



Centro Universitario de la Defensa en la Escuela Naval Militar

FINAL YEAR PROJECT

*Integration and configuration of a safe hotspot through a
communication tunnel on TOR net*

Mechanical Engineering Bachelor Degree

STUDENT: Ernesto Golmayo Fernández

SUPERVISORS: Rafael Asorey Cacheda

ACADEMIC YEAR: 2016-2017

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

FINAL YEAR PROJECT

*Integration and configuration of a safe hotspot through a
communication tunnel on TOR net*

Mechanical Engineering Bachelor Degree

Naval Technology Specialization

Naval Branch

UniversidadeVigo

ABSTRACT

The present project develops the design and integration of a TOR's net redirecting device into a Raspberry Pi (versions 2 model B and 3 model B). Therefore, information will be encrypted between clients and servers.

According to nets' menaces, system will provide security within LAN and WAN by the means of virtual private networks and protection software (an antivirus and a firewall). Acting as a hotspot it will generate a Wi-Fi area (shell with wireless encryption, WPA2), supplying certificates to the workstations to authenticate themselves.

Last sections analyse the capabilities of the device created, studying possible solutions to the problems presented. Finally, the document concludes displaying profiles of potential users and future lines of investigation.

KEYWORDS

Raspberry Pi, hotspot, TOR's redirection, encryption, tracking

RESUMEN

El actual documento recoge el diseño y la implementación de un sistema de redirección de tráfico de datos a través de un canal de comunicación en la red TOR en una Raspberry Pi 2 modelo B y en una Raspberry Pi 3 modelo B. El objetivo es crear un instrumento capaz de encriptar toda la información transmitida creando un punto de acceso seguro a una red abierta.

La red TOR consiste en una malla de nodos interconectados, en la cual, cada uno de ellos únicamente conoce la unidad que le envía la información y la cual a la que tiene que enviársela. De esta manera, la identidad del usuario queda resguardada ya que en ningún momento dichos nodos saben que están enviando ni a donde. La Raspberry Pi, entonces, tendría que generar una red local y actuar como puerta de acceso a la red mencionada.

Al crear una red local aparecen nuevos factores y amenazas a tener en cuenta. Los mismos peligros que presenta Internet están relacionados con las redes LAN (Red de área local), ya que la estructura es la misma, solo que a menor escala. De esta manera, se necesitarían medios de protección adicionales que asegurasen las comunicaciones de los usuarios ante posibles intentos de acceso indebido. Ante dicha tesitura, entrarían en juego aplicaciones como las redes virtuales capaces de codificar los intercambios de datos entre dos estaciones mediante certificados y autoridades certificadoras. Estas redes se podrían reforzar con software destinado a proteger las redes inalámbricas como es WPA2 (Acceso protegido a Wi-Fi).

Todas las medidas incluidas en el proyecto son analizadas posteriormente, con el fin de determinar cuál de ellas no ha sido efectiva, y así poder investigar posibles soluciones a los problemas surgidos. La presente memoria se cierra definiendo los campos de aplicación para los que está diseñado y líneas de mejora relacionadas con los resultados del estudio de sus capacidades.

PALABRAS CLAVE

Raspberry Pi, hotspot, direccionar tráfico, encriptar, seguimiento

TABLE OF CONTENTS

Table of contents	1
Figures index	6
Tables index	10
Charts index.....	12
Equations index	14
1 Introduction & Objectives	15
1.1 Motivation.....	15
1.1.1 Introduction.....	15
1.1.2 Hackers	16
1.1.3 A brief look into Internet's framework.....	17
1.1.4 Encrypting and tunnelling.....	17
1.2 Objectives.....	18
1.3 Resources	18
1.3.1 Initial material.....	18
1.3.2 Software and programs	20
1.3.3 Workstations	20
1.3.4 Additional material	20
1.4 Structure of the document	22
2 State of the art.....	23
2.1 Introduction.....	23
2.2 Raspberry Pi as a router	24
2.2.1 Router	24
2.2.2 Raspberry Pi [29].....	26
2.3 Malware & Intercepting devices	26
2.3.1 Network Analysis and Man in the middle [35].....	26
2.3.2 Viruses	29
2.3.3 Phishing [61].....	33
2.3.4 Risks	34
2.4 Safe Untracking Programs & Devices	35
2.4.1 Defences against malware analysed	35
2.4.2 TOR net and VPN's [64]	36
2.4.3 SSL [12].....	37
2.4.4 Onion Pi [68]	38

2.4.5 OpenVPN [69]	39
2.4.6 WEP, WPA and WPA2 [73]	40
2.4.7 Antivirus	41
2.4.8 Firewall [79]	41
2.4.9 DNS Server	42
2.5 Conclusion	42
3 Development & Settings	44
3.1 Introduction	44
3.2 Set an OS	44
3.2.1 Downloading the OS image	44
3.2.2 Formatting MicroSD and burning the image	45
3.2.3 Setting first steps in Raspberry Pi	45
3.2.4 Working parameters	48
3.3 Set an Access Point [33]	49
3.3.1 Set up an DHCP server and a subnet	49
3.3.2 Set up a static IP	50
3.3.3 Configure hostapd	51
3.3.4 NAT	53
3.3.5 Start the hotspot service	54
3.4 Set Tor [87]	57
3.4.1 Install tor	59
3.4.2 IP tables [66]	60
3.5 Set OpenVPN Server/Client [92]	64
3.5.1 Install OpenVPN	64
3.5.2 Set a OpenVPN Server	64
3.5.3 Create Clients	66
3.5.4 WinSCP	68
3.6 ClamAV antivirus [93]	75
3.7 Uncomplicated Firewall [80]	75
3.8 Crontab	76
3.9 DNS cache proxy [94]	77
3.10 VNC Server [95]	78
4 Testing & Validation	80
4.1 Tests	80
4.1.1 Introduction	80
4.1.2 Previous comparison between resources (1.3 Resources)	80

4.1.3 Security	80
4.1.4 Anonymity	91
4.1.5 Navigation experience	92
4.1.6 Most popular services and apps	100
4.1.7 Battery.....	101
4.2 Unable to test	101
4.3 Tests conclusions resume.....	102
4.3.1 Security	102
4.3.2 Anonymity	103
4.3.3 Speed & Experience	103
5 Conclusions and future advances	105
5.1 Overview	105
5.2 Scope of application.....	106
5.3 Development directions	108
6 Bibliography	109
I. Attached document I: Safety Measures	118
I. General measures	118
II. Anonymous measures.....	118
III. Protection measures ³¹	118
II. Attached document II: Flow Diagrams.....	119
I. General Flow Diagram	119
II. UFW Flow Diagram.....	119
III. TOR Flow Diagram	120
IV. OpenVPN Diagram Flow.....	120
V. OpenVPN and TOR Diagram Flow	121
III. Attached document III: Clients generator	122
I. Clients generator file.....	122
II. Generating clients.....	124
IV. Attached document IV: Virus test.....	125
V. Attached document V: Wireshark Test	126
I. First Wireshark test.....	126
II. Second Wireshark test	128
III. Third Wireshark test.....	129
IV. Fourth Wireshark test.....	130

V. Fifth Wireshark test.....	131
VI. Attached document VI: Popular services and applications test	133
I. Streaming media (Spotify).....	133
II. Social Networks' applications (Facebook).....	133
III. Streaming media Social Networks (Instagram)	134
IV. Download manager (Play Store).....	134
V. Streaming media (YouTube).....	134
VI. News broadcasting applications (Al Jazeera News)	135
VII. Outlook	135
VIII. Messenger applications (Whatsapp)	136
IX. Summary of popular services and applications test.....	136
VII. Attached document VII: Downloading and Resolving delay Charts clear access.....	137
I. Readings without DNS Server	137
II. Readings with DNS Server.....	138
III. No DNS vs. DNS	139
IV. Line Charts.....	140
V. Bar Charts.....	141
VIII. Attached document VIII: Downloading and Resolving delay Charts TOR Redirection	143
I. Readings without DNS Server	143
II. Readings with DNS Server.....	144
III. No DNS vs. DNS	145
IV. Line Charts.....	146
V. Bar Charts.....	147
IX. Attached document IX: Downloading and Resolving delay Charts TOR and Ovpn.....	149
I. Readings without DNS Server	149
II. Readings with DNS Server.....	150
III. No DNS vs. DNS	151
IV. Line Charts.....	152
V. Bar Charts.....	153
X. Attached document X: Downloading and Resolving delay Raspberry Pi 2.....	155
I. DNS, TOR and OVPN activated	155
XI. Attached document XI: Downloading and Resolving delay Comparison	156
I. Clear Access vs. TOR Tables	156
II. Clear Access vs. TOR Bar Charts	157
III. Clear Access vs. TOR and OVPN	158

IV. TOR vs. TOR and OVPN	160
V. Clear Access vs. TOR vs. TOR and OVPN Bar Charts	161
VI. Raspberry Pi 2 vs. Raspberry Pi 3	162
VII. Distance Analysis	163

FIGURES INDEX

Figure 1-1 Basic Internet's topology (edited from [3]).....	16
Figure 1-2 Internet's Framework (edited from [3])	17
Figure 1-3 VPN and TOR's tunnels illustration (edited from [3]).....	18
Figure 1-4 Raspberry Pi 2B	19
Figure 1-5 Raspberry Pi 3 Model B	21
Figure 1-6 Both Raspberry Pi and adapters.....	21
Figure 2-1 Preview of malware and safety devices (edited from [3]).....	24
Figure 2-2 Image of a router (taken from [26])	24
Figure 2-3 IP tables process flow (taken from [28])	25
Figure 2-4 Raspberry Pi Router (taken from [32]).....	26
Figure 2-5 TEMPEST's protection methods (taken from [40])	27
Figure 2-6 TEMPESTING cartoon example (taken from [43])	28
Figure 2-7 Wireshark's interface (taken from [26]).....	28
Figure 2-8 Cluster of viruses related concepts (taken from [26])	29
Figure 2-9 Four examples of screen locking (taken from [46])	31
Figure 2-10 Increase of ransomware success (taken from [48])	31
Figure 2-11 DNS Translation (edited from [3])	32
Figure 2-12 Example of a botnet (taken from [51])	32
Figure 2-13 Example of phishing website (taken from [62]).....	33
Figure 2-14 Real PayPal website.....	34
Figure 2-15 PayPal's Certificate	34
Figure 2-16 Malware summary (edited from [3])	35
Figure 2-17 TOR Layers (taken from [65]).....	36
Figure 2-18 TOR's working mode (taken from [64])	36
Figure 2-19 Relaying and decoding process (edited from [3]).....	37
Figure 2-20 Location of SSL protocol layer (taken from [12]).....	37
Figure 2-21 Onion Pi (take from [68])	38
Figure 2-22 OpenVPN logo (taken from [26]).....	39
Figure 2-23 Decoding and coding process (taken from [26])	39
Figure 2-24 Certification process (taken from [72])	40
Figure 2-25 DNS resolving process (taking from [82])	42
Figure 2-26 MZ and DMZ (edited from [3]).....	43
Figure 3-1 Choosing OS (taken from [15])	44
Figure 3-2 Screenshot of SDFormatter formatting MicroSD.....	45
Figure 3-3 Screenshot of Win32 Disk Imager burning OS image	45

Figure 3-4 Raspberry Pi's interfaces (edited from [3])	47
Figure 3-5 Screenshot of networks' configuration example	48
Figure 3-6 Screenshot of an example of PuTTY session	48
Figure 3-7 Raspberry pi hotspot (edited from [3])	49
Figure 3-8 Screenshot of DHCP's pool configuration	50
Figure 3-9 Screenshot of final interfaces' file appearance	51
Figure 3-10 Screenshot of Wi-Fi setting	52
Figure 3-11 Screenshot of checking internet's file	54
Figure 3-12 Screenshot of Hostapd's service status checking	55
Figure 3-13 Screenshot of DHCP's server status checking	55
Figure 3-14 Screenshot of Hostapd's service activation 1 st Step	56
Figure 3-15 Screenshot of Hostapd's service activation 2 nd Step	56
Figure 3-16 Screenshot of Hostapd's service activation 3 rd Step	56
Figure 3-17 Screenshot of Hostapd's service activation 4 th Step	57
Figure 3-18 Example of Whonix working mode (taken from [88])	58
Figure 3-19 Whonix supported platforms (taken from [90])	58
Figure 3-20 Tor Transproxy (edited from [3])	59
Figure 3-21 Screenshot of Toriptables' file final appearance (1)	62
Figure 3-22 Screenshot of Toriptables' file final appearance (2)	63
Figure 3-23 Screenshot of Toriptables' file final appearance (3)	63
Figure 3-24 Check TOR status (taken from [91])	63
Figure 3-25 OpenVPN Server (edited from [3])	64
Figure 3-26 Screenshot of a WinSCP Session	68
Figure 3-27 Screenshot of WinSCP root session	69
Figure 3-28 Screenshot copying ovpn file	69
Figure 3-29 Screenshot importing a Profile	70
Figure 3-30 Screenshot naming the profile	70
Figure 3-31 Screenshot OpenVPN's options	73
Figure 3-32 Screenshot Initialization Scheme	74
Figure 3-33 Screenshot Successful Windows Connection	74
Figure 3-34 Screenshot Successful Android Connection	74
Figure 3-35 ClamAV antivirus (edited from [3])	75
Figure 3-36 Uncomplicated Firewall (edited from [3])	75
Figure 3-37 Screenshot UFW status	76
Figure 3-38 Screenshot of a VNC interface creation	78

Figure 4-1 Screenshot of scanning summary message.....	81
Figure 4-2 Wireshark sniffing structures (taken from [99]).....	82
Figure 4-3 Wireshark Monitoring Framework (edited from [3])	82
Figure 4-4 Screenshot of Wireshark homepage	83
Figure 4-5 Screenshot of Raspberry Pi IP searching.....	84
Figure 4-6 Screenshot of filtering victim's traffic	84
Figure 4-7 Screenshot of HTTP filtering	85
Figure 4-8 Screenshot of JPEG file seizing.....	85
Figure 4-9 Screenshot of a JPEG image stolen	86
Figure 4-10 Screenshot of another example of stolen file.....	86
Figure 4-11 Screenshot of VNC desktop proving TOR's disabling	87
Figure 4-12 Screenshot of Tablet's interface showing Garbo TOR's redirection	88
Figure 4-13 Screenshot of Tablet's interface exhibiting Garbo connection	88
Figure 4-14 Screenshot of lacking packets intelligence	89
Figure 4-15 Screenshot of encrypted communication monitoring.....	89
Figure 4-16 Screenshot of local traffic TOR redirection.....	90
Figure 4-17 Screenshot checking once more TOR workstations' traffic redirection.....	90
Figure 4-18 Screenshot of Wireshark trying to get Raspberry Pi local traffic	90
Figure 4-19 Screenshot of Tab A information obtained by Fing	91
Figure 4-20 Screenshot of Fing results.....	91
Figure 4-21 Speed tests' structure (edited from [3])	93
Figure 4-22 Screenshot of a curl's and dnsmasq's responses example	94
Figure 4-23 Screenshot of speed test while using OpenVPN and Spotify	100
Figure 4-24 Screenshot of a live stream experiment while using OpenVPN.....	100
Figure II-1 General Flow Diagram.....	119
Figure II-2 UFW Flow Diagram	119
Figure II-3 TOR Flow Diagram	120
Figure II-4 OpenVPN Diagram Flow	120
Figure II-5 OpenVPN and TOR Diagram Flow	121
Figure IV-1 Screenshot downloading Eicar's virus	125
Figure IV-2 Screenshot of a scan executed	125
Figure IV-3 Screenshot of a pi's mail checking	125
Figure V-1 Screenshot of packets seized during first test (1/3)	127
Figure V-2 Screenshot of packets seized during first test (2/3)	127
Figure V-3 Screenshot of packets seized during first test (3/3)	128
Figure V-4 Screenshot of packets seized during third test	130

Figure V-5 Screenshot of packets seized during fourth test.....	131
Figure V-6 Screenshot of packets seized during fifth test.....	132
Figure VI-1 Screenshot of Spotify test.....	133
Figure VI-2 Screenshot of Facebook test	133
Figure VI-3 Screenshot of Instagram test.....	134
Figure VI-4 Screenshot of Play Store test	134
Figure VI-5 Screenshot of YouTube test	134
Figure VI-6 Screenshot of Al Jazeera News application test	135
Figure VI-7 Screenshot of Outlook test	135
Figure VI-8 Screenshot of Whatsapp test.....	136
Figure VI-9 Screenshot of popular services and applications test's summary	136

TABLES INDEX

Table 2-1 Attack risks	34
Table 2-2 Protection software vs. probable attacks.....	35
Table 2-3 Antivirus's comparison	41
Table 4-1 Overview of Raspberry Pi 2 and Raspberry Pi 3's features	80
Table 4-2 Example of data gathering	96
Table 4-3 Changing TOR node example.....	99
Table 4-4 Downloading delay NO DNS vs. DNS / TOR and OVPN	100
Table 4-5 Raspberry Pi's battery's life expectancy	101
Table 5-1 Users' profile and risks.....	106
Table VII-1 Downloading delay readings NO DNS / NO TOR / NO OVPN / Clear access.....	137
Table VII-2 Requesting delay readings NO DNS / NO TOR / NO OVPN / Clear access	137
Table VII-3 Downloading delay readings NO DNS / NO TOR / NO OVPN / Clear access.....	137
Table VII-4 Requesting delay readings NO DNS / NO TOR / NO OVPN / Clear access	137
Table VII-5 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access	138
Table VII-6 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access	138
Table VII-7 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access	138
Table VII-8 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access	138
Table VII-9 Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN.....	139
Table VII-10 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access	139
Table VII-11 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access	139
Table VII-12 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access	140
Table VIII-1 Downloading delay readings NO DNS / NO OVPN / TOR Redirection	143
Table VIII-2 Requesting delay readings NO DNS / NO OVPN / TOR Redirection	143
Table VIII-3 Downloading delay readings NO DNS / NO OVPN / TOR Redirection	143
Table VIII-4 Requesting delay readings NO DNS / NO OVPN / TOR Redirection	143
Table VIII-5 Downloading delay readings DNS / NO OVPN / TOR Redirection	144
Table VIII-6 Requesting delay readings DNS / NO OVPN / TOR Redirection	144
Table VIII-7 Downloading delay readings DNS / NO OVPN / TOR Redirection	144
Table VIII-8 Requesting delay readings DNS / NO OVPN / TOR Redirection	144
Table VIII-9 Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection	145
Table VIII-10 Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection	145
Table VIII-11 Table IV 10 Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection	145
Table VIII-12 Table IV 10 Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection	146

Table IX-1 Downloading delay readings NO DNS / TOR and OVPN.....	149
Table IX-2 Requesting delay readings NO DNS / TOR and OVPN.....	149
Table IX-3 Downloading delay readings NO DNS / TOR and OVPN.....	149
Table IX-4 Requesting delay readings NO DNS / TOR and OVPN.....	149
Table IX-5 Downloading delay readings DNS / TOR and OVPN.....	150
Table IX-6 Requesting delay readings DNS / TOR and OVPN	150
Table IX-7 Downloading delay readings DNS / TOR and OVPN.....	150
Table IX-8 Requesting delay readings DNS / TOR and OVPN	150
Table IX-9 Downloading delay NO DNS vs. DNS / TOR and OVPN.....	151
Table IX-10 Requesting delay NO DNS vs. DNS / TOR and OVPN.....	151
Table IX-11 Downloading delay NO DNS vs. DNS / TOR and OVPN.....	151
Table IX-12 Requesting delay NO DNS vs. DNS / TOR and OVPN.....	152
Table X-1 Downloading delay readings NO DNS / TOR and OVPN / Raspberry Pi 2	155
Table X-2 Requesting delay readings NO DNS / TOR and OVPN Raspberry Pi 2	155
Table X-3 Downloading delay readings NO DNS / TOR and OVPN / Raspberry Pi 2	155
Table X-4 Requesting delay readings NO DNS / TOR and OVPN / Raspberry Pi 2	155
Table XI-1 Downloading delay Clear access vs. TOR / DNS	156
Table XI-2 Requesting delay Clear access vs. TOR / DNS	156
Table XI-3 Downloading delay Clear access vs. TOR / DNS	156
Table XI-4 Requesting delay Clear access vs. TOR / DNS	157
Table XI-5 Downloading delay Clear access vs. TOR and OVPN / DNS.....	158
Table XI-6 Requesting delay Clear access vs. TOR and OVPN / DNS.....	159
Table XI-7 Downloading delay Clear access vs. TOR and OVPN / DNS.....	159
Table XI-8 Requesting delay Clear access vs. TOR and OVPN / DNS.....	159
Table XI-9 Downloading delay TOR vs. TOR and OVPN / DNS.....	160
Table XI-10 Requesting delay TOR vs. TOR and OVPN / DNS	160
Table XI-11 Downloading delay TOR vs. TOR and OVPN / DNS.....	160
Table XI-12 Requesting delay TOR vs. TOR and OVPN / DNS	160
Table XI-13 Downloading delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS.....	162
Table XI-14 Requesting delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS.....	163
Table XI-15 Downloading delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS.....	163
Table XI-16 Requesting delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS.....	163
Table XI-17 Distance to Europe's centre.....	163

CHARTS INDEX

Chart 2-1 TOR's users chart (taken from [22])	23
Chart 2-2 TOR's users chart (taken from [22]).....	23
Chart 4-1 Bar Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN.....	96
Chart 4-2 Bar Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN.....	96
Chart 4-3 Bar Chart Delay vs. Distance	97
Chart 4-4 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection	97
Chart 4-5 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection	98
Chart 4-6 Bar Chart Requesting delay Clear access vs. TOR / DNS	98
Chart 4-7 Bar Chart Downloading delay Clear access vs. TOR vs. TOR and OVPN	99
Chart 4-8 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN	99
Chart VII-1 Line Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN.....	140
Chart VII-2 Line Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN	140
Chart VII-3 Line Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN.....	141
Chart VII-4 Line Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN	141
Chart VII-5 Bar Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN	141
Chart VII-6 Bar Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN.....	142
Chart VIII-1 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection	146
Chart VIII-2 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection ...	146
Chart VIII-3 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection	147
Chart VIII-4 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection ...	147
Chart VIII-5 Bar Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection .	147
Chart VIII-6 Bar Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection.....	148
Chart IX-1 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN.....	152
Chart IX-2 Line Chart Requesting delay NO DNS vs. DNS / TOR and OVPN.....	152
Chart IX-3 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN.....	153
Chart IX-4 Line Chart Requesting delay NO DNS vs. DNS / TOR and OVPN.....	153
Chart IX-5 Bar Chart Downloading delay NO DNS vs. DNS / TOR and OVPN	153
Chart IX-6 Bar Chart Requesting delay NO DNS vs. DNS / TOR and OVPN	154
Chart XI-1 Bar Chart Downloading delay Clear access vs. TOR / DNS	157
Chart XI-2 Bar Chart Requesting delay Clear access vs. TOR / DNS.....	157
Chart XI-3 Bar Chart Downloading delay Clear access vs. TOR / DNS	158
Chart XI-4 Bar Chart Requesting delay Clear access vs. TOR / DNS.....	158
Chart XI-5 Bar Chart Downloading delay Clear access vs. TOR vs. TOR and OVPN.....	161
Chart XI-6 Bar Chart Requesting delay TOR vs. TOR and OVPN / DNS	161
Chart XI-7 Bar Chart Downloading delay TOR vs. TOR and OVPN / DNS	162

Chart XI-8 Bar Chart Requesting delay TOR vs. TOR and OVPN / DNS	162
Chart XI-9 Bar Chart delay vs. Distance.....	164

EQUATIONS INDEX

Equation 4-1 Power101

Equation 4-2 Life's expectancy101

1 INTRODUCTION & OBJECTIVES

1.1 Motivation

1.1.1 Introduction

Since its release to the whole world, Internet has become the first communication system. Its capabilities have created a new universe which mixes reality with virtual reality. Marketing companies, governments even organized crime; no one is blind to this goldmine. The amount of information carried is priceless and it is one of the nowadays biggest sources of power.

In this line, Internet value has led to many attempts to control the net traffic and the same to evade that surveillance. Control supporters claim for security, while its opponents, for privacy. The thin line that divides them move backward and forward every day, as new policies are approved or new ways of deception appear.

Within this controversy, communication services struggle to guarantee and to protect the access and the use of the net. Known as CIA triad (or AIC triad), a series of policies categorizes the areas that IT security must defend in order to provide a fast, reliable and safe exchange of information [1].

Due to the complexity of computer networks, in 2002 Donn Parker proposed a wider classification, adding three new properties to focus on; thus, the final classification would be divided into six different groups [2]:

- 1. Authenticity**
It is in charge of proving servers' or clients' identity.
- 2. Availability**
User's communication services disposal at any time and circumstance.
- 3. Confidentiality**
Access right reserved for transmitter and receiver.
- 4. Control**
Any packet lost is susceptible of being decrypted or used.
- 5. Integrity**
Information must not be modified during the exchange.
- 6. Utility**
Unreachable resources or information are useless.

Not only must the system be reliable, but people do. In spite of the office IT, in a common network, human beings are placed at opposite sides. Usually, in order to summarize, the whole process

is reducing into five relay points: the transmitter and receiver people, their net access devices and Internet (Figure 1-1).



Figure 1-1 Basic Internet's topology (edited from [3])

This project is focus on preserving the data system against potential threats to its privacy. The aim will be encrypting the messages and tunnelling them to the extreme points. Thus, the track would be hidden so packets filled with sensitive information would be mixed up with worthless ones.

1.1.2 Hackers

In addition to the properties of the system, is essential to define who it is confronted with and what they are searching for. As it is mentioned before, there are many corporations involved. It does not matter whether they are criminals or just companies; these organizations seek their own benefit.

According to the damage of their action, they will be harmless o dangerous to the user. The so-called hackers are mostly cyberspace experts which use malware (malicious software) to perform attacks. Although there are various types of hackers regarding on their level or their objectives [4], like ethic hackers which play their knowledge to analyse and to fix security leaks, from this section on, the term “hacker” will be used to refer to dangerous ones.

On the other side, the new trend to raise the number of sales is denominated “Group profiling” [5]. A compilation of algorithms studies the patterns of traffic of a specific user, finding out what is suitable for him to be purchased. Then, advertises fill the pages’ gaps, even pop up, just to increase users hunger for buying. As moral values around the data mining are being constantly assessed, it will be considered in this project denying that correlation.

Once the menace is settled it will be easier to limit their lines of action. General classifications overlap virus categories attributing more than one vector of attack. However, they will only be taken into account those related with confidentiality breaches [6]:

- **Eavesdropping**
Both wired and wireless telecommunications interceptions by a third party.
- **Backdoors**
Free access guaranteed without filtering or authentication procedures.
- **Malware**
Any kind of software designed to infect IT devices stealing information or resources.
- **DDoS Attacks**
It refers to denial of service by means of, for example, requesting blitz.
- **Ransomware**
Data seized, normally vital for a company, until ransom is delivered.
- **Social engineering & Data mining**
Manipulation of people to get access to private knowledge.

The most likely irruptions that could be perpetrated, related to this project, would be monitoring client’s activity or intercepting data and decrypting it. Assuming these targets, it only remains to determine where they might take place.

1.1.3 A brief look into Internet's framework

In spite of registering daily billions of web browser searches, social network posts or emails sent, a large number of users have little idea of how does Internet really works [7] [8] [9]. Probably, they would be surprised if they knew that the operational principle is the same as the two-plastic cup thread connected phone's one. Obviously, it is much more complex than that, but it does constitute a good approach to the entire spider web made of nodes and cables.

Communication is compound by a bits flow which carries requests or messages across a long way of processors, buffers, wires, routers and so on. Because of every single relaying device follows its specific algorithm language, protocols are necessary in the translation and the understanding among machines.

Internet architecture is structured by five stories denominated layers and protocols [10]. Highest levels (Figure 1-2) control the interfaces human-machine displaying the information in a screen. Routers and switchers, at the bottom, are in charge of finding out and choosing the best route.

Computers, on both sides of the picture, are the server and the client's station. Last one, the centre cloud symbolizes the net, in other words, all the electronic systems interconnected.

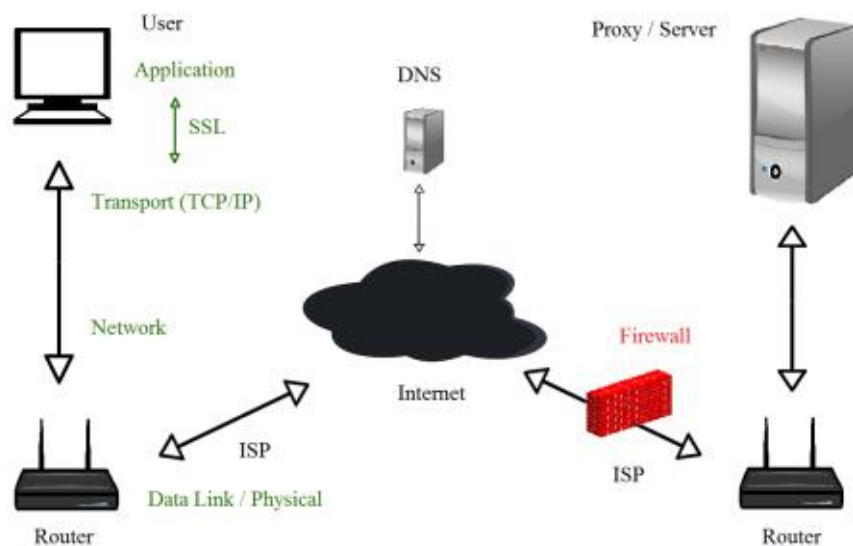


Figure 1-2 Internet's Framework (edited from [3])

Concerning the designing of the safe hotspot, it will consider that once the packets come across the gateway heading to the server they are safe. Therefore, risk zones start at the workstation and finish at the access point (Figure 1-3). All the same, TOR net has limits, what forces to know them to avoid possible leaks.

1.1.4 Encrypting and tunnelling

The principal method will be virtual private networks (VPNs). In this manner, the link remains concealed below the Internet surface. In addition, messages will be encrypted by private and public keys sheltering the conversation between transmitting device and the access point (Figure 1-3).

VPN's are based on virtual circuits built on logical nodes and virtual paths (VPs). Gateways are in charge of overlaying the packets and guarding the tunnel. They filter incoming packets by encapsulating them into new IP (Internet Protocol) heading addresses, with their own private keys [11]. As long as VPN's select a trustworthy path eavesdroppers will not be able to reach to any packet.

Meanwhile, symmetric keys and certifications are produced by the Secure Socket Layer protocol (SSL) which resides above the TCP/IP and below the HTTP (Hyper Text Transfer Protocol) protocols (Figure 1-2). By means of their public keys and a certification authority, SSL identifies servers and generates a safe shared password [12].

The Onion Router project (TOR) joins together both pieces of software. However, this application has some leaks that will be studied, and it will be assisted by other programs such antivirus or firewalls. Moreover, connection between the users' station and hotspot are clear and out of TOR limits what creates the necessity of a third VPN between those devices. A wider view of all these elements will be cover later on, in the State of the art section.

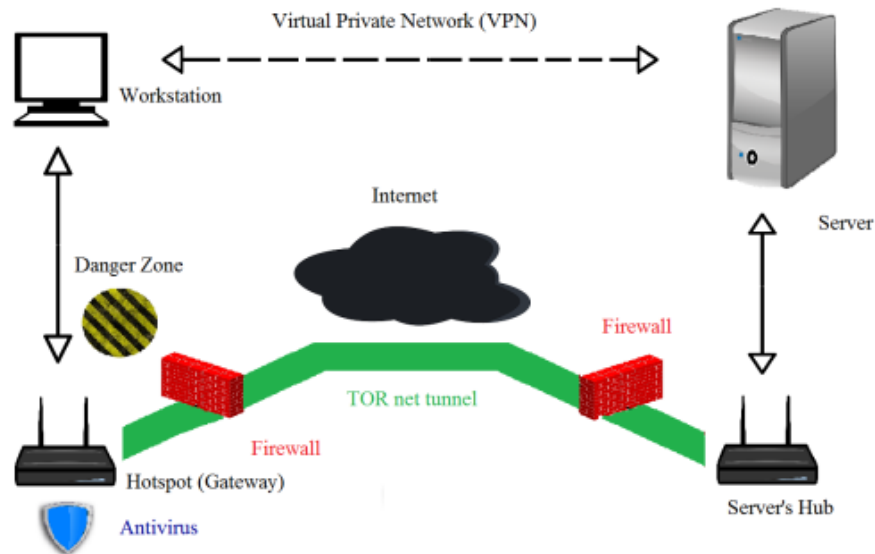


Figure 1-3 VPN and TOR's tunnels illustration (edited from [3])

1.2 Objectives

The main objective of this project will be producing portable device able to anonymize all workstation's traffic through a virtual private connection. It must include a proper antivirus and a firewall to secure gateways to the tunnel and the communication with the workstation.

