika honen xedea da ikasleek protokolo-analizatzaile baten oinarrizko funtzionalitateak ezagutzea eta protokolo sinple batzuk aztertzeko erabili ahal izatea.

Sarrera

Protokoloen aztertzailea sareko protokoloak eta aplikazioak garatzeko eta arazteko tresna da. Ordenagailuak sareko hainbat fotograma har ditzake aztertzeko, denbora errealean edo harrapatu ondoren. Aztertuz gero, programak harrapatutako fotograma protokolo zehatz batekoa dela jakin dezake (TCP, ICMP ...) eta deskodetutako informazioa erakusten dio erabiltzaileari. Praktika honetan erabiliko dugun protokoloaren aztertzailea **Wireshark** da.

Wireshark komunikazio sareetako arazoak aztertzeko eta konpontzeko erabiltzen da, softwarea eta protokoloak garatzeko eta irakasteko tresna gisa. Protokolo analizatzaile baten ezaugarri estandar guztiak ditu.
Zuzenean sare batetik edo diskoan gordetako harrapaketa fitxategi batetik datuak arakatzeko aukera ematen du. Wireshark-ek linean harrapatutako edo diskoan gordetako informazioetatik ikusi nahi duguna iragazteko hizkuntza osoa dakar.

Wireshark software librea da, eta Unix eta sistema eragile bateragarri gehienetan funtzionatzen du, Mac OS X, baita Microsoft Windows ere.

Programa jaisteko esteka: http://www.wireshark.org/download.html

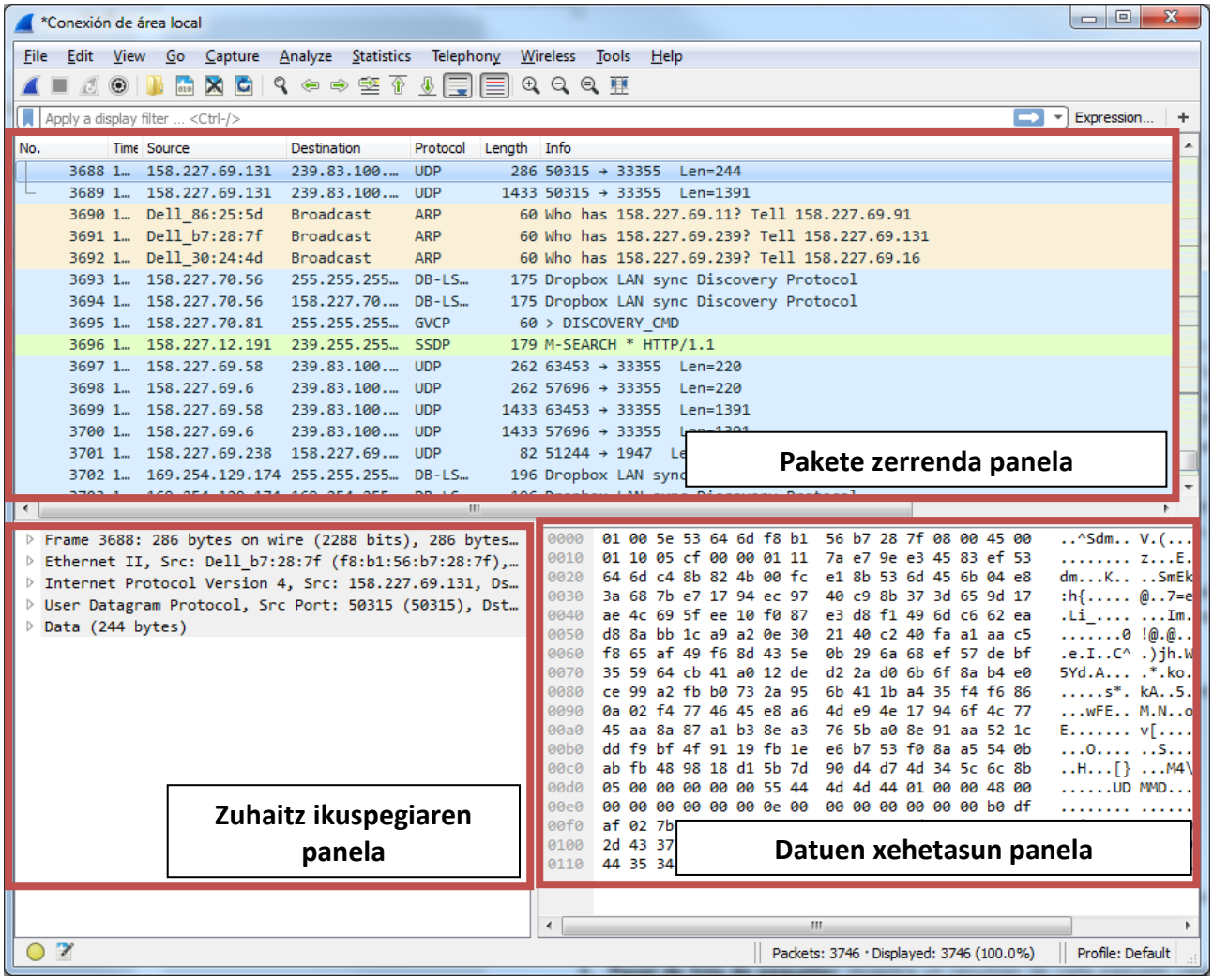
1. ATALA: LEHENENGO URRATSAK WIRESHARKAREKIN

