# PRÀCTICA 3b: Protocol DNS

## PART 1: PREPARACIÓ

**1.-** Utilitza la configuració de la targeta de xarxa i del serveir DNS de la teva màquina virtual **xxxyyy-m08.fjeclot.net** que vas fer servir a la pràctica **m08uf1pr3a**.

**2.-** Instal·la **wireshark** a la màquina virtual **ubuntu** que vas utilitzar a la màquina **m08uf1pr3a**.

**3**- Configura una màquina virtual **ubuntu** de la mateixa manera que va ser configurada a la pràctica **m08uf1pr3a**. Comprova que pots fer ping, utilitzant el nom, a la màquina **xxxyyy-m08.fjeclot.net**. Comprova que pots fer ping també a **www.fjeclot.net** i **dns.fjeclot.net**. Comprova que si fas un ping amb el seu nom a la màquina **windows 7** de la pràctica **m08uf1pr3a**, tot i que no funcioni, sí que es mostra la que hauria de ser la seva IP.

**4.-** Posa en marxa el **wireshark** de la teva màquina virtual **ubunutu** i realitza captures de missatges únicament del protocol **DNS**. Per fer això només cal configurar **wireshark** perquè treballi amb el filtre **dns and udp.port=53**.

## PART 2: PRÀCTICA

**1.-** Des de la màquina **ubuntu**, amb **wireshark** funcionant amb el filtre **dns and udp.port=53**, des del terminal fes la següent consulta al servei **DNS** de la màquina **xxxyyy-m08.fjeclot.net**:

**host -t a nom_equip_windows.fjeclot.net**

(Has de canviar nom_equip_windows pel nom real del teu equip windows)

Selecciona el missatge de **query** (pregunta) enviat per l'ordinador **ubuntu** i mostra clarament:

**a)** El valor identificador de transacció
**b)** El flag que identifica el missatge com un de tipus **query**.
**c)** La quantitat de preguntes o queries que porta el missatge.
**d)** El contingut de la consulta, indicant de quin és nom que es vol consulta, tipus de registre (A, NS, MX, SOA...) i la classe (que a efectes pràctics sempre serà la mateixa).
**e)** Indica quina part és de capçalera del missatge DNS i quina part és de dades del missatge DNS.

**2.-** Seleciona de l'apartat anterior el missatge de **response** (reposta) enviat pel servidor. S'ha de veure clarament:

**a)** El valor identificador de transacció que ha de coincidir amb el missatge de **query** enviat pel client.
**b)** El flag que identifica el missatge com un de tipus **response**.
**c)** Comprova si el servidor és autoritatiu o no.
**d)** Comprova la quantitat de preguntes (Questions) i de registres de resposta (Answer RRs) rebuts .
**e)** Comprova en la part de respostes (Answers) si es pot trobar l'adreça IP del nom d'equip demanat.
**f)** Comprova que en la part anomenada "Authoritative nameservers" s'ha enviat el nom del servidor DNS autoritatiu que ha donat la resposta a la query (pregunta) realitzada. Comprova que la quantitat de servidors DNS rebuts és igual a el valor "Authority RRS".
**g)** Comprova que dins d'Additional records, es dóna informació sobre l'adreça IP del servidor DNS del qual s'ha donat el nom a l'apartat anterior

**3.-** Des de la màquina **ubuntu**, amb **wireshark** funcionant amb el filtre **dns and udp.port=53**, des del terminal fes la següent consulta al servei **DNS** de la màquina **xxxyyy-m08.fjeclot.net**:

**host -t ns fjeclot.net**

(Has de canviar nom_equip_windows pel nom real del teu equip windows)

Selecciona el missatge de **query** (pregunta) enviat per l'ordinador **ubuntu** i mostra clarament:

**a)** El valor identificador de transacció.

**b)** El contingut de la consulta, indicant de quin és nom que es vol consulta, tipus de registre (A, NS, MX, SOA...) i la classe (que a efectes pràctics sempre serà la mateixa).

**4.-** Seleciona de l'apartat anterior el missatge de **response** (reposta) enviat pel servidor. S'ha de veure clarament:

**a)** El valor identificador de transacció que ha de coincidir amb el missatge de **query** enviat pel client.

**b)** Comprova la quantitat de preguntes (Questions) i de registres de resposta (Answer RRs) rebuts .

**c)** Per què Authority RRs val 0?. Existeix la secció "Authoritative nameserver"?. Per què?.

**d)** Comprova en la part de respostes (Answers) si es pot trobar el nom del servidor DNS.

**5.-** Des de la màquina **ubuntu**, amb **wireshark** funcionant amb el filtre **dns and udp.port=53**, des del terminal fes la següent consulta al servei **DNS** de la màquina **xxxyyy-m08.fjeclot.net**:

**host -t mx fjeclot.net**

Selecciona el missatge de **response** (reposta) enviat pel servidor. S'ha de veure clarament:

**a)** El número de respostes enviades?. Per què té aquest valor?

**6.-** Des de la màquina **ubuntu**, amb **wireshark** funcionant amb el filtre **dns and udp.port=53**, des del terminal fes la següent consulta al servei **DNS** de la màquina **xxxyyy-m08.fjeclot.net**:

**host -t cname www.fjeclot.net**

Selecciona el missatge de **response** (reposta) enviat pel servidor. S'ha de veure clarament:

**a)** El nom que s'estava consultant

**b)** El veritable nom de l'equip consultat.

DOCUMENTACIÓ

**a)** Tot sobre DNS: http://acacha.org/mediawiki/Servidor_DNS

**b)** Protolcol i missatge DNS en concret: http://acacha.org/mediawiki/Servidor_DNS#Protocol_DNS

**c)** Més sobre protocol i missatge DNS: http://www.zytrax.com/books/dns/ch15/

**d)** Servidor autoritatiu: https://www.dnsknowledge.com/whatis/authoritative-name-server/

**e)** Servidor autoritatiu: http://acacha.org/mediawiki/Servidor_DNS#Servidor_de_noms_autoritzat

**f)** Servidor recursiu: http://whatis.techtarget.com/definition/recursive-DNS-server

**Forma de lliurament de la pràctica**

**1-** Treball individual.

**2-** S'han d'enviar les **respostes a les preguntes 1 a 6** de la **PART 2**.

**3-** El nom del fitxer ha de tenir el següent format **asix2_cognom1_nom_m08uf1pr3b.pdf**

**3-** Envieu la solució proposada per correu electrònic:

Adreça: **cf@collados.org**

Assumpte: **asix2_cognom1_nom_m08uf1pr3b**

**4-** La **data límit** de lliurament de la pràctica és el dia **21/01/18** a les **23.59 hores.**

**5-** Format Lletra: **Arial 10**

**6-** Marges (superior, inferior, esquerra, dreta): **2cm**