This device will be a Raspberry Pi, acting as a hotspot, equipped with the material exposed in section 1.3. There will be two different VPNs; one will be based on TOR, to communicate with the WAN (Wide Area Network), and the other, in OpenVPN to guard the LAN (Local Area Network). Wireless access will be WPA2 (Wi-Fi Protected Access) protected. Antivirus and firewalls will have to filter and to process the incoming and outgoing data.

Finally, the user must experience seamlessly web navigation. Therefore, navigation speed must be in accordance with the standard for a fluid exchange of information.

1.3 Resources

1.3.1 Initial material

The material used will be:

- A Raspberry Pi 2 Model B (Figure 1-4)
 - CPU: 900 MHz ARM Quad-Core
 - RAM: 1 GB
 - GPU: Broadcom Video Core IV

- Inputs/Outputs:
 - 4 x USB 2.0
 - 1 x HDMI
 - 1 x Ethernet
 - 1 x MicroSD
 - 1x Audio Jack
- Dimensions (W x D x H): 12.7 x 10.2 x 7.6 cm
- Weight: 136 g



Figure 1-4 Raspberry Pi 2B

- An 8 GB MicroSD
- An AC Adapter
 - Model No.: ANU-050200A
 - Input: 100-240 V AC 0.3 A
 - Working frequency: 50/60 Hz
 - Output: 5 V (2000 mA)
- A TP Link Wireless (Adapter Figure 1-6):
 - Model No: TL-WN823N
 - Dimensions (W x D x H): 39 x 18.35 x 7.87 mm
 - Frequency Range: 2.4 – 2.4835 GHz
 - Chipset: 8192cu
 - Speed: 300 Mbps
- Wireless Raspberry Pi Adapter (Figure 1-6):
 - Model No.: 2ABCB-WLU6331
 - Dimensions (W x D x H): 29.5 x 16.2 x 8.35 mm
 - Frequency Range: 2.412 – 2.462 GHz
 - Chipset: brcmfmac
 - Speed: 150 Mbps
- Ethernet cable
- Battery
 - Power: 13000 mAh / 48.1 Wh

- Outputs and Inputs:
 - iSmart USB 1 (2.1 A)
 - Micro-USB Input (2 A)
 - iSmart USB Output 2 (2.4 A)

1.3.2 Software and programs

- SDFormatter [13]
- Win32DiskImager [14]
- Raspbian Jessie Lite OS [15]
- Putty & VNC [16] [17]
- OpenVPN [18]
- ClamAV Antivirus [19]
- Wireshark [20]

1.3.3 Workstations

In order to check hotspot service next stations has been included into the process:

- Acer Aspire
 - Model No.: AS-5749
 - OS: Windows 7 Home Premium 64 bits version 6.1
 - Compilation version: 7601
 - CPU: Intel Core i3-2350M
 - GPU: Intel HD Graphics 3000
 - Storage: 500 GB HDD
 - RAM: 4GB DDR3
 - Integrated Wireless card: Acer Nplify 802.11 b/g/n
- Galaxy S5 Neo smartphone
 - Model No.: SM-G903F
 - OS: Android version 6.0.1
 - Kernel version: 3.10.61-8140803
 - Storage: 16 GB
 - RAM: 2 GB
- Samsung Galaxy Tab A
 - Model No.: SM-T555
 - OS: Android version 6.0.1
 - Kernel version: 3.10.49-7931139
 - Storage: 16 GB
 - RAM: 2 GB

1.3.4 Additional material

During the realization of the project the following instruments has been acquired to check possible alternatives and better outputs:

- A Raspberry Pi 3 Model B (Figure 1-5)
 - CPU: 1.2 GHz ARM Quad-Core
 - RAM: 1 GB
 - Inputs/Outputs
 - 4 x USB 2.0
 - 1 x HDMI

- 1 x Ethernet
- 1 x MicroSD
- 1x Audio Jack
- Integrated Wi-Fi BCM2387 chipset
 - Frequency Range: 2.400 – 2.4835 GHz



Figure 1-5 Raspberry Pi 3 Model B

- A 16 GB MicroSD
- An AC Adapter
 - Model No: ANU-050300A
 - Input: 100-240 V AC 0.3 A
 - 50/60 Hz
 - Output: 5 V (3000 mA)
- 2 Raspberry Pi cases



Figure 1-6 Both Raspberry Pi and adapters

1.4 Structure of the document

The document is divided into 5 sections:

1. Introduction:

Preface of the issue of this project, as well as a brief look into internet's structure and cybercriminals (hackers). This part includes the objective that is pretended to achieve and the resources employed to do it.

2. State of the art:

Study of current applications and software developed in order to increase both communication and cyber security. Moreover, the most common malware and tracking gadgets and algorithms are analysed to discern the threat axis.

3. Development:

In this section hotspot is set up. A small tutorial explains through a number of steps how to turn a Raspberry Pi into a safe gateway to Internet. It starts from a blank Raspberry Pi which eventually will become a small useful gadget to grant clients LAN secure connection wherever they carry it.

4. Testing:

The fourth part contains various reports to prove hotspot features and performance. Speed, anonymous level or security, among other characteristics, are checked to show the device capability to accomplish the aim that it was designed for.

5. Conclusion:

The last section contains a summary and conclusions of the whole process. Results on section four are assessed determining whether they are successful, acceptable or inadmissible. It also draws guidelines pointing for future improvements and scope of application.

2 STATE OF THE ART

2.1 Introduction

After the big impact of Edward Snowden's disclosures (June 2013 [21]), the self-consciousness about Internet privacy has decreased. Yet, the insight in security methods and the use of untracking applications are higher than before the CIA agent's revelations (Chart 2-1 and Chart 2-2).

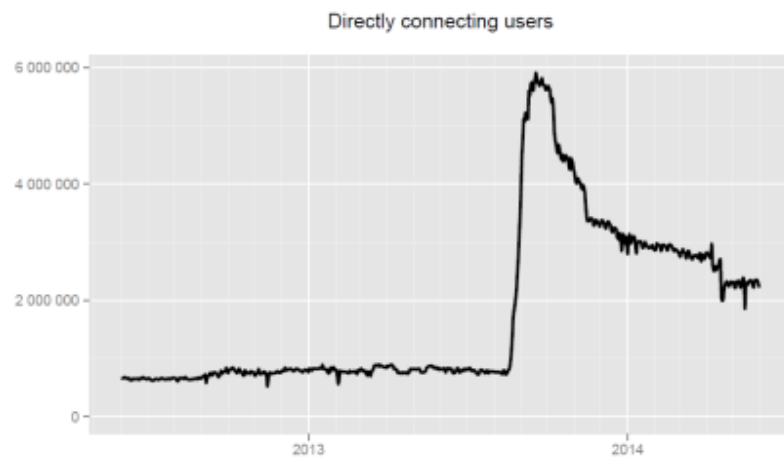


Chart 2-1 TOR's users chart (taken from [22])

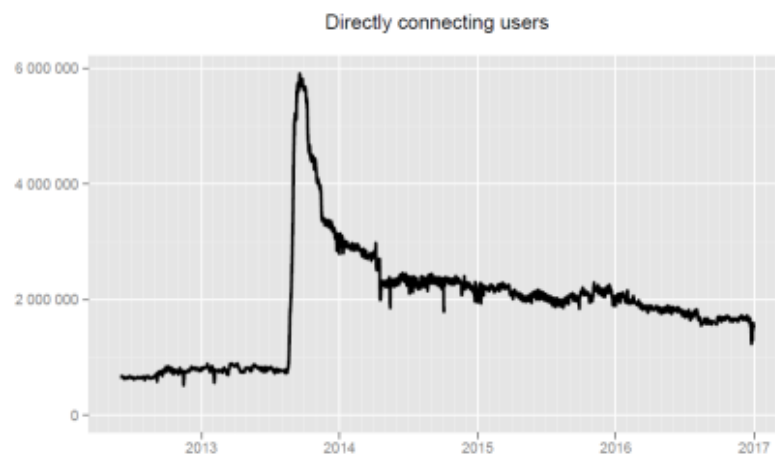


Chart 2-2 TOR's users chart (taken from [22])

In this section those applications will be reviewed together with current protection software as well as monitoring and hazardous malware. Given the huge number of tools conceived to both aims, they will just take into account the most suitable ones to be fitted into the hotspot.

Likewise, the introduction to the project, general concepts will open the topic, followed by malware and finishing enumerating the untracking tools to protect the system. Figure 2-1 serves as a preview of what is expected hotspot to look like.

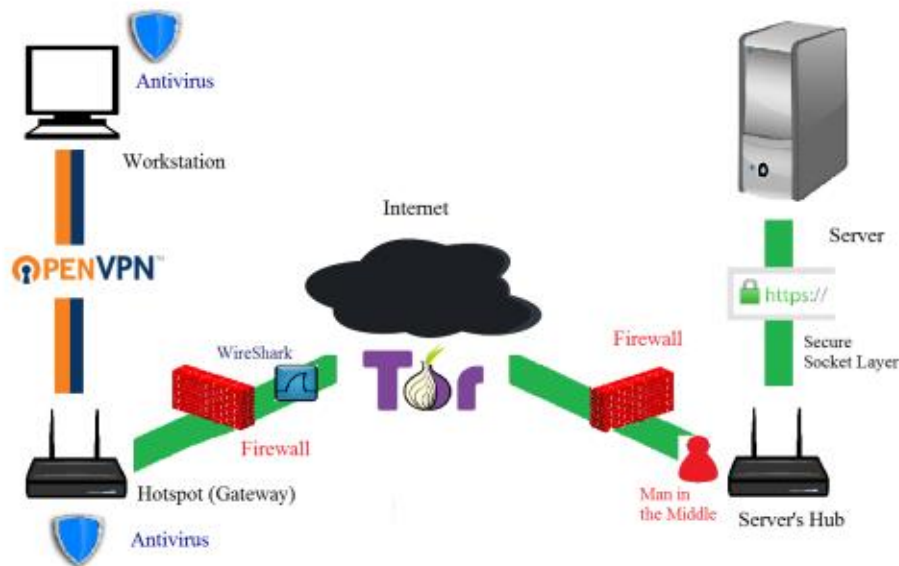


Figure 2-1 Preview of malware and safety devices (edited from [3])

2.2 Raspberry Pi as a router

2.2.1 Router

Interconnections between WAN and stations are controlled by bridges called Routers. They generate local area networks (LAN) being able to forward packets, filtering and dropping them regarding on custom rules [23] [24] [25].



Figure 2-2 Image of a router (taken from [26])

Apart from those functions routers (Figure 2-2), usually, communicate stations wireless and wired. NAT (Network Address Translation) is the most important routers' protocol. It is in charge of linking local IP addresses with the external ones [27]. Owing to routers' capabilities types are:

- **Brouter**
Bridge Router

- **Core router**
Internal Network Router
- **Edge router**
Entrance to the Network's Core
- **Virtual router**
Protocol to prevent network downtime
- **Wireless router**
Access point

Among all of them, hotspot will act as wireless router providing an interface for LAN access and other to WAN. IP tables are a compilation of rules that manage the packets transfer (Figure 2-3). IP tables' rules are Filter, NAT, Mangle and Raw [28]:

- **Filter Table:**
It performs the firewall's purpose making decisions about dropping or redirecting packets.
- **NAT Table:**
It implements network address translation modifying sources and destinations.
- **Mangle Table:**
It alters IP header according to the route.
- **Raw Table:**
Its mission is to relate packets to deliver them in order.

Forwarding flow goes across tables a couple of times, but each time is different, as they pull triggers according to the step of the process [28]:

- Prerouting
- Input
- Forward
- Output
- Postrouting

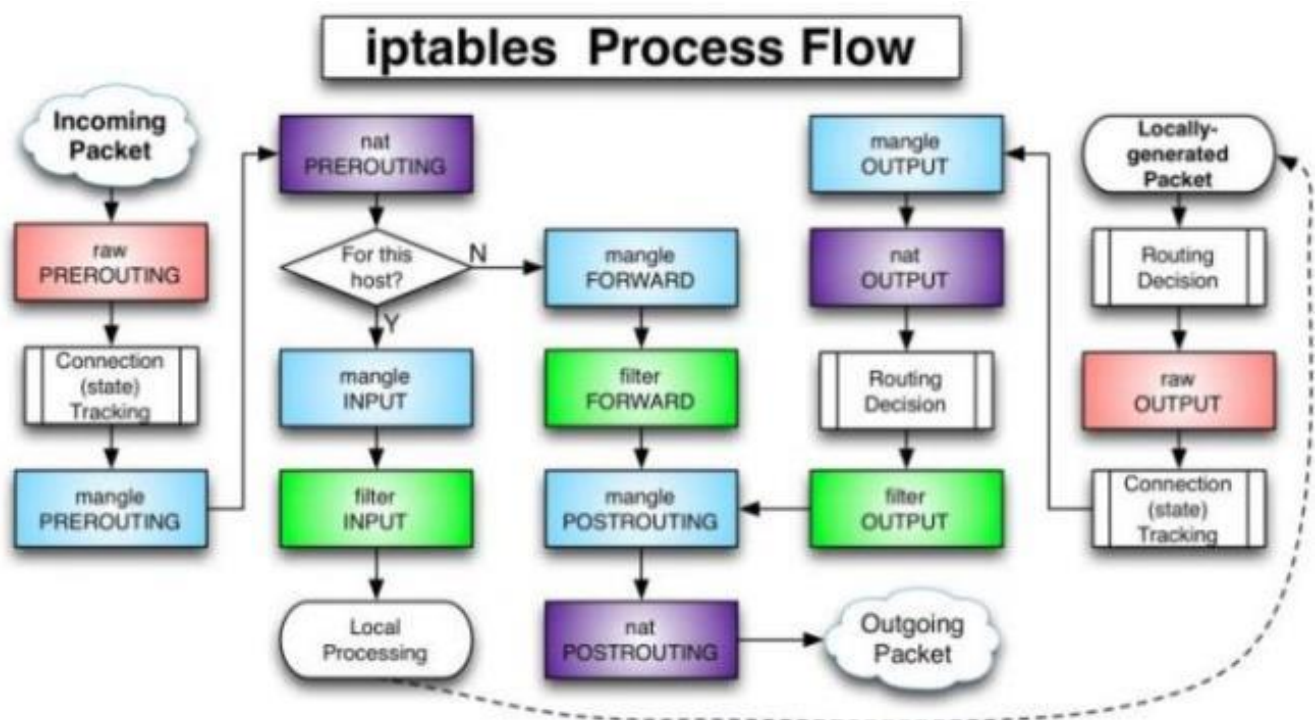


Figure 2-3 IP tables process flow (taken from [28])

2.2.2 Raspberry Pi [29]

Raspberry Pi Foundation is an educational charity dedicated in advancing electronic field knowledge. Offering a low-cost computer boards, that can process a wide ranging of activities from a traditional computer desktop to an automatic robot.

Raspberry Pi foundation defines a Raspberry Pi as a small and cheap computer designed to smooth the programming world entrance way to people in general, and youngsters in particular. Featuring countless functions Raspberry Pi takes part in the supplying of the huge demand of new programmers.

Powered by an USB phone charger, run by an OS MicroSD and displayed on a screen support the education and the acquisition of new skills. Moreover, it is employed worldwide within multitude of experiments, studies and research [30].

Networks' overview picks basic and challenging Raspbian coding. Although Raspberry Pi Foundation gives little practical concepts, there is a large number of contributors releasing new projects [31]. Raspberry Pi principal virtue is that it does not matter first version of the project is perfect. Popular applications and experiments will soon gain fans which makes their own versions reaching to a polished one.



Figure 2-4 Raspberry Pi Router (taken from [32])

With reference to a Raspberry Pi acting as a router (Figure 2-4) there are a couple of tutorials and discussions about replacing home hotspots or creating an anonymous redirection access point [33]. Whether they work joint or separated and number and types of interfaces will be debated in Settings' section.

2.2.2.1 Secure Shell (SSH) [34]

Most common ways to manage Raspberry Pi are through a monitor or a SSH connection. Secure Shell control remote login through a strong encryption inside an insecure network. It works as Secure Socket Layer protocol, but on the Transport layer.

SSH authentication set is less complex than SSL because it involves fewer machines. For this reason, working methods will be explained in SSL's section (2.4.3).

2.3 Malware & Intercepting devices

2.3.1 Network Analysis and Man in the middle [35]

Network analysis or Sniffing is the process of monitoring, seizing packets and study the patterns of traffic. Despite that experts could get information directly from packets, it would be a slow process as to do it manually. As a result, there are programs prepared to decode data and to display it in a readable format.

Similarly, a man-in-the-middle attack names net broken into attempts. This fact is exploited by eavesdroppers to intercept packets of information: who could even modify it or steal our identity. Data

modification, spoofing or ransomware, for example, are kinds of attacks related to this issue, thus they will be studied, henceforward, as a whole.

Leading the ranking of hardware tracking system correspond to TEMPEST while software one to Wireshark. Both were planned to reveal electromagnetic emanations leaks and system failures, but eventually were also dedicated to sniffing purposes. They will represent attacks produced in its fields.

2.3.1.1 TEMPEST

In the last decade, some nations' armed forces have implanted measures to enclose electromagnetic leaks [36] [37] [38]. Emanations originated by IT devices are susceptible of being intercepted and easily reconstructed. These leaks are known by the name of TEMPEST. The term come from the late 1960s by the US government, it was a code word which, apparently, stand for Telecommunications Electronics Material Protected Emanating Spurious Transmissions [39].

TEMPEST is also used to refer the techniques which try to prevent electromagnetic interception. In spite of the fact that defending methods are neither cheap nor easy installed (except for the image processing software), electromagnetic field is not simple place for newbies to act. Actually, TEMPEST is mostly use to study the emanations of an equipment to discover where might fail (Figure 2-5).

	Method	Purpose
Hardware	filter/adapter	prevention of emanation from parts (USB, serial connector etc) of IT devices
	infrastructure	prevention of emanation from the buildings or rooms (e.g. shielded room)
	jamming	interception of the receiving by generating another emanation
Software	image processing	transformation of images which does not generate strong emanation (e.g. TEMPEST fonts [12])

Figure 2-5 TEMPEST's protection methods (taken from [40])

Nowadays high likely compromised victims are credit cards' chips. Even inside a wallet carried in a handbag or in a pocket, easy payment can be misled by small wireless devices, which cross near to it, to pay fake bills. This constitutes just one example from the famous Internet of Things [41], which is becoming threatened by electromagnetic energy gatherers. Emanations can be divided regarding the leaks' whereabouts [42]:

- 1. Electromagnetic emanations through radio**

Devices which carry radio emitters like mobile phones can irradiate radio waves which hold relevant information.

- 2. Electromagnetic crosstalks**

Describes gaps occurred within a conversation or exchange of information between electronic gadgets.

- 3. Electromagnetic emanations through keyboards**

- 4. Electromagnetic emanations through video**

Three and four can be mix up into wire emanations, when the travel data that run through it is freed to the surrounding space.

At any rate, out of credit cards vulnerabilities, larger stations will be just exposed toward medium size antennas and low interferences spaces. As caricatured in Figure 2-6, hacker equipment would be noticeable.



Figure 2-6 TEMPESTING cartoon example (taken from [43])

On account of these methods to steal data, would be Raspberry Pi hotspot a possible target? Focusing on the idea of portability, it should not. As remarked in the objectives hotspot is meant to provide a safe and anonymous navigation anywhere, then, and supposing users will not be under vigilance, there will not be reasons to believe that the access point would be threaten. Anyhow, section 2.3.4 goes deep into what really suppose a menace and what do not.

2.3.1.2 Wireshark [44]

Wireshark is open source network analyser design to interpret traffic and to present it in a graphic interface unit. Spreaded on Internet, there can be found multitude of similar applications, nevertheless, Wireshark is actively maintained, free and has a large collection of authors.

Wireshark first came to the world with the name of Ethereal in 1997 by the hand of Gerald Combs, although it was not released until July 1998 due to troubleshooting. Progressive growth has permitted to gain compatibility with a long list of snooping programs format (like Tcpdump, Novel LANalyzer or Catapult DCT2000).

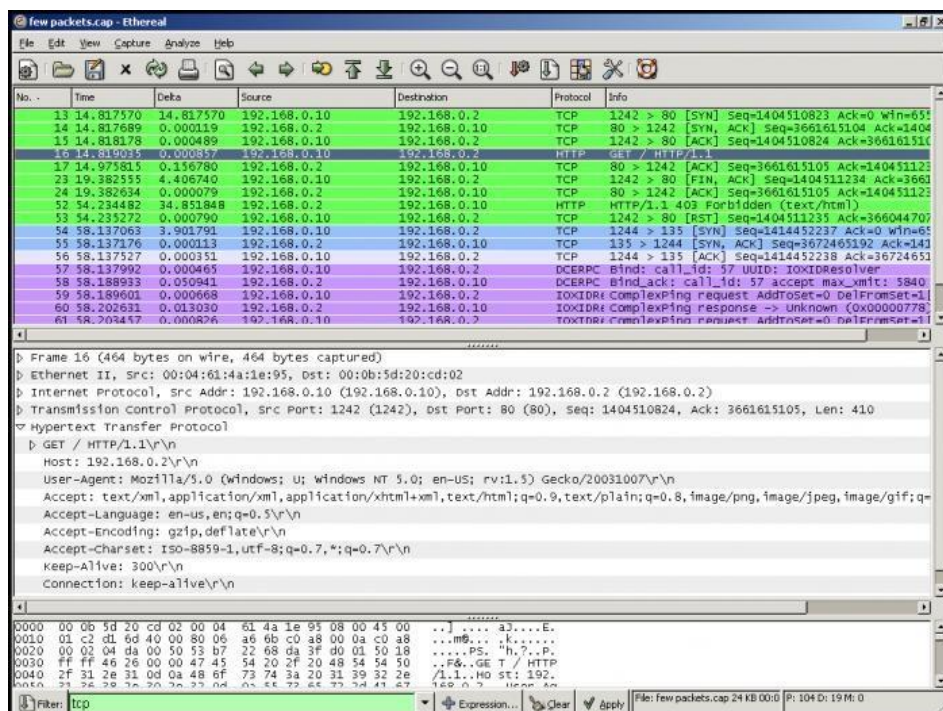


Figure 2-7 Wireshark's interface (taken from [26])

As shown in Figure 2-7, packets are divided by protocol and they point to the final address. Then, filtering valuable information is just a matter of IP translation (in other words, finding out what IP's

correspond to bank webpages, social networks or email accounts) and decoding, or even sending the same packets to impersonate client's identity.

2.3.2 Viruses

Worldwide feared as the IT nemesis, viruses infect machines altering their normal mode of functioning. Threat vectors vary from physical inputs, like usb ports, to virtual entrance doors, like e-mails or P2P programs. Viruses are a form of mobile code which reproduce themselves and execute harmful processes in our computers [45].

Usually, viruses come attached to documents or executing files; therefore, by the time they are executed, the malicious software spread itself infecting as many documents as antivirus let it. It does not always blow as soon as they are activated; some of them remain concealed because their objective requires discretion (Ransomware or Backdoors), or just because their trigger is a specific action or in a specific date (Logic bombs) [6].



Figure 2-8 Cluster of viruses related concepts (taken from [26])

As biological viruses, they have become an enormous problem of difficult solution. There is a saying which asserts that everything that falls on Internet is impossible to delete it. From what can be inferred that, any malware that has been ever produced has a host and every host has a virus. Following the example of biological virus, being infected is not a synonym of being ill. Host might not endure the consequences of hosting a virus, either for its antivirus protection or just because virus has another target, but it can transfer malware to computers less prepared to face them.

Viruses' classifications differ according to host's requirement, spreading capabilities or damage caused. Before selecting the most critical for the Raspberry Pi hotspot, well-known ones are listed below [6] (Figure 2-8):

- **Viruses**
Variable codes as commented before. Normally, they modify or take control of some documents.
- **Worms**
They stand out for replicate automatically and reproduce themselves to consume host's resources. They can use those resources for carrying DDoS [attacks] (Denegation of Service).
Worms are subdivided as regards their way of work in categories such mail worms or rabbits.
- **Logic bombs**
These are the stealthy malware mentioned before. They wait until a legitimate application performs its detonator. This trigger might be a number of files inside a folder; when the users save that amount all the files will be deleted.

As the majority of viruses they can be assigned to useful functions. Last case, for example, could be motioned to free some space.

- **Trojan horses**

Perhaps the simplest malware. Copying the wooden horse which names it, they attract their victims with outstanding tools or even camouflaging their code on a real application.

Most dangerous Trojans are password-stealing and backdoors. Password-stealing principle is similar to Phishing (2.3.3) they disguise as common applications to deceive users inviting them to introduce their credentials. Meanwhile, backdoors allow remote access without firewall filtering.

Conspiracy theories affirm that all devices come with backdoors preinstalled, either for a government control or big companies. Whether is real or not, Trojan horses will not be covered by the safe hotspot been designed, as they appeal to user innocence. However, through the whole statement will be treated as to reduce their probability of success.

- **Germes**

First generation of viruses. They do not suppose a real menace.

- **Exploits**

They are often set to expose concrete vulnerabilities. It is an example of the ethic hack discussed in the introduction.

- **Downloaders**

They download and install a share of programs in the host. It does not have to be malicious content; for example, P2P programs could set a Downloader in a Trojan horse, then as it is sent and executed for another user it would download contents from the first one, in this way the first user can save its material elsewhere.

- **Spam**

Unbearable list of e-mails. It refers to commercial and malicious adverts blitzing clients' email accounts. They are not such harmful except from the viruses they can have attached and the denial of service they can generate by consuming servers' resources.

Outside of this enumeration they have been left Ransomware and Botnets. Ransomware refers to information locked by cryptographic algorithms made by hijackers, who ask for a ransom to decrypt it. Whereas Botnets, to nets of unmanned computers which commit singular attacks, as DDoS. They deserve a deeper background to determine the degree of the threat.

2.3.2.1 Ransomware

One of the most profitable malware, ransomware locks computers through a law enforcement impersonation to intimidate users. Most common hoax consists in blocking the system and displaying a warning (with seals of government law departments) claiming users having been detected of possessing or distributing illegal material (

Figure 2-9). It charges the user with an affordable fine but urges him to pay; otherwise, he will be arrested. Within confusion and fear many victims pay the ransom.

Once more viruses, phishing, resource denial, social engineering, and so on are mix up in a single action. What really characterizes ransomware is the barrier that block out the information. More aggressive attempts aim to small companies, being a crypto locker algorithm their only weapon. Those companies do not want to put valuable files at risk so instead of reporting it, they pay the ransom.



Figure 2-9 Four examples of screen locking (taken from [46])

The Ransomware boom exploded in 2012 [46], likely motivated by Megaupload website closure [47], which contributes to raise fears related with infringing copyrights. Being aware of these kinds of danger would have prevented victims of falling in the trap.



Figure 2-10 Increase of ransomware success (taken from [48])

The success rate still its upward trend (Figure 2-10), though the increase is not as big taking into account that Internet users has also growth (half a billion in the last two years, [49]). Regarding the security of the hotspot its danger will come determined by its capabilities to restrict the access to key files, which beforehand will be the certificates and the IP tables. Yet, as long as hotspot accomplishes its function it can be stated that communications are safe.

Noted ransomware applications are Cryptowall, TorrentLocker, CTB-Locker and TeslaCrypt. Vector attacks are infected USBs, e-mails and non-safety web pages. A normal navigation, an updated antivirus and a firewall should be more than sufficient to avoid users' data to be captured. Anyhow, under no circumstance, whenever workstation or hotspot would infect, will ransom be paid. If that happened first antivirus and cleaners must be applied to try to erase the virus. In case of failing, hotspot would be easily and quickly formatted and reconfigure. Meanwhile, workstation would be advisable to take it to a technician.

To conclude, encrypting applications are not to be marked just as harmful. Programs like Cryptowall can be employed to restrict the admission of a third party to clients' documents (Attached document I: Safety Measures).

2.3.2.2 DDoS attacks (Botnets)

Recently, DNS's servers suffer a cyber-attack that brought down many webpages worldwide. Shown in Figure 1-2 DNS is crucial element of Internet, which translate IP directions to an understandable format for a person (Figure 2-11).

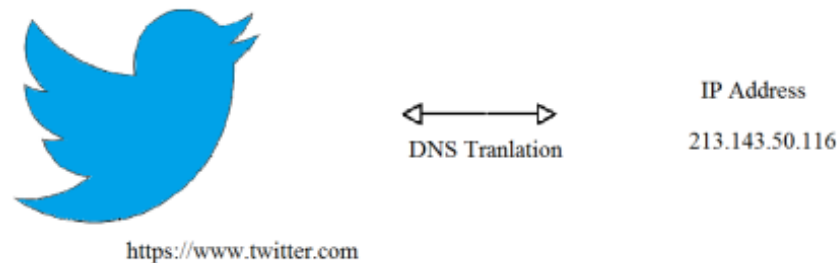


Figure 2-11 DNS Translation (edited from [3])

Although there are several servers distributed for the whole world, if more than one fell, the amount of directions to translate would be added to the others, slowing down the system which could even reach to collapse. It not must the DNS have big failures to cause a catastrophe, the only fact that users would have to go further DNS servers would reduce their navigation speed until an insufferable rate to continue.

As concerned to the subnet generated by the hotspot, there resides the first DDoS possible target. If hotspot is not able to traduce workstations' MACs (workstation personal address/ Media Address Control) addresses it would never communicate with them. Next are DNS official servers attacks, if ever exists any method to overcome them, it will be installed, though, DNS down servers last less than a day to get fixed [50].

Botnets are employed to execute those attacks. A Botnet is an army of zombie or infected computers which are remote controlled (Figure 2-12). Producing uncountable IP translations requests DNS servers will get overloaded and they will eventually fall. Another way to perform them is sending request spoofing DNS Server IP; as a result, they will generate response which will block it.

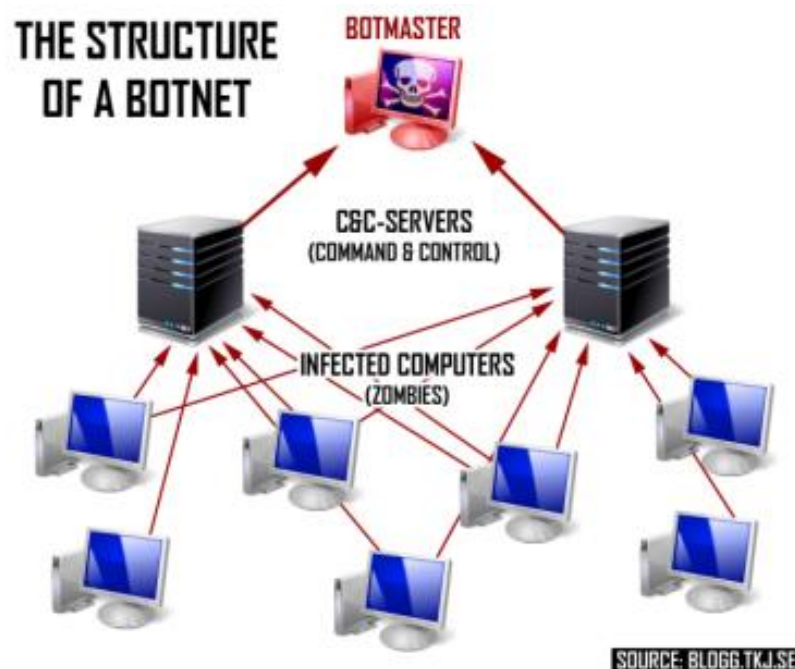


Figure 2-12 Example of a botnet (taken from [51])

2.3.2.3 Most dangerous Viruses

Viruses' Golden Age backs to the beginning of the millennium. Apart from ransomware, it has not appeared any critical virus in the recent years [52] [53]. Current emergence of IoT (Internet of Things), together with social networks, has given place to viral trends where an electronic device takes part [54] [55] [56]. Therefore, the new most attractive targets are all net connected electronic machines.