1. irudi honetan programaren pantaila nagusia agertzen da. Hiru panel desberdin bereiz daitezke:

1. **Pakete zerrenda panela:** harrapatutako pakete bakoitzaren laburpena erakusten du. Panel honetako paketeetan klik eginez gero, beheko beste bi panelen edukia kontrolatzen da.

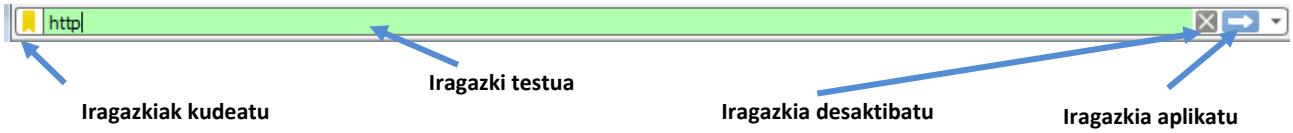
2. **Zuhaitz ikuspegiaren panela:** hautatutako paketea goiko panelean (1) erakusten du xehetasun gehiagorekin, protokoloen maila desberdinetara sarbidea ahalbidetuz. Maila bakoitzean klik eginez gero, maila horri dagokion paketearen datuak nabarmentzen dira beheko panelean (3).

3. **Datuen xehetasun panela:** hautatutako paketearen edukia goiko panelean (1) bistaratzen du hamaseitar eta ASCII formatuan.



1. Irudia. WireShark programaren hasiera pantaila

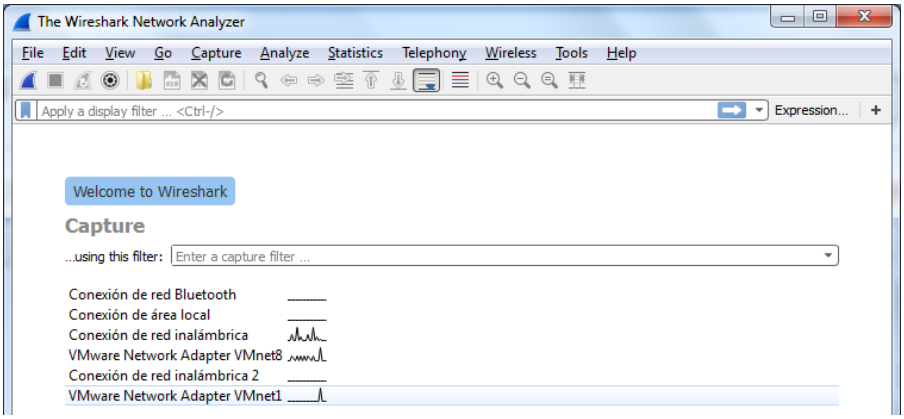
Hiru panel nagusiez gain, **iragazkiekin lan egiteko barra** nabarmendu dezakezu, WireShark pantailaren goialdean eskuragarri:



2. Irudia. Iragazkiekin lan egiteko barra

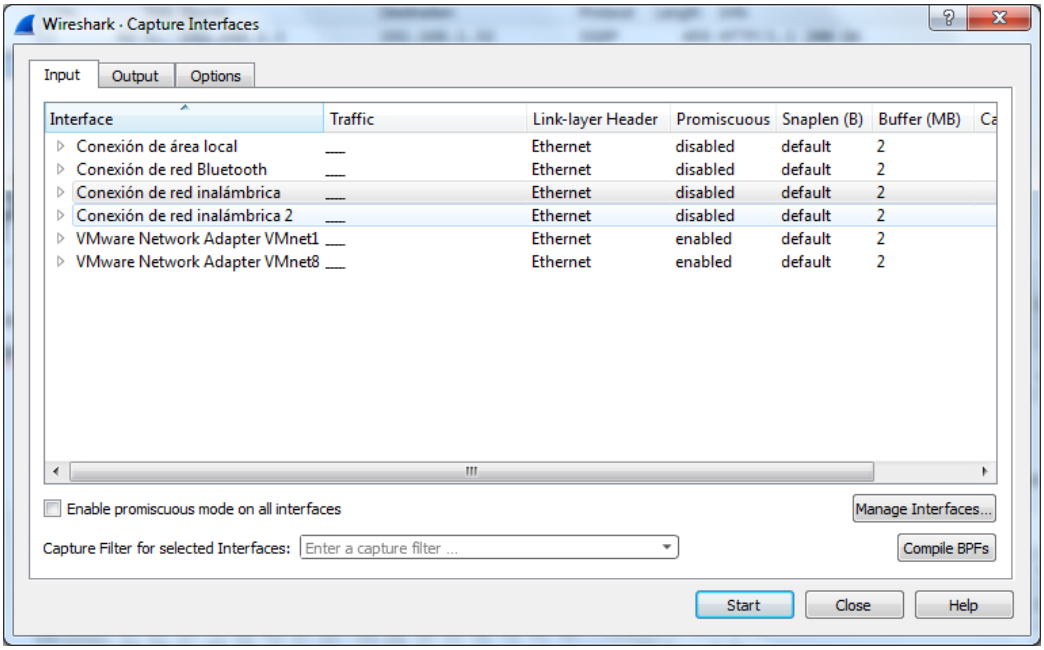
Datu harrapaketa

Datuak harrapatu nahi dituzun sarea hautatuz hasten da. *Ordenagailuak modem bat badu edo hainbat sare txartel baditu, aztertu nahi duzuna hautatu beharko duzu. Honako honen antzeko pantaila bat ikusiko dugu*



3. Irudia. Hasiera Pantaila

Interfazea hautatuta, ateratzeko aukerak alda daitezke **Capture > Options** menuan hautatuta. Horrela, elkarrizketa-koadro hau bistaratuko da.

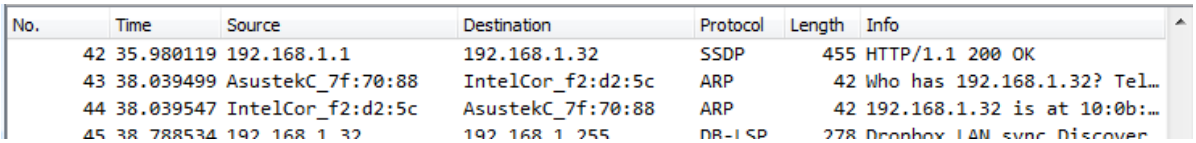


4. Irudia. Capture Options

Datuak harrapatzeari uzteko, erabili **Capture > Stop** menu aukera. Kapturaren hasierarako zein amaierarako menu-barrako botoiak erabil ditzakezu.

Paketeak harrapatu ahala bistaratzen dira. Aukera hau desaktiba daiteke "**Update list of packets in real time**" desaktibatuta, harrapatzeko aukeren elkarrizketa-koadroko **Options** erlaitzean.

