

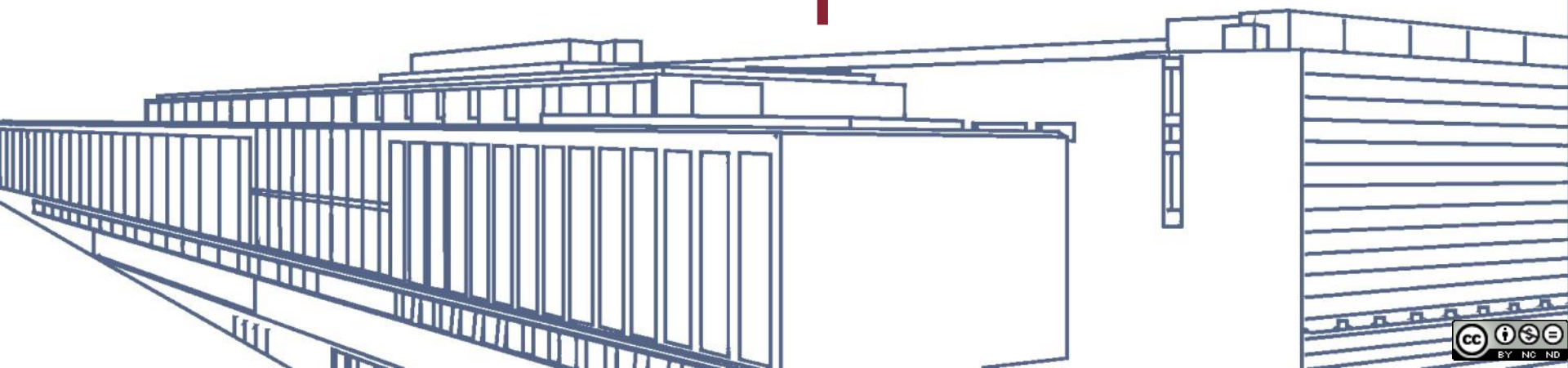


ESCOLA TÈCNICA SUPERIOR
D'ENGINYERIA
Universitat Rovira i Virgili



Xarxes de Dades i Internet

Pràctica: Anàlisi de protocols



Anàlisi de protocols

■ Introducció

- En aquesta pràctica estudiareu el comportament dels protocols que heu vist a teoria, per mitjà d'un escoltador de xarxa ("sniffer").
- La pràctica es fa en grups de tres estudiants.
- Els resultats d'aprenentatge a assolir són:
 - **RT13.** Comprèn el funcionament dels protocols d'Internet
 - **RT13.** Comprèn el funcionament dels serveis d'Internet
 - **RT13.** Comprèn el mecanisme de transmissió d'informació sobre Internet

■ Recursos

- Per fer aquesta pràctica necessiteu un sistema operatiu Linux (per a la part de tcpdump) i un Linux o Windows per a la part de Wireshark.

Anàlisi de protocols

■ Lliurament

- El dia de l'entrevista **el professor us demanarà que li feu una petita demostració de Wireshark**, que ha de mostrar algunes de les característiques bàsiques del programa. En aquesta presentació heu de participar per igual tots els membres de l'equip.
- També heu de confeccionar **un document amb una taula que indiqui l'assoliment** o no de les diferents tasques que us proposem i, si escau, observacions i comentaris que vau fer en el seu dia. Cada estudiant farà un lliurament, que serà el mateix per tots els membres del grup. A la portada del document s'indicarà el nom de tots els components. El lliurament es farà a través de Moodle durant la sessió de presentació.
- La qualificació de la pràctica serà excel·lent, notable o aprovat, amb equivalència numèrica 10, 7 i 5 respectivament. Aquesta qualificació és individual i dependrà, en part, de l'actitud durant l'entrevista.

Anàlisi de protocols

■ Analitzadors de trames

- Permeten analitzar els paquets (trames) que es capturen al nostre domini de col·lisió dins la xarxa d'àrea local. D'aquesta manera també ens permeten analitzar els protocols telemàtics.
- Les principals utilitats són:
 - Fer estadístiques del tipus de tràfic.
 - Comprendre el funcionament d'algun protocol.
 - Depurar protocols que estem desenvolupant.
 - Usos maliciosos: esbrinar contrasenyes, interceptar correus o xats...
 - Verificar l'efectivitat dels sistemes de control (tallafocs, proxy, ...)
 - Monitoritzar una xarxa per a detectar i analitzar errors.
 - Fer enginyeria inversa de protocols, etc.