IoT encompasses from internal cars' Wi-Fi connection to electronic coffee machines. Almost every tool computer processed motioned is compromised to infections [57] [58] [59] making the matter change from what can a virus destroy to how can systems be secured [60].

To sum up, there is no specific measures against code transformation and documents altering virus as there is no a specific pattern. Every action take to protect the system will support virus defence.

2.3.3 Phishing [61]

Phishing attacks are worth of mention due to they will remain outside of hotspot's capabilities limits. Social engineering aims to the innocence and the predisposition to help of the human being. Hackers place spider webs carefully and wait for preys.

On one hand, there are offensive attacks in which hackers interact with the victim impersonating a confidence person or organization. Once trust is gained, the impostor will ask for personal and confidential data. Criminals will not only have the time between credentials have been got and the victim realized it, but also there is a period before reporting it because of the shame of having been fooled.

On the other hand, passive attacks rely on spam. They use the earlier mentioned spider webs in shape of fake web pages or links. Familiar looks are able to swindle naïve clients, often by promising rewards or incredible offers. Companies never will demand for credentials and will always address clients by their name to differ from spam, nevertheless, they send adverts weekly or monthly and covetousness will impede users discard them at a glance, giving place to a possible into trap falling.

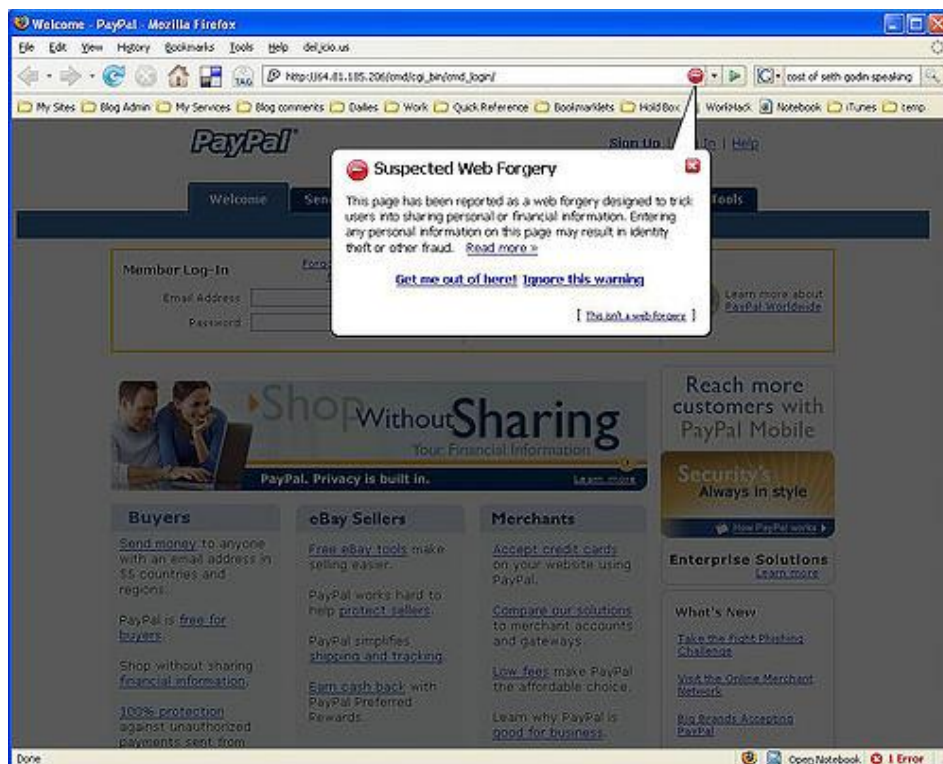


Figure 2-13 Example of phishing website (taken from [62])



Figure 2-14 Real PayPal website



Figure 2-15 PayPal's Certificate

Although home pages are totally different (take into account Figure 2-13 and Figure 2-14 have been shot within ten years of distance), familiar appearance feeds confusion. Concerning phishing, it has been created certificates authorities that confirm the identity of an organization. Figure 2-15 is an example of certificate security which is related to the Secure Socket Layer. Both of them are widely discussed in section 2.4.3.

In conclusion, these kinds of attacks can only be avoided by users. Less wary situations, where a fail is more probable, it is during a rush of activity paying less attention to secure precaution. However, antivirus and web browser usually register a list of suspicious codes and websites warning clients if they mistakenly enter on one of them.

2.3.4 Risks

Commonly, Security Agencies and Operational Security Departments classify risks according to the probability of suffering an attack and the damage they could commit. In the table here below (Table 2-1), degree of risk is highlighted in colours and depending on characteristics mentioned. Red stands for the higher one, green for the lowest and orange and yellow for medium risk.

Probability \ Damage	High	Medium	Low
High		Virus	
Medium	Wireshark	Phishing	
Low	Ransomware	TEMPEST	DDoS Attack

Table 2-1 Attack risks

Even though, anonymity would be granted blocking them, a misuse could compromise security. It should not be forgotten that, even providing a high degree of protection, hotspot is meant for hide navigation tracks. Giving personal data or use accounts (whether they are social networks or mails) is an invitation to chasers to link client's workstation to its traffic raising the curtain to leave everything uncovered.

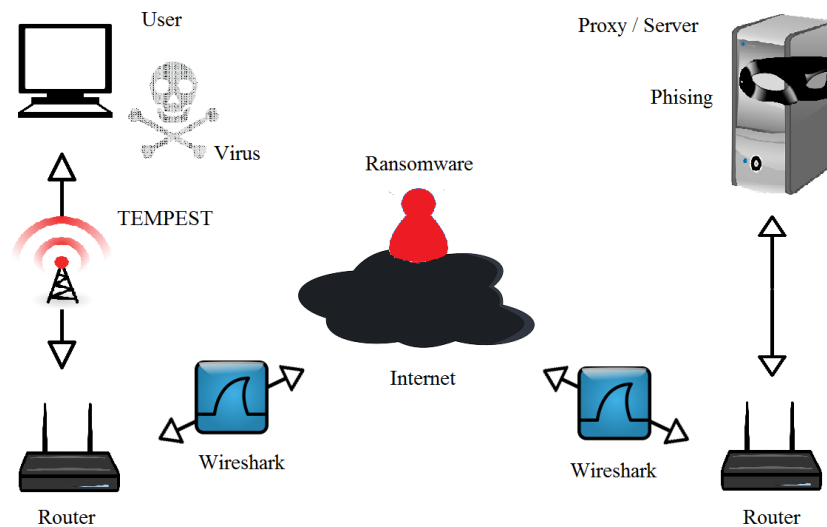


Figure 2-16 Malware summary (edited from [3])

All the same, it provides a high degree of sheltering which could be wasted. As far as public places are a nest for eavesdroppers and hackers (Figure 2-16), protecting users' information is highly recommended [63]. Thus, tips for surfing anonymous on the web will be written down separately as an optional profile of use.

2.4 Safe Untracking Programs & Devices

2.4.1 Defences against malware analysed

Program \ Attack	TEMPEST	Wireshark	Virus	Phishing
The Onion Router		Hiding route		No protection
SSL		Encryption	Warning	Authenticating
OpenVPN		Encryption		No protection
Antivirus	No protection	No protection	Killing processes	Warning
Firewall	No protection	No protection	Disabling links	Warning

Table 2-2 Protection software vs. probable attacks

With reference to risks (section 2.3.4) studied, and given the damage level, Wireshark monitoring and viruses will denote the most important prevention techniques. In Table 2-2, possible guarding software is analysed. Green highlighted boxes stand for strong protection, yellow ones, for hindering actions and red, for no protection at all. Crossed boxes means there is no significant data. Besides, it is included a word remark the cause.

Firstly, as presented in the same table, TOR provides the best defence against surveillance. Nevertheless, is a close concealing system because it just encrypts the information up to the last TOR node; like will be explained in the next section. OpenVPN also offers good features against monitoring. Therefore, it will joint TOR to shell the communications.

Secondly, Viruses will be covered by firewalls and antivirus. It is essential they are up to date and constantly updated to supply Raspberry with an inviolable wall. Thus, antivirus and firewalls adapted to Raspbian will be studied to get the one which fits the more.

Lastly, Wireless security (WPA2) and DNS server could back up those applications increasing the level of security and the speed respectively. To summarize, tests are to be carried out to check every system is contributing in the main mission of the hotspot.

2.4.2 TOR net and VPN's [64]

The Onion Router (TOR) is free software based on virtual connections built through physical bridges which conceals the real traffic. Its name refers to the layers that cover the original message.

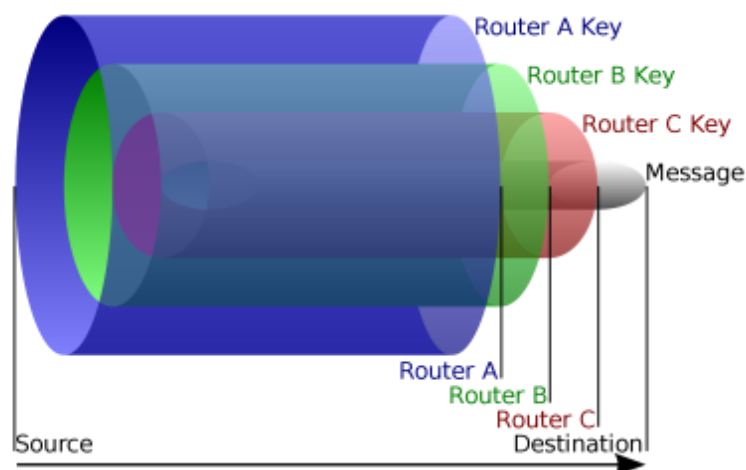


Figure 2-17 TOR Layers (taken from [65])

The gateway to TOR tunnel knows the nodes packets have to cross, thus it encrypts the message with every single key so each node will only be aware of the previous and next step (Figure 2-17). However, from last TOR node to the final destination communications are clear, unless SSL encapsulated packets, with the consequent dangers.

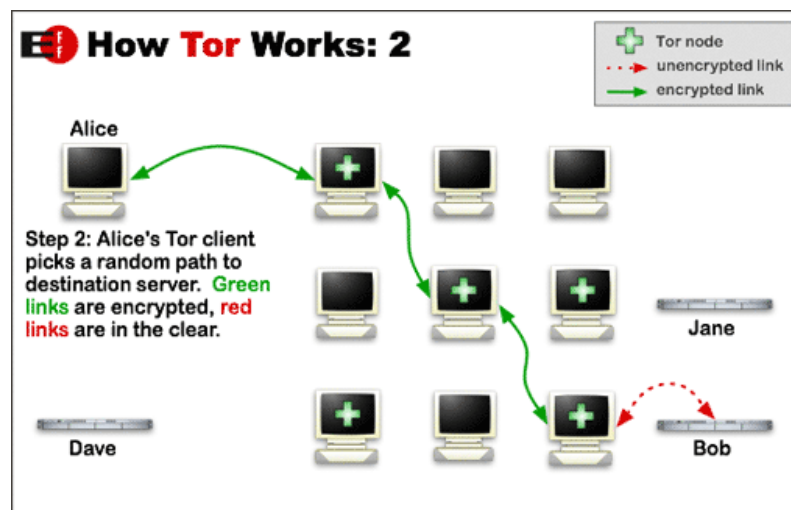


Figure 2-18 TOR's working mode (taken from [64])

First of all, a directory server (Dave in Figure 2-18) provides the user a list of Tor nodes. Next stage, client (Alice in Figure 2-18) will choose a random path opening a virtual private network (VPN). Once connection is settled, both users will encapsulate messages as if they were matryoshka dolls. Throughout the trajectory, each node will decode the message discovering a new destination

follow by another message (Figure 2-19). Minimum number of hops is three and connections last no more than ten minutes, approximately, in order to avoid monitoring.

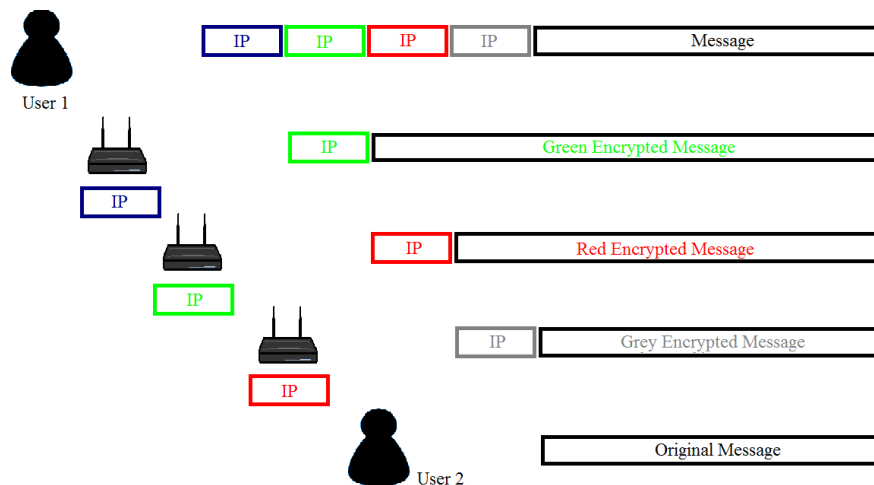


Figure 2-19 Relaying and decoding process (edited from [3])

Even though it is considered being among the best hiding track web browsers, it has some bugs that compromise its security [66]. Most of them depending on its correct employment, obliging to include navigation tips. They will be written down in Attached document I: Safety Measures, owing to leaks are also based on the TOR proxy chosen (Section 3.4).

2.4.3 SSL [12]

In February 1995, Netscape produced the Secure Socket Layer protocol, becoming the standard Internet protocol for securing communications. Placed below hypertext transfer protocol (HTTP) it invokes encryption protocol encoding information before plunging into TCP/IP layer (Figure 2-20).

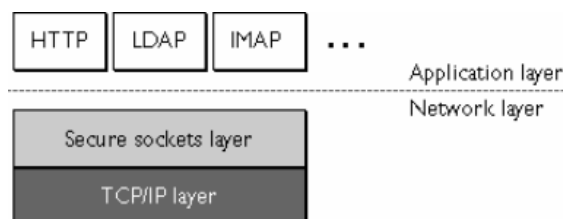


Figure 2-20 Location of SSL protocol layer (taken from [12])

SSL handshake and SSL record sub-protocols support SSL protocol. Together with the certificates they are in charge of establishing communications, choosing data format and authenticate the server (and, sometimes, client too), respectively.

Session will always start exchanging messages (SSL Handshake) allowing the server to authenticate itself using public keys. During the process server will generate a private key¹ for ciphering. It will be accompanied by the web's certificate, which will prove server's identity; otherwise, client would reject the link and would drop the key.

“Certificates are digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a specific public key does in fact belong to a specific individual [...]. As commonly used, a certificate also contains an expiration date, the name of the certifying authority that issued the certificate, a serial number, and perhaps other information.” [12]

¹ In Ph.D. William Stallings's book, Network and Internetwork security principles and practice, Chapters 4 and 5, the author expose public and private keys theory [124].

Concerning the level of validation and the number of subdomains certificates are classified in [67]:

- **Validation Level**
 - **Domain Validation**
It covers domain's ownership name registration
 - **Organization Validation**
It adds organization details
 - **Extended Validation**
Highest degree of authentication providing up to physical and legal identification
- **Number of subdomains**
 - **Single**
Just one domain
 - **Wildcard**
Principal domain and subdomains
 - **Multi-Domain**
Multiple domains not necessarily related

As far as concerned to the project, certificates will be procured by web servers. At any rate, it is mandatory to shell the Workstation-Hotspot's link; hence, certificates' issue will be resumed at OpenVPN server section (2.4.5).

2.4.4 Onion Pi [68]

Onion Pi TOR proxy is a project developed by Adafruit Learning System which consists on a transparent TOR proxy in charge of redirecting all the traffic through the TOR net (Figure 2-21). An access point acts as router Wi-Fi provider, while an Ethernet cable links the Raspberry Pi processed data with the Wide Area Network (WAN).

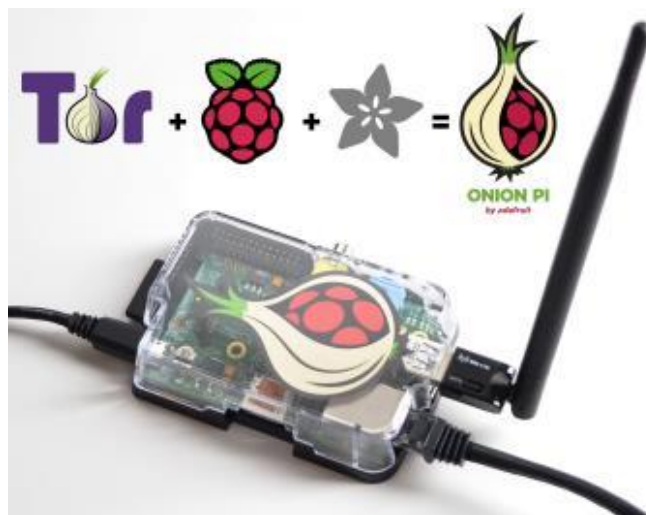


Figure 2-21 Onion Pi (take from [68])

At this point, it may arise the question is not this the hotspot which is being designed? It is, but, as is it highlighted at the end of the initial page of the configuration tutorial, the post was published on 2013/06/14 and last update was made on 2015/05/04. Raspberry Pi 3 replaced Raspberry Pi 2 Model B in February 2016, what means that has not been formally set and tested and that the original Onion Pi was limited to Raspberry Pi 2 Model B features.

Last conclusion connotes the most hindering fraction. Raspberry Pi 2 Model B counts with no area network access but one Ethernet output. Although one wireless interface is edited, it will need of a wireless adapter. Furthermore, as this project is thought as a portable device, another virtual wireless

interface would have to be plugged in. First one will play as access point, whilst the second one as WAN access interface. In this line, Onion pi was made for home use.

On the other side, Raspberry Pi 3 has a Wi-Fi internal card. It solves previous problems and reduces the number of extra tools, being more suitable to perform as portable. As it integrates a more powerful processor, it is hoped a faster process, without noticing the encryption and firewall's evaluation, giving users the sense of seamlessly navigation.

To sum up, Onion Pi project will be the starting point and the reference to assess whether the gadget generated is a real advance or not.

2.4.5 OpenVPN [69]

As previously discussed, the most dangerous zone would be the gap between any workstation and the hotspot (Figure 1-3). Certificates were also mentioned as to authenticate server's web and clients (Section 2.4.3). Joining them together it has been come up with the solution to strengthen the weakest chain.

OpenVPN is an open source (Figure 2-22), invented in 2001 by James Yoman [70], that holds a certification authority server (CA) allowing multiple clients to have a safe exchange of data. CA issues digital certificates validating individual entities [71]. Provided that workstations receive client certificates, CA would be able to recognise friend devices and yield access to them.



Figure 2-22 OpenVPN logo (taken from [26])

Operation mode of OpenVPN comprehension resides in the understanding of the differences between public and private keys and how they work. In the same manner that former cryptographic machines alter communications, computers cryptography is formulated by two algorithms, one for encrypt and another for decrypt.

Despite all its complexity, it presents same debilities as back to Enigma machine; workstation or server could be intercepted (or infected) and key could be found out. Computers processing speed makes them ideal for deciphering almost any key. Moreover, strong and wide data bases are able to save and compare already used codes. Lastly, it is impossible to face nowadays scalability with paired keys.

Given those difficulties, it arose, first, Diffie-Hellman (1976) algorithm, and then, RSA's one (Rivest, Shamir and Adelman, 1978), which generate such a dissimilar couple of keys that was almost impossible to decipher [10].

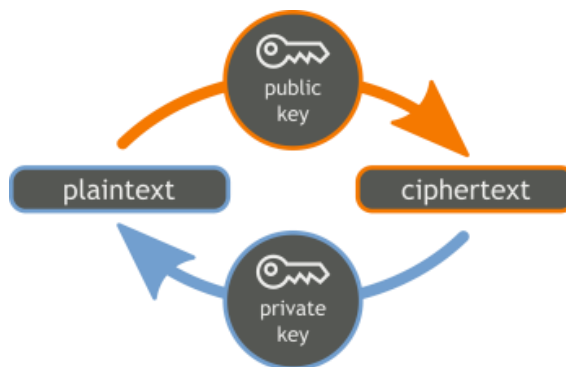


Figure 2-23 Decoding and coding process (taken from [26])

A public key is shared and used to cypher data that can only be decipher by the private key retained by the owner (Figure 2-23). However, public key's disadvantage is the slowing down caused due to numerous encryptions for just one key solver.

In the middle resides the effectiveness. Firstly, website is authenticated with its own certificate, provided by a CA (Figure 2-24). Then, public key is employed to share a private key. At the end, both client and web supplier codify their communication with that symmetric key.



Figure 2-24 Certification process (taken from [72])

2.4.6 WEP, WPA and WPA2 [73]

WEP (Wired Equivalent Privacy) was the first encryption algorithm for wireless security. It was developed in September of 1999 by a group of volunteer IEEE members. In spite of being uploaded and its key being lengthen WEP encryption was easily cracked, how a FBI commission showed in 2005 [74]. WEP vulnerabilities were attributed principally to a short range of encrypting keys, poor key management and no access point authentication [75] .

Although diverse solutions were released by companies and individuals, they were not enough. Therefore, an 802.11 (Wi-Fi standard) working group studied the mechanism to assure encryption, data privacy and integrity, authentication and access control. WPA (Wi-Fi Protected Area) was ratified in 2003.

Most common type of WPA security is WPA-PSK (WPA-Pre Shared Key) that generates a password which is distributed to the clients. However, protocols recycled from WEP security gave place to intrusion vulnerabilities, proving it unable for accomplishing the requirements.

Finally, in 2006, WPA was officially substituted for WPA2. The new system forced to apply AES (Advanced Encryption Standard) algorithms (it was patched in WPA but it was not mandatory). It also included a cipher exchanger for interoperability (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol - CCMP) with WPA.

Attack vectors need previous network access. Debilities are considered on enterprises or public LANs, but have no practical consideration on private area networks. Moreover, WPS (Wi-Fi Protected Setup), approved in 2007, was designed to help administrators to carry a proper management of the net.

WPS is constituted by three components; AP (Access Point) infrastructure, Logging (Credential authentication by the client) and Register (Granting and revoking credentials by the administrator). WPS allows 4 types of securing client access by means of PIN (password), WPS button access, near-field or USB. As a matter of fact, all of them introduce one step before connecting in which client must have access to the router [76].

In conclusion, WPA2 plus AES encryption will be the best setup for our hotspot. It will be an addition measure considering that clients will need a certificate to authenticate themselves. Besides, a MAC filter could be settled to establish one more wall against malicious intruders.

2.4.7 Antivirus

Computers antivirus range counts with an innumerable amount of software regarding on its OS or platform, both free or paid services and the malware that is specialized for. Within such quantity, best way to tackle the selection of the best antivirus for our Raspberry Pi will be skimming forums and user's opinions and from there analyse the more suitable.

Even though, the most times proposed is ClamAV² antivirus, it will be compared to some other ones to verify or deny its superiority. Other programs recommended are Sophos and Comodo. Owing to ESET, AVG or Avast are paid services, they will not be taken into account, yet, they are very strong software, thus, and ever they fulfil the requirements they would be a perfect alternative.

Antivirus	Installation	Resources needed	Easy-to-use Interface	Lightweight	Updating / Support
ClamAV	Easy & Fast	RAM 1 GB	Clam TK GUI		Open Source
Sophos [77]	Easy & Fast	RAM 1 GB	Own GUI	1 GB	Org. Support
Comodo [78]	Easy & Fast	RAM 2 GB	Own GUI	210 MB	Org. Support

Table 2-3 Antivirus's comparison

As shown in Table 2-3, characteristics are similar and all of the antivirus will be quite suitable for the Raspberry Pi. All the same, ClamAV-Raspbian couple executes a fine compatibility and ClamAV versatility let it work with multiple signatures and formats. Furthermore, even not having a preinstalled interface is considered a disadvantage (Clam TK GUI yellow cell), a CLI interface control gives a more direct and manual control of the application. Lastly, Sophos and Comodo depend on organizations meaning that clients should be subject to their policies.

ClamAV general features are the followings:

- Open Source
- CLI scanner
- Milter interface for sendmail
- Advance database updater and Virus database up-to-date
- Various formats support like Zip, RAR, Gzip, SIS and others
- Built-in support popular documents MSOffice, PDF, HTML, Flash and PDF
- GUI available

To sum up, there are a high number of possibilities in this aspect, which will come determined for each client's situation. Concerning to this tutorial it has been chosen ClamAV; nevertheless, many options would be equally valid. Although it is not discussed, workstation's antivirus is as important as hotspot's, thus, client should protect its workstation with the most appropriate one.

2.4.8 Firewall [79]

Traffic going into and out of a station is filtered by programs denominated firewalls. Packets are distributed into ports as regards to their protocol and, at the same time, these ports are related to an application.

² Forums and webs background [119], [120] and [121]

Similarly to real life, authorities can implant embargo or blockades, impeding or cutting certain routes. Firewall will act as Customs imposing taxes and regulating free access. Firewall way of work is through IP tables which recognise packets destinations and applies administrator's policies.

IP tables are divided in mangle, filter, NAT (Network Address Translation) and raw tables that redirect the traffic shaping the packet. They will be a fundamental pillar in the structure which is being built and it will be essential to comprehend how to use them (section 2.2.1).

Coming back to the Firewall, Linux based operating system simplest is UFW (Uncomplicated Firewall). When this application is installed, it sets default rules for the average user. Furthermore, UFW understand normal syntax like enable/disable and port's name like SSH (Secure Shell) instead of port 22 [80].

2.4.9 DNS Server

The Domain Name System (DNS) is a worldwide database created to organize system mapping. Originally a document periodically updated resolved address translation until Internet escalation made impossible to be held by this method [81].

DNS is a distributed method, counting with servers across the world, which participate in requesting address translations and webpages downloads. They contain domain name directories and redirect clients request resolving the names and IP directions (Figure 2-25). In case the server had not the IP address, it would send the information to a higher-level server [10].

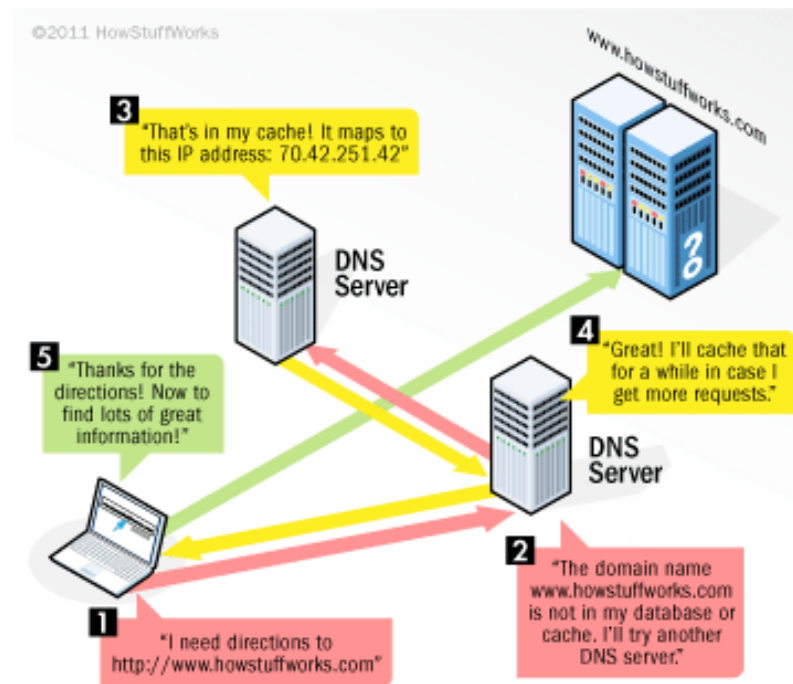


Figure 2-25 DNS resolving process (taking from [82])

DNS cache servers save most visited and popular webpages getting the information closer to the users. In this manner, web downloading times decrease potentially. Installing a DNS server into the Raspberry Pi will balance out encrypting delays.

2.5 Conclusion

Demilitarized Zone (DMZ) and Militarized Zone (MZ) refer apiece to the unprotected and protected locations of the network (Figure 2-26). Menaces enumerated in section 2.3 can be divided regarding if they act inside or outside of the Militarized Zone.

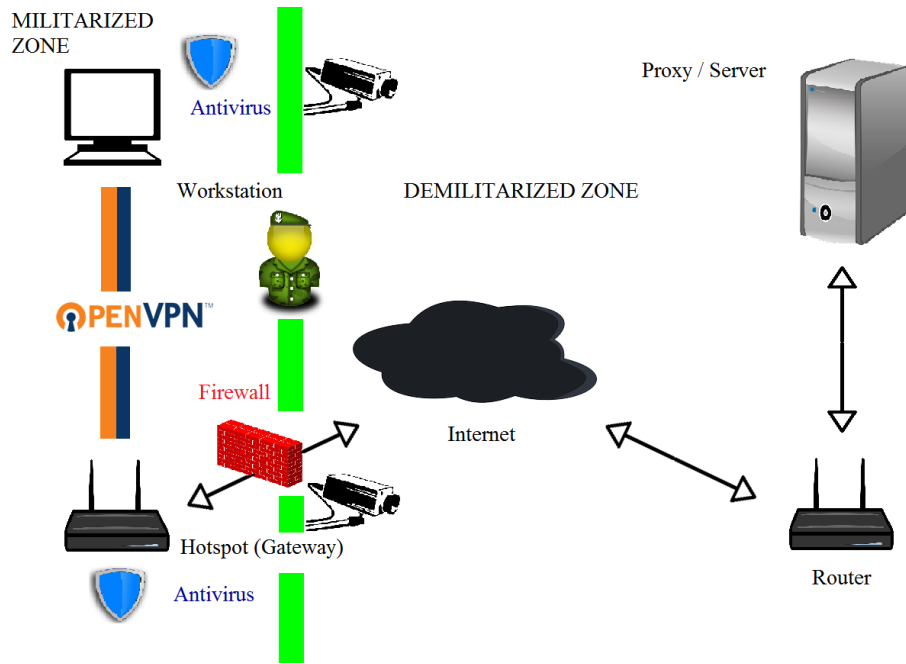


Figure 2-26 MZ and DMZ (edited from [3])

In accordance with all the knowledge given, there is a wide amount of software involved into this project. Summarizing there are three vital areas; the Militarized Zone, the Demilitarized Zone and the wall that divides them. Across the following sections each part will be guarded and tested, by developing and installing the programs above discussed.

3 DEVELOPMENT & SETTINGS

3.1 Introduction

During this section, it will be explained in detail the steps to set a hotspot that provides OpenVPN connections and redirects the whole traffic to the TOR net. This guide has been realized according to the materials refer in section 1.3 and the resolutions adopted in the previous chapter.

3.2 Set an OS

3.2.1 Downloading the OS image

The very first step is downloading the Raspbian image from the Official Raspberry Pi foundation webpage (Figure 3-1). The raspberry community offers three operative systems based on Debian. Although the Raspbian was built by the Raspbian community, the image produced by Raspberry Foundation is better supported as is installed by many Raspberry pi users [83].

NOOBS, Raspbian with PIXEL and Raspbian Jessie Lite name the three OS. According to the fluent navigation the developed device must provide, the majority of the resources possible will be reserved. Raspbian Jessie Lite image is the lightest one as it just includes the minimum software and has no extra applications.

The following tutorial is entirely based and tested on Raspbian Jessie Lite. However, as NOOBS and Raspbian with PIXEL are wider versions they should support it. Therefore, Raspbian Jessie Lite OS will be downloaded the from the Raspberry Foundation webpage [15].

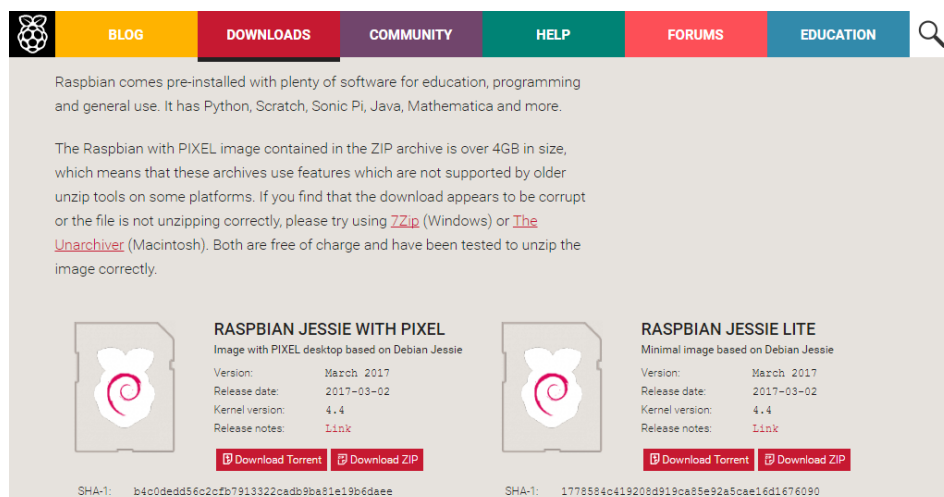


Figure 3-1 Choosing OS (taken from [15])

3.2.2 Formatting MicroSD and burning the image

In second place, SDFormatter and Win32 Disk Imager will have to be acquired. Both programs can be replaced for any software that runs the same functions.

