**IMT Atlantique** Département Informatique Technopôle de Brest-Iroise - CS 83818 29238 Brest Cedex 3 URL: www.imt-atlantique.fr



**Networking Introduction** Fall 2020

# Lab DNS: Domain Name System

Edited: September 3, 2021 Version: 1.3-2020-09

**Report filled-in by:** 



**IMT Atlantique** Bretagne-Pays de la Loire École Mines-Télécom

# 1. Objectives

This lab aims at helping you to:

- Understand how the domain names system of the Internet works
- Get familiarised with the packet analyser software Wireshark initial objective

# 2. Pre-LAB

- Study the linux commands ifconfig, ip address, ip route, dig, host, ping. You can, for instance, read the man page of these commands by typing on a UNIX terminal man <command> (For the ip tools commands, you must replace the space with a dash, e.g. man ip-address).
- Investigate the different types of resource records existing for the Internet class in the DNS, and their purpose. In particular, complete Table 1.
- Investigate what are iterative DNS queries and recursive DNS queries.
- Readings:
  - The introduction of this lab
  - Serveur DNS faisant autorité: définition, by Stéphane Bortzmeyer: https://www.bortzmeyer. org/serveur-dns-faisant-autorite.html
  - Résolveur DNS : définition https://www.bortzmeyer.org/resolveur-dns.html
  - On the usage of DNS by CDNs: https://labs.ripe.net/Members/emileaben/how-ripe-atlas-help
  - On censorship applied through DNS queries: https://labs.ripe.net/Members/stephane\_ bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes (optional)
  - Nouvelles attaques facilitant l'empoisonnement DNS: https://www.bortzmeyer.org/ dns-attaques-shulman.html

# 3. Introduction

#### 3.1. The Domain Names System

We, as humans, are used to refer to Web pages, mailboxes, and other network resources by using a readable, easy to remember name, like for instance www.imt-atlantique.fr. However, network equipments understand and use numerical addresses (e.g. IP addresses). Having only IP address to refer to network resources would mean, for instance, accessing the Web page hosted at 2001:660:7302:2::21 (or 192.108.117.237), which is not only hard to remember, but supposes that if the Web page changes its location, then we, users, should be aware of this change. As a consequence, a high-level readable names system is used in the Internet in order to allow to decouple machine *names* from machine *addresses*.

How to achieve this decoupling and the mapping between names and addresses at the Internet scale? How to have unique names all across the Internet? How to avoid having a central entity managing the mapping? How to accomplish a system at the Internet-scale avoiding huge files/data bases? The way the Internet community has solved this is called Domain Name System (DNS), and has become a key component of the Internet.

The essence of DNS is a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme. It is primarily used for mapping host names (often referred to as Fully Qualified Domain Names (FQDN)) to IP addresses but can also be used for other purposes [8]. DNS



Figure 1: Example of the DNS Name space

is defined in multiple RFCs [1], [2], [3] and more than 20 others. RFCs (Request for Comments) are documents published by the Internet Engineering Task Force [7], Internet community defining Internet standards.

#### 3.1.1. The DNS Name Space

In order to avoid name collisions, the DNS name space is organized in a hierarchical way. The top of the naming hierarchy for the Internet is managed by the ICANN (Internet Corporation for Assigned Names and Numbers), an organization created in 1988 for this purpose. Figure 1 shows some of the so-called top-level domains and several sub-domains, in a tree representation. The leaves of the tree represent domains that have no sub-domains (but can of course contain one or thousands of *records*). Each domain is named by the path upward from it to the (unnamed) root. The components (*labels*) are separated by a dot.

Each domain, sub-domain or *zone* of the tree can be managed by a different authority. In this way, the database containing the name system information is hierarchically divided into non-overlapping zones. Divisions are made by *delegation* of a zone by the managing authority of the immediately upwards zone. The data base corresponding to a zone is managed by the zone's *authoritative name servers*.