Hartutako paketei buruzko informazioa



No.	Time	Source	Destination	Protocol	Length	Info
42	35.980119	192.168.1.1	192.168.1.32	SSDP	455	HTTP/1.1 200 OK
43	38.039499	AsustekC_7f:70:88	IntelCor_f2:d2:5c	ARP	42	Who has 192.168.1.32? Tel…
44	38.039547	IntelCor_f2:d2:5c	AsustekC_7f:70:88	ARP	42	192.168.1.32 is at 10:0b:…
45	38.788534	192.168.1.32	192.168.1.255	DB-LSP	278	Dropbox LAN sync Discover

5. Irudia. Leiho nagusian jasotako paketei buruzko informazioa

Leiho nagusiko **paketeen zerrendan**, harrapatutako paketei buruz agertzen den informazioa hau da:

- **No.** Harrapatutako paketearen aurkibidea
- **Time -** kapturatzen hasi zenetik pakete hau harrapatu arte igarotako denbora
- **Source -** Paketearen iturriaren IPa
- **Destination -** Paketearen helmuga IP
- **Protocol -** Paketea bidaltzeko erabiltzen den protokoloa
- **Info -** Paketearen deskribapen txikia

Harrapatutako informazioa iragaztea

Lanean ari den bitartean sareko txartelean zehar zirkulatzen duen informazio kopuru handia ikusita, bereziki erabilgarria da informazio hori nolabait mugatu ahal izatea eta aztertu nahi duzun sareko trafiko zehatzaren analisian kontzentratu ahal izatea. .
WireShark-ek hainbat **informazio iragazteko** aukera eskaintzen du: protokoloaren bidez iragaztea, harrapaketa iragaztea **eta informazioaren aurkezpenean iragaztea**. Azken horrekin bakarrik arituko gara.

Aurkezpen iragazketa

Aztertu nahi dituzun datu paketeak panel nagusian (1) erakutsiko dituen iragazkia defini dezakezu, gainerakoa ezkutatuta.

Aurkezpen iragazkia erabiltzeko, zure adierazpena zuzenean iragazkiaren testu koadroan idatz dezakezu eta aplikatu (2. irudia). Beste alternatiba bat dago, hau da, kudeatu iragazkiaren botoia sakatzea; orduan, iragazkiak definitutako elkarrizketa-koadroa agertuko da.

PRAKTIKA HAU EGITEKO LABORATEGIKO ORDENAGAILUAK ERABILI BEHAR DIRA

&& : AND logikoa (eta)
|| : OR logikoa (edo)
contains : eduki
== : berdin
!= : ezberdin

Txostena. 1. Galdera: Esperimentatu iragazki batzuekin:

dns
ip.src == XXX.XXX.XXX.XXX (Zure IPa jarri)
*ip.dst == XXX.XXX.XXX.XXX (EHU/UPV weborriaren zerbitzariaren IPa jarri) **
*http.host == ehu.eus **

** Seguraski, iragazki hauekin ez dira paketerik ikusiko. Zergatik? Ez ahaztu paketeak ager ditzaten konexioren bat ezarri behar dela, hau da, weborria ireki behar da, adibidez.*

Erabili sareko *ipconfig* komandoa zure ordenagailuaren IPa eta atebide lehenetsia jakiteko. Nola jakin EHU / UPV weborriaren zerbitzariaren IPa? Zer erakusten digu gure aztertzaileak aurreko iragazkiekin?

Txostena. 2. galdera: Hurrengoa egiten duten iragazkiak definitu:

- Aurkeztu **host1** iturburuko IP helbidea eta **host2** helmuga IP helbidea duten paketeak (eta alderantziz, bi iragazki ezberdin)
- Jatorria eta helmuga **host1** eta **host2** ostalari, edo **host2** eta **host1**, duen trafiko guztia harrapatu (iragazki bakarra)
- Ikusi trafiko guztia **host1** izan ezik

* **host1** eta **host2** gisa zure helbidea eta ikasgelako beste ordenagailu bat aukeratu.