SDFormatter will empty the MicroSD and prepare it to host the Raspbian OS. Selecting the correct drive is essential to avoid possible corruptions of another card or hard disk. Format size adjustment will also be activated before beginning the format (Figure 3-2).

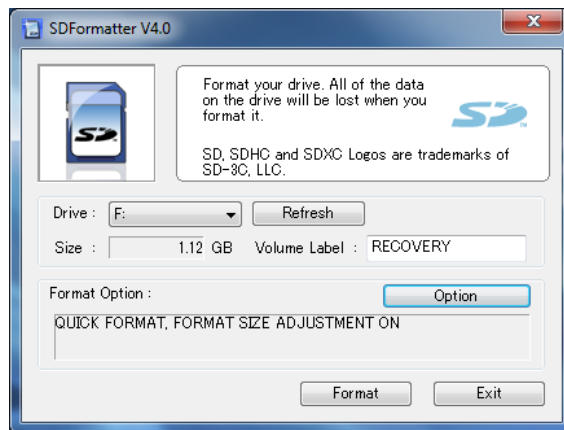


Figure 3-2 Screenshot of SDFormatter formatting MicroSD

Next, image will be burned out as it shown in Figure 3-3. Once it is finished, MicroSD will be ready to work with the Raspberry Pi.

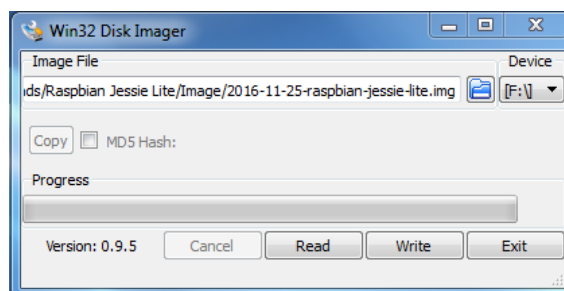


Figure 3-3 Screenshot of Win32 Disk Imager burning OS image

3.2.3 Setting first steps in Raspberry Pi

Raspberry Pi has not remote access support but connected to a screen via HDMI. For this reason, and until and SSH or another input access would be granted, they will need a cable and a monitor. Whereas Raspberry Pi 3 could enter Internet across its internal card, Raspberry pi 2 is restricted to an Ethernet cable or a wireless adapter. Linking the device to the router through Ethernet will make the process simpler (whether using any of both models).

First time, Raspbian will boot into the command line (CLI). There are 4 kinds of boot interfaces; CLI with and without logging and the same for desktop boot. Raspbian Jessie Lite has not any desktop preinstall so it must be downloaded later on.

To begin, next commands are to be typed:

- **sudo apt-get update**
It will renew available software packets
- **sudo apt-get upgrade**
It will install previous downloaded packets
- **sudo raspi-config**

- **Expand File System**

Allows the OS to use the whole MicroSD memory space

- **Change user password**

It is mandatory as to increase the security. Follow tips in General measures (Attached document I: Safety Measures) to create a strong and safe password. If ever the pass is lost, mounting the microSD card into a computer and deleting the “x” from “pi:x:1000:1000 [...]” in /etc/passwd file will grant access without password request.

- **Boot Options [84]**

There is the possibility of designing users’ own desktop. Default GUIs are PIXEL, LXDE, XFCE and MATE. Although is not mandatory, a virtual desktop still facilitates many aspects of the guide.

PIXEL is the lightest with a weight of 76 MB toward 97 MB, 107 MB and 101 MB respectively. Despite every byte counts, weight difference is not as high as to give place to slower processes. Installing commands to introduce in the CLI are:

- **sudo apt-get install –no-install-recommends xserver-xorg**
- **sudo apt-get install –no-install-recommends xinit**
Both will install managers for the virtual display
- **sudo apt-get install raspberrypi-ui-mods**

Now, coming back to raspi-config interface they have been presented three options. First of them is the booting interface explain in the second paragraph of this chapter. Second one defines itself with their own name (Wait for Network at Boot). It should be enabled but we will do it in case. Lastly, Splash Screen displays the classic computers’ brand initial screen, as it will have no practical use, is up to the user, due to security reasons.

It will be more comfortable work in the CLI until the end of the tutorial; anyhow booting desktop will not be as primordial as to set a specific one. All the same, is not recommendable choosing one without password logging.

- **Localisation options**

Locales are a framework to switch between multiple languages and allow users to use their language, character or collocation order.

Into Change local section, space bar will be pressed to select and deselect languages. For time zone each client will select his continent and country’s capital. Keyboard layout might be the most important parameter because correlates the CLI with client’s keyboard. Meanwhile, Wi-Fi country will define legal wireless channels.

- **Interfacing options**

SSH and VNC must be enabled to grant CLI and desktop access.

Next raspi-config options will remain as they are settled. Once this first step is finished, Raspbian will demand to reboot the system. Remember using the new password.

- **ip a** (abbreviation of ip address show)

– **sudo nano /etc/network/interfaces³**

Interfaces file controls interfaces' IP acquisition. First IP that will be established will be eth0 one. Figure 3-4 and section 3.2.4 show expected configuration. If ever user's framework were dissimilar he should change it for the proper interface.

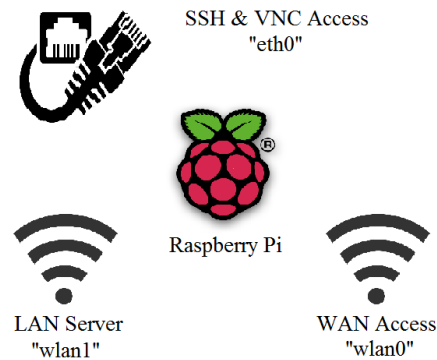


Figure 3-4 Raspberry Pi's interfaces (edited from [3])

In the file they will be added the following static parameters and commented eth0's iface manual line (Add a '#' (hash) before that phrase)⁴:

```
auto eth0
# allow-hotplug
# iface eth0 inet manual
iface eth0 inet static
    address 169.254.102.15
    netmask 255.255.255.0
```

Save and close the file. Being connected directly to WAN or router by Ethernet, the new iface will bring down the Internet access. Thus, it is necessary to activate wireless access. Easy way is switching to desktop GUI by pressing Ctrl+F7 (Ctrl+F1 to come back to the CLI) and clicking wireless manager. On the contrary, CLI method is by editing wpa_supplicant.conf file.

– **sudo nano /etc/wpa_supplicant/wpa_supplicant.conf⁶**

Add following lines regarding Wi-Fi network available.

```
network={
    ssid="Wi-Fi's name"
    psk="password"
    proto=RSN
    key_mgmt=WPA-PSK
    pairwise=CCMP
    group=CCMP
    auth_alg=OPEN
}
```

³ Saving commands are Ctrl + X or F3 and document closing commands, Ctrl + Y or F2.

⁴ In Figure 3-9 eth0 interface can be verify.

⁵ Static IP is based on IEEE standards for local subnets. Check part 3.2.4.

⁶ Variables explained in section 3.3.3 while preparing hotspot parameters.

These commands set the security discussed in chapter 2.4.6. There is no limit in networks typed. Figure 3-5 gives an example of network configuration. Once typed, save and close the file.

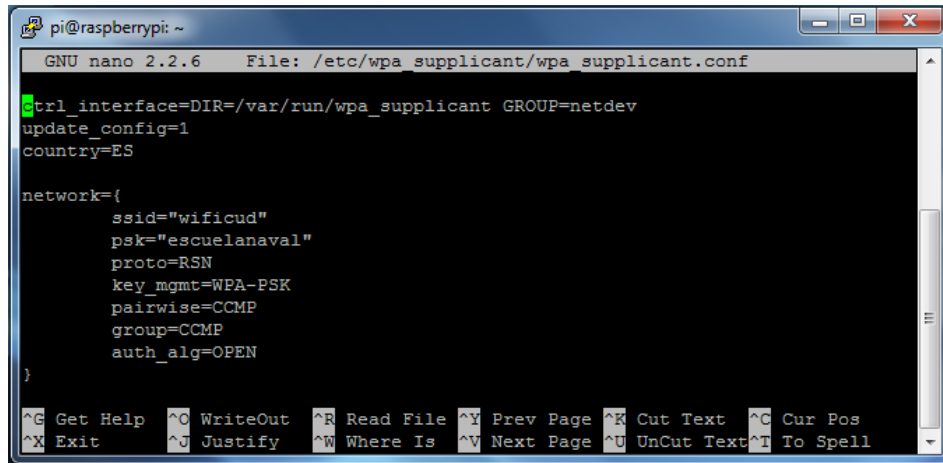


Figure 3-5 Screenshot of networks' configuration example

Initial steps already introduced will allow SSH access using Putty program. As a result, any workstation with an Ethernet input could be used to manage the Raspberry Pi.

– **sudo reboot**

As long as there is an HDMI display will not be necessary to connect through SSH. If that is not the case, PuTTY will manage SSH sessions into the Raspberry Pi. Introducing static IP address established earlier, SSH connection and port 22 stations will enter into CLI. Saving the session is feasible in the box below as shown in Figure 3-6.

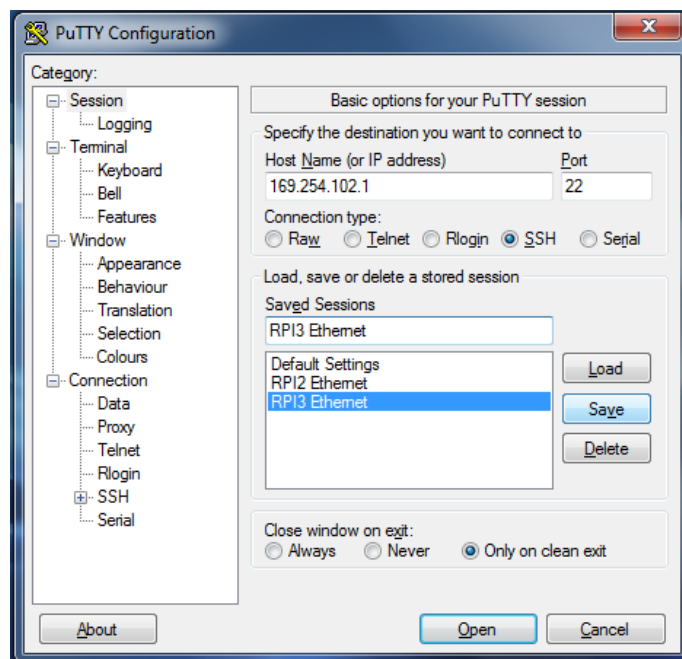


Figure 3-6 Screenshot of an example of PuTTY session

3.2.4 Working parameters

Before dealing with the configuration of the hotspot, some variables must be emphasised, in order to avoid possible confusions and every Raspberry Pi, where it would be installed, set its own parameters.

- **Raspberry Pi 3 Model B**
Raspberry Pi 2 Model B configuration's pattern is the same.
- **Interfaces**
SSH interface "**eth0**"
AP interface "**wlan1**"
Internet interface "**wlan0**"
OpenVPN interface "**tun0**"
- **IPs⁷**
 - **IP's pools**
Subnet: **192.168.42.0/24** Range: **192.168.42.10 – 192.168.42.50**
OpenVPN: **10.8.0.0/24** Range: **10.8.0.10 – 10.8.0.12**
 - **Static IPs**
Access Point: **192.168.42.1**
OpenVPN Server: **10.8.0.1**
"eth0" interface: **169.254.102.1**
- **Workstations (Section 1.3.3)**

3.3 Set an Access Point [33]

An access point, also known as hotspot, is any wireless adapter or antenna able to create a local network and provide Internet access (Figure 3-7). This means that it owes offer IPs (DHCP) and execute Network Address Translation (NAT). This section will resolve that matter:

- **sudo apt-get install hostapd isc-dhcp-server**
It will get a domain host configuration protocol
- **sudo apt-get install iptables-persistent**
Iptables controls the inside routing. This packet will auto save all the configurations at the same time it would have been typed it.
Raspbian will request clients about saving current IP rules (IPv4 and IPv6). It should be agreed.

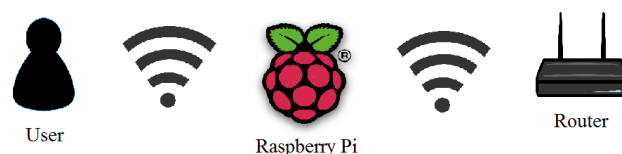


Figure 3-7 Raspberry pi hotspot (edited from [3])

3.3.1 Set up an DHCP server and a subnet

- **sudo nano /etc/dhcp/dhcpd.conf**
Firstly, next lines should be commented

```

option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

```

⁷ LAN IP 192.168.42.1/24 is taken from [33] tutorial. Any subnet could be configured. Notwithstanding, as IANA reserves 192.168.0.0/16 for wireless LAN, it would be recommended users staying inside those limits as to avoid IP conflicts.

In order to obtain:

```
#option domain-name "example.org";  
#option domain-name-servers ns1.example.org, ns2.example.org;
```

Secondly, hash will be removed from authoritative, located below the local DHCP sentences. The result will be:

```
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;
```

Thirdly, at the bottom the local network will be added (Figure 3-8)

```
subnet 192.168.42.0 netmask 255.255.255.0 {  
    range 192.168.42.10 192.168.42.50;  
    option broadcast-address 192.168.42.255;  
    option routers 192.168.42.1;  
    default-lease-time 600;  
    max-lease-time 7200;  
    option domain-name "local";  
    option domain-name-servers 8.8.8.8, 8.8.4.4;  
}
```

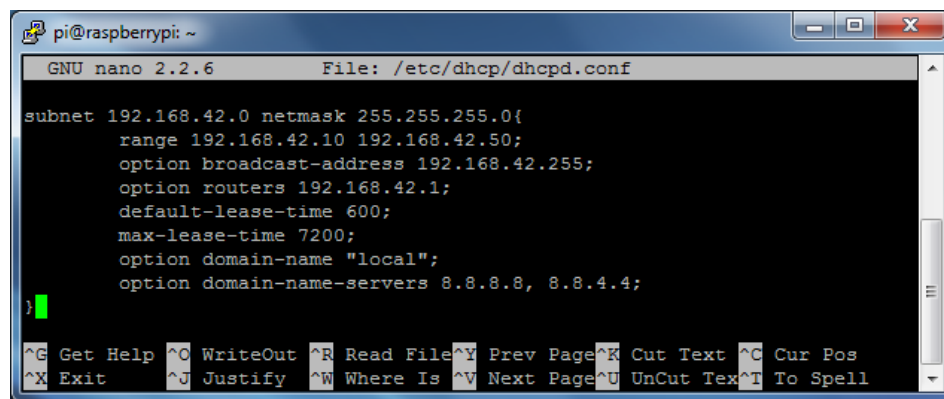


Figure 3-8 Screenshot of DHCP's pool configuration

- **sudo nano /etc/default/isc-dhcp-server**
Enter the adapter's interface, in this case wlan1

```
INTERFACES="wlan1"
```

3.3.2 Set up a static IP

- **sudo nano /etc/network/interfaces⁸**
Dynamic wlan1 will be commented out and will be substituted by a static one (Figure 3-9).

⁸ Static IP must be the Gateway configured in 3.3.1. Likewise, netmask must be in accordance with the range established.

```
#iface wlan1 inet manual
#wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf
#iface default inet dhcp
iface wlan1 inet static
    address 192.168.42.1
    netmask 255.255.255.0
```

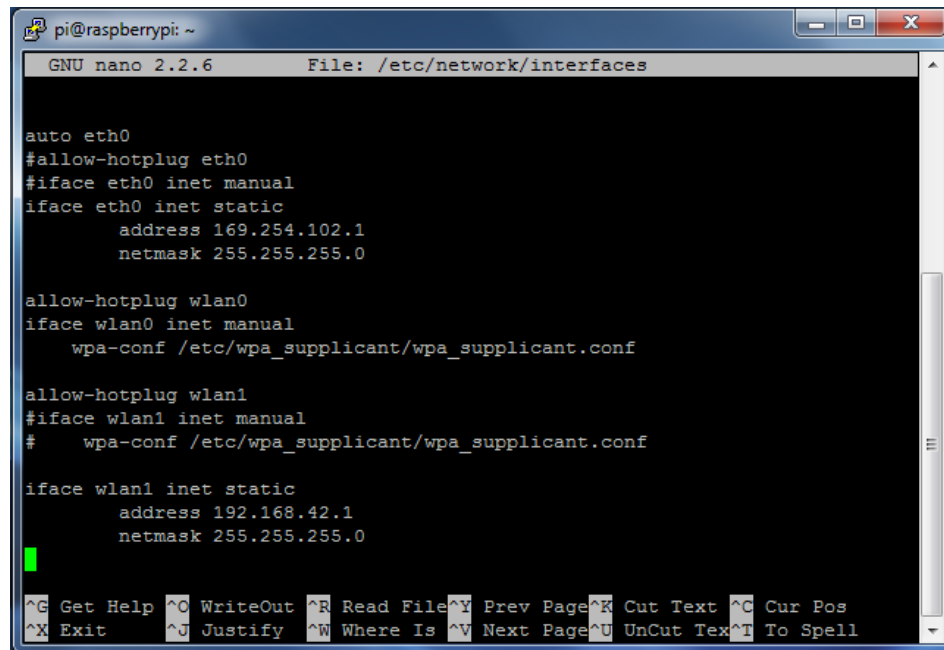


Figure 3-9 Screenshot of final interfaces' file appearance

3.3.3 Configure hostapd

Within hostapd.conf hotspot aspect will be shaped (Figure 3-10).

– **sudo nano /etc/hostapd/hostapd.conf**

```
interface=wlan1
ssid=name
country_code=ES
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=1
wpa=2
wpa_passphrase=password
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
```

```
wpa_group_rekey=86400
ieee80211n=1
wme_enabled=1
```

Explanation:

interface = Hostapd's interface

ssid = Wi-Fi network's name. Our will be named Garbo in the shake of Juan Pujol García [85]

country_code = Code settled in 3.2.3

hw_mode = 802.11 modulation standard (2.4 GHz band)

channel= Band channel's number

macaddr_acl = Accept all MAC addresses. Owing to the certificates, MAC filter will not be necessary

auth_algs = Use WPA authentication

ignore_broadcast_ssid = In order to hide the net select "1", it will increase security

wpa = Use WPA2

wpa_passphrase = Strong password for your AP. Follow tips in Attached document I: Safety Measures

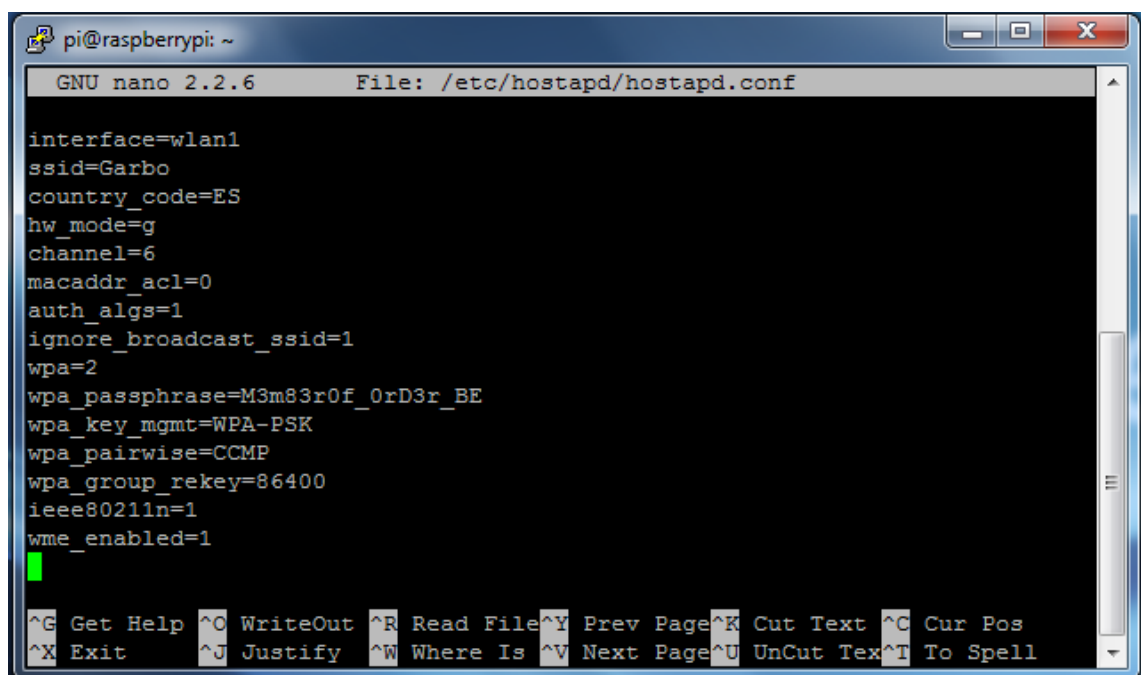
wpa_key_mgmt = Use of pre-shared key

wpa_pairwise = AES encryption

wpa_group_rekey = Re-keying duration in seconds

ieee80211n = Enable IEEE 802.11n standard

wme_enabled= Enable clients contact each other



```
pi@raspberrypi: ~
GNU nano 2.2.6      File: /etc/hostapd/hostapd.conf

interface=wlan1
ssid=Garbo
country_code=ES
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=1
wpa=2
wpa_passphrase=M3m83r0f_0rD3r_BE
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_group_rekey=86400
ieee80211n=1
wme_enabled=1
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Tex ^T To Spell
```

Figure 3-10 Screenshot of Wi-Fi setting

- **sudo nano /etc/default/hostapd**

Tell Daemon where to find host configuration

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

- **sudo nano /etc/init.d/hostapd**

```
DAEMON_CONF=/etc/hostapd/hostapd.conf
```

3.3.4 NAT

- **sudo nano /etc/sysctl.conf**
Scroll to the bottom and add

```
net.ipv4.ip_forward=1
```

- **sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"**

Adafruit tutorial refers, at this moment, to IP tables. As they will be erased in TOR's setting this step can be omitted. Nonetheless, because it will help users to tell whether hotspot is working properly, it is advisable.

- **sudo nano /etc/checkinternet.sh**
Making a specific file (Figure 3-11) will simplify the process and it will be able to be activated it every when needed, typing just one command.

```
#!/bin/sh
```

```
###Clear Internet access configuration
```

```
#Accept all the traffic in order not to lock you out
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
#Flush previous iptables
```

```
iptables -F
```

```
iptables -t nat -F
```

```
#Forwarding
```

```

iptables -t nat -A POSTROUTING -o wlan09 -j MASQUERADE

iptables -A FORWARD -i wlan0 -o wlan1 -m state --state RELATED,ESTABLISHED -j
ACCEPT10

iptables -A FORWARD -i wlan1 -o wlan0 -j ACCEPT

```

Save and close. The understanding of iptables' way of routing is indispensable as well as the insight of the interfaces use (check notes in section 2.2.1).

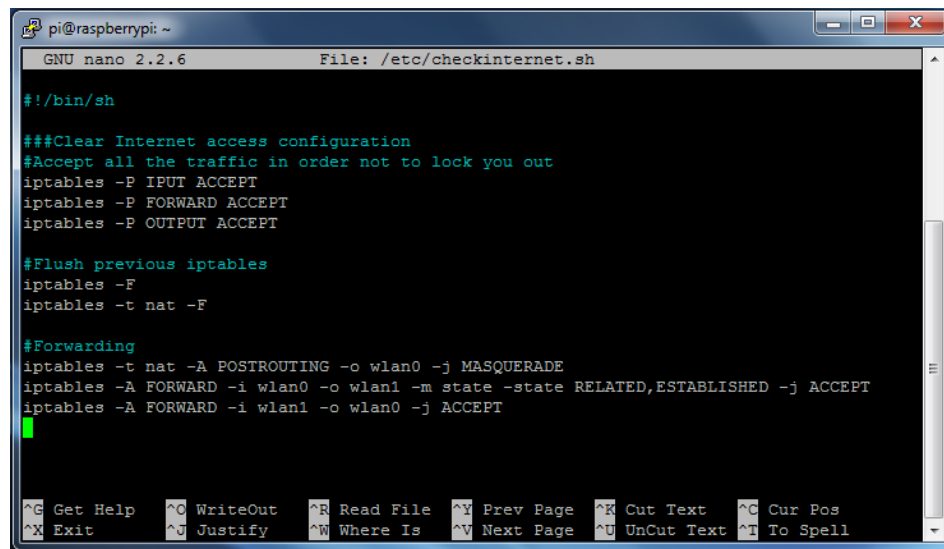


Figure 3-11 Screenshot of checking internet's file

– **sudo chmod 755 /etc/checkinternet.sh**

Chmod changes the permissions of a directory or a file. Octal numbers resolve these permissions for the owner “user”, members of the group who own the file “group” and anyone else “other” [86].

Each number is a sum of 3 digits:

- 4 is equal to “read”
- 2 is equal to “write”
- 1 is equal to “execute”
- 0 means no permissions

So client would have been authorized to read, write and execute and the rest to read and execute.

– **sudo sh /etc/checkinternet.sh**

It will start up iptables saved before. If it is desirable they could be checked out running the commands *sudo iptables -S* and *sudo iptables -t nat -S*

– **sudo sh -c “iptables-save > /etc/iptables/rules.v4”**

This command prints iptables from booting.

3.3.5 Start the hotspot service

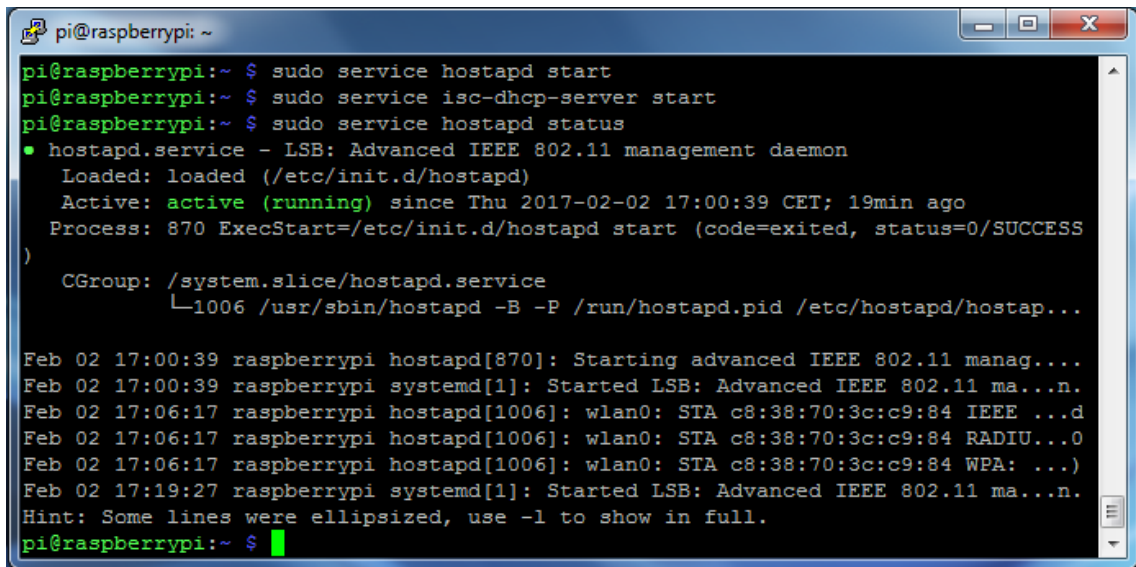
– **sudo service hostapd start**

⁹ Interfaces are in accordance with section 3.2.3 & Figure 3-4.

¹⁰ Command lines here referred must be typed in one single line.

- **sudo service isc-dhcp-server start**
- **sudo service hostapd status**
- **sudo service isc-dhcp-server status**

Running these commands services will be started and it could be verified nothing went wrong (Figure 3-12 and Figure 3-13).



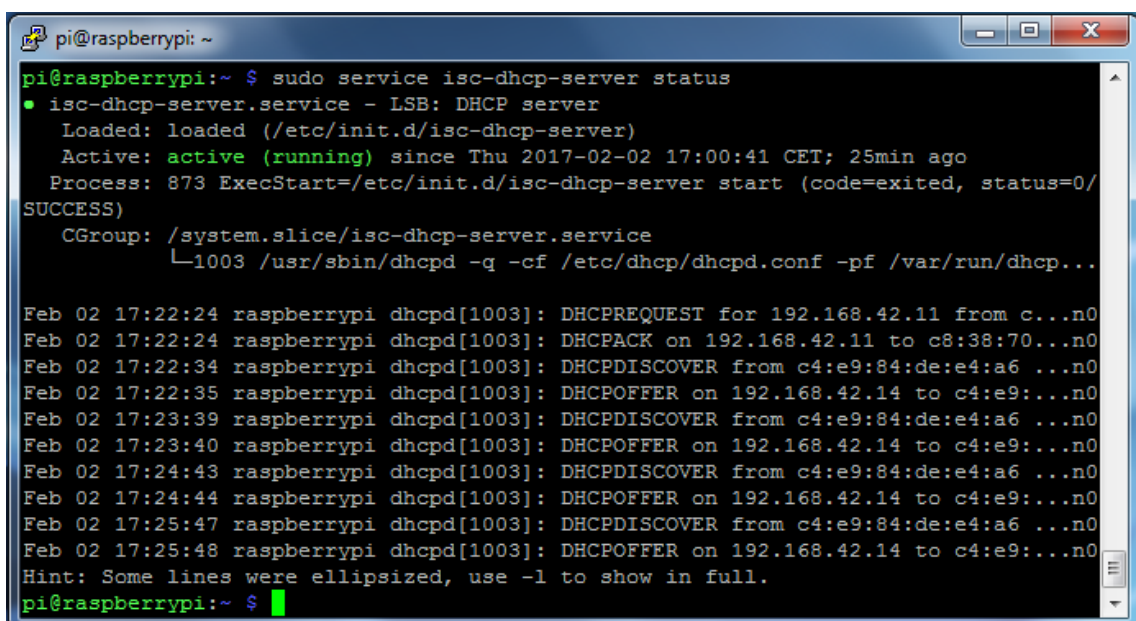
```

pi@raspberrypi: ~
pi@raspberrypi:~ $ sudo service hostapd start
pi@raspberrypi:~ $ sudo service isc-dhcp-server start
pi@raspberrypi:~ $ sudo service hostapd status
• hostapd.service - LSB: Advanced IEEE 802.11 management daemon
   Loaded: loaded (/etc/init.d/hostapd)
   Active: active (running) since Thu 2017-02-02 17:00:39 CET; 19min ago
   Process: 870 ExecStart=/etc/init.d/hostapd start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/hostapd.service
           └─1006 /usr/sbin/hostapd -B -P /run/hostapd.pid /etc/hostapd/hostap...

Feb 02 17:00:39 raspberrypi hostapd[870]: Starting advanced IEEE 802.11 manag....
Feb 02 17:00:39 raspberrypi systemd[1]: Started LSB: Advanced IEEE 802.11 ma...n.
Feb 02 17:06:17 raspberrypi hostapd[1006]: wlan0: STA c8:38:70:3c:c9:84 IEEE ...d
Feb 02 17:06:17 raspberrypi hostapd[1006]: wlan0: STA c8:38:70:3c:c9:84 RADIU...0
Feb 02 17:06:17 raspberrypi hostapd[1006]: wlan0: STA c8:38:70:3c:c9:84 WPA: ...
Feb 02 17:19:27 raspberrypi systemd[1]: Started LSB: Advanced IEEE 802.11 ma...n.
Hint: Some lines were ellipsized, use -l to show in full.
pi@raspberrypi:~ $

```

Figure 3-12 Screenshot of Hostapd's service status checking



```

pi@raspberrypi: ~
pi@raspberrypi:~ $ sudo service isc-dhcp-server status
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server)
   Active: active (running) since Thu 2017-02-02 17:00:41 CET; 25min ago
   Process: 873 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/isc-dhcp-server.service
           └─1003 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcp...

Feb 02 17:22:24 raspberrypi dhcpd[1003]: DHCPREQUEST for 192.168.42.11 from c...n0
Feb 02 17:22:24 raspberrypi dhcpd[1003]: DHCPACK on 192.168.42.11 to c8:38:70...n0
Feb 02 17:22:34 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:22:35 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:23:39 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:23:40 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:24:43 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:24:44 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:25:47 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Feb 02 17:25:48 raspberrypi dhcpd[1003]: DHCPDISCOVER from c4:e9:84:de:e4:a6 ...n0
Hint: Some lines were ellipsized, use -l to show in full.
pi@raspberrypi:~ $

```

Figure 3-13 Screenshot of DHCP's server status checking

If everything would have gone as it should the access point should be activated. Due to it is a hidden service it should be generated a new network in the workstation. Figure 3-14 to Figure 3-17 are an example of Android network creation, yet, all the OS performs it similar. To set it on boot, type the last two commands.