The data base of the DNS is formed by the so called *resource records*. These records can be of different types, according to the information they contain. For instance, a record of class internet and type AAAA maps a name into an IPv6 address. In general, a resource record contains 5 fields, namely *owner* (*domain name*), *Time to live*, *Class*, *Type*, *rdata* (*value*).

#### Question 3.1.

Within the Internet class, there are several types of records. Investigate the purpose of each type of record and complete Table 1. Write down below the name of further records, and their purpose, if you know more of them.

We have provided here a very brief description of the DNS. Students should refer to other sources such as [8, 9] to further understand this key component of the Internet.

Туре	Purpose	Example domain name	Example value
A	Maps a domain name to an IPv4	www.imt-atlantique.fr	192.108.117.237
AAAA			
NS			
MX			
CNAME			
PTR			
SOA			
RRSIG			

Table 1: Common DNS resource records in the Internet class.

### **3.1.2.** The DNS Main Actors

In order to better understand the functioning of the DNS is important to understand -and distinguish- the following terms:

- Authoritative name server a server managing a zone, containing the records corresponding to that specific zone.
- **Resolver** server that is queried by a client (for instance your host) and which performs the DNS queries in order to resolve a mapping. DNS queries are addressed to authoritative name servers. Resolvers usually store records into their cache.
- **Resource Record** constitute the DNS database, see description in the previous subsection.
- **Root servers** authoritative name servers maintaining records of the top-level domains.

#### 3.1.3. DNS Security Extensions (DNSSEC)

DNSSEC is a set of extensions that makes it possible for resolvers to validate the **authenticity** and **integrity** of DNS data. The original design of DNS did not consider security aspects, and DNSSEC has been an important effort aiming to include data authentication and integrity. This set of extensions do not provide confidentiality neither availability, though. DNSSEC prevents users to get fake or manipulated data, that could be created by attacks against DNS resolvers such as cache poisoning (See readings above). DNSSEC is mainly defined by three RFCs: [4], [5], and [6].

### 3.2. The Packet Analyser Wireshark

Wireshark [10] is an opensource network packet analyser. It allows you to capture network packets and to display the packets data in a detailed user friendly way. "You could think of a network packet analyzer as a

