1. PRAKTIKA: SARRERA WIRESHARK

PROTOKOLO AZTERTZAILEA

CURSO 2019- 2020

Konputagailu Sareen Oinarriak

Irakaslea: Oskar Casquero Oyarzabal

Sistemen Ingeniaritza eta Automatika Saila

PRAKTIKAREN HELBURUAK

Praktika honen helburua ikasleak protokolo aztertzaile baten oinarrizko funtzionalitateak ezagutzea eta horiek erabiliz prokolo arrunt batzuk aztertzeko gai izatea da.

Sarrera

Protokolo aztertzaile bat sareko protokolo eta aplikazioak garatzeko eta harazteko balio duen tresna da. Horretarako, protokolo aztertzaileak saretik hedatzen diren bilbeak harrapatzen ditu, hauen azterketa denbora errealean edo harrapaketaren ondoren egiteko aukera ematen duelarik. Bilbearen azterketak bera osotzen duten protokolo-pilaren egitura ezagutzeko aukera ematen du, bere edukia dekodifikatuz. Ikastaroan zehar erabiliko dugun protokolo aztertzailea **Wireshark** da.

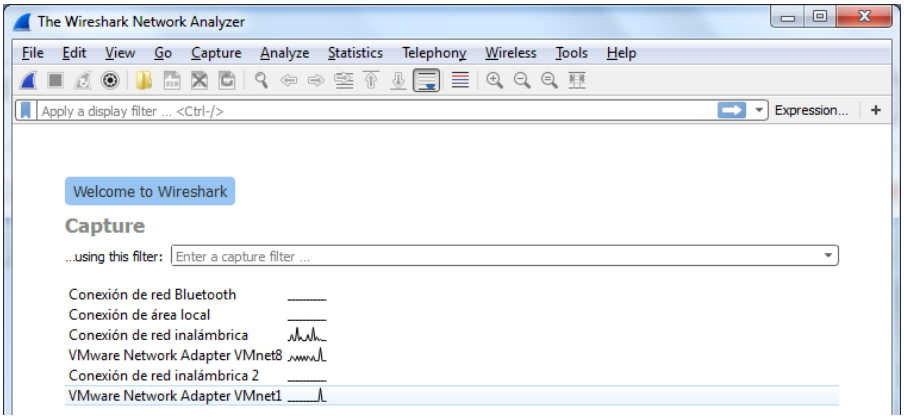
Wireshark sare baten ager daitezkeen arazoak aztertzeko eta konpontzeko, aplikazioak eta protokoloak garatzeko, eta tresna didaktiko bezela erabiltzen da. Wireshark-ek protokolo aztertzaile baten ezaugarri estandarrak ditu. Sare bizi batetik zuzenean harrapatutako edo fitxategi batean harrapaketa ondoren gordetako datuak aztertu ditzake. Azterketa errazteko, Wireshark-ek datuak iragazteko lengoaia bat du.

Wireshark software ireki eta plataforma-anitzduna da. Programa ondorengo estekan eskuragarri dago: http://www.wireshark.org/download.html