- **sudo update-rc.d hostapd enable**
- **sudo update-rc.d isc-dhcp-server enable**

Android network addition corresponds to the next images. Enter into Network settings and follow the instructions to complete the set.

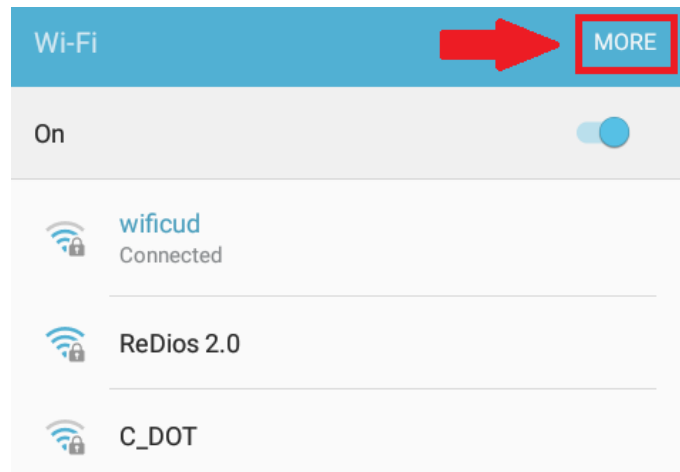


Figure 3-14 Screenshot of Hostapd's service activation 1st Step

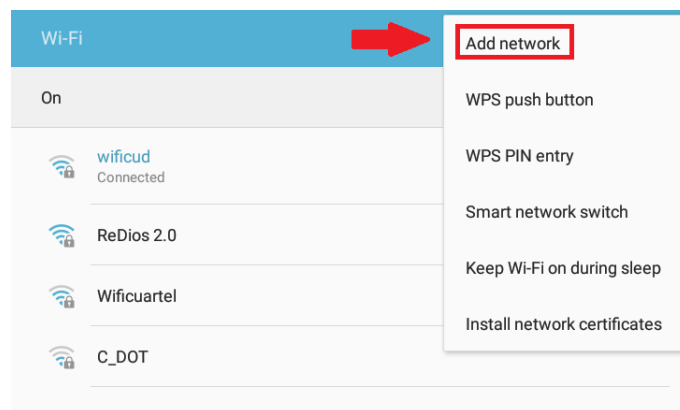


Figure 3-15 Screenshot of Hostapd's service activation 2nd Step

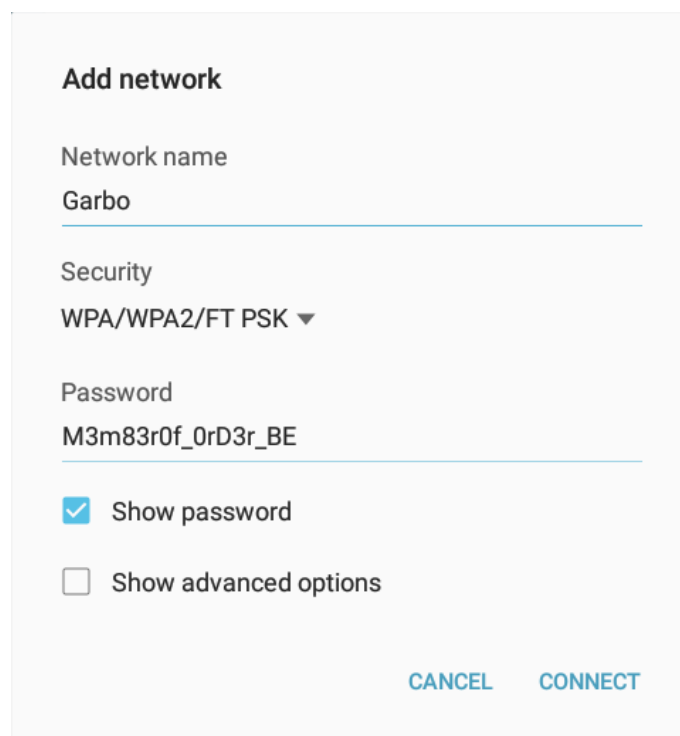


Figure 3-16 Screenshot of Hostapd's service activation 3rd Step

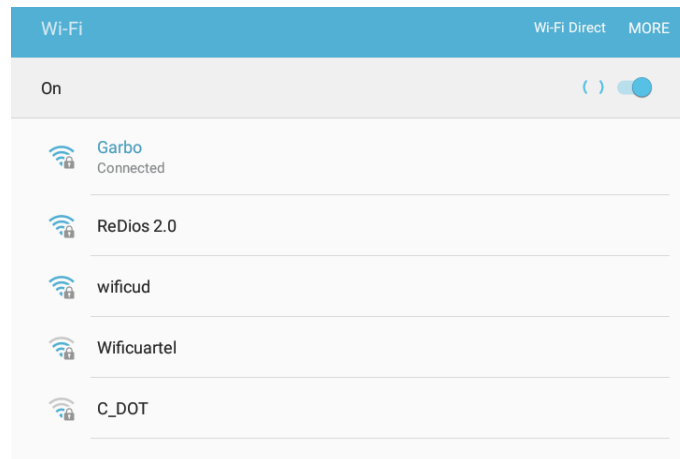


Figure 3-17 Screenshot of Hostapd's service activation 4th Step

In case something went wrong hostapd's initiation could be checked with the next command, which should return AP-ENABLED:

- **`sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf`**

3.4 Set Tor [87]

Tor project community has developed two types of anonymizing proxies. These netfilters receive a list of TOR nodes together with their public keys. Consequently, they play as a firewall filtering LAN incoming traffic and redirecting it through the TOR net.

Both of the anonymizing proxies can also transfer their local processed packets across the same route. Their principal difference lie in their capability to tell among protocols choosing what should be sent through TOR nodes and what should not. This skill is essential to avoid compromising information travelling through TOR reveal client identity.

- **Transparent Proxy (AKA Transproxy)**

Less complicated and, therefore, most likely to have leaks, transparent proxies do not divide traffic according to the application that produce them. Its advantage against traditional proxy methods, like socks, is the fact that it does not have to set one application by one.

However, within its advantage resides its disadvantage. Transproxy leaks basically are debt to send identification information through the TOR net facilitating correlation between the traffic and the workstation where it comes from.

Next are the most commons bugs in reference to TOR community [66]:

- **Windows / Android**

- Commercial software's serial number while updating
- Antivirus remote scanning
- Play Store update search using Gmail user
- Windows drivers installation
- Applications error reporting

- **Linux / Mac**

In general, Linux and Mac do not suffer from other OS problems because of the fact that most of their software is free and do not rest on so many drivers.

– **Isolating Proxy** [88]

Best solution to a transparent proxy would be thwarting workstation self-identification, in other words, do not teach workstation its IP address. In this manner, despite any program send credentials it would be impossible to correlate them with its deliverer.

Whonix executes this function by means of an isolating proxy and a transparent one. Either they are virtual or physical whonix needs of two machines. One of them, concretely, isolating proxy, will have access to the clear net and it will move all the client application's susceptible identification traffic. At the same time, transparent proxy will still perform as it already did, redirecting the rest of the packets (Figure 3-18).

Whonix Anonymous Operating System

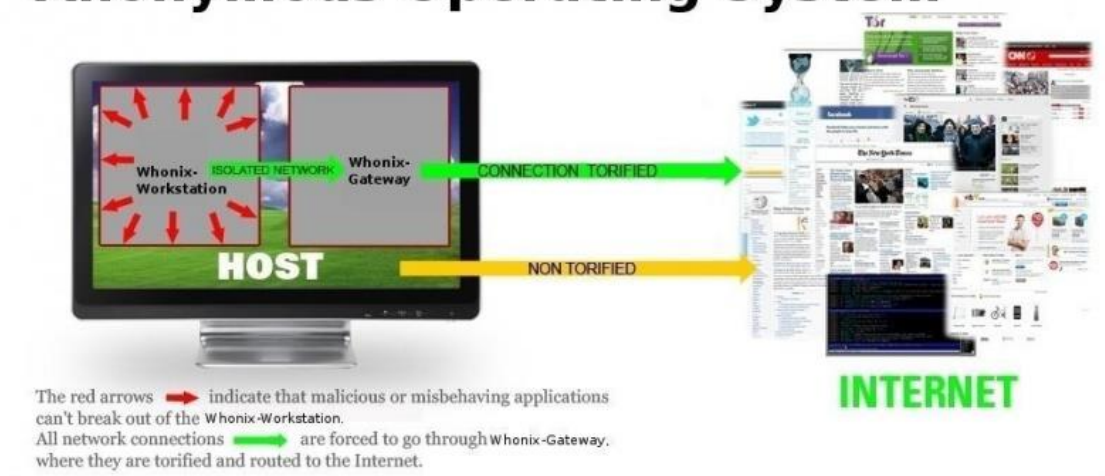


Figure 3-18 Example of Whonix working mode (taken from [88])

Summarizing, Whonix will fit incredibly to achieve project objective. Unfortunately, Raspberry Pi is not supported yet (Figure 3-19). Last thread about a Raspberry Pi Whonix configuration was on December 2014 [89], thus, same Onion Pi's assumption will be made, and Raspberry Pi former models were not capable of performing such filtering. Unluckily, bash Raspbian Whonix design is as complex as the whole hotspot setting becoming a new project's matter.

anonymous use [\[edit\]](#)

- Whonix-Gateway
 - This really does not have to be a big desktop computer or ordinary server. There are alternatives.
 - smartphone [\[2\]](#),
 - UMPC [\[3\]](#)
 - pad, tablet,
 - notebook, netbook,
 - Raspberry Pi [\[4\]](#): needs contributor, [development thread](#) [🔒](#)
 - router [\[5\]](#),
 - set top box,
 - etc.
 - how to utilize such a device as a linux server is beyond the scope of this guide, there are already better resources
- anonymous 3G modem (see below) or anonymous wifi adapter (see below)
- Whonix-Workstation

Figure 3-19 Whonix supported platforms (taken from [90])

Regarding all the troubles presented, it will be essayed to create a Whonix custom structure. A pragmatic solution is the OpenVPN subnet discussed before. As a matter of fact, OpenVPN opens a private LAN and regulates the traffic. Treating TOR net as another private subnet (Figure 3-20),

Raspberry Pi will become the bond between them both, translating addresses and protocols. In this way, a hacker will be never able to correlate a piece of specific traffic with its workstation.

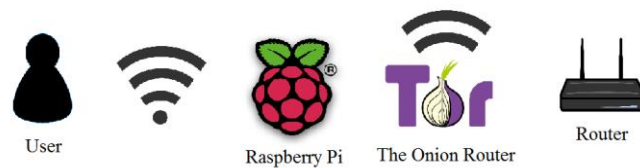


Figure 3-20 Tor Transproxy (edited from [3])

Nevertheless, in spite of the fact that casual identification spreads are almost armoured, clients can unconsciously reveal their identity. This means, giving observers the opportunity to match identify flow with non-identify one.

An instance could be publishing post or photos in social networks or forums. User's profile gives his credentials and post's time provides the moment the message was generate by the workstation. Among a small population, a library for example, one like (social network's button) could be enough, worst scenario two or three. Due to the fact that TOR uses the same node for a small period of time, work would be done, a data flow would have been correlated with a person, even if workstation will never be discovered.

Given TOR's incapability to protect from statistical analysis, clients will not remain anonymous without prevention. On account of that prevention will entail not using social networks, emails and any account that compromises users, TOR's encryption capabilities will be wasted. For these reason, hotspot can be understand hotspot employment in two different aspects:

1. Anonymous profile

Those who want remain anonymous and protect their information. They must follow the tips list in Anonymous measures (in Attached document I: Safety Measures) gather from Internet's correct TOR use manuals.

One example of anonymous profiling would be a freelance reporter in war zone who would want to prevent himself from being hijacked.

2. Sheltering profile

Those who want encrypt their information but do not care whether hackers or law enforcement monitor their activity.

For instance, a student connected to a library public Wi-Fi or a traveller connected to the airport one.

3.4.1 Install tor

- **sudo apt-get install tor**
- **sudo nano /etc/tor/torrc**

It is to be configured running tor file adding below the FAQ notice:

Log notice file /var/log/tor/notice.log

VirtualAddrNetwork 10.192.0.0/10

AutomapHostsSuffixes .onion, .exit

AutomapHostsOnResolve 1

TransPort 9040

TransListenAddress 192.168.42.1

DNSPort 53

DNSListenAddress 192.168.42.1

3.4.2 IP tables [66]

Likewise to the clearnet iptables file, a new one will be edited to define TOR redirecting tables (Figure 3-21, Figure 3-22 and Figure 3-23).

– **sudo nano /etc/toriptables.sh**

Some lines are referred to notes at the bottom. Checking them is mandatory to succeed in the configuration.

```
#!/bin/sh
```

```
###Set variables
```

```
#TOR UID (run “-u debian-tor” in case you do not know)
```

```
_tor_uid="109"
```

```
#TOR's TransPort11
```

```
_trans_port="9040"
```

```
#TOR DNSPort11
```

```
_dns_port="53"
```

```
#TOR Virtual Address Network IPv411
```

```
_virt_addr="10.192.0.0/10"
```

```
#Outgoing/Incoming, SSH and interfaces
```

```
_out_if="wlan0"
```

```
_inc_if="wlan1"
```

```
_ssh_if="eth0"
```

```
#LAN destinations not routed through TOR
```

```
_non_tor="127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16"12
```

¹¹ Same data as torrc file

¹² Those are IP pools reserved for IANA to subnets. The TOR subnet created should be inside that range, in case it would not is mandatory to include it.

#Other IANA destinations not routed through TOR

*_resv_iana="0.0.0.0/8 100.64.0.0/10 169.254.0.0/16 192.0.0.0/24 192.88.99.0/24
198.18.0.0/15 198.51.100.0/24 203.0.113.0/24 224.0.0.0/3"''¹³*

#Accept all the traffic in order not to lock you out¹⁴

iptables -P INPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -P OUTPUT ACCEPT

#Flush previous iptables

iptables -F

iptables -t nat -F

#TOR iptables

iptables -t nat -A PREROUTING -i \$_ssh_in -p tcp --dport 22 -j REDIRECT --to-ports 22

*iptables -t nat -A PREROUTING -i \$_inc_if -p udp --dport 53 -j REDIRECT --to-ports
\$_dns_port¹³*

*iptables -t nat -A PREROUTING -i \$_inc_if -p udp 5353 -m udp --dport 5353 -j REDIRECT
--to-ports \$_dns_port¹³*

*iptables -t nat -A PREROUTING -i \$_inc_if -p tcp -m tcp --syn -j REDIRECT --to-ports
\$_trans_port¹³*

#Allow LAN access in IANA reserved blocks

for _lan in \$_non_tor; do

iptables -t nat -A PREROUTING -i \$_inc_if -d \$_lan -j RETURN

done

for _iana in \$_resv_iana; do

iptables -t nat -A PREROUTING -i \$_inc_if -d \$_iana -j RETURN

done

#Local redirection

iptables -t nat -A OUTPUT -p udp --dport 53 -j REDIRECT --to-ports \$_dns_port

iptables -t nat -A OUTPUT -p tcp -m tcp --syn -j REDIRECT --to-ports \$_trans_port

¹³ Command lines here referred must be typed in one single line.

¹⁴ It should not be necessary having followed the tutorial but is recommended to add it to avoid lock yourself out in testing cases

```
iptables -t nat -A OUTPUT -m owner --uid-owner $_tor_uid -j RETURN
```

```
iptables -t nat -A OUTPUT -o lo -j RETURN
```

```
#Allow LAN access in IANA reserved blocks
```

```
for _lan in $_non_tor; do
```

```
    iptables -t nat -A OUTPUT -i $_inc_if -d $_lan -j RETURN
```

```
done
```

```
for _iana in $_resv_iana; do
```

```
    iptables -t nat -A OUTPUT -i $_inc_if -d $_iana -j RETURN
```

```
done
```

Save and close.

- **sudo chmod 755 /etc/toriptables.sh**
- **sudo sh /etc/toriptables.sh**
- **sudo sh -c “iptables-save > /etc/iptables/rules.v4”¹⁵**

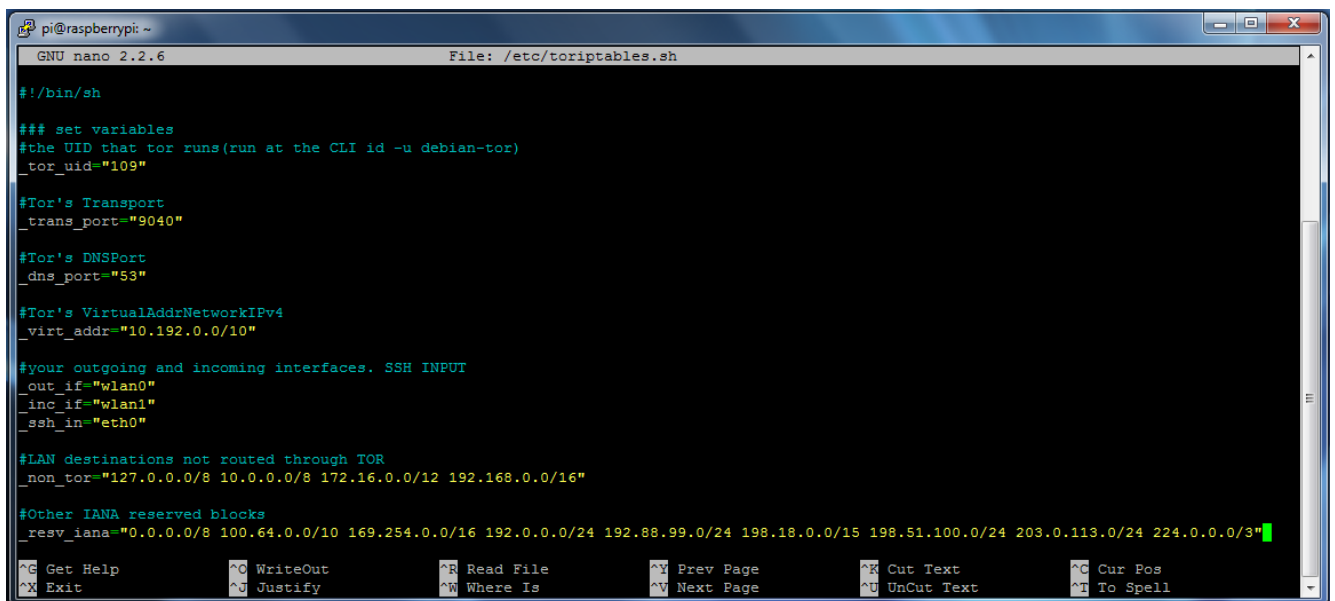
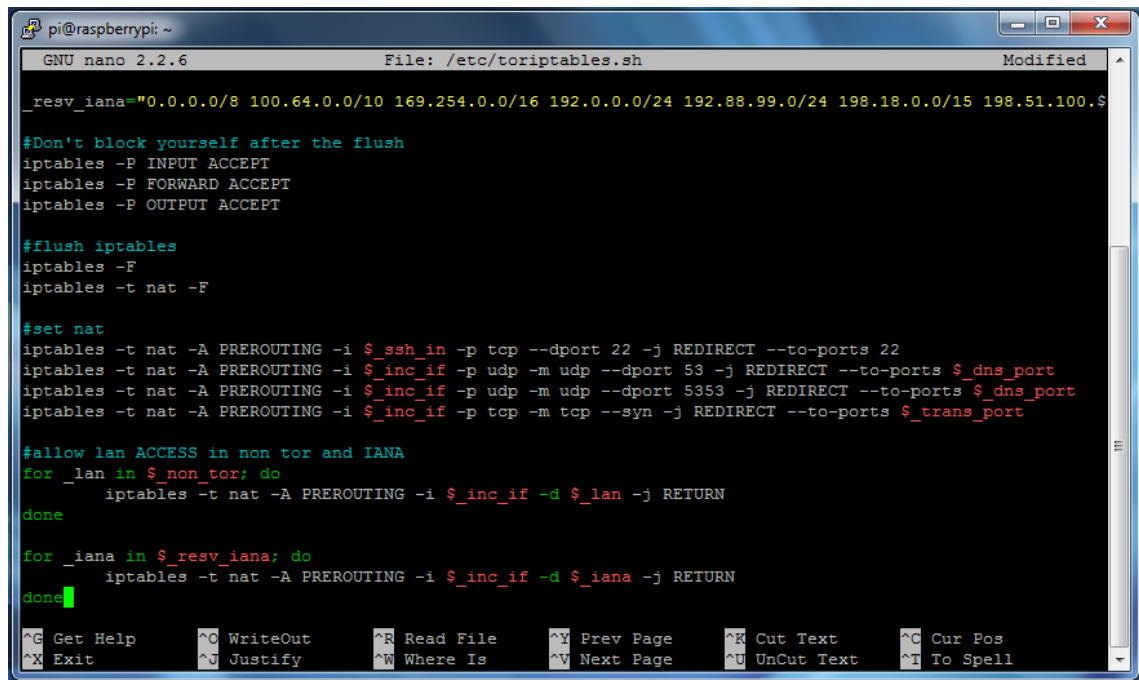


Figure 3-21 Screenshot of Toriptables' file final appearance (1)

¹⁵ Skim section 3.8 after saving iptables.



```

pi@raspberrypi: ~
GNU nano 2.2.6      File: /etc/toriptables.sh      Modified
_resv_iana="0.0.0.0/8 100.64.0.0/10 169.254.0.0/16 192.0.0.0/24 192.88.99.0/24 198.18.0.0/15 198.51.100.0/24"

#Don't block yourself after the flush
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

#flush iptables
iptables -F
iptables -t nat -F

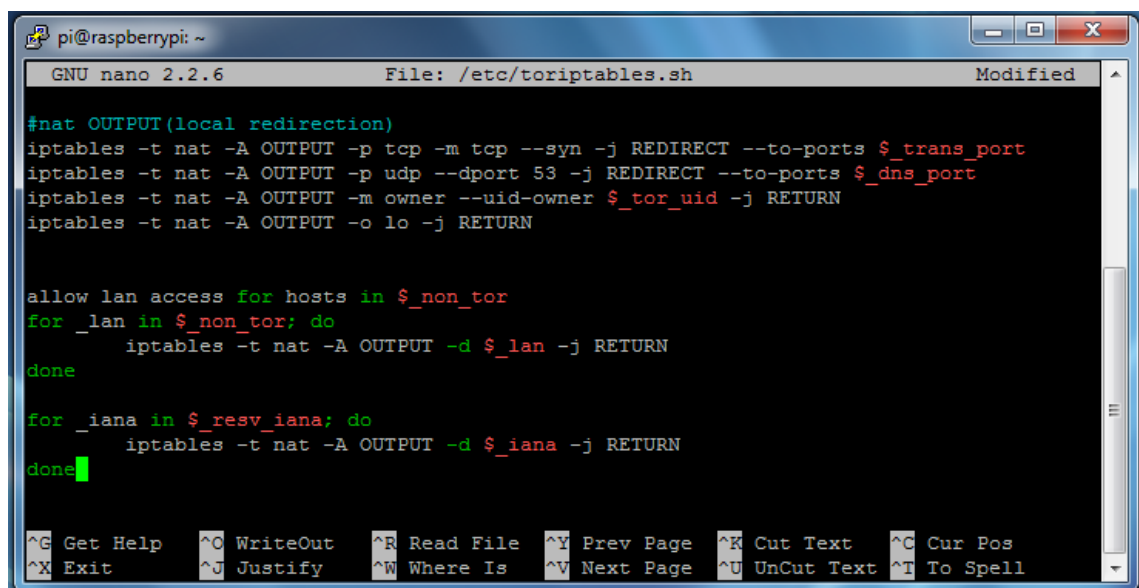
#set nat
iptables -t nat -A PREROUTING -i $_ssh_in -p tcp --dport 22 -j REDIRECT --to-ports 22
iptables -t nat -A PREROUTING -i $_inc_if -p udp -m udp --dport 53 -j REDIRECT --to-ports $_dns_port
iptables -t nat -A PREROUTING -i $_inc_if -p udp -m udp --dport 5353 -j REDIRECT --to-ports $_dns_port
iptables -t nat -A PREROUTING -i $_inc_if -p tcp -m tcp --syn -j REDIRECT --to-ports $_trans_port

#allow lan ACCESS in non tor and IANA
for _lan in $_non_tor; do
    iptables -t nat -A PREROUTING -i $_inc_if -d $_lan -j RETURN
done

for _iana in $_resv_iana; do
    iptables -t nat -A PREROUTING -i $_inc_if -d $_iana -j RETURN
done

```

Figure 3-22 Screenshot of Toriptables' file final appearance (2)



```

pi@raspberrypi: ~
GNU nano 2.2.6      File: /etc/toriptables.sh      Modified
#nat OUTPUT(local redirection)
iptables -t nat -A OUTPUT -p tcp -m tcp --syn -j REDIRECT --to-ports $_trans_port
iptables -t nat -A OUTPUT -p udp --dport 53 -j REDIRECT --to-ports $_dns_port
iptables -t nat -A OUTPUT -m owner --uid-owner $_tor_uid -j RETURN
iptables -t nat -A OUTPUT -o lo -j RETURN

allow lan access for hosts in $_non_tor
for _lan in $_non_tor; do
    iptables -t nat -A OUTPUT -d $_lan -j RETURN
done

for _iana in $_resv_iana; do
    iptables -t nat -A OUTPUT -d $_iana -j RETURN
done

```

Figure 3-23 Screenshot of Toriptables' file final appearance (3)

At this point, having everything worked alright, TOR Transproxy should be installed. Torproject help clients to check if they are using TOR paths (Figure 3-24) through their web Check Tor [91].



Figure 3-24 Check TOR status (taken from [91])

3.5 Set OpenVPN Server/Client [92]

3.5.1 Install OpenVPN

An OpenVPN server installed in the Raspberry Pi will control LAN access (Figure 3-25). In order to achieve that goal, it must be created an authentication authority that generates certificates and those certificates must be sent to the clients through a safe via.

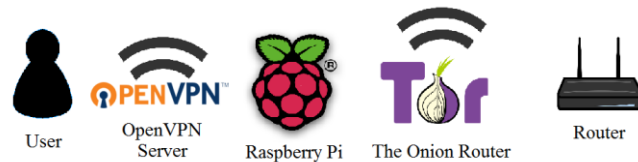


Figure 3-25 OpenVPN Server (edited from [3])

- **sudo apt-get install openvpn easy-rsa**
- **sudo su**
Due to security issues, some OpenVPN folders are restricted but to the root. Typing `sudo su` user will perform as root
- **gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf**
Decompress and copy server code in OpenVPN folder where it will be managed

3.5.2 Set a OpenVPN Server

- **nano /etc/openvpn/server.conf**
Search for the lines written down below and uncomment them.

First look:

;push "redirect-gateway def1 bypass-dhcp" (All IP traffic will go through TOR)

;push "dhcp-option DNS 208.67.222.222" (Certain network settings can be pushed inside)

;push "dhcp-option DNS 208.67.220.220"

;tls-atuh ta.key 0 (Extra security versus DDoS attacks)

;cipher AES-128-CBC (More security added to WPA2)

;max-clients 100 (Selecting a maximum is another way to avoid hackers entering our subnet)

;user nobody (Disable anyone of having rights of editing)

;group nogroup (Same prohibition for groups)

Final appearance:

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 208.67.222.222"

push "dhcp-option DNS 208.67.220.220"

tls-atuh ta.key 0

cipher AES-128-CBC

max-clients 3

user nobody

group nogroup

If there ever was any doubt about the parameters, all of them could be checked as they have their own explanation on the file.

- **cp -r /usr/share/easy-rsa/ /etc/openvpn**

Within easy-rsa folder there will be authentication authority and certificates.

- **mkdir /etc/openvpn/easy-rsa/keys**

- **nano /etc/openvpn/easy-rsa/vars**

Here, personal or company authentication details will be edited:

export KEY_SIZE=2048 (Change it from 1024 to 2048 to generate a longer key)

export KEY_COUNTRY="ES" (2 digits country's key)

export KEY_PROVINCE="Pontevedra" (Province's name)

export KEY_CITY="Marin" (City's name)

export KEY_ORG="Armada Española" (Organization's name)

export KEY_EMAIL="ernestogolmayo@hotmail.com" (Organization or personal's email)

export KEY_OU="Centro Universitario de la Defensa" (Organizational Unit's name)

export KEY_NAME="Sever" (Server's name)

Save and close it.

- **openssl dhparam -out /etc/openvpn/dh2048.pem 2048**

It will originate a Diffie-Hellman key of 2048 bits length.

- **cd /etc/openvpn/easy-rsa/¹⁶**

- **source .vars**

- **./clean-all**

It will delete all previous passwords and certificates.

- **./build-ca**

It will produce authority's certificate.

- **./build-key-server Server**

Command to make the server. Place your server's name instead of "Server".

- **openvpn --genkey --secret keys/ta.key**

- **cd ../**

- **nano ./Server.conf**

¹⁶ Until we deliberately change folder all commands are supposed to be introduced there. Even though, some of them do not depend on it.

OpenVPN servers needs to know routes to certificates and keys. Leaving them in keys folder they will remain conceal and protected because root is the only with permissions to read and modify that folder. Next lines are to be found and replaced:

First look:

```
ca ca.crt
cert server.crt
key server.key
```

```
dh dh1024.pem
```

```
tls-atuh ta.key 0
```

Final appearance:

```
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/Server.crt
key /etc/openvpn/easy-rsa/keys/Server.key
```

```
dh /etc/openvpn/dh2048.pem
```

```
tls-atuh /etc/openvpn/easy-rsa/keys/ta.key 0
```

- **/usr/sbin/openvpn /etc/openvpn/Server.conf**
Use this command to check OpenVPN starting. It will teach us where there are mistakes.
- **service openvpn start**
- **service openvpn status**

3.5.3 Create Clients

- **cd ./easy-rsa/**
- **source .vars**
- **./build-key Client1**
- **cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/easy-rsa/keys/client.ovpn**
- **cp ./keys/client.ovpn¹⁷**

Next lines will be modified as follows:

First look:

```
remote my-server-1 1194
```

```
;user nobody
;group nogroup
```

```
ca ca.crt
cert server.crt
```

¹⁷ Check Attached document III: Clients generator.

key server.key

;tls-atuh ta.key 1

;cipher x

Final appearance:

remote 192.168.42.1 1194

user nobody

group nogroup

#ca ca.crt

#cert server.crt

#key server.key

tls-atuh ta.key 1

cipher AES-128-CBC

***Notice certificates have been commented and thus because they are going to be introduced them into the file. As to make it, they will be added them at the bottom.**

<ca>

(Press Ctrl+R to insert one document. It will request for the document's name. Introduce "ca.crt", without apostrophes)

</ca>

<cert>

(Repeat the same action but changing ca.crt to "Client1.cert" or whatever is the name of the client's file)

</cert>

<key>

(Same action for "Client1.key")

</key>

It should have a look like:

<ca>

-----BEGIN CERTIFICATE-----

[...]

-----END CERTIFICATE-----

</ca>

```
<cert>
Certificate:
[...]
-----BEGIN CERTIFICATE-----
[...]
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
[...]
-----END PRIVATE KEY-----
</key>
```

Save and close. The .ovpn document is the client's certificate, which should be transfer to it for authenticating itself.