The property of the constraints of the property during a finite part of the property						*eth0	x			
<pre>     Prove the set of the se</pre>	Fich	ier <u>E</u> diter ⊻ue ∦	<u>Aller Capture Analyser S</u>	atistiques Telephonie <u>W</u> i	reless <u>O</u> util	s <u>A</u> lde				
Applepring the first definition         Operation         Ope		📕 🙋 🛞 🗎	= 🖹 🖹 🙆 🍳 🔶	• 🔿 🖀 🐔 👱 📃	E C					
No.         The set is a scalar base of the second integration of the second integratint of the second integratintegration of the second integ	🔲 Appliquer un filtre d'affichage <ctri></ctri>									
S 0.24000000       Text: 000000000000000000000000000000000000	No.	Time	Source	Destination	Protocol	Length Info				
<pre>splitstrage field control if field for field control is a split field for field c</pre>		56 3.629459509	fe80::d998:bb13:f9ef:f0_	ff02::c	SSDP	208 H-SEARCH * HTTP/1.1				
25 00000000             125 0000000             125 0000000             125 0000000             125 0000000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 00000             125 0000             125 0000             125 0000             125 0000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000             125 000            125 000             125		57 3.629471200	fe80::d998:bb13:f9ef:f0.	ff02::C	SSDP	208 M-SEARCH * HTTP/1.1 RE Naighbar Soliditation for fogguigeEstate: 27.75fd from 18:50:0ft41:cc:be				
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		59 3.685796974	10.29.230.125	224.0.0.251	MDNS	175 Standard guery 0x0000 PTR homekit tcp.local. '0" guestion PTR sleep-proxy, udg.local. "0" guestion PTR 50-34-10-70.1 time capsule 1.	sleep-			
<ul> <li></li></ul>		60 3.689550438	fe80::f6:553f:ce4a:61c2	ff02::fb	MDNS	195 Standard query 0x0000 PTR _homekit. tcp.local, "QH" question PTR _sleep-proxyudp.local, "QH" question PTR 50-34-10-70.1 time capsule 1.	sleep-			
		61 3.689567025	10.29.224.3	224.0.0.2	HSRP	62 Hello (state Standby)				
i = 0.0007/0112       bolt (accord)       Fromework       Fromework       bolt (accord)       Fromework       bolt (accord)		63 3.950827955	HuavelTe_e8:bf:f1	Broadcast	ARP	55/ NU127 ~ N1171.1 88 Who has 10 - 29.224.12 Tell 10.29.229.128				
et 3.9945020         et J		64 3.961773115	Dell_ad:ca:c6	Broadcast	ARP	60 who has 10.29.227.1187 Tell 10.29.227.29				
# # 10074021       11,822714       10,222715       100       0000       0000       0000		65 3.969461692	Dell_2a:42:f0	Broadcast	ARP	60 who has 10.29.227.145? Tell 10.29.227.177				
# # 1.00714100         Free::sec::exe::exe::exe::exe::exe::exe::e		66 4.193764328	10.29.227.146	10.29.231.255 Broadcast	UDP	305 54915 → 54915 L0n=263 20 U - fune-YD- 2628 UUL LCAR Tadividual CCAR UUL LCAR Command				
<ul> <li></li></ul>		68 4.300794169	fe80::6600:6aff:fe8c:60.	ff12::8384	UDP	50 G, Halferzie, Solit Hole Low Individual, Solit Hole Low Command				
7       4.30050100       Cites, Fr. 60::00       Freedoatt       APP       60 Why has 10.52, 223.27       10.22, 227.10       12.22, 22.21         7       7.4.30070710       12.22, 22.21       12.22, 22.22       12.22, 22.21       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22       12.22, 22.22, 22.22, 22.22       12.22, 22.22, 22.22, 22.22		69 4.300817242	10.29.227.113	10.29.231.255	UDP	111 53451 → 21027 Len=69				
1       1		70 4.300858100	Cisco_f9:60:c0	Broadcast	ARP	60 who has 10.29.224.31? Tell 10.29.224.2				
1         1		71 4.304713063	10 20 227 192	192 44 75 10	TCHPA8	/8 Heighnor Solicitation for Te80::ce91:/afr:Te53:T572				
74       4.385712240       Chlumbal 53.75:12       products APP       60 Grautions APP       60 Grautions APP         74       4.385712240       Chlumbal 53.75:12       products APP       60 Grautions APP       60 Grautions APP       60 Grautions APP         74       4.50712400       Likes A0 Bits       Proc 10       50 Grautions APP       60 Gr	÷.	73 4.360700788	192.44.75.10	10.29.227.182	DNS	341 Standard query response 0x5815 A www.imt-atlantique.fr A 192.108.117.237 NS dns-int3.imt-atlantique.fr NS dns-int.imt-atlantique.fr NS dns	s-int4.			
73 4.22349886       F88/123712 KD1 (2012) (201		74 4.385712243	ChiunMa1_53:f5:f2	Broadcast	ARP	60 Gratuitous ARP for 10.29.229.205 (Reply)				
000       B3 47 40 Cf cf 00 00 23 eb fp 00 c 0 00 00 45 0 0 et al.       Source and the state of th		75 4.422849886	Teso::2579:a201:6156:6a.	TT02::C	SSDP TOMPY2	SSS NOTIFY * HTTP/1.1				