Anàlisi de protocols

■ Dominis de col·lisió

- En entorns cablejats basats en concentrador (*hub*) els *sniffers* permetien capturar tot el tràfic generat al domini de col·lisió de manera que, fins i tot, es podia registrar tota l'activitat a la xarxa de cada estació de la LAN! Avui dia això és complex: els commutadors (*switch*) generen múltiples dominis de col·lisió (un per enllaç) de manera que només es captura el tràfic entrant o sortint a l'estació que executa l'analitzador de paquets, o bé el tràfic de difusió (com ara les preguntes ARP, un protocol que haureu vist o veureu a teoria). Hi ha atacs informàtics que permetrien analitzar el tràfic d'una xarxa, però això es correspon a altres assignatures ☺. Pel que fa els entorns Wi-Fi, la quantitat de paquets que es poden capturar varien en funció de la tecnologia, del controlador, de la protecció usada, etc.

Anàlisi de protocols

■ tcpdump

- TCPdump és un programa de consola, disponible per defecte a les distribucions Linux, Mac OS X que permet capturar paquets de la xarxa i fer una anàlisi en temps real d'acord amb una sèrie de paràmetres, regles i filtres.
- També permet capturar la informació i desar-la en un arxiu per poder-la analitzar més endavant. L'entrada a la Wikipedia proporciona alguns exemples d'ús, per exemple:

```
tcpdump -D          # Mostra les interfícies de xarxa
```

Al web de TCPdump hi trobareu ajuda.
http://www.tcpdump.org/tcpdump_man.html

Anàlisi de protocols

■ Tasca 1. Captura amb tcpdump

- Utilitza la següent comanda per activar la captura amb TCPdump i que desí les captures en un fitxer

```
tcpdump -s 1500 -w datagrams.txt
```

- Obre el navegador, visita www.google.cat i www.urv.cat
- Atura la captura amb Ctrl + C i mostra per pantalla l'arxiu (amb cat)

■ Tasca 2. Mostra de paquets capturats amb tcpdump

- Ara pots mostrar la informació d'una manera més polida per mitjà de la següent comanda

```
tcpdump -tn -r datagrams.txt
```

- Què fan els paràmetres -tn?

Anàlisi de protocols

■ Tasca 3. Filtres amb tcpdump

- Pots destriar paquets per mitjà de regles i filtres, com ara:

```
tcpdump -tn -r datagrams.txt tcp port 80
```

```
tcpdump -tn -r datagrams.txt tcp port 80 and dst host www.urv.cat
```

```
tcpdump -tn -r datagrams.txt udp port 53 or tcp port 80
```

```
tcpdump -tn -r datagrams.txt not \(dst host www.google.cat\)
```