1. ZATIA: LEHENENGO PAUSUAK

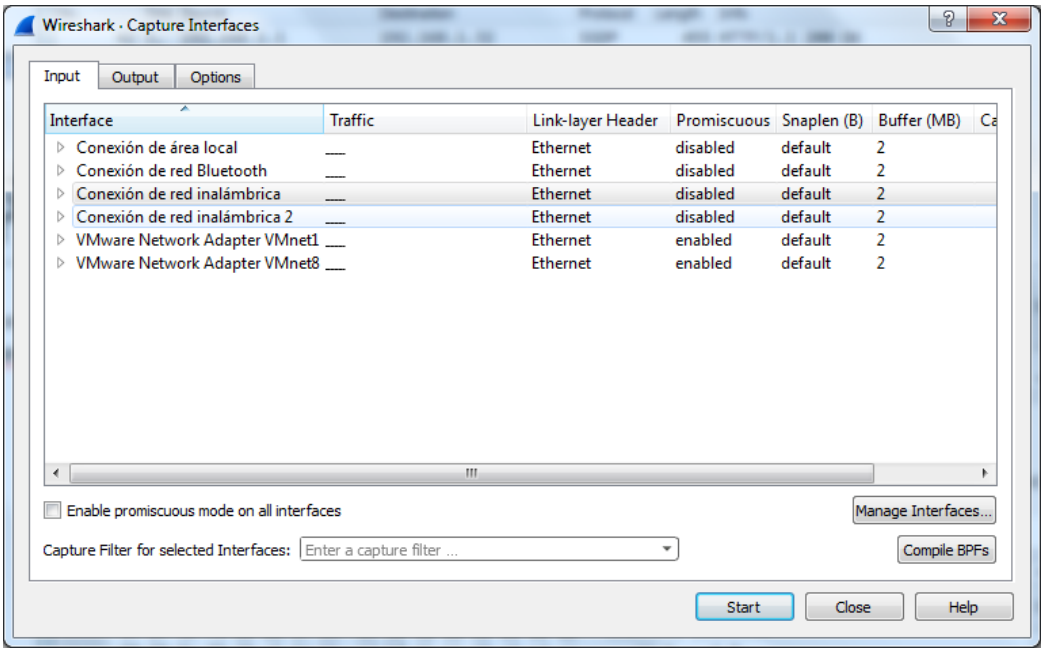
Datuen harrapaketa

Hasteko, datuak zein saretan hartu nahi diren hautatzen da. Hurrengoaren antzeko pantaila bat ikusiko dugu:



1. irudia. Hasierako pantaila

Interfazea hautatu ondoren, **Capture > Options** menuan harrapaketaren aukerak alda daitezke. Hori egitean, hurrengo elkarrizketa-koadroa agertuko da:



2. irudia. Kaptura-intefazeak

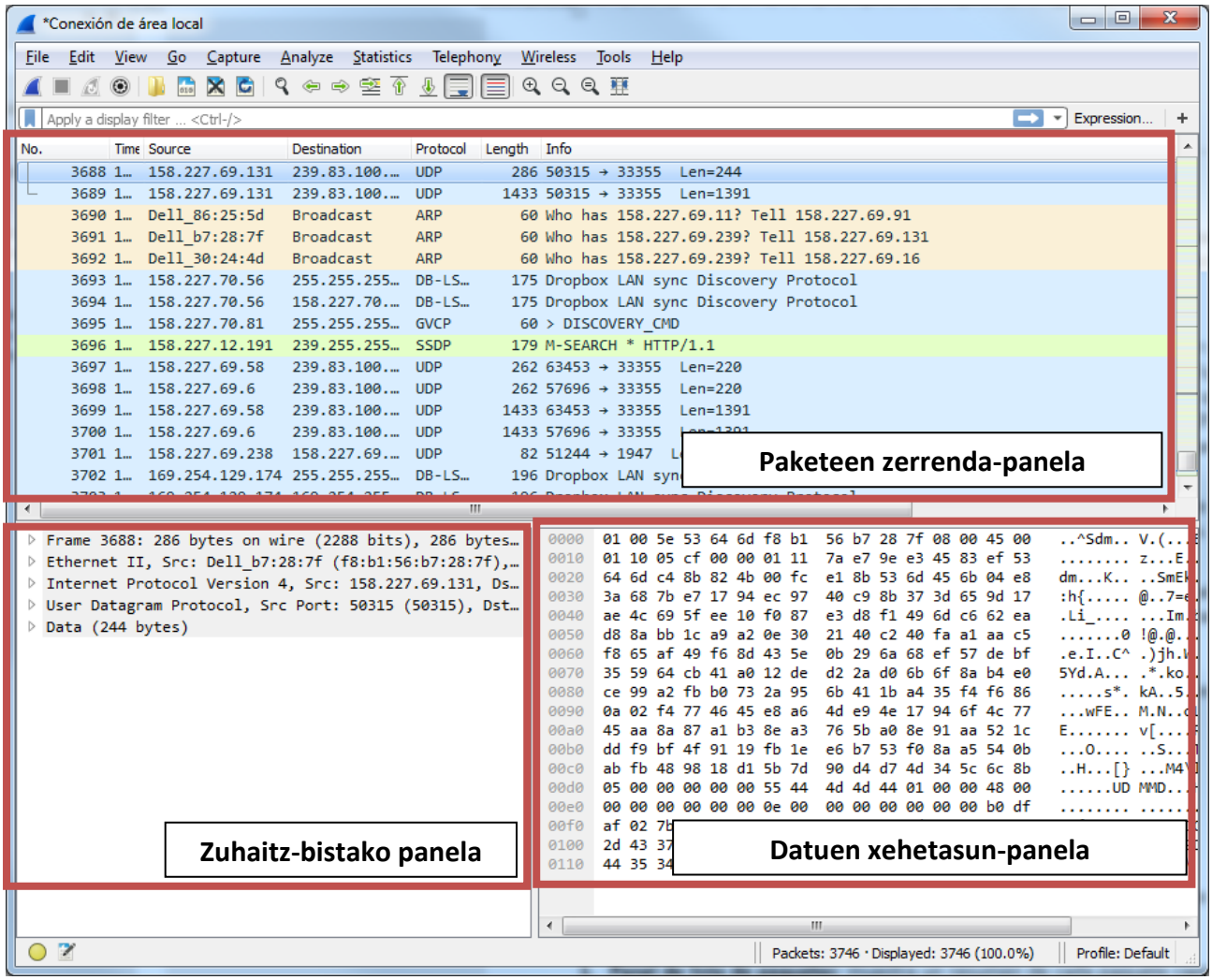
Datuen harrapaketa gelditzeko, menuko **Capture > Stop** aukera erabiltzen da. Harrapaketa hasteko zein amaitzeko, menuko barrako botoiak erabil daitezke.

3. irudian programaren pantaila nagusia agertzen da. Bertan, paketeak harrapatu ahala erakusten dira. Hiru panel bereiz daitezke:

1. **Paketeen zerrenda-panela.** Harrapatutako pakete bakoitzaren laburpena erakusten du. Panel honetako paketeetan sakatuta, beheko beste bi panelen edukia kontrolatzen da.

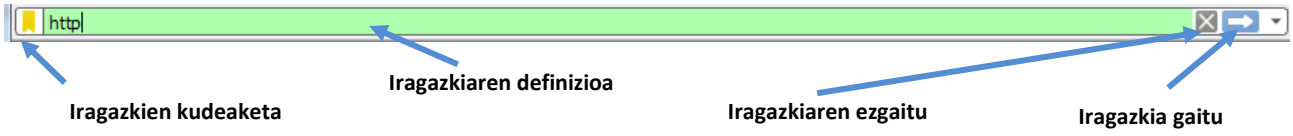
2. **Zuhaitz-bistako panela.** Goiko panelean (1) aukeratutako paketea xehetasun gehiagorekin erakutsi eta protokolo-maila guztietara sartzeko aukera ematen du. Maila bakoitzean sakatzean, beheko panelean maila horri dagozkion paketearen datuak nabarmentzen dira (3).

3. **Datuen xehetasun-panela.** Goiko panelean (1) aukeratutako paketearen edukia hamaseitar eta ASCII formatuetan erakusten du.