78 4.09055492 ::::::::::::::::::::::::::::::::::::		77 4.560732618	Cisco 6d:a8:09	PVST+	STP	40 Hennet and we work ( your 2010) and ( all all all all all all all all all a				
79 4.639781788       FMG::223:eDf::Missec:0       ICUPYS       118 Router Advertises:15:80:0         81 4.639631       FMG::1151:15:15:15:15:15:15:15:15:15:15:15:		78 4.609356492		ff02::16	ICMPv6	90 Multicast Listener Report Message v2				
0000       12 4 050000000       11111000       11100000       1111100000       1111100000       1111100000       11111000000       111110000000       1111100000000000       11111100000000       1111100000000       1111100000000000000000000000000000000		79 4.639781788	fe80::223:ebff:fef9:60c0	ff02::1	ICMPv6	118 Router Advertisement from 00:23:eb:f9:80:00				
12 4.468423273 :::       ff22:15       ICMPV8 9P NUICEST Listener Report Resage v2       >         1       Ffame 73: 341 bytes on uire (2728 bits). 541 bytes caburde (2728 bits) on interface 0       >         1       Ffame 73: 341 bytes on uire (2728 bits). 541 bytes caburde (2728 bits) on interface 0       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Internet Producel Version 4, 5rc: 102.0; 271.02       >         1       Present Numes Condition 3D: Doddis       >         1       The: Iso 3D: Doddis       >         1       Autority Res: 6		81 4.650653495		ff02::1:fffc:657a	TCMPV6	78 Heighnor Sullilation for 2001/868/3502/5/69/3503/37fc/857a				
Image: 73: 341 bytes on uire (2728 bits), 341 bytes captured (2728 bits), 051: 0612, 07: 47: 47: 47: 47: 47: 47: 47: 47: 47: 4		82 4.669423273		ff02::16	ICMPv6	90 Multicast Listener Report Message v2				
Frame 71: 341 bytes on unite (228 bits), 341 bytes captured (278 bits) on inferface 0         Ethernet 17: 357: Lisco (558:00, 053: 00, 053: 00, 053: 00, 053: 00, 023: 047:47:47:47:47:47:47:47:47:47:47:47:47:4	4	00 1 345000053	4.00.0070.0004.0400.04	4400	0000	ETAL ILATTERIA & LITTERIA A	•			
<pre>&gt; Ethernet IT, Src: Class_Classical (#Sign Cr), Det: Dell_07:cf108 (20:47:47:47:47:47:47:47:47:47:47:47:47:47:</pre>	► E	rame 73: 341 bytes	on wire (2728 bits), 341	bytes captured (2728 bits	) on interf	ace 0				
<pre>&gt; Internet regreted versite s, bet: bt. bt. bt. bt. bt. bt. bt. bt. bt. bt.</pre>	► E	thernet II, Src: C	isco_f9:60:c0 (00:23:eb:fs	0:60:c0), Dst: Dell_d7:cf:	00 (20:47:4	7:d7:cf:00)				
<pre></pre>		ser Datagram Protocol V	ersion 4, Src: 192.44.75.3 col Src Port: 53 Det Por	.0, DST: 10.29.227.182						
(facuer 1: 0: 72)         (There: 0: 0255415 seconds]         (There: 0: 0255415 seconds]         (Facuer 1: 0: 72)         (Jassi 0: 0356 standard query response, No error         (Quef 1: 005: 1)         Answer R8: 1         Allor(1) Kes: 6         (Jassi 0: 0356 standard query response, No error         (Quef 1: 05: 0)         (Jassi 0: 0356 standard query response, No error         (Jassi 0: 036 query response, No error         (Jassi 0: 036 query response)         (Jassi 0: 036 query	- DI	omain Name System	(response)							
Image: 0.0215816 seconds]         • Flags: 0.8258 standard query response, No error         Amser Rs: 0         Additional Rs: 7         • Querise         • Additional Rs: 7         • Querise         • Additional Rs: 7         • Additional Rs: 7         • Querise         • Additional Rs: 7         • Additional Rs: 7         • Additional Rs: 7         • Additional records         • Out Additional records         • Additional records         • Out Additional records         • Additional records         • Out Additional records         • O		[Request In: 72]								
P Flags: basis 5 standard query response, No error Questions: 1 Answer R8: 1 Althority R8: 6 Authority R8: 6 Authority R8: 6 Authority R8: 6 Authoritative nameservers Additional records       0000     E0 47 47 GF of 00 00 23 eb f9 60 c0 00 00 45 00 Authoritative nameservers     6000.00     E0 00 00 23 eb f9 60 c0 00 00 45 00 Authoritative nameservers       0001     E0 47 47 GF of 00 00 23 eb f9 60 c0 00 00 45 00 E0 10 00 60 00 70 77 77 78 66 60 72 45 01 Authoritative nameservers     6000.00       0002     E0 47 47 GF of 00 00 23 eb f9 60 c0 00 00 45 00 E0 10 00 56 00 70 77 77 77 66 66 67 24 51 0 Authoritative ff		[Time: 0.0021594	15 seconds]							
0000         D0 47 47 d7 cf 00 00 23         eb f9 80 c0 00 00 15 00         508		Flags: 0x8580 St	andard query response. No	error						