3.5.4 WinSCP

1. Select SCP protocol and press Advanced options (Figure 3-26).

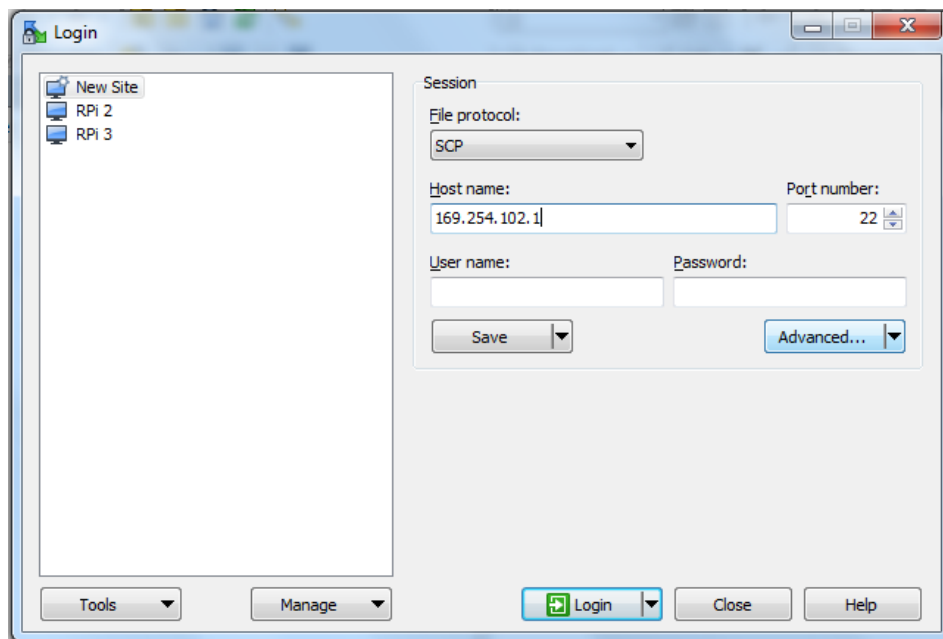


Figure 3-26 Screenshot of a WinSCP Session

2. Shell sudo su – will log into root session (Figure 3-27).

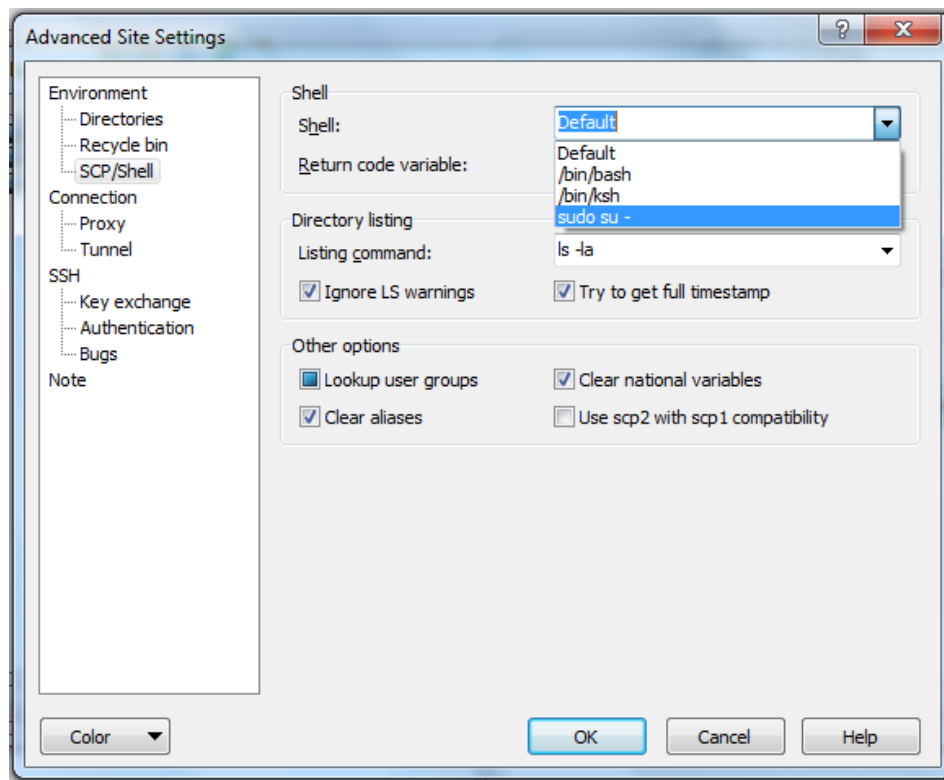


Figure 3-27 Screenshot of WinSCP root session

3. Copy Client1.ovpn into a folder of the Workstation (Figure 3-28).

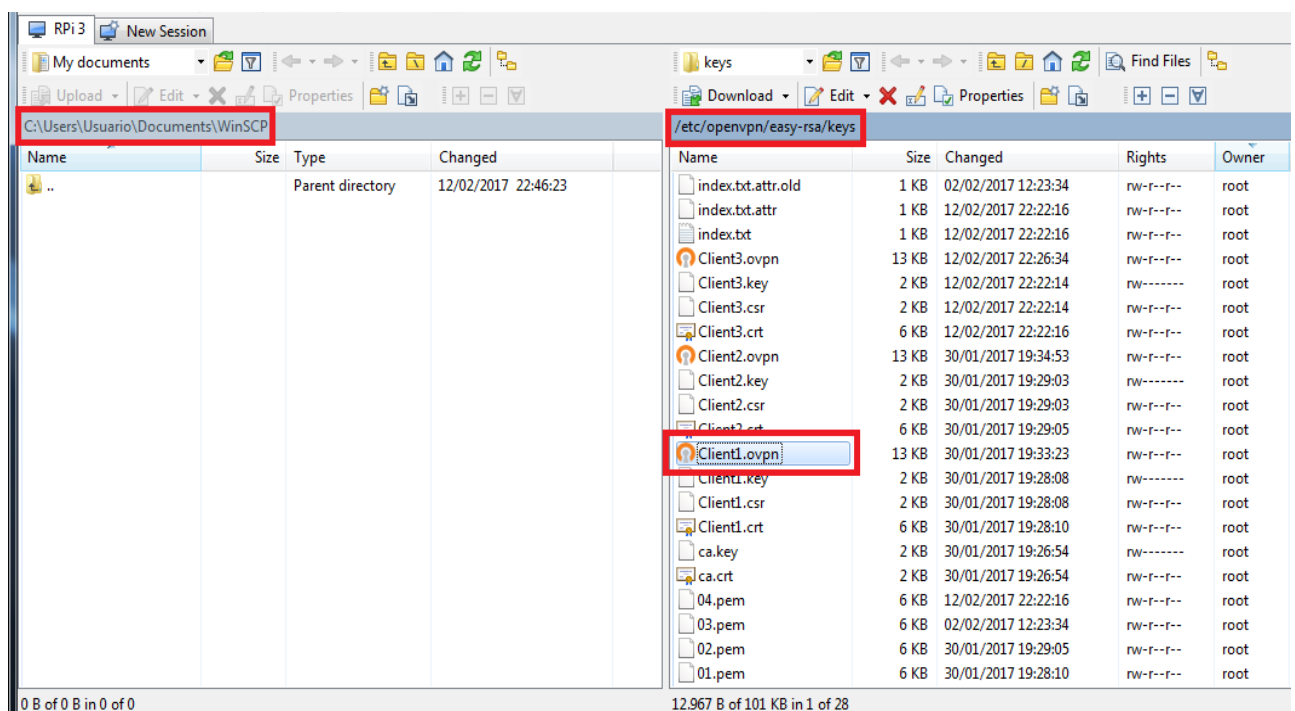


Figure 3-28 Screenshot copying ovpn file

By the moment, WinSCP will maintained as transferring method and, once the file is on a Windows station, moving it into our Workstation by means of a pen drive or a USB cable. Lastly, OpenVPN program must know where to find Client1.ovpn:

- In **Windows** move the file to the link:
C:\Program Files\OpenVPN\config
- In **Android** it will be enough to route a new profile (Figure 3-29 and Figure 3-30):

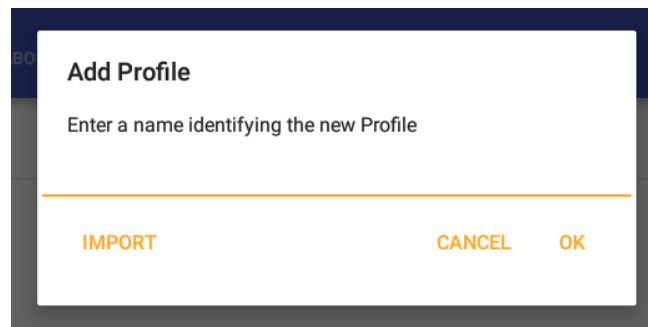


Figure 3-29 Screenshot importing a Profile

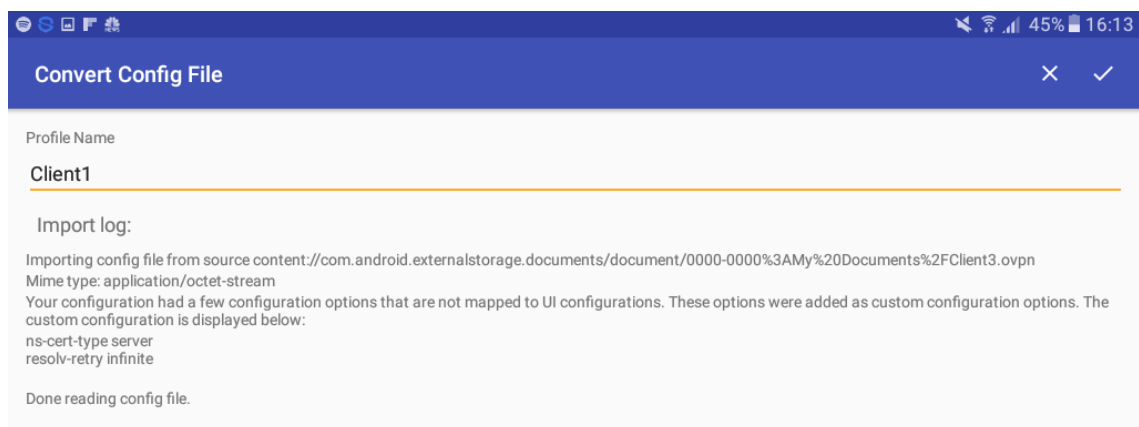


Figure 3-30 Screenshot naming the profile

- In **Mac OS** not tested¹⁸, neither on **iOS**
- **ifconfig tun0**
Starting tunnel failures is a symptom of a misstep. If everything went alright checking openvpn server it should not fail, yet, if it does skim the guide again looking for misspelling typing.
- **exit**
- **sudo nano /etc/hosts**
Clients are going to request DNS servers for the OpenVPN one. Owing that the Raspberry Pi is providing us net access, it could answer that question warning us that it is the server.

Typing the server address and dubbing it with the server address internal NAT will resolve it:

192.168.42.1 Server

Save and close.
- **sudo nano /etc/openvpniptables.sh**¹⁹

¹⁸ Tutorial [122]

¹⁹ Respect same rule about keeping single lines

Same clear net and toriptables' access process will be repeated. It could even work in toriptables copying the same document with openvpn's name (sudo cp /etc/toriptables.sh /etc/openvpn.sh). Scroll down and type last missing part.

```
#!/bin/sh
```

```
###Set variables
```

```
#TOR UID (run "-u debian-tor" in case you do not know)
```

```
_tor_uid="109"
```

```
#TOR's TransPort
```

```
_trans_port="9040"
```

```
#TOR DNSPort
```

```
_dns_port="53"
```

```
#TOR Virtual Address Network IPv4
```

```
_virt_addr="10.192.0.0/10"
```

```
#Outgoing/Incoming, SSH and tun interfaces
```

```
_out_if="wlan0"
```

```
_inc_if="wlan1"
```

```
_ssh_if="eth0"
```

```
_tun_if="tun0"
```

```
#LAN destinations not routed through TOR
```

```
_non_tor="127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16"
```

```
#Other IANA destinations not routed through TOR
```

```
_resv_iana="0.0.0.0/8 100.64.0.0/10 169.254.0.0/16 192.0.0.0/24 192.88.99.0/24  
198.18.0.0/15 198.51.100.0/24 203.0.113.0/24 224.0.0.0/3"20
```

```
#Accept all the traffic in order not to lock you out
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

²⁰ Command lines here referred must be typed in one single line.

iptables -P OUTPUT ACCEPT

#Flush previous iptables

iptables -F

iptables -t nat -F

#TOR iptables

iptables -t nat -A PREROUTING -i \$_ssh_in -p tcp --dport 22 -j REDIRECT --to-ports 22

iptables -t nat -A PREROUTING -i \$_inc_if -p udp --dport 53 -j REDIRECT --to-ports \$_dns_port²¹

iptables -t nat -A PREROUTING -i \$_inc_if -p udp 5353 -m udp --dport 5353 -j REDIRECT --to-ports \$_dns_port²¹

iptables -t nat -A PREROUTING -i \$_inc_if -p tcp -m tcp --syn -j REDIRECT --to-ports \$_trans_port²¹

#Allow LAN access in IANA reserved blocks

for _lan in \$_non_tor; do

iptables -t nat -A PREROUTING -i \$_inc_if -d \$_lan -j RETURN

done

for _iana in \$_resv_iana; do

iptables -t nat -A PREROUTING -i \$_inc_if -d \$_iana -j RETURN

done

#Local redirection

iptables -t nat -A OUTPUT -p udp --dport 53 -j REDIRECT --to-ports \$_dns_port

iptables -t nat -A OUTPUT -p tcp -m tcp --syn -j REDIRECT --to-ports \$_trans_port

iptables -t nat -A OUTPUT -m owner --uid-owner \$_tor_uid -j RETURN

iptables -t nat -A OUTPUT -o lo -j RETURN

#Allow LAN access in IANA reserved blocks

for _lan in \$_non_tor; do

iptables -t nat -A OUTPUT -i \$_inc_if -d \$_lan -j RETURN

done

²¹ Command lines here referred must be typed in one single line.


```
for _iana in $_resv_iana; do
    iptables -t nat -A OUTPUT -i $_inc_if -d $_iana -j RETURN
done

# Masquerading
iptables -t nat -A POSTROUTING -o $_out_if -j MASQUERADE

#OpenVPN iptables
iptables -t nat -A PREROUTING -i $_tun_if -p udp --dport 53 -j REDIRECT --to-ports
$_dns_port22
iptables -t nat -A PREROUTING -i $_tun_if -p udp 5353 -m udp --dport 5353 -j REDIRECT
--to-ports $_dns_port22
iptables -t nat -A PREROUTING -i $_tun_if -p tcp -m tcp --syn -j REDIRECT --to-ports
$_trans_port22
```

- **sudo chmod 755 /etc/toriptables.sh**
- **sudo sh -c “iptables-save > /etc/iptables/rules.v4”**
- **Starting OpenVPN Connection²³**

- **Windows**

Run OpenVPN program and it will show up at tools bar (Figure 3-31). Then press it and select the client .Workstation must be connected to hotspot’s LAN, if not, client will never find the server (Figure 3-32 and Figure 3-33).



Figure 3-31 Screenshot OpenVPN’s options

²² Command lines here referred must be typed in one single line.

²³ Mac OS and iOS not formally tested

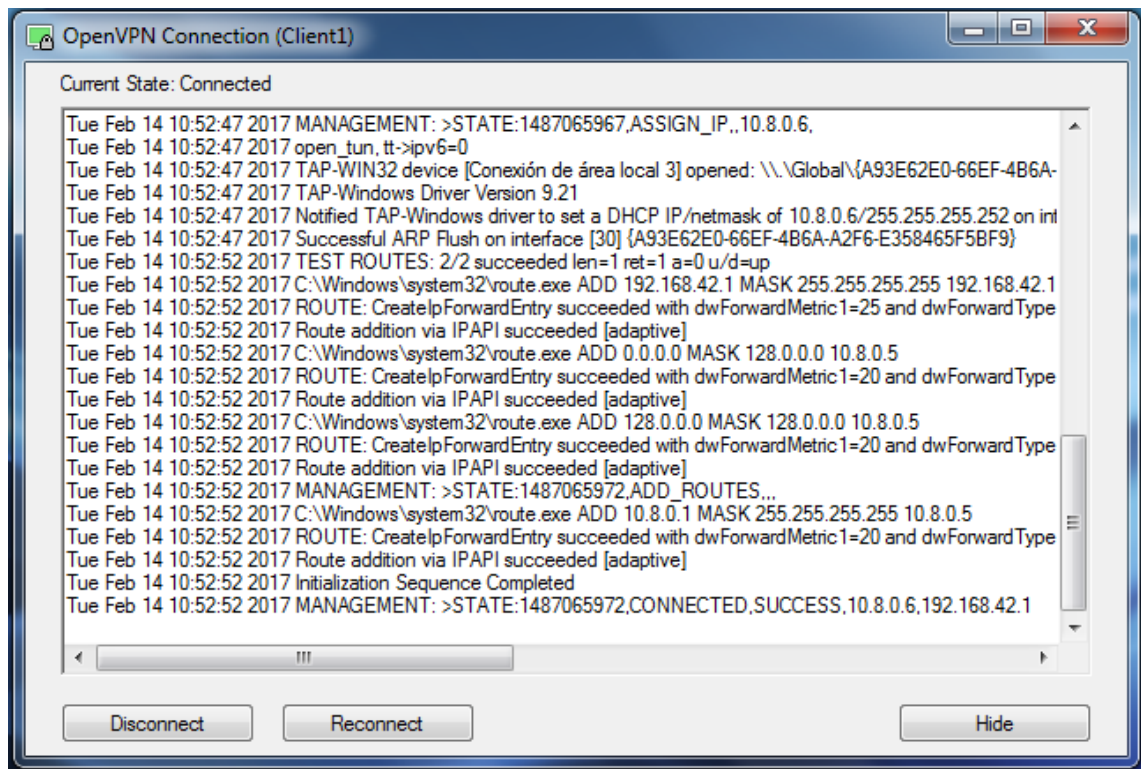


Figure 3-32 Screenshot Initialization Scheme

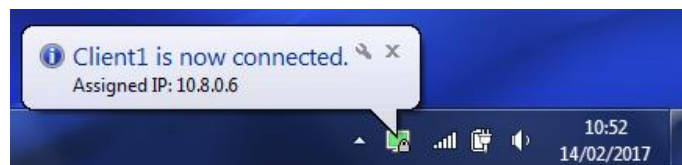


Figure 3-33 Screenshot Successful Windows Connection

- **Android**
Starting client's profile set earlier is enough. It should display a Figure 3-34's similar look.

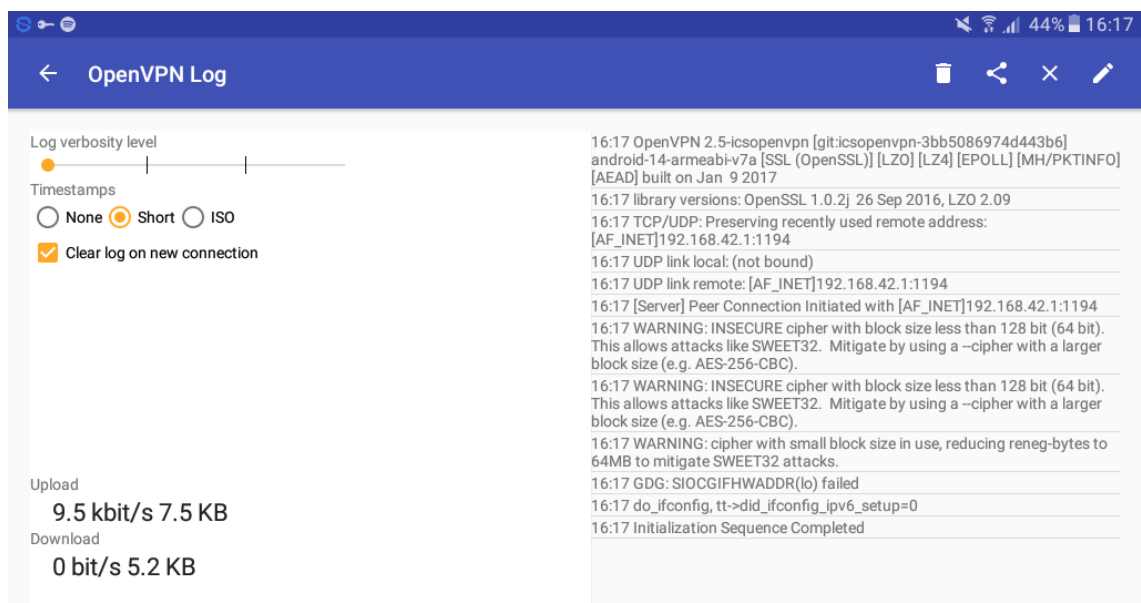


Figure 3-34 Screenshot Successful Android Connection

3.6 ClamAV antivirus [93]

Given the analysis debated in section 2.4.7 ClamAV is the antivirus chosen to protect Raspberry Pi hotspot (Figure 3-35). First command will install ClamAV program and second one its managing interface. At any moment, it would be possible to execute a scan introducing the command “clamscan”:

- **sudo apt-get install clamav**
- **sudo apt-get install clamtk**

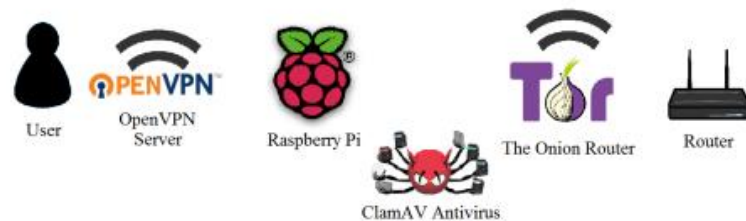


Figure 3-35 ClamAV antivirus (edited from [3])

3.7 Uncomplicated Firewall [80]

UFW contains a catalogue of common filtering rules. All the same, it will be necessary to load VPN's iptables. Both codes must not interfere, UFW will retain filtering rules while OpenVPN and TOR nat ones (Figure 3-36).

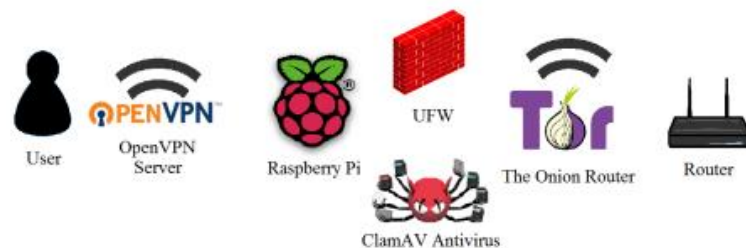


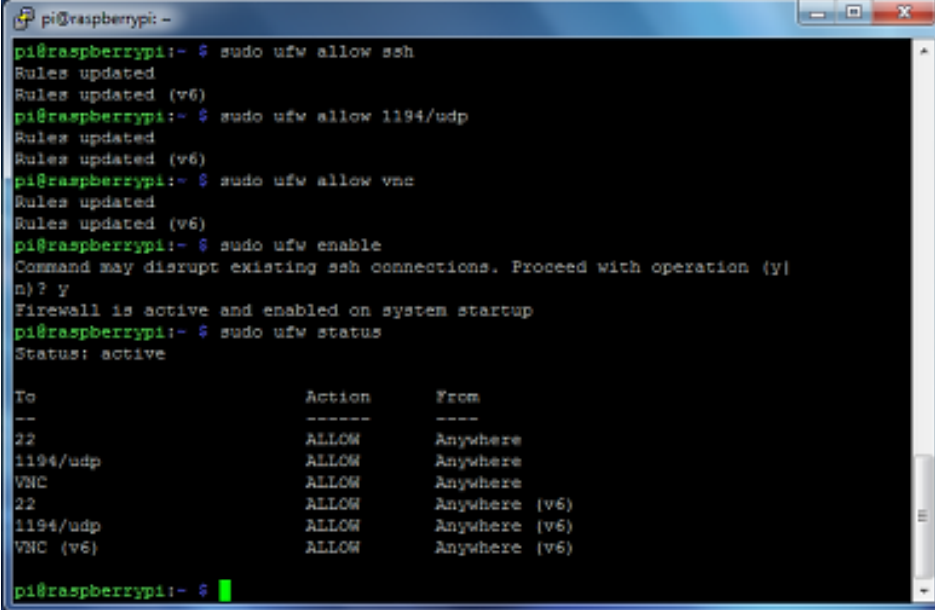
Figure 3-36 Uncomplicated Firewall (edited from [3])

- **sudo apt-get install ufw**
- **sudo ufw allow 1194/udp**
- **sudo ufw allow ssh**
- **sudo ufw allow 53**
- **sudo ufw allow 5353**
- **sudo ufw allow 9040**
- **sudo ufw allow vnc**

Those commands will add allowing rules to ports OpenVPN, SSH, VNC and TOR respectively. In case ufw vnc rule does not recognize VNC enter attempts, specific port is to be introduced (sudo ufw allow 590n, replacing “n” for the number of the VNC profile)²⁴.

- **sudo service ufw start**
- **sudo service ufw status** (Figure 3-37)

²⁴ VNC server transport port is 5900 and, ever a profile is created, it will designate it the number of that profile plus 5900 port.



```

pi@raspberrypi:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
pi@raspberrypi:~$ sudo ufw allow 1194/udp
Rules updated
Rules updated (v6)
pi@raspberrypi:~$ sudo ufw allow vnc
Rules updated
Rules updated (v6)
pi@raspberrypi:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
pi@raspberrypi:~$ sudo ufw status
Status: active

To Action From
--
22 ALLOW Anywhere
1194/udp ALLOW Anywhere
VNC ALLOW Anywhere
22 ALLOW Anywhere (v6)
1194/udp ALLOW Anywhere (v6)
VNC (v6) ALLOW Anywhere (v6)

```

Figure 3-37 Screenshot UFW status

- **sudo nano /etc/openvpniptables.sh**
Commenting “iptables F” filtering tables will not be flushed, keeping UFW rules.
- **sudo sh /etc/openvpniptables.sh**

3.8 Crontab

Coming back to the State of the art, where it was reviewed TOR working method, it was explained that a TOR server provided a list of TOR nodes to our hotspot (Section 2.4.2). Forcing hotspot to redirect even local traffic through TOR, it will never find a path to reach those nodes. Thus, Raspberry Pi needs a small period to receive that list.

Crontab is a Raspbian function which executes files or commands at the booting, or at any time selected. In the light of the above, local redirection will be delayed. It must not be forgotten that hotspot is meant to be portable, from where we can infer that user will take a short time to search for a Wi-Fi LAN and to connect it.

To edit Crontab follow the commands below:

- **crontab -e**²⁵
It will request for a text editor; pressing enter without typing anything will apply nano text editor.
Crontab format is @period (daily, weekly, monthly, annually or reboot) plus rule. Sleep command will be used to delay beginning. 180 seconds will be enough to connect a new router and 30 if the LAN is already set:

@reboot sleep 30; sudo sh /etc/openvpniptables.sh #Active local redirection

- **sudo cp /etc/openvpniptables.sh /etc/startingiptables.sh**
- **sudo /etc/startingiptables.sh**
Scroll down until local redirection nat tables and comment these lines:

²⁵ Do not use sudo because it will edit root's crontab.

```
#Local redirection
#iptables -t nat -A OUTPUT -p udp --dport 53 -j REDIRECT --to-ports $_dns_port
#iptables -t nat -A OUTPUT -p tcp -m tcp --syn -j REDIRECT --to-ports $_trans_port
#iptables -t nat -A OUTPUT -m owner --uid-owner $_tor_uid -j RETURN
#iptables -t nat -A OUTPUT -o lo -j RETURN
```

```
#Allow LAN access in IANA reserved blocks
#for _lan in $_non_tor; do
#    iptables -t nat -A OUTPUT -i $_inc_if -d $_lan -j RETURN
#done
```

```
#for _iana in $_resv_iana; do
#    iptables -t nat -A OUTPUT -i $_inc_if -d $_iana -j RETURN
#done
```

- **sudo chmod 755 /etc/startingiptables.sh**
- **sudo sh -c “iptables-save > /etc/iptables/rules.v4”**

At this moment, Raspberry Pi will boot with a clear access to Internet but workstations will remain conceal down TOR and OpenVPN layers. After sleeping time has been consumed, hotspot will also redirect its own traffic through the TOR net. Furthermore, it can be edited a periodically scan:

- **crontab -e²⁶**

```
30 * * * * /usr/bin/freshclam --quiet; /usr/bin/clamscan --recursive --infected #Clamscan
```

Saving and closing the file the system will execute a scanning each half an hour.

3.9 DNS cache proxy [94]

As a matter of fact, the bottle neck caused by the filter will slow down navigation experience. Hence, Raspberry Pi will require of other methods to speed up the process, like an own DNS resolver.

Linux based on operative systems' building packet to perform as DNS cache server is called dnsmasq. Basically, the application will store DNS queries to subsequent requests. Contrary to what might be supposed, dnsmasq hosts do not consume much of MicroSD capacity and their life period is determined for its TTL (Time to Live. Labelled on its original webpage).

Besides, DNS utils will be downloaded to test service caching. A correct active working should increase the speed after a first search. Introduce what follows:

- **sudo apt-get install dnsmasq**

²⁶ Do not use sudo because it will edit root's crontab.

- **sudo apt-get install dnsmutils**
- **sudo nano /etc/dnsmasq.conf**

Editing this file DNS will listen to wlan1. Pressing Ctrl+W and writing #interface it will scroll directly to that line. Interface must be uncommented and wlan1 typed, without apostrophes. Final look will be:

```
interface=wlan1
```

- **sudo nano /etc/resolv.conf**

In case it would not be present, DNS queries are to be redirected to the server:

```
nameserver 127.0.0.1
```

- **sudo service dnsmasq start**
- **sudo service dnsmasq status**

DNS masquing status is not evidence enough to validate DNS caching. DNS utils packet will light answering time, proving if there really is an improvement.

- **time nslookup www.australia.gov.au**
- **time nslookup www.australia.gov.au**

3.10 VNC Server [95]

VNC program runs Raspberry Pi's desktop on another station. Concerning to this project it will serve to visualize all the steps carried out. It will also be a more comfortable interface to manage LAN connection.

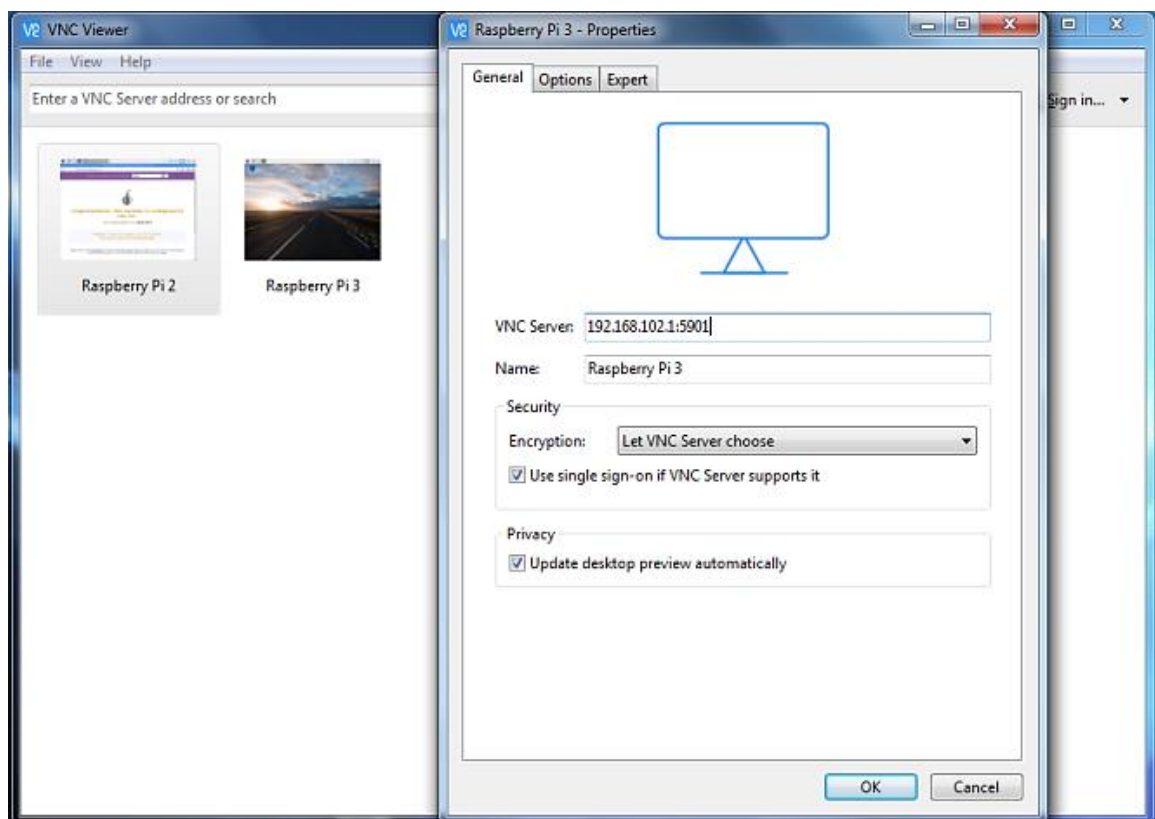


Figure 3-38 Screenshot of a VNC interface creation

VNC needs of a Raspbian packet and a VNC viewer for the station. Next steps result on the installation and configuration of a VNC interface:

- Typing next commands into Raspberry Pi's CLI:
 - **sudo apt-get install tightvncserver**
 - **sudo vncserver :1**
It generates a default desktop.
- VNC Viewer is to be downloaded from [17].
- IP address will be introduced plus the port produced, as shown in Figure 3-38

4 TESTING & VALIDATION

4.1 Tests

4.1.1 Introduction

Unless TOR hotspot would sustain a safe and steady experience, it will be useless. In order to assess their capabilities some tests will be prepared. Both centres of evaluation will be security, anonymity, as main objectives of this project, and speed, ensuring a fluent navigation.

4.1.2 Previous comparison between resources (1.3 Resources)

Features	CPU	RAM	WAN Access	Storage	LAN Adapter	Price [96]
RPi 2	900 MHz	1 GB	Adapter Raspberry Pi	8 GB		29.09 £
	ARM Quad-Core		2ABCB-WCU6331		TP-Link Adapter	34 €
RPi 3	1,2 GHz	1 GB	Integrated Wi-Fi card	16 GB	TL-WN823	32.99 £
	ARM Quad-Core		BCM2387			38.53 €

Table 4-1 Overview of Raspberry Pi 2 and Raspberry Pi 3's features

Table 4-1 exposes Raspberry Pi 3's predominance toward its predecessor, yet its features do not exceed outstandingly to Raspberry Pi 2's ones. Concerning to such close characteristics and regarding some of them are almost equal (like dimensions or inputs/outputs); it is not to be expected strong discrepancies between their performances.

With reference to this previous evaluation, the ridiculous price difference and the absence of an integrated Wi-Fi card into Raspberry Pi 2 would give advantage to the newest model. Saved wireless adapter could be invested in a more powerful accessory. In this case, only superior feature will be MicroSD's storage.

Supposing a similar behaviour, assessing both devices with the whole configuration set will be enough. In case the results showed a great disparity, more tests would be carried out to determine where it could come from.

4.1.3 Security

Viruses are the most dangerous within the Militarized Zone, meanwhile a Man in the Middle monitoring or sniffing, beyond the firewall. Tests designed to show security gaps will have to try to

break into the system and to seize information both, inside workstations and travelling to its respective destinations.

Antivirus will be tested by means of downloading viruses to check if ClamAV warns or forbids the action. On the other hand, Wireshark will be used to spy communications and to capture packets of valuable information.

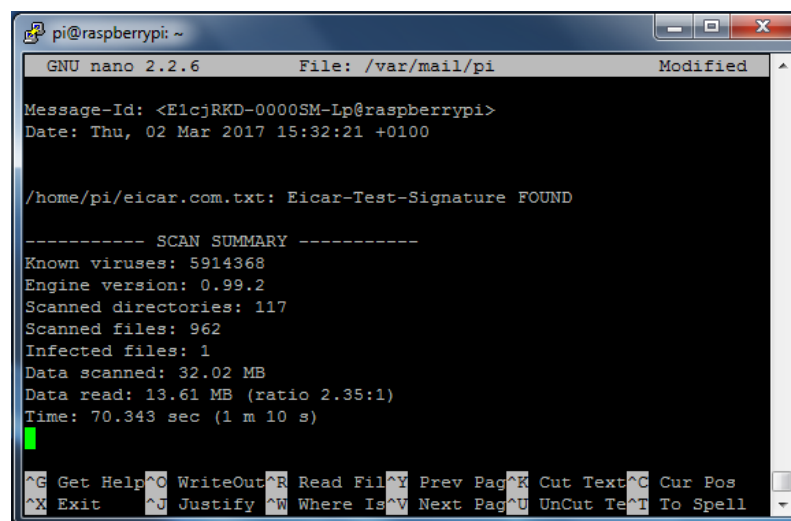
Expected behaviours are; popping-up authorizations warnings that request permission to continue executing a suspect marked code, denial of certain dangerous actions, virus detection through scans and lack of clear exchange of data, and of encryption leaks.

4.1.3.1 Virus test

European Institute for Computer Anti-Virus Research developed a text file implementing a small malicious code to check the functioning of firewalls and antivirus [97]. Regardless detecting Eicar virus does not mean being all-viruses-proof; it serves to determine whether the antivirus is activated.

Coming back to section 3.6 and 3.8, ClamAV was installed and a periodical scan was established. Thus, if a virus is download it should be recognized, logged and deleted it. In order to test it, following commands are to be typed [98]:

- **wget https://secure.eicar.org/eicar.com.txt**
Download eicar virus code
- **ls**
eicar.com.txt should appear into the folder
- **clamscan**
- **sudo nano /var/mail/pi**
Whenever the system warns that user has a message it will send it to mail folder. Related to this topic, it is notifying the result of a scan. Last two commands should present the inspection's summary (Figure 4-1).



```

pi@raspberrypi: ~
GNU nano 2.2.6      File: /var/mail/pi      Modified
Message-Id: <E1cjRKD-0000SM-Lp@raspberrypi>
Date: Thu, 02 Mar 2017 15:32:21 +0100

/home/pi/eicar.com.txt: Eicar-Test-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 5914368
Engine version: 0.99.2
Scanned directories: 117
Scanned files: 962
Infected files: 1
Data scanned: 32.02 MB
Data read: 13.61 MB (ratio 2.35:1)
Time: 70.343 sec (1 m 10 s)

^G Get Help ^O WriteOut ^R Read Fil ^Y Prev Pag ^K Cut Text ^C Cur Pos
^X Exit    ^J Justify ^W Where Is ^V Next Pag ^U UnCut Te ^T To Spell

```

Figure 4-1 Screenshot of scanning summary message

ClamAV has proved being capable of finding out the virus but it has not made any action apart from logging and notifying it. Eicar virus has had to be deleted manually (Attached document IV: Virus test). Deeper configuration is to be set concerning to ClamAV antivirus and more specific attacks should be perpetrated to search guarding debilities. Is to be remark that workstation security should be granted by an own antivirus.

4.1.3.2 Wireshark test

With reference to the National Cybersecurity of Spain, Wireshark have four different locations to spoofing packets [99] (Figure 4-2). In this case, the most suitable will be Bridge mode, placing a Wireshark installed computer between the hotspot and the WAN (Figure 4-3).

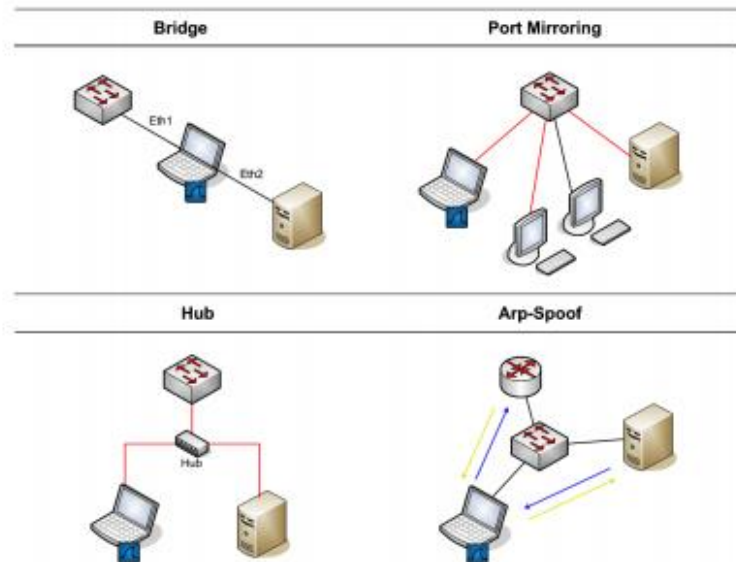


Figure 4-2 Wireshark sniffing structures (taken from [99])



Figure 4-3 Wireshark Monitoring Framework (edited from [3])

For this purpose, hotspot is forced to swap its IP tables to redirect the outgoing traffic through Ethernet. It would be also possible to keep current configuration and to create an access point from the mentioned computer using any of the adapters. Next guide builds first structure:

- Connecting Raspberry Pi 3 to the computer through SSH and switching on.
- Execute the following commands:
 - **sudo cp /etc/checkinternet.sh /etc/checkwireshark.sh**
By editing outgoing interface Ethernet enables.

```
#!/bin/sh
```

```
###Clear Internet access configuration
```

```
#Accept all the traffic in order not to lock you out
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

#Flush previous iptables

iptables -F

iptables -t nat -F

#Forwarding

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

iptables -A FORWARD -i eth0 -o wlan1 -m state --state RELATED,ESTABLISHED -j ACCEPT²⁷

iptables -A FORWARD -i wlan1 -o eth0 -j ACCEPT

– **sudo sh /etc/checkwireshark.sh**

- Sharing Internet connection [100] (Windows and MAC)
- Opening Wireshark and clicking on the preshared LAN. [Figure 4-4]

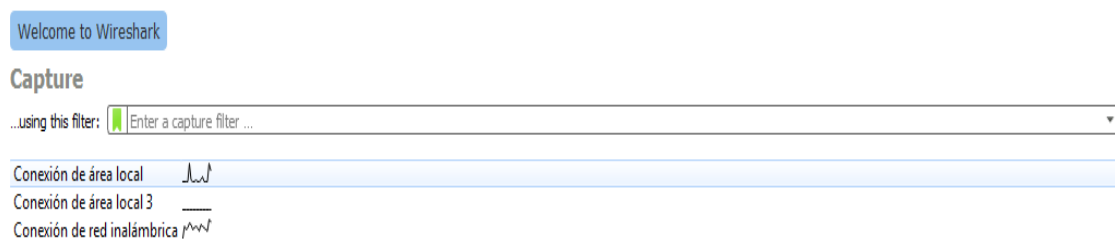


Figure 4-4 Screenshot of Wireshark homepage

- Browsing on internet with a third party device through Garbo Wi-Fi hotspot.

At this point, Wireshark will start to display a list of packets which contains the information between endpoints. Even though Socket secured pages certificate and authenticate them, as to increase the speed of the interacting experience these webs only encrypt initialization and passwords exchanging. Therefore, the rest of the information is susceptible of being sniffed. This experiment is divided into five different aims named and developed in the following sections.

4.1.3.2.1 Monitoring traffic

Opening Statistics menu into tools bar, and Endpoints within it, it will be opened a window containing all the workstations present in the net.

²⁷ Command lines here referred must be typed in one single line.

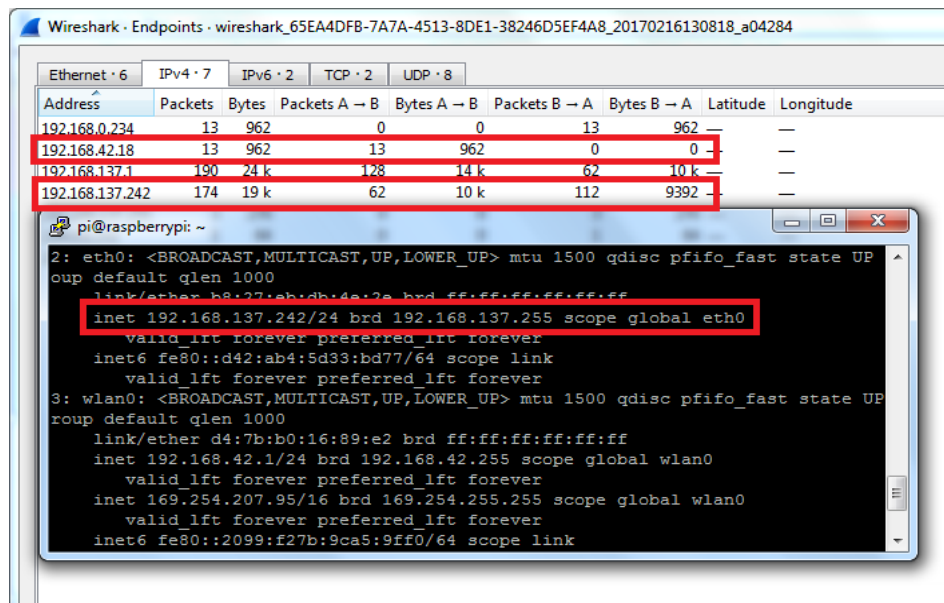


Figure 4-5 Screenshot of Raspberry Pi IP searching

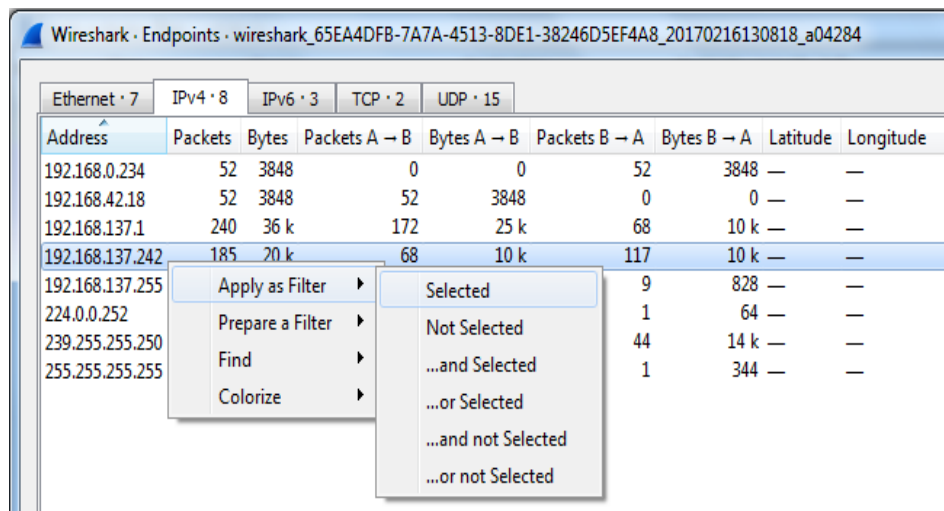


Figure 4-6 Screenshot of filtering victim's traffic

Results in first two test (Attached document V: Wireshark Test) not only display the Raspberry hotspot, but the workstations connected to it, further intelligence than it was predicted, as shot in Figure 4-5. Wireshark has the capability of filtering one IP address, thus, by right-mouse-bottom-clicking the drop-down, in Figure 4-6, this function will be offered.

4.1.3.2.2 Seizing worthy files

Owing to Internet traffic is clear; Wireshark should be able to sniff some files. Apart from filtering addresses, Wireshark is able to arrange communications protocols and it does highlight them in colours.

Hyper Text Transfer Protocol (HTTP) is one of the prime Internet protocols as it manages the majority of application and webs. It will be in there where packets will be captured.

No.	Time	Source	Destination	Protocol	Length	Info
98	3.206114	192.168.137.103	scontent-mad1-1.cdn...	HTTP	378	GET /t51.2885-19/s150x150/11363800_1930...
99	3.207010	192.168.137.103	scontent-mad1-1.cdn...	HTTP	388	GET /t51.2885-19/s150x150/14704983_3494...
118	3.221891	scontent-mad1-1.cdn...	192.168.137.103	HTTP	158	HTTP/1.1 200 OK (JPEG JFIF image)
123	3.223002	scontent-mad1-1.cdn...	192.168.137.103	HTTP	543	HTTP/1.1 200 OK (JPEG JFIF image)
304	9.486175	192.168.137.103	scontent-mad1-1.cdn...	HTTP	393	GET /t51.2885-15/s640x640/e15/16789118...
305	9.486640	192.168.137.103	scontent-mad1-1.cdn...	HTTP	392	GET /t51.2885-15/s240x240/e35/14591118...
312	9.507174	192.168.137.103	scontent-mad1-1.cdn...	HTTP	393	GET /t51.2885-15/s240x240/e35/16585649...
320	9.507955	scontent-mad1-1.cdn...	192.168.137.103	HTTP	154	HTTP/1.1 200 OK (JPEG JFIF image)
342	9.519144	192.168.137.103	scontent-mad1-1.cdn...	HTTP	406	GET /t51.2885-15/s240x240/e35/c0.14.720...
357	9.522136	192.168.137.103	scontent-mad1-1.cdn...	HTTP	403	GET /t50.2886-16/16783708_1255973697813...
366	9.537664	192.168.137.103	scontent-mad1-1.cdn...	HTTP	393	GET /t51.2885-15/s240x240/e15/16790054...
368	9.538523	scontent-mad1-1.cdn...	192.168.137.103	HTTP	339	HTTP/1.1 200 OK (JPEG JFIF image)
424	9.555679	scontent-mad1-1.cdn...	192.168.137.103	HTTP	903	HTTP/1.1 200 OK (JPEG JFIF image)
466	9.566957	scontent-mad1-1.cdn...	192.168.137.103	HTTP	764	HTTP/1.1 200 OK (JPEG JFIF image)
474	9.570929	scontent-mad1-1.cdn...	192.168.137.103	HTTP	932	HTTP/1.1 200 OK (JPEG JFIF image)
478	9.580495	192.168.137.103	scontent-mad1-1.cdn...	HTTP	408	GET /t51.2885-15/s240x240/e35/c114.0.85...

Frame 123: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface 0
 Ethernet II, Src: QuantaCo_7a:0f:17 (04:7d:7b:7a:0f:17), Dst: Raspberr_db:4e:2e (b8:27:eb:db:4e:2e)
 Internet Protocol Version 4, Src: scontent-mad1-1.cdninstagram.com (31.13.83.52), Dst: 192.168.137.103 (192.168.137.103)
 Transmission Control Protocol, Src Port: 80, Dst Port: 57448, Seq: 4195, Ack: 323, Len: 477
 [4 Reassembled TCP Segments (4671 bytes): #120(1398), #121(1398), #122(1398), #123(477)]
 Hypertext Transfer Protocol
 JPEG File Interchange Format

Figure 4-7 Screenshot of HTTP filtering²⁸

Figure 4-7 is an example of the traffic eavesdropped on hotspot. That traffic belongs to Instagram Android's application, a trustworthy supposed program. As discussed before, this type of application would be very stressing and useless if their reloading time was long because of the encryption. Therefore, once the user is logged and authenticated, the communication turns clear.

No.	Time	Source	Destination	Protocol	Length	Info
91	14.54	HTTP	393	GET /t51.2885-15/s240x240/e35/16123780...
95	14.55	HTTP	393	GET /t51.2885-15/s240x240/e35/15877124...
97	14.55	HTTP	392	GET /t51.2885-15/s240x240/e35/16110379...
98	14.55	HTTP	408	GET /t51.2885-15/s240x240/e35/c255.0.57...
137	14.57	HTTP	1396	HTTP/1.1 200 OK (JPEG JFIF image)
148	14.58	HTTP	1366	HTTP/1.1 200 OK (JPEG JFIF image)
185	14.60	HTTP	998	HTTP/1.1 200 OK (JPEG JFIF image)
189	14.61	HTTP	1068	HTTP/1.1 200 OK (JPEG JFIF image)
190	14.61	HTTP	393	GET /t51.2885-15/s240x240/e35/16110413...
195	14.62	HTTP	408	GET /t51.2885-15/s240x240/e35/c130.0.33...
199	14.64	HTTP	406	GET /t51.2885-15/s240x240/e35/c135.0.81...
207	14.64	HTTP	115	HTTP/1.1 200 OK (JPEG JFIF image)
218	14.65	HTTP	71	HTTP/1.1 200 OK (JPEG JFIF image)
219	14.65	HTTP	408	GET /t51.2885-15/s240x240/e35/c135.0.81...
223	14.66	HTTP	407	GET /t51.2885-15/s240x240/e35/c135.0.81...
231	14.67	HTTP	1381	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 218: ...
 Ethernet II ...
 Internet Protocol ...
 Transmission ...
 [11 Reassembled ...]
 Hypertext Transfer Protocol
 JPEG File Interchange Format

Figure 4-8 Screenshot of JPEG file seizing

Right-clicking on the packets intended to sniff it will deploy a menu which gives the opportunity to “show packets bytes” (Figure 4-8), in other words, to display the original file.

²⁸ New IP is due to experiments were made in different periods. In this line, in Attached document V: Wireshark Test both experiments' results are presented, making possible to tell the difference.

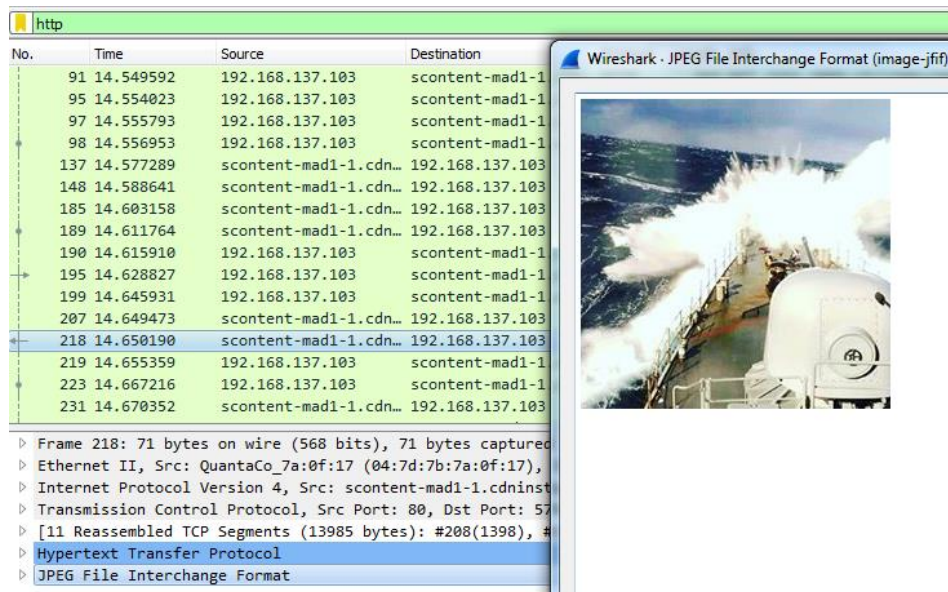


Figure 4-9 Screenshot of a JPEG image stolen

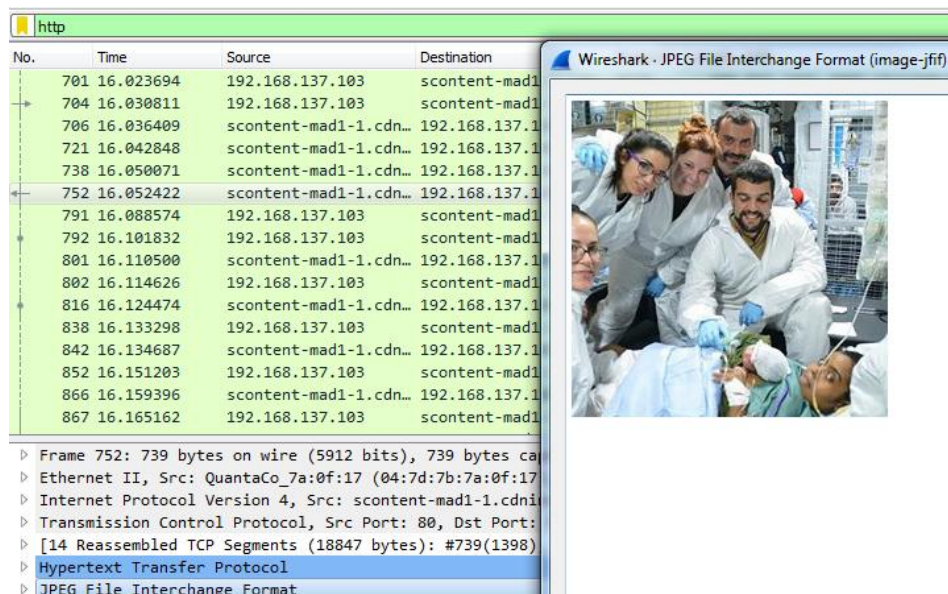


Figure 4-10 Screenshot of another example of stolen file

Previous figures (Figure 4-9 and Figure 4-10) exhibit examples of files seized. In spite of operating in a personal and private account, a third station has gained full admission to the data.²⁹

4.1.3.2.3 Hiding traffic through TOR

Next experiment seeks for determining whether TOR is able to deceive eavesdroppers. First thing will be reset TOR IP tables, for which it should be created a new IP tables file on the basis of toriptables.sh file. Assessing local redirection and workstation traffic within isolated tests, it will be possible to tell between specific leaks, bringing them to light. Therefore, following steps are to be taken:

- Copy and modify startingiptables.sh file on the CLI:

²⁹ Pictures have been gathered from Armada Española Instagram's account. Accomplishing articles 5 and 6 from the Second title of the Organic Law 15/1999, 13 December of Protection of Personal Data of the Spanish legislation, personal pictures captured have not been included in the document [123].

- **sudo cp /etc/toriptables.sh /etc/securitytestiptables.sh**
- **sudo nano /etc/securitytestiptables.sh**
Scroll down and comment those lines obtaining:

#Local redirection

```
#iptables -t nat -A OUTPUT -p udp --dport 53 -j REDIRECT --to-ports $_dns_port
#iptables -t nat -A OUTPUT -p tcp -m tcp --syn -j REDIRECT --to-ports $_trans_port
#iptables -t nat -A OUTPUT -m owner --uid-owner $_tor_uid -j RETURN
#iptables -t nat -A OUTPUT -o lo -j RETURN
```

#Allow LAN access in IANA reserved blocks

```
#for _lan in $_non_tor; do
```

```
#    iptables -t nat -A OUTPUT -i $_inc_if -d $_lan -j RETURN
```

```
#done
```

```
#for _iana in $_resv_iana; do
```

```
#    iptables -t nat -A OUTPUT -i $_inc_if -d $_iana -j RETURN
```

```
#done
```

- **sudo sh /etc/securitytestiptables.sh**
- Checking TOR enabling and disabling by entering in check tor webpage [91] in both Raspberry Pi and workstation (Figure 4-11 and Figure 4-12).
- Browsing on the Internet or using any online application (Figure 4-13).

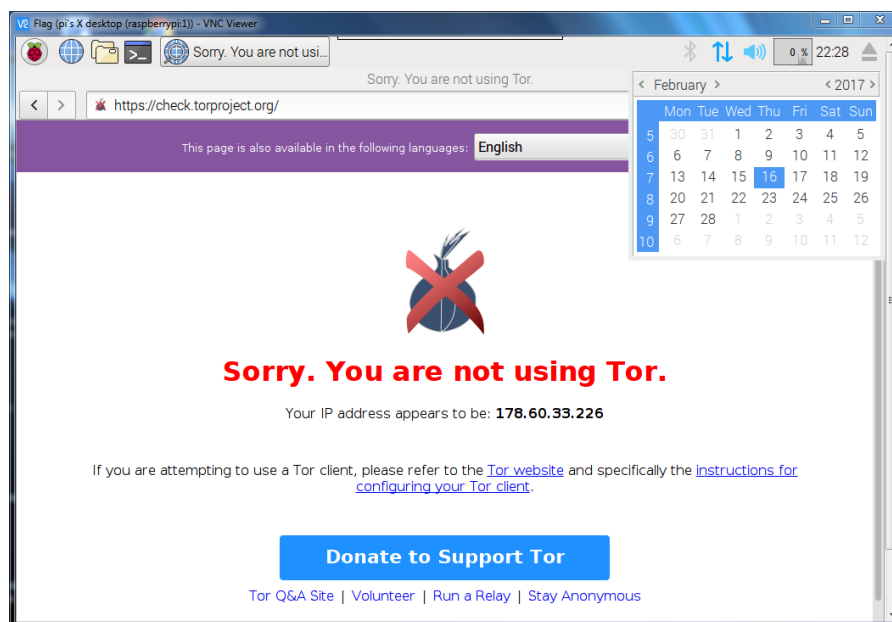


Figure 4-11 Screenshot of VNC desktop proving TOR's disabling

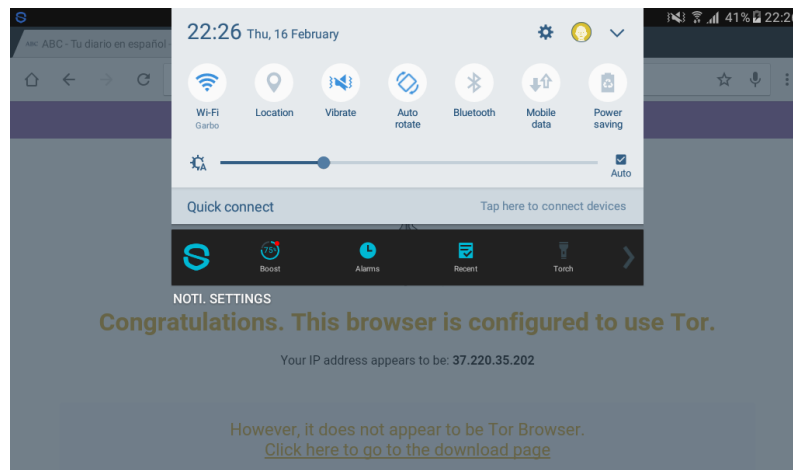


Figure 4-12 Screenshot of Tablet's interface showing Garbo TOR's redirection

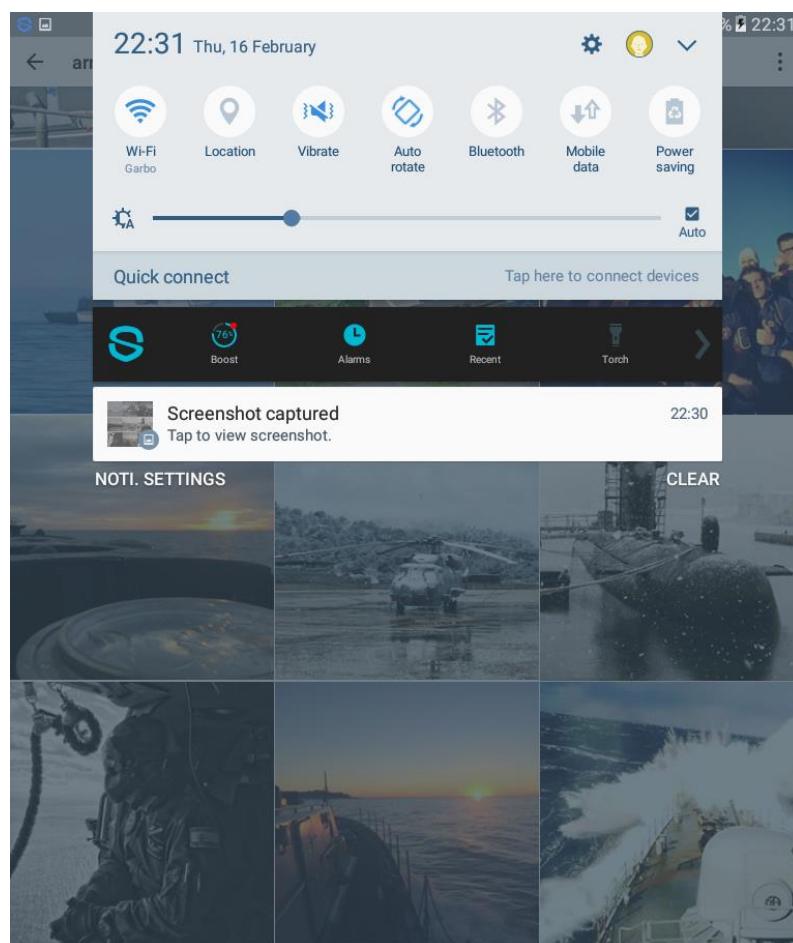


Figure 4-13 Screenshot of Tablet's interface exhibiting Garbo connection

Provided that the flow is crossing through Wireshark station it should not be blind to it. However, it must have no evidence of what it is transporting. In case it was attempted to get the same data as in the second test, it should be able, as much, to observe encrypted packets coming and going from hotspot.