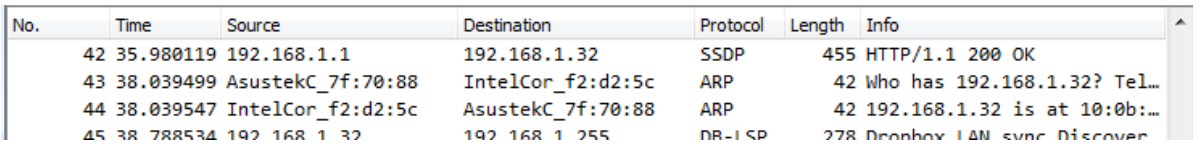
3. irudia. Wireshark programaren pantaila nagusia

Hiru panel nagusiez gain, **iragazkiekin lan egiteko barra** ere azpimarra daiteke, WireShark pantailaren goiko aldean dagoena:



4. irudia. Iragazkiekin lan egiteko barra

Harrapatutako paketeei buruzko informazioa



5. irudia. Harrapatutako paketeen informazioa leiho nagusian

Leiho nagusiko **paketeen zerrenda-panelean**, honako hau da harrapatutako paketeei buruz adierazten den informazioa:

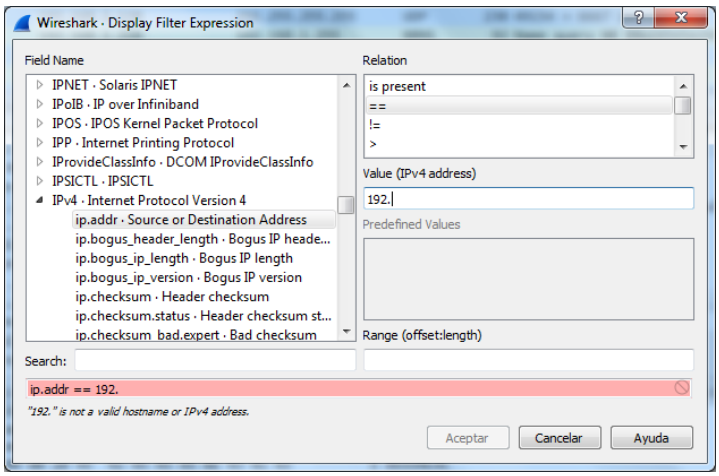
- **Zk. -** Harrapatutako paketearen indizea
- **Time -** Harrapaketa hasi zenetik pakete hori harrapatu arte igaro den denbora
- **Source -** Paketearen jatorriaren IP
- **Destination -** Paketearen helmugako IPa
- **Protokoloa -** Paketea bidaltzeko erabilitako protokoloa
- **Length -** Paketearen luzera bytetan
- **Info -** Paketearen deskribapen txikia

Harrapatutako informazioaren iragazpena
Funtzionatzen ari den bitartean, sareko txartel batek trafiko handia (bilbe kopuru handia) jasotzen duenez, bereziki baliagarria da informazio hori nolabait mugatu eta aztertu nahi den sareko trafiko zehatzaren azterketan arreta jarri ahal izatea. Wireshark-ek informazioa iragazteko hainbat aukera eskaintzen ditu: harrapaketaren iragazpena eta bistaratzearen iragazpena.

Harrapaketaren iragazpena
Iragazkian adierazitako baldintzak betetzen dituzten paketeak bakarrik hartzeko ezartzen dira. Bat ere ezartzen ez bada, Wireshark-ek trafiko guztia harrapatu eta pantaila nagusian aurkeztuko du.

Bistaratzearen iragazpena
Wireshark-en pantaila nagusian bistaratzen ari diren paketeengan iragazki bat ezartzen da. Iragazki hauek malguagoak eta eraginkorragoak dira.

Bistaratze-iragazki bat erabiltzeko, haren adierazpena iragazkiaren testu-laukian zuzenean idatz eta aplika daiteke (4. irudia). Badago iragazkiak sortzen laguntzen duen elkarrizketa-leiho bat (*Display Filter Expression*).