Althority R8: 1 Althority R8: 6 Variable Register R8: 1 Attribute Register R8: 1 Attribute R8: 6 Additional records Additional		Questions: 1								
Autority es: 5 ) Guriss 5 ) Guriss 5 ) Autoritative nameservers ) Additional records		Answer RRs: 1								
• Gurriss Answers > Authoritative nameservers > Additional records           0000         10         47         67         67         60         00         10         47         67         67         60         00         10         60         10		Additional RRs: 6	7							
<ul> <li>A startstitter nameservers</li> <li>Additional records</li> <li>Gonomia and a starts and a start and a st</li></ul>		Queries								
Additional records           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 45 00         G086.           0000         D0 47 47 07 cf 00 00 23 eb f9 50 c0 00 00 40 c0 c0         G086.           0000         D0 40 00 80 07 17 77 77 86 60 74 20 10         G08		Answers								
0000       10: 47: 47: 67: 67: 60: 60: 23: eb: f0: 60: c0: 60: 90: 45: 50:       50		Authoritative na	neservers							
6000         20         47         47         67         cf         00         00         20         47         47         67         cf         00         00         14         97         84         60         98         11         85         17         00         00         14         97         84         60         98         11         16         17         00         16         11         16         17         00         10         1         10		Additional recor	us							
00000         126         47         47         67         cf         00         00         45         66         66										
0000         20         47         47         67         cf         00         00         23         eb         19         60         00         10         1.47         57         84         60         95         1.1         eb         17         107         84         60         95         1.1         eb         17         107         84         60         95         1.1         eb         1.7         67         86         66         67         1.47         57         78         86         66         74         67         1.47         57         78         86         67         42         1.47         1.47         57         78         86         67         42         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.47         1.41										
00000         126         47         47         d7         cf         00         00         92         sb         f9         60         60         60         60         60         f5         f3         f3 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>										
0000         20         47         47         cf         cf         000         00         147         57         84         00         09         13         15         15         00         16         147         57         84         00         09         13         15         15         00         16         147         57         84         00         09         13         15         10         00         10         147         57         84         00         09         13         10										
0000         100         47         47         d7         cf         000         100         47         47         d7         cf         000         100         40         40         100										
0000 10 47 47 07 cf 00 92 23 eb f 96 06 00 82 23 eb f 96 06 00 80 45 60 508E. 0010 11 47 77 86 00 99 811 10 17 07 24 06 88 11 50 50										
0010 01 4 4 5 5 6 00 00 36 1 1 6 1 7 6 0 2 4 0 0 4 0 1 1 5 0020 6 3 5 6 0 0 0 3 7 7 7 7 2 6 5 1 5 6 0 0 0 1	0000	20 47 47 d7 cf	30 00 23 eb f9 60 c0 08 0	0 45 88 GG#	Ε.					
1000 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0010	01 47 97 84 00 0 e3 b6 00 35 d8	30 30 11 00 17 c0 2c 4b 0 37 01 33 7f 12 50 15 05 0	a da 10>,K.						
0046 Pt 46 61 68 71 75 65 02 68 72 60 00 10 40 0055 01 12 60 00 12 60 11 60 15 15 80 00 40 82 750	0030	00 01 00 06 00	07 03 77 77 77 0e 69 6d 7	4 2d 61	- a.					
	0040	74 6C 61 6e 74 0		0 01 00 tlantiqu e.fr						
	0050	01 CD 0C 00 01	30 01 00 01 51 80 00 04 c	0 6C 75Q	lu					
Valuare 171 A amenae 171 Actare	0000	Z Eramo (frame)	241 octate			Parulate: 1212 - 54%cháe: 1212 (100.063)	ili Dofault			