2. ATALA: PROTOKOLOAK AZTERTZEN WIRESHARK-EN BIDEZ

1.- Behin ingurunea ezagututa, aurreko praktikan ikusi genuen ping komandoa aztertuko da, kasu honetan benetako paketeak aztertuko ditugu, ez simulazio bat. Horretarako:

A.- Harrapatu sareko paketeak ping bat ikasgelako beste ordenagailu batera bidaltzen duzunean.

B.- Iragazi paketeak parte hartzen duten ordenagailuen arteko **ICMP protokolo** paketeak ikusteko (**iragazkia: ip.addr == host1 && ip.addr == host2 && icmp**) (Agian aldatu beharrekoa)

C.- **Txostena. 3. galdera:** informazioa aztertu eta irudikapen eskematikoa egin. Packet Tracer simulazioan ikus genezakeen gauza bera al da?

D.- **Txostena. 4. galdera**: Onartu pakete guztiak ikustea. Ba al dago **ARP protokolo** paketerik? Pakete honetako informazioa aztertu eta protokolo honen funtzionalitatea zein den azaltzen saiatu.

2.- Nola funtzionatzen du TRACEROUTER-ak?

Traceroute sare diagnostiko tresna da, sistema operatibo gehienetan dagoena. Tresna honek pakete batek hartutako bidea zehazteko aukera ematen du.

Traceroute komandoa sistema operatiboaren arabera desberdina da

- UNIX / Linux sistemetan: **traceroute** helmuga.izena
- Windows sistemetan: **tracert** helmuga.izena

Oro har, **tracert** batek egiaztatu nahi dugun pakete batek egiten duen ibilbidea helmugaraino erakusten du.

```
Erabilera: tracert [-d] [-h max_hops] [-j host_list] [-w timeout]
helmuga_izena

Aukerak:
 -d Ez bihurtu helbideak ostalari izenetara.
 -h maximum_hops Gehienezko jauzi kopurua helburuaren bila.
 -j ostalari-zerrenda Iturburu-ibilbide lasaia ostalari-zerrendan zehar.
 -w wait_time Saiakeren arteko milisegundo kopurua
```

Sareko komando hau gure ordenagailuan exekutatzen badugu honen antzeko zerbait lortuko dugu:

6. Irudia. Tracer-Router exekuzioaren emaitza

(Jakin-mina baduzu IP horiek nori dagozkien egiaztatu dezakezu, adibidez, sarean https://bandaancha.eu/whois)

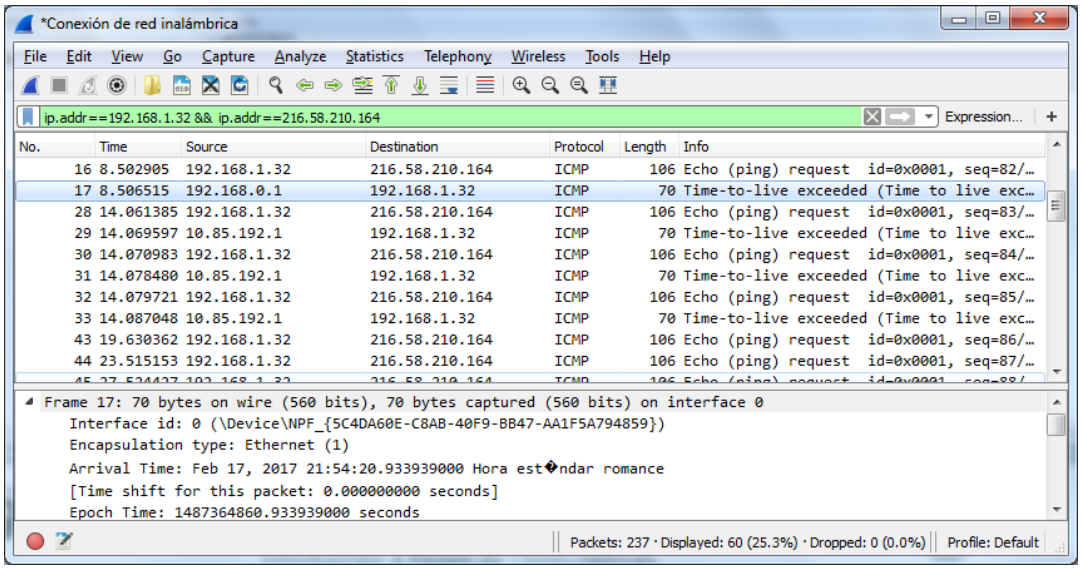
Lehenengo zutabeko zenbakia salto zenbakia da, ondorengo hiru zutabeak bidalitako paketeen erantzun denborak dira (izartxo batek erantzunik ez dela lortu adierazten du) eta azkenik igarotzen den nodoaren izena edo IP helbidea.