6. irudia. Display Filter Expression

1. galdera: *Esperimentatu iragazki batzuekin*
dns, tcp, udp,
ip.src == XXX.XXX.XXX.XXX (zure IP-a jarri),
ip.dst == XXX.XXX.XXX.XXX (UPV/EHU-ko IP-a jarri)
ip.addr == XXX.XXX.XXX.XXX (zure IP-a jarri),
http.host == www.google.com

*Erabili **ipconfig** sareko komandoa zure PC-aren IP-a eta lotura-ate lehenetsia ezagutzeko.*
Nola ezagutu dezakezu UPV/EHU zerbitzariaren IP-a?
Zer bistaratzen du aztertzaileak aurreko iragazkiak erabiltzen direnean?

Ondorengo taulan, iragazkietan erabil daitezkeen eragile batzuk ageri dira:

And	&&	Logical AND
or	||	Logical OR
not	!	Logical NOT
eq	==	Equal
ne	!=	Not Equal

2. galdera: *Definitu iragazki hauek:*

- *Aurkeztu jatorrizko IP helbidea host1 duten paketeak eta helmugako IP helbidea host2 dutenak (edo alderantziz).*
- *Harrapatu jatorri bezela host1 edo host2 duen trafikoa*
- *Bistaratu trafiko guztia, host1-i dagokiona izan ezik*

* *host1* eta *host2* gisa, aukeratu zure helbidea eta gelako beste ordenagailu batena.

2. ZATIA: PROTOKOLOEN AZTERKETA WIRESHARK ERABILIZ

1.- Behin ingurua ezagututa, **ping** komandoa aztertuko da Wireshark erabiliz.

PING (Kaixo, sarean al zaude?)

Ping ordenagailu-sareetan diagnostikoa egiteko tresna da, zeinek eskaera eta erantzun ICMP (Internet Control Message Protocol) paketeak bidaliz host lokal batek urruneko ekipo batekin edo batzuekin duen konexio-egoera egiaztatzen du.

Ping komandoak TCP/IP protokoloaren sare mailan lan egiten du. Ping eta ICMP protokoloaren funtzionamendua, oro har, 792. RFC-an zehaztuta dago.

IP protokoloak ICMP mezua pakete batean kapsulatu eta bidatzen du, **ICMP paketea** deitzen dena, alegia. Paketean bi datu-multzo bereiz daitezke: **IP goiburua**, sare-kaparen datu estandarrak dituena; eta **ICMP azpipaketea**, protokoloaren kontrol-datuak dituena. **IP goiburuan**, **protokoloa** honela zehazten da: 0x1 (ICMP protokoloari dagokion balioa) eta **zerbitzu mota**: 0 (errutinazkoa). **ICMP azpipaketean** honako balio hauek zehazten dira: ICMP **mezu mota** 0x8 eskaera batean (Echo) edo 0x0 erantzun batean (Echo replay); eta **Kodea** 0x0 eskaerarako zein erantzunerako akatsik ez badago.

7. irudia. ICMP paketea

IP goiburuaren tamaina osoa 160 bitekoa da (20 byte), horren ondoren ICMP mezua jarriko delarik, 64 biteko (8 byte) tamaina estandarrarekin.

(Informazio gehiago behar baduzue, bilatu ezazue)

Azterketa burutzeko:

A.- Ikasgelako beste ordenagailu bati ping egin, bitartean paketeen harrapaketa egiten duzuelarik.

B.- Iragazki bat sartu ping-ean parte hartzen duten host-en artean ICMP protokoloko paketeekin soilik geratzeko:

iragazkia: *ip.addr==host1 && ip.addr==host2 && icmp*

C.- ***3. galdera:*** *ICMP paketeen informazioa behatu eta trukatutako paketeen irudikapen eskematikoa egin.*

D.- **4. galdera:** *Pakete guztiak ikusteko aukera ezarri.* ***ARP protokoloko*** *mezuren bat agertzen da? Aztertu mezu honen informazioa eta saiatu protokolo honen funtzionaltasuna azaltzen.*

2.- Zelan funtzionatzen du TRACEROUTER-ek?