Figure 2: A wireshark packet capture example source [10]

measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course)." [10]

Figure 2 shows an example wireshark capture. We can distinguish the sequence of captured packets, followed by the detailed, human-readable content of the selected packet, finally followed by the packet data in hexadecimal.

#### **3.3.** Capturing traffic

In order to capture traffic in a wired interface in a unix system using wireshark make sure to have the adequate privileges (e.g. on Debian and based distributions, the user should be part of the *wireguard* group).

wireshark &

Once in wireshark, before starting a capture, you must select the interfaces where you want to capture traffic. To do so, click Capture  $\rightarrow$  Options  $\rightarrow$  select interface start.

At any moment you can save one capture to analyse it later on. You can also change the visualisation options, to get more or less columns, activate/desactivates colors, etc.

### 4. Hands On

#### 4.1. Some useful unix commands.

1) Start the course's VM and open a new terminal in the VM

#### Question 4.1.

Use the command ip a (shortcut for ip address) to obtain the information of the network interfaces available in your working VM. Are they IP addresses v4 or v6? Write down the obtained address(es).

#### Question 4.2.

Which DNS resolver is your working VM using? For obtaining that information show the content of file /etc/resolv.conf. You can for example execute cat /etc/resolv.conf

Note that the information from the two previous questions will be useful when you will inspect network packets in Section 3.2.

#### 4.2. DNS basic functioning and commands

#### Question 4.3.

Use the command dig -x to query the domain name associated to the 2620:0:2d0:200::7 address, and write it down. What kind of query (lookup) is it? (Clue: look at man dig).

#### Question 4.4.

Indicate the IPv4 address associated to www.brest.fr. You can again use command dig again.

#### Question 4.5.

Which type of DNS record allows you to obtain such information?



Figure 3: DNS resolution of www.fing.edu.uy. Image based on https://en.wikipedia.org/wiki/ File:Example\_of\_an\_iterative\_DNS\_resolver.svg

#### Question 4.6.

Use **dig** to obtain the IPv6 address associated to www.nic.cl. Write down the address and the full command you need to use.

#### Question 4.7.

Query now the A record of www.fing.edu.uy showing all the hierarchy. You can use **dig** with the **+trace** option (along with **+multiline** for a more human-readable output). Who send the messages numbered 1, 2 and 3 from Figure 3 (Look at the "Received . . . from" lines in the output)? Complete the answers from the uy. and fing.edu.uy nameservers. What can you conclude about the functioning of the domain service? Explain.

#### 4.3. Analysing DNS traces

We are now going to use Wireshark to see what is going on down the wire.

1) Open a terminal on your virtual machine and type the command wireshark to open wireshark. In wireshark, start a new capture in the eth0 interface.

- 2) In another terminal, issue a one-time ping (ping -c 1) to www.imt-atlantique.fr
- 3) In Wireshark examine the captured packets.

#### Question 4.8.

What protocols do you see? Why?

- 4) Use a visualisation filter to see only the DNS messages.
- 5) Locate the DNS query and response sent and received due to your previous command.

#### Question 4.9.

Are them sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port of DNS response message?

#### Question 4.10.

To what IP address is the DNS query message sent? Compare this to the resolver used by your working VM (see your answers to part 4.1). Are these two IP addresses the same?

6) Now, we will find out the serves managing e-mail for imt-atlantique.fr (you can refer to Table 1). In a terminal use the dig MX program to find out the servers exchanging mails for imt-atlantique.fr

#### Question 4.11.

What information did you get?