Oinarritutako kontzeptuak:

Tracert-ek IP goiburuko **Time To Live (TTL)** eremua erabiltzen du. Eremu hau pakete bat sarean mugagabe gera ez dadin erabiltzen da. **TTL** eremua igarotzen den nodo bakoitzari 1 kendutako zenbaki oso bat da. Modu honetan, TTL eremuak 0 balioa lortzen duenean jada ez da birbidaltzen, baina une horretan maneiatzen ari den nodoak baztertzen du.
Nodo batek pakete bat uzten duenean, igorleari kontrol mezu berezi bat bidaltzen dio **(ICMP-Internet Kontrol Mezuen Protokoloa)** gertaera jatorrizko nodoari adieraziz. **Tracert komandoak erantzun hau erabiltzen du paketea bota duen nodoaren IP helbidea jakiteko.**

1. Erabili **tracert** komandoa pakete batek www.google.es helbidera edo beste helbide batera heltzeko jarraitu behar duen ibilbidea ezagutzeko. Lortutako emaitzak aztertu. Tarteko zenbat nodoetatik igarotzen da mezua?

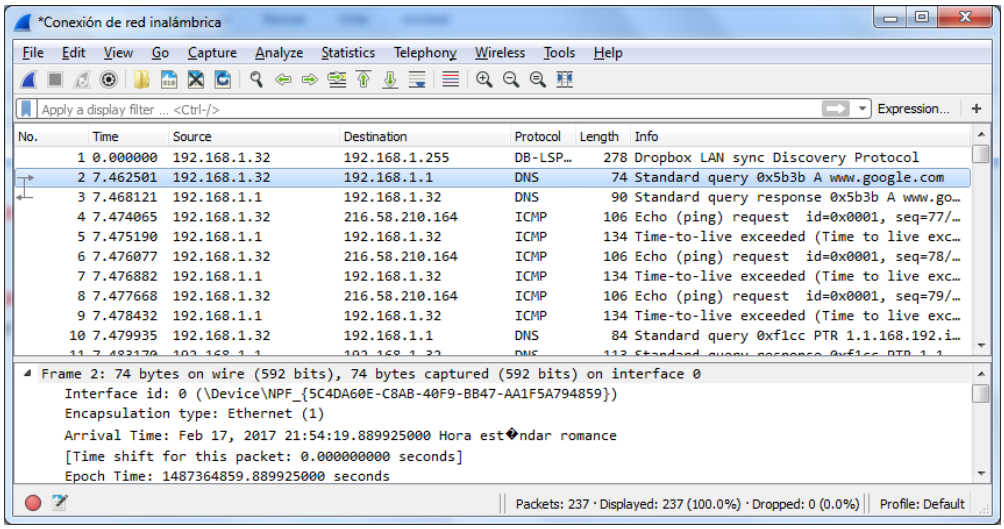
2. Errepikatu komandoa berriro, baina orain **aztertzailearekin tramak harrapatu**.



7.Irudia. Trace-Router kaptura.

1. **Txostena. 5. Galdera:** Aztertu egindako harrapaketa (Tracerouter) eta azaldu komandoak nola funtzionatzen duen (gogoratu iragazkiak erabiltzen bakarrik hauek ikusteko)

2. **Txostena. 6. Galdera:** Aztertu aurreko ICMP paketeen aurretik agertzen diren DNS protokolo paketeak. Zure ustez, zer funtzio du protokolo honek? Zein da zure DNS zerbitzariaren helbidea? DNS mezu bat (response) deskribatu, bertan dauden goiburu bakoitza (eta goiburu bakoitzeko eremu esanguratsuenak) xehatuz.



8. Irudia- DNS paketeak