Traceroute sareak harazteko tresna bat da, sistema eragile gehienetan eskuragarri dagoena. Tresna honi esker, pakete batek jatorrizko host batetik helmugako host batera egindako ibilbidea zehaztu daiteke**.**

Traceroute komandoak ezberdintasun txikiak azaltzen ditu sistema eragilearen arabera:

- UNIX / Linux: **traceroute** izena.helburua
- Windows: **tracert** izena.helburua

```
Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
nombre_destino

Opciones:
 -d No convierte direcciones en nombres de hosts.
 -h saltos_máximos Máxima cantidad de saltos en la búsqueda del objetivo.
 -j lista-de-host Enrutamiento relajado de origen a lo largo de la lista de
hosts.
 -w tiempo_espera Cantidad de milisegundos entre intentos
```

Sareko komando hau gure ordenagailuan exekutatzen badugu, honako hau lortuko dugu:

```
Traza a la direcci¢n www.google.com [216.58.211.36]
sobre un m ximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  158.227.69.1
  2    <1 ms    <1 ms    <1 ms  10.0.92.5
  3     1 ms     1 ms     1 ms  pa-internal.lgp.ehu.es [10.0.1.4]
  4     3 ms     6 ms     1 ms  150.241.255.137
  5     9 ms     9 ms     9 ms  I2BASQUE.XE2-2-0.uva.rt1.cyl.red.rediris.es [130.206.201.125]
  6    17 ms    16 ms    17 ms  UVA.AE1.unizar.rt1.ara.red.rediris.es [130.206.245.13]
  7    29 ms    26 ms    26 ms  UNIZAR.AE6.telmad.rt4.mad.red.rediris.es [130.206.245.94]
  8    19 ms    19 ms    19 ms  google-router.red.rediris.es [130.206.255.2]
  9    19 ms    19 ms    19 ms  108.170.253.225
 10    20 ms    20 ms    20 ms  108.170.234.221
 11    19 ms    19 ms    19 ms  muc03s14-in-f36.1e100.net [216.58.211.36]

Traza completa.
```

8. irudia. Tracerouter exekuzioaren emaitza

Lehenengo zutabearen zenbakia jauzi zenbakia da, ondorengo hiru zutabeak bidalitako paketeentzako erantzun denborak dira eta azkenik paketeak bere ibilbidean zeharkatzen duen nodoaren izena edo IP helbidea.

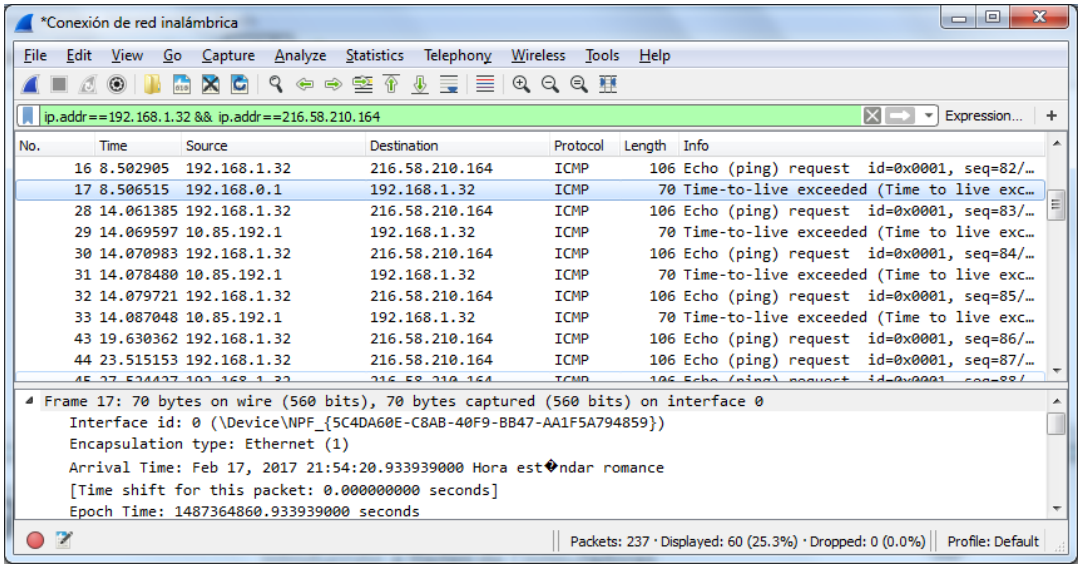
Jakin-mina baduzu, kontsultatu nori dagozkion IP horiek (adibidez, https://bandaancha.eu/whois webgunean)