Anàlisi de protocols

■ Wireshark

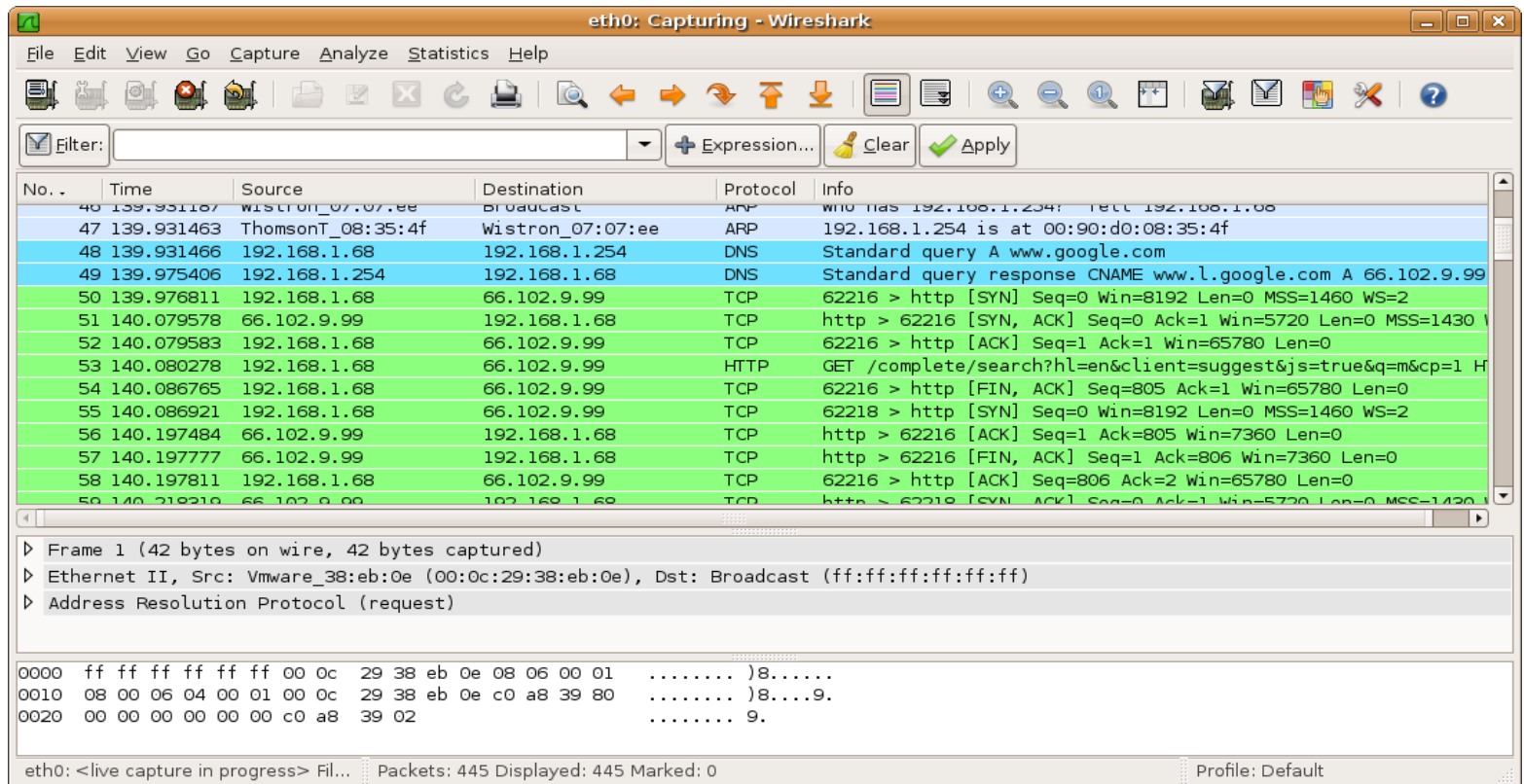
- Antigament Ethereal, és una aplicació que cal instal·lar a banda. L'avantatge sobre TCPdump és que disposa d'una interfície gràfica i permet aplicar filtres d'una manera més fàcil i potent.
- Presenta un resum dels paquets capturats amb diferents colors per poder diferenciar, per exemple, entre protocols. En la mateixa interfície hi ha disponible una barra de filtres que permet triar quins dels paquets capturats es mostren. Conté un generador de filtres molt senzill d'utilitzar.
- Conté un menú d'estadístiques.

Al web <http://www.wireshark.org> trobareu una potent guia d'usuari.

Anàlisi de protocols

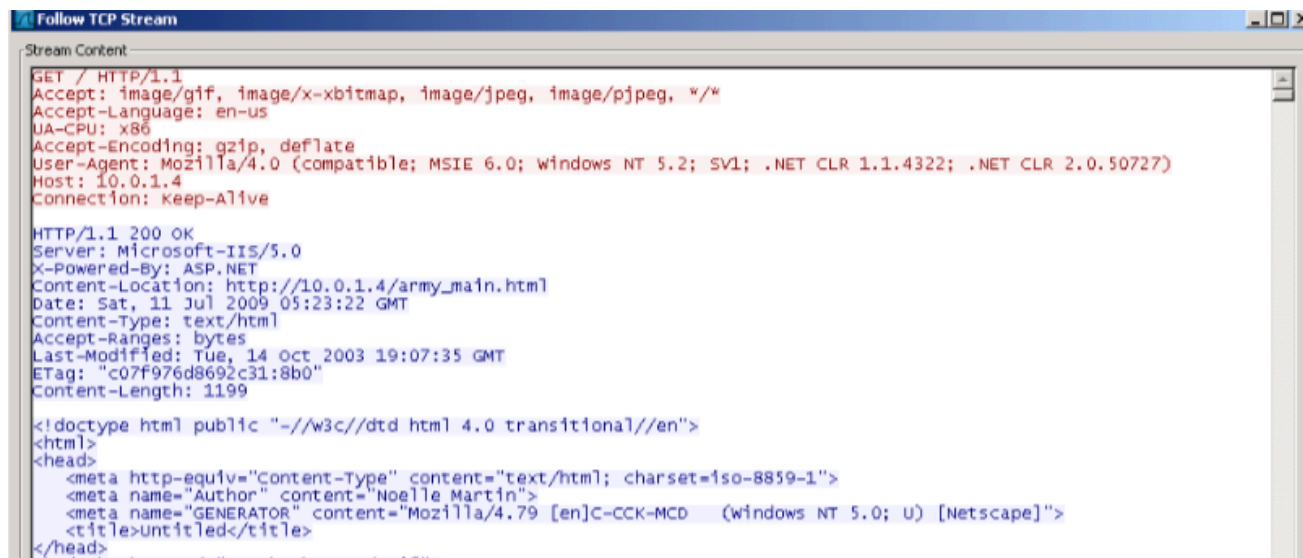
■ Wireshark

- Aquí podeu veure un exemple de la interfície de Wireshark amb una captura de paquets de diferents protocols:



Anàlisi de protocols

- En fer clic en un dels paquets se'ns mostren els detalls a la part inferior de la pantalla. A més, té eines específiques per al seguiment de tràfic TCP (*Follow TCP stream*).
 - La següent imatge mostra el resultat d'executar aquesta utilitat sobre un paquet que contenia un missatge del protocol HTTP:



```
Stream Content:
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: 10.0.1.4
Connection: keep-alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
X-Powered-By: ASP.NET
Content-Location: http://10.0.1.4/army_main.html
Date: Sat, 11 Jul 2009 05:23:22 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Tue, 14 Oct 2003 19:07:35 GMT
ETag: "c07f976d8692c31:8b0"
Content-Length: 1199

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <meta name="Author" content="Noelle Martin">
  <meta name="GENERATOR" content="Mozilla/4.79 [en]C-CCK-MCD (Windows NT 5.0; U) [Netscape]">
  <title>untitled</title>
</head>
```

Anàlisi de protocols

■ Tasca 4. Captura amb Wireshark

- Comenceu una captura de Wireshark.
- Navegueu a `http://www.example.com` i, després, a `https://www.example.com`
- Atureu la captura de paquets.

Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

[More information...](#)

■ Tasca 5. Filtrat de paquets

- Apliqueu un filtre per tal que mostri els paquets corresponents al protocol DNS.
- Desactiveu el filtre anterior i seleccioneu un paquet corresponent al protocol HTTP. Demaneu-li de reconstruir la conversa.
- Identifiqueu ara la connexió d'HTTPS. Quina diferència bàsica hi ha?

A què correspon la S de l'acrònim HTTPS?

Anàlisi de protocols

■ Tasca 6. Anàlisi del tràfic total

- Feu una captura de trames d'uns 10 segons de durada, mentre la qual feu un pings a altres màquines del laboratori. **Han de ser màquines contra les quals feu ping per primera vegada.**
- Atureu la captura i analitzeu aproximadament quin percentatge d'aquest tràfic es correspon a broadcast.
 - Com podeu definir un filtre per detectar quin tràfic correspon a broadcast?
- A quins protocols es correspon aquest tràfic?
- Captureu de nou el tràfic i torneu a fer pings a les mateixes màquines. Quines diferències trobeu respecte la primera execució?

Observareu un fenomen relacionat amb el protocol ARP

Anàlisi de protocols

■ Tasca 7. Anàlisi d'un ping

- Analitzeu una captura que hagueu fet mentre s'executa dos pings:
 - Un ping serà contra una màquina Linux
 - Un altre ping contra una màquina Windows
 - (el professor us anotarà les IP a la pissarra)
- Quines dades transporta el datagrama?
- Utilitza UDP, TCP...?
- On trobareu el valor del TTL? Quines diferències trobeu a nivell de TTL entre la màquina Windows i la Linux?

Anàlisi de protocols

■ Tasca 8. Anàlisi d'una connexió TCP

- Feu una captura mentre accediu a una URL sota el protocol HTTP (aneu en compte que no sigui HTTPS), si escau el professor us anotarà una URL a la pissarra.
- Seleccioneu tots els paquets que formen part d'aquesta connexió.
- Quines són les adreces IP que intervenen? I els ports?
- Sobre el protocol TCP, examineu els paquets corresponents al "three-way handshake". Quines característiques tenen?
- Quina és la mida dels paquets més grans? Per què?

Recordeu què era la fragmentació IP?
I les sigles MTU?

Anàlisi de protocols

■ Tasca 9. Anàlisi d'una petició HTTP

- Activeu un servidor Apache a la vostra màquina (usant apt-get en Linux, activant el XAMPP, etc.)

Pregunteu al professor si teniu dubtes!

- Des d'un altre ordinador, captureu amb Wireshark una connexió a aquest servidor mitjançant el navegador web.
- Trobeu el flag PSH activat en algun paquet? Què vol dir?
- Què vol dir el codi 200 OK que haureu trobat en alguns missatges?

Anàlisi de protocols

■ Tasca 10. Eines d'estadística

- En aquest darrer apartat us demanem que captureu tràfic i proveu **tres eines d'estadístiques de Wireshark**.
- Per a cada eina, comenteu al document breument quina és la seva utilitat, poseu una captura del resultat i feu-ne alguna observació.