7) Observe the captured DNS traces

#### Question 4.12.

Examine the DNS query message. What "Type" of DNS records does the query ask for? Does the query message contain any "answers"?

#### Question 4.13.

Examine the DNS response message. What name servers does the response message provide? Does this response message also provide the IP addresses of the name servers?

- 8) Find out the authoritative name server of the tools.ietf.org domain.
- 9) Start a new capture, if you have stopped the previous one
- **10**) In a terminal, run the command dig tools.ietf.org @ip\_authoritative server where ip\_authoritative server is one of the IPs found out in step **8**)
- 11) Repeat the command several times.
- 12) Now, type command dig tools.ietf.org @80.67.188.188 Repeat the action several times.
- 13) You can now stop the capture

#### Question 4.14.

Observe the Wireshark capture. Compare the responses obtained from the authoritative and the recursive servers. In what do they differ? Look at the TTLs. Explain.

#### 4.4. Validating DNS query answers with DNSSEC

For taking advantage of the security provided by DNSSEC, two conditions have to be fulfilled: (1) the domain zone that you want to query about has to be signed, and (2) your DNS resolver must be able to verify the record signatures.

Before answering the questions in this section, check first whether your DNS resolver validates or not the DNS answers. For that you can use two tools:

- The dnssec-failed.org domain, whose **signature is invalid**. Run dig dnssec-failed.org, and you should get a **SERVFAIL** message if the resolver validates the answer, or a **NOERROR** message with the full answer if it does not.
- The http://dnssec.vs.uni-due.de/ website: provides an easy to use "DNSSEC resolver test". Simply click on the Start test button.

If you find out the resolver is not DNSSEC-able, compare the query for the *dnssec-failed.org* domain against a validating resolver:

14. Query a validating server, such as ns0.ldn-fai.net or 1.1.1.1, about the domain dnssecfailed.org:

dig dnssec-failed.org @1.1.1.1.

#### Question 4.15.

What do you get? Explain.

15. Query now a non-signed domain and a signed domain:

dig +dnssec hola.com @1.1.1.1

dig +dnssec ripe.net @1.1.1.1

#### Question 4.16.

The difference is not very visible for the end user, but compare the **flags** in the **HEADERs** of both answers. What is (or should be) the difference between them (how the answer tells you the answer has **Authenticated Data (AD)** or not)?

16. Query again ripe.net using the dig command, including the +dnssec and +multiline options.

#### Question 4.17.

Explain what is the new record and its contents that you can read in the answer.

# 5. Conclusion

### Question 5.1.

What is the purpose of the DNS protocol? Give an answer as complete as possible (which can be brief at the same time).

#### Question 5.2.

Why does the DNS protocol uses UDP as a transport protocol? What do you think are the advantages and disadvantages for this?

#### Question 5.3.

What are advantages and disadvantages of a distributed data base, as the one managing domain names?

#### Question 5.4.

Would you say that DNS is a secure protocol or not? Be as precise as you can in answer. What is DNSSEC for and what does it provide? Does DNSSEC provides confidentiality in the DNS messages exchange?

## References

- [1] RFC 1034 DOMAIN NAMES CONCEPTS AND FACILITIES, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc1034.
- [2] RFC 1035 DOMAIN NAMES IMPLEMENTATION AND SPECIFICATION, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc1035.
- [3] RFC 2181 Clarifications to the DNS Specification, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc2181.
- [4] RFC 4033 DNS Security Introduction and Requirements, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc4033.
- [5] RFC 4034 Resource Records for the DNS Security Extensions, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc4033.
- [6] RFC 4035 Protocol Modifications for the DNS Security Extensions, The Internet Engineering Task Force, [online] https://tools.ietf.org/html/rfc4033.
- [7] The Internet Engineering Task Force [online] https://ietf.org/about/.
- [8] Computer Networks, 5th edition, Andrew S. Tanenbaum, David J? Wetherall, PRENTICE HALL
- [9] Les réseaux, 4th edition, Guy Pujolle, EYROLLES
- [10] Wireshark network packet analyser [online] https://www.wireshark.org/