Zeintzu kontzeptutan oinarritzen da:

tracert-ek **IP goiburuko Time To Live (TTL) eremua** erabiltzen du. Eremu honek pakete bat modu mugagabean sarean gelditu ez daiten balio du. TTL eremua zenbaki oso bat da, zeini nodo bakoitzean 1 kentzen zaio. Horrela, TTL eremua 0 baliora iristen denean, paketea ez da gehiago berbidaltzen, eta une horretan bera darabilen nodoak baztertu eta igorleari ICMP mezu bat bidaltzen dio gertaera jakinarazteko. Tracert komandoak erantzun hau erabiltzen du paketea baztertu zuen nodoaren IP helbidea jakiteko.

1. **tracert** komandoa erabili pakete batek www.google.es edo beste helbide batera iristeko jarraitu behar duen ibilbidea ezagutzeko. Lortutako emaitzak aztertu. Zenbat bitarteko nodo zeharkatzen ditu mezuak?

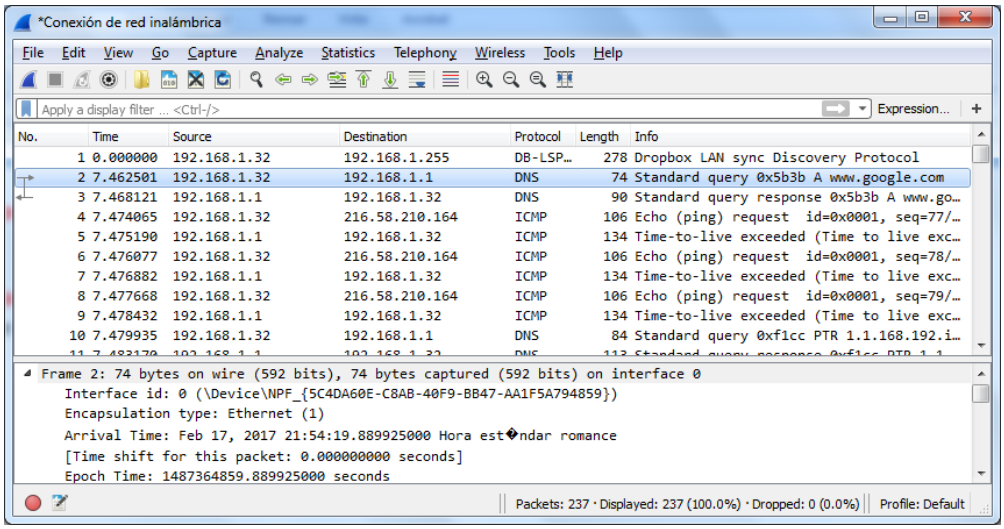
2. Komandoa berriro exekutatu, baina orain bilbeak aztertzailearekin harrapatuz.



9. irudia. Tracerouter trafikoaren harrapaketa

3. ***5. galdera:*** *Aztertu egindako harrapaketa eta azaldu xehetasunez Tracerouter komandoak nola funtzionatzen duen (gogoratu iragazkiak erabiltzea)*

4. **6. galdera:** *Aztertu aurreko paketeen aurretik agertzen diren DNS protokoloko paketeak. Zure ustez, zer funtzio du protokolo honek? Zein da zure DNS zerbitzariaren helbidea?*



10. irudia. DNS paketeak