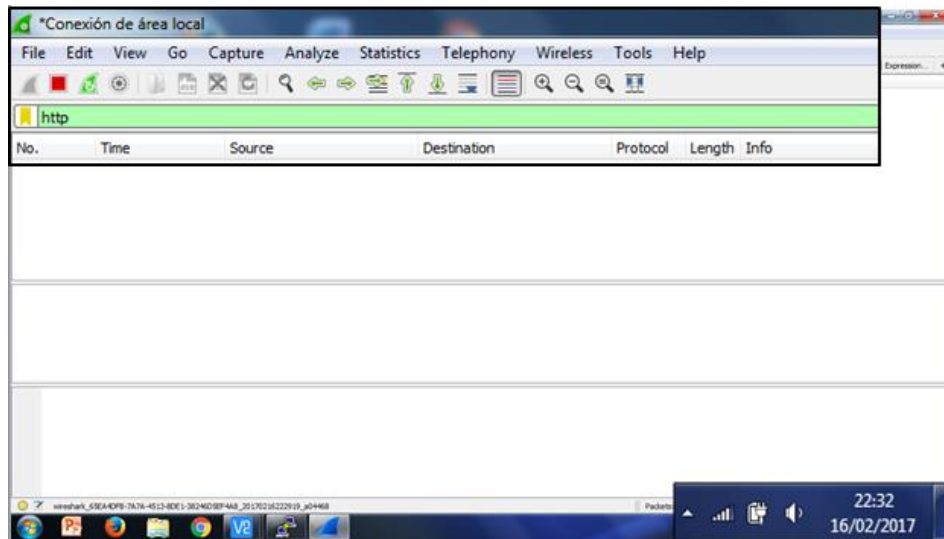


Figure 4-14 Screenshot of lacking packets intelligence

No.	Time	Source	Destination	Protocol	Length	Info
4565	225.463963	192.168.137.193	192.168.137.1	SSH	134	Server: Encrypted packet (len=80)
4574	226.076615	192.168.137.193	192.168.137.1	SSH	438	Server: Encrypted packet (len=384)
4577	226.143938	192.168.137.193	192.168.137.1	SSH	518	Server: Encrypted packet (len=464)
4580	226.502621	192.168.137.193	192.168.137.1	SSH	134	Server: Encrypted packet (len=80)
4582	226.502819	192.168.137.193	192.168.137.1	SSH	134	Server: Encrypted packet (len=80)
4584	226.533396	192.168.137.193	192.168.137.1	SSH	182	Server: Encrypted packet (len=128)
4586	226.574342	192.168.137.193	192.168.137.1	VNC	1321	
4589	226.575137	192.168.137.193	192.168.137.1	TCP	60	5901 → 50390 [ACK] Seq=195948 Ack=453 Win=229 Len=0
4591	226.945515	192.168.137.193	192.168.137.1	SSH	150	Server: Encrypted packet (len=96)
4593	228.072277	192.168.137.193	192.168.137.1	VNC	933	
4596	228.073087	192.168.137.193	192.168.137.1	TCP	60	5901 → 50390 [ACK] Seq=196827 Ack=463 Win=229 Len=0
4598	228.490733	192.168.137.193	192.168.137.1	SSH	118	Server: Encrypted packet (len=64)
4601	228.959422	192.168.137.193	192.168.137.1	SSH	118	Server: Encrypted packet (len=64)
4604	228.984538	192.168.137.193	192.168.137.1	SSH	118	Server: Encrypted packet (len=64)
4607	229.011852	192.168.137.193	192.168.137.1	SSH	118	Server: Encrypted packet (len=64)
4610	229.037325	192.168.137.193	192.168.137.1	SSH	118	Server: Encrypted packet (len=64)

Figure 4-15 Screenshot of encrypted communication monitoring

In the last two pictures (Figure 4-14 and Figure 4-15), obtained from data in the Fourth Wireshark test (Attached document V: Wireshark Test), it can be inferred that hotspot has accomplished, up to this point, with what was design for. This assumption is based on the lack of non SSH packets, independently the port they are using; HTTP, RTPS, SIP and so on.

4.1.3.2.4 Concealing Local traffic

Fourth test will be carried out with the complete TOR's set. Staring from toriptables.sh file the whole redirection will be activated, except from the OpenVPN one. As IP tables are configured both workstation and hotspot must be checked (Figure 4-16 and Figure 4-17):

- Typing “sudo /etc/toriptables.sh on the CLI
- Opening web browser and enter to check tor webpage [91]

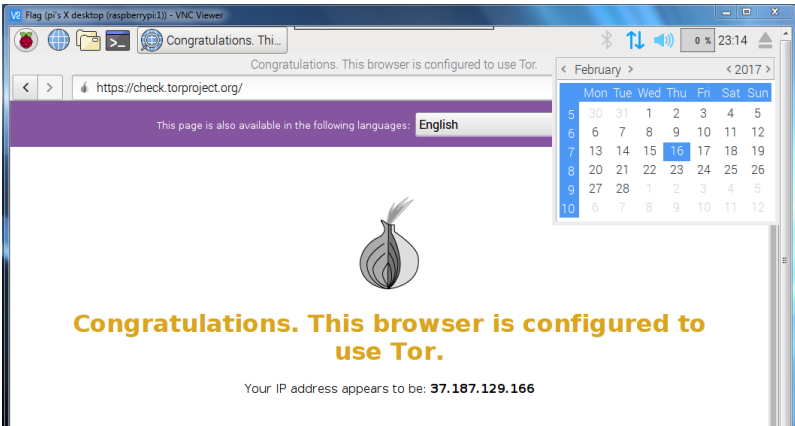


Figure 4-16 Screenshot of local traffic TOR redirection

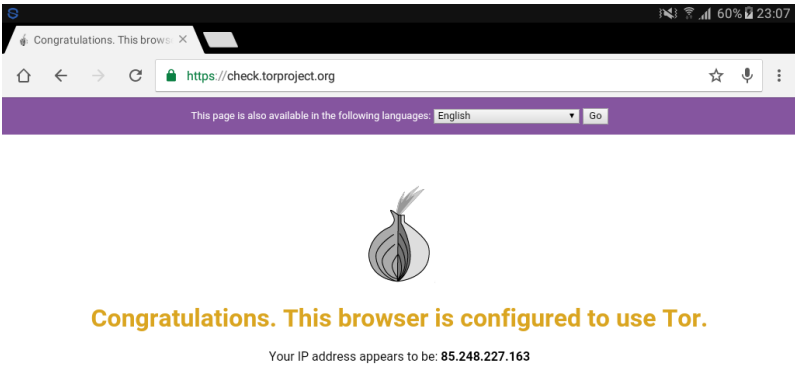


Figure 4-17 Screenshot checking once more TOR workstations' traffic redirection

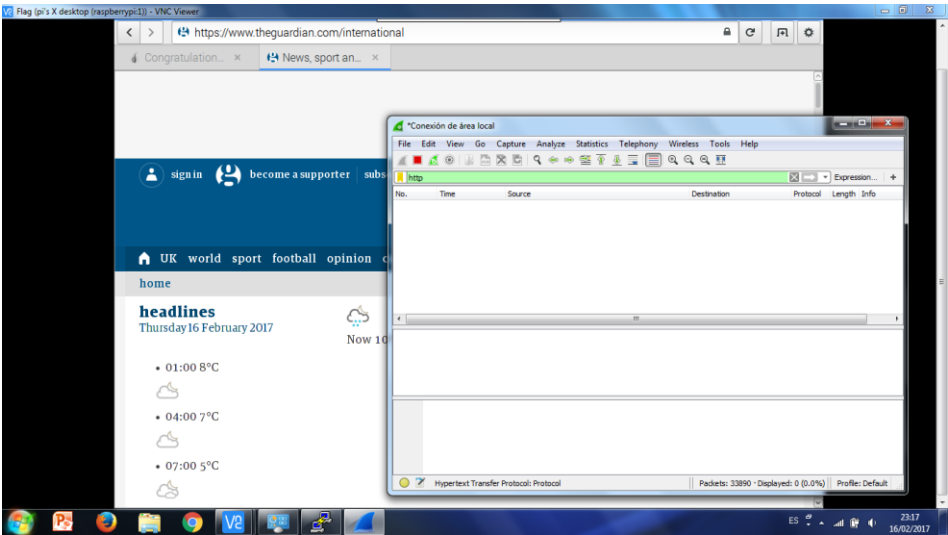


Figure 4-18 Screenshot of Wireshark trying to get Raspberry Pi local traffic

Last test, collected in the Attached document V: Wireshark Test (Fifth Wireshark test), gave the same results as the previous one. No valuable packet was seized (Figure 4-18). However, readings showed the further subnet. Although it is not vital leakage, it can compromise the security.

Presumably, OpenVPN will not cover that gap, in spite of the fact that it works with an own IP pool. Most likely line of action to solve the problem will be IP forwarding. Within the firewall, IP forwarding table are able to filter the incoming and outgoing traffic according to a series of rules. Thus, all the packets not properly encrypted could be dropped.

4.1.4 Anonymity

Given the results of the Wireshark experiment, it lasts to analyse how much information can be obtained from auxiliary protocols and association between messages and devices. Due to the fact that further identification has been subnet IP addresses, a network analyser or IP searcher will be employed. Fling has been downloaded and run inside and outside the hotspot's subnet.

Subnet's readings are pessimistic as they show devices' name (Figure 4-19) and their addresses (MAC and IP). Luckily and even providing the subnet's IP pool, outside the hotspot's LAN it gives no more than Raspberry Pi ID and address. It is to be noticed that it does not discover OpenVPN server's pool (Figure 4-20).

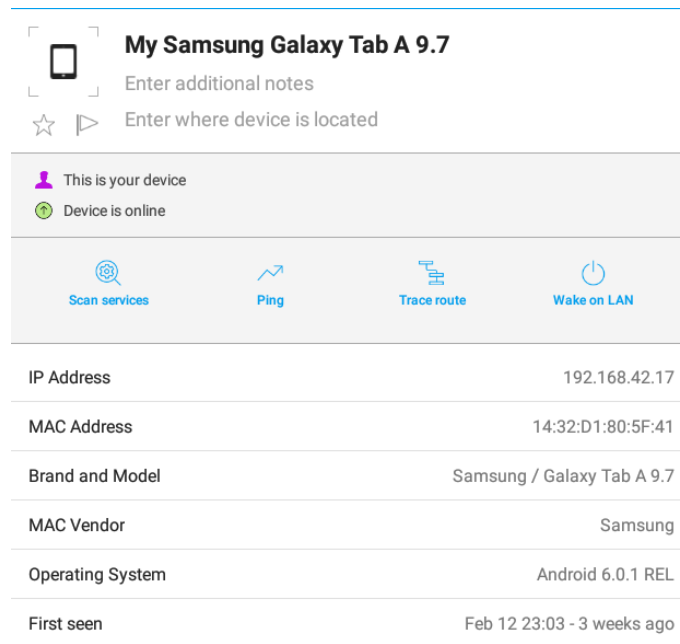


Figure 4-19 Screenshot of Tab A information obtained by Fling

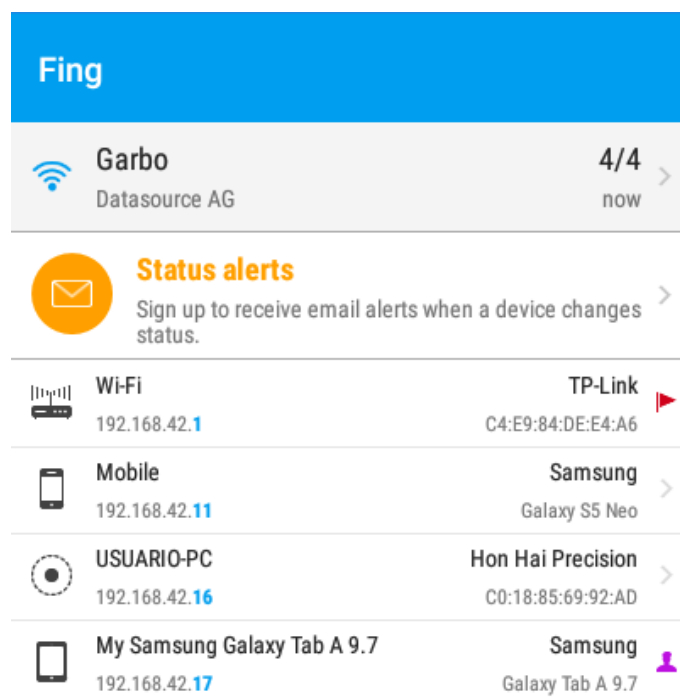


Figure 4-20 Screenshot of Fling results

In light of this new scene, threats will be remote connection and users' correlation with their devices. This inconvenience could be turned into an advantage dubbing stations and Raspberry Pi again with a false station code. Besides; SSH connection should be restricted just to Ethernet interface or by MAC filtering, pi user could be renamed and forward filtering table refined.

Coming back to TOR encryption, after last node there were no protection but the one provided by the webpage. As seen in the previous section, that will not be enough to assure anonymity, hence, tips in Anonymous measures section (Attached document I: Safety Measures) must be taken.

4.1.5 Navigation experience

As far as companies concerned, Internet speed stands for thousands and millions of loses in sales [101] [102]. Whether by employees working flow or by users' frustration, the enterprises cannot allow delays in their service.

By reducing webpages weight, approaching servers to clients (DNS cache servers) and providing broad bandwidths, they can ensure seamlessly navigation. Comfortable experience differs regarding on the source. Mrs Fiona Fui-Hooh Nah made a deep and magnificent research on downloading page bearable time of response. Basing her study on several sources, she places the loss of interest at an average of 10 seconds and the frustration point between 15 and 41 seconds-delays [103].

In navigation experience's tests, Raspberry Pi 3 will be subject to webpages downloading and resolving timing. The structure will be such that permits to measure the activity with and without the application installed for the hotspot: DNS, TOR and OpenVPN. Raspbian counts with two packets destined to monitor download speed and DNS resolve, denominated curl and dnslookup respectively.

Curl is a command which downloads a webpage and shows the duration it has got to the user to receive the file. Unfortunately, it does not calculate the displaying time which would add a few seconds more, depending on the internal processor. Concerning to dnslookup, it is a utility of dnsutils packet, a group of codes designed for analyse DNS servers' functions. Concretely, dnslookup command measures the addresses resolution time.

Taking into account the available material, test speed architecture will be; a workstation equipped with curl and dnslookup (Raspberry Pi 2), a hotspot with a DNS server, TOR project redirection and an OpenVPN server implemented (Raspberry Pi 3) and a WAN access instrument (a router).

The experiment will consist in a gathering of navigation data, which will be recorded through three different hotspot configurations. Within each configuration, they will be register ten readings with DNS hotspot server deactivated, and other ten with the system activated.

Configurations cover from non-application activated (DNS, TOR and OpenVPN not running) to hotspot's highest extent. Readings will be the results of running curl and nslookup command to a sum of popular webs and some other pages distanced from the WAN access.

4.1.5.1 Speed test

Due to the nature of this experiment, unlike Wireshark one, it will be preferable to complete the whole data gathering before assessing it. To summarize, and to specify, next are the steps followed:

1. Preparing the test

Aiming structure is the one on Figure 4-21. First in being set is Raspberry Pi 3, then it will be placed apart as hotspot and the working interface will be the Raspberry Pi 2. Raspberry Pi 3 is to be switch on and connect to a station trough SSH to run continuing commands:

- **sudo sh /etc/checkinternet.sh**
Activating clear internet access maximum speed available can be checked.
- **ping www.google.com**

Inspecting it is operating. A third station, like a mobile or a tablet, can be used to determine if forward is also working, connecting to the access point (Garbo) and trying to browse anything.

- **sudo service dnsmasq stop**
Disabling DNS masking.
- **sudo service dnsmasq status**
It should display dnsmasq parameters highlighting that it is inactive.

Once Raspberry Pi 3 is set, it will be disconnected without turning it off and Raspberry Pi 2 will be configured according to the same steps. However, before pinging to Google, Raspberry Pi 2's wireless interface must be linked to Garbo LAN.

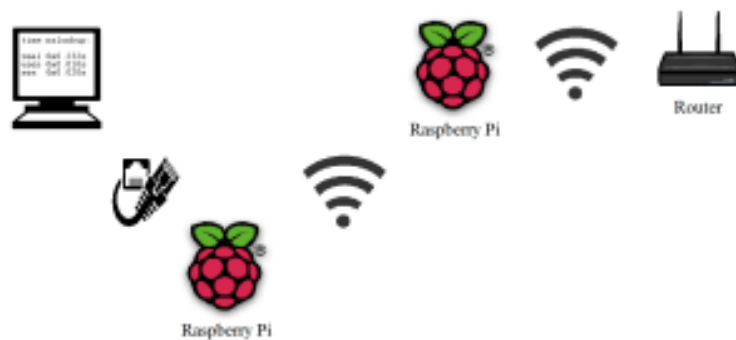


Figure 4-21 Speed tests' structure (edited from [3])

2. Assuming no failures in previous step and correct configuration of dnsutils in section 2.4.9, it only lasts to decide the subjects of the proof. Popular webpages chosen from various websites rankings [104] [105] [106] are:

- Google – www.google.com
- YouTube – www.youtube.com
- Facebook – www.facebook.com
- Amazon – www.amazon.com
- Wikipedia – www.wikipedia.com
- Twitter – www.twitter.com
- LinkedIn – www.linkedin.com
- Instagram – www.instagram.com
- Yahoo – www.yahoo.com

Supposing last TOR node in Central Europe, and in accordance that test are taking place in Pontevedra (Spain), Europe's servers should be the fastest in answering, regardless the navigation is clear or TOR redirected. Hence, the five countries webs selected are, in order of proximity:

- Russia – www.mid.ru (Russian Ministry of Foreign Affairs)
- India – www.rugbyindia.in (Indian Rugby Football Union)
- Argentina – www.afa.org.ar (Argentinian Football Association)
- South Africa – www.gov.za (South African Government)
- New Zealand – www.navy.mil.nz (New Zealand Navy)

It is to be noticed that sites belong to different national organizations. Not only must the organizations be official to grant a decent service, but also they have to end in a national domain.

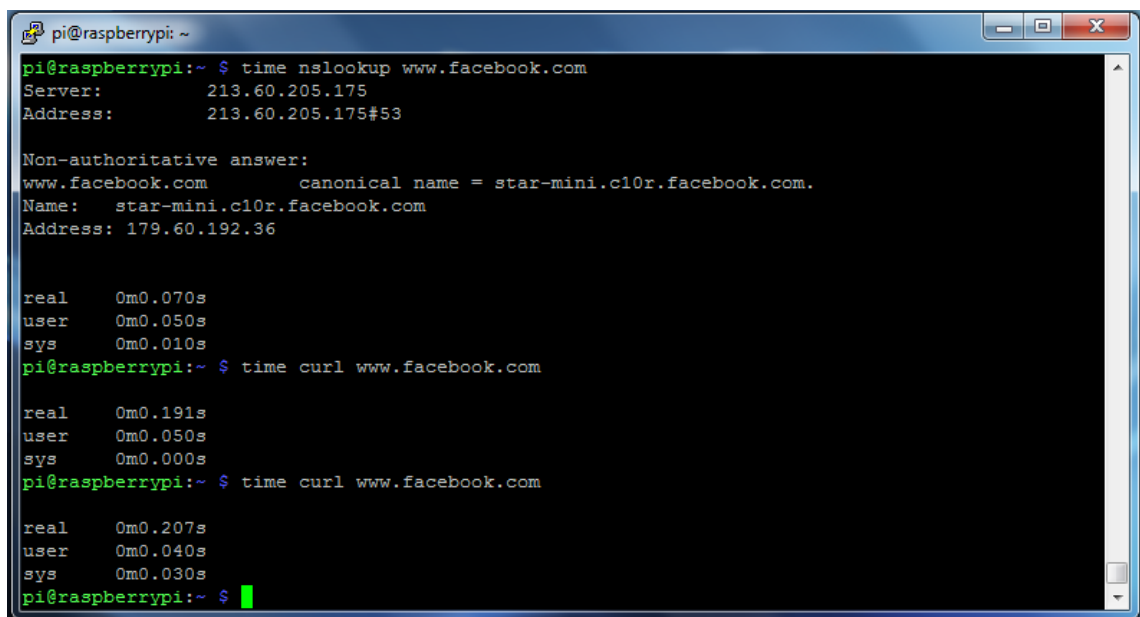
3. At this moment, system is ready to start with the test. An excel sheet or a notebook will be needed to write down the outputs. Next commands have to be typed:

- **time curl www.google.com**

It will return downloading time, as in Figure 4-22. It will be run ten times with a space of two or three seconds. The process is to be repeated with all the webs.

- **time nslookup www.google.com**

It will return translation to IP number time, as in Figure 4-22. Same repetitions as curl command are to be executed.



```

pi@raspberrypi: ~
pi@raspberrypi:~ $ time nslookup www.facebook.com
Server:      213.60.205.175
Address:     213.60.205.175#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 179.60.192.36

real    0m0.070s
user    0m0.050s
sys     0m0.010s
pi@raspberrypi:~ $ time curl www.facebook.com

real    0m0.191s
user    0m0.050s
sys     0m0.000s
pi@raspberrypi:~ $ time curl www.facebook.com

real    0m0.207s
user    0m0.040s
sys     0m0.030s
pi@raspberrypi:~ $

```

Figure 4-22 Screenshot of a curl's and dnsmasq's responses example

4. When all the readings have been taken, DNS masking will be activated. In this manner, Raspberry Pi 2 must be disconnected without turning it off. Connecting once more hotspot Raspberry and executing the commands below DNS server will be activated again:

- **sudo service dnsmasq start**
- **sudo service dnsmasq status**

From step two, the test will be carried out another time until step five and omitting the fourth step.

5. This time, by following previous step, TOR must be set. Owing to TOR has not being disabled it is just a matter of restablising TOR iptables:

- **sudo sh /etc/toriptables.sh**

Now it only can be checked with a third party because of being redirecting tables.

- **sudo service dnsmasq stop**

- **sudo service dnsmasq status**

For third and fourth time, the whole process will take place from two until four, jumping straight to sixth step by the time TOR has been analysed both with dnsmasq and without.

6. Lastly, it remains to analyse OpenVPN server fluency. In the same way that in step 5, OpenVPN iptables will be configured:

- **sudo sh /etc/toriptables.sh**
Now it only can be checked with a third party because of being redirecting tables.
- **sudo service dnsmasq stop**
- **sudo service dnsmasq status**

Workstation will need a client certificate, therefore, and according to section 2.4.5 by means of WinSCP, an authentication file will be transferred to “openvpn” folder within “etc” one.

A parallel Putty or VNC connection must be initiated due to first CLI opened will stand by while it is connected to the OpenVPN server. In case of wanting to start a VNC interface link consult section 3.10.

- **sudo openvpn /etc/Client1.ovpn**

For the last time, steps two, three and four will display readings of system speed. Eventually, all the data assembled will be analyse in an excel program or similar.

Beforehand, it is predictable that both Raspberry Pis are going to perform similar for a clear Internet access. Besides, tests are too laborious and easily ruined making ineffective its study. Thus, Raspberry Pi 2 will only pass through the whole configuration test to tell possible differences with Raspberry Pi 3.

4.1.5.2 Clear access (Without TOR & Without OpenVPN)

Speed data is gathered categorized in Microsoft Excel spread sheets and presented in the attached documents from I to XI. Charts represent the flow in an easy view format. Nevertheless, collected information must be processed in advance. The aim is to discard not representative considered readings.

All the same, out of normal data will be also useful to comprehend nets' behaviour. They are going to be orange highlighted (Table 4-2), and included into the study and the charts, if they respond to normal net bugs. In case they do not, they are going to be red highlighted and they will be destined to analyse peculiar happenings.

Without dnsmasq / Time nslookup											
Web / Delay	First	Second	Third	Fourth	Fifth	Sixth	Seventh	Eight	Ninth	Tenth	Average
New Zealand Navy	0,443	0,451	0,416	0,416	0,439	0,111	0,088	0,089	0,11	0,439	0,3002
South Africa Government	0,314	0,313	0,293	0,104	0,135	0,101	0,107	0,131	0,126	0,108	0,1732
Russia foreign ministry	0,129	0,127	0,13	0,108	0,126	0,091	0,096	0,0109	0,133	0,117	0,10679
Argentinian afa	0,305	0,319	0,306	0,306	0,085	0,1	0,294	0,104	0,105	0,104	0,2028
Rugby India	0,13	0,106	0,138	0,837	0,139	0,133	0,862	1,106	0,862	0,077	0,439
Average	0,2642	0,2632	0,2566	0,3542	0,1848	0,1072	0,2894	0,28818	0,2672	0,169	0,244398

Table 4-2 Example of data gathering

From DNS resolving and downloading page speed readings (Chart 4-1 and Chart 4-2), it can be observed that not only is the system much faster than the tolerable time for Internet loading, but also than the computer response endurable time [103].

In addition, it is proved that, whether by proxy cache or by lighter pages, popular webs downloading speed is much quicker than the rest regardless of the distance to their mother countries. However, DNS server provides a noticeable decrease on information exchange (Chart 4-3).

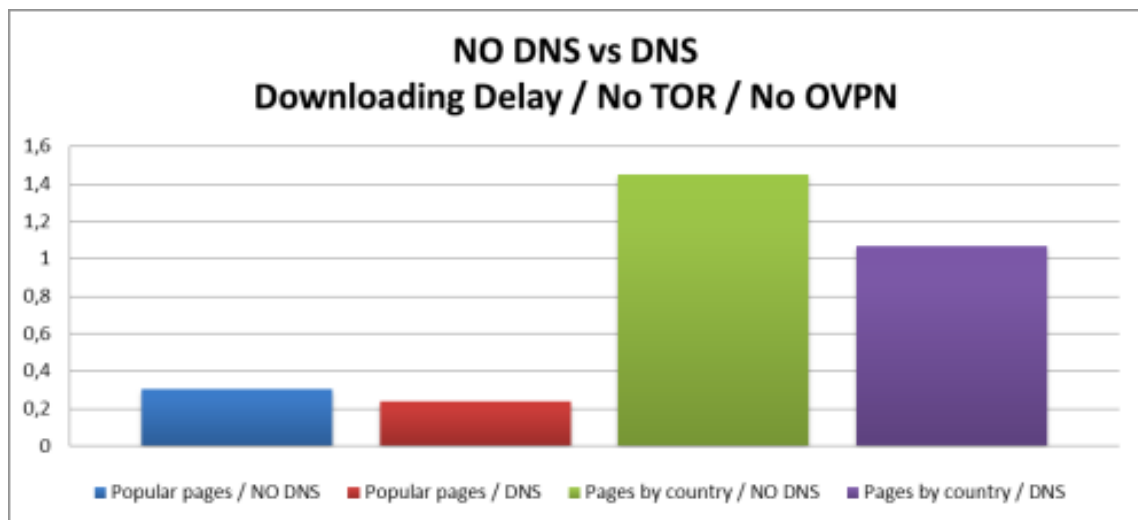


Chart 4-1 Bar Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN

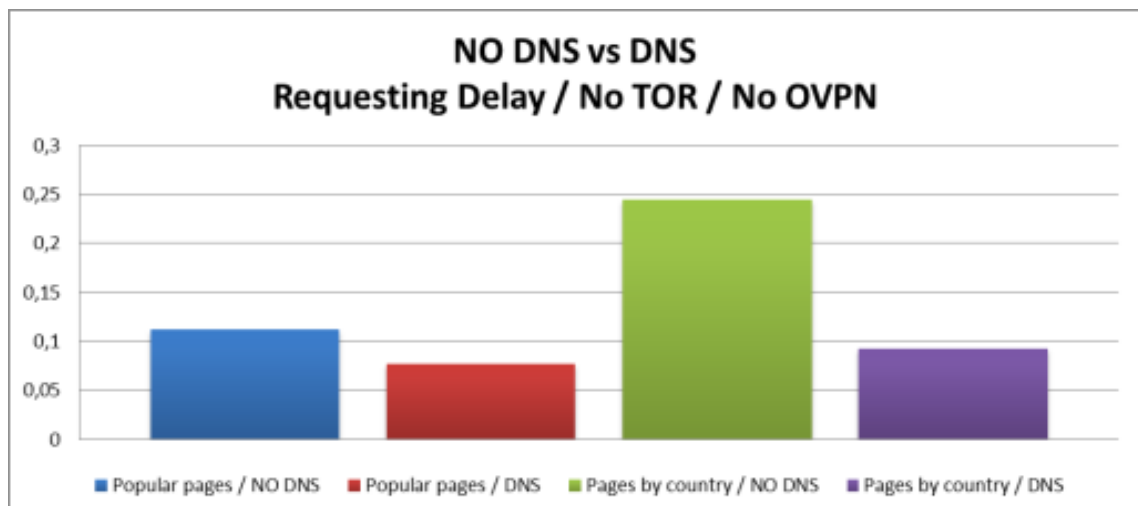


Chart 4-2 Bar Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN

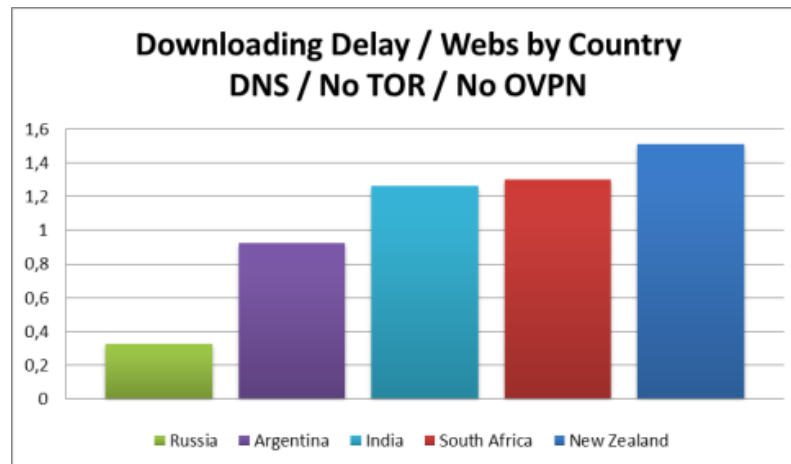


Chart 4-3 Bar Chart Delay vs. Distance

With reference to nor popular neither vast visited pages, their responding time is correlated with their distance to the emitter. Proxy cache server will not waste memory on saving information of those websites, thus, the request will have to travel across the different DNS servers up to the national domain it is addressing for. Then, packets will have to make the entire route backwards to report the translation, beginning by that time with the downloading. Consequently, delay will grow gradually.

4.1.5.3 With DNS & TOR (Without OpenVPN)

Encryption will obviously slow down the process. Overall, hotspot will pass the test if it keeps the navigation speed below the 10 seconds limit marked. DNS will guard speed does not boost uncontrollably.

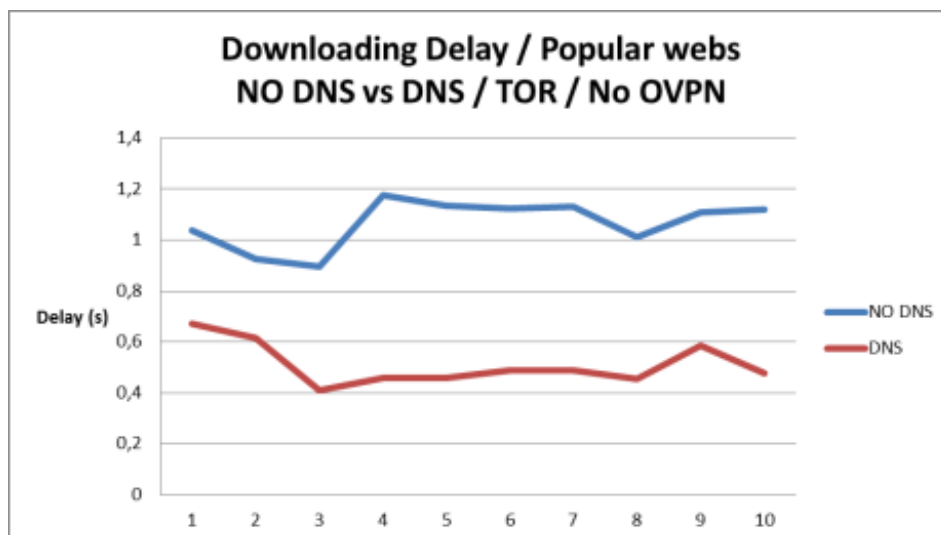


Chart 4-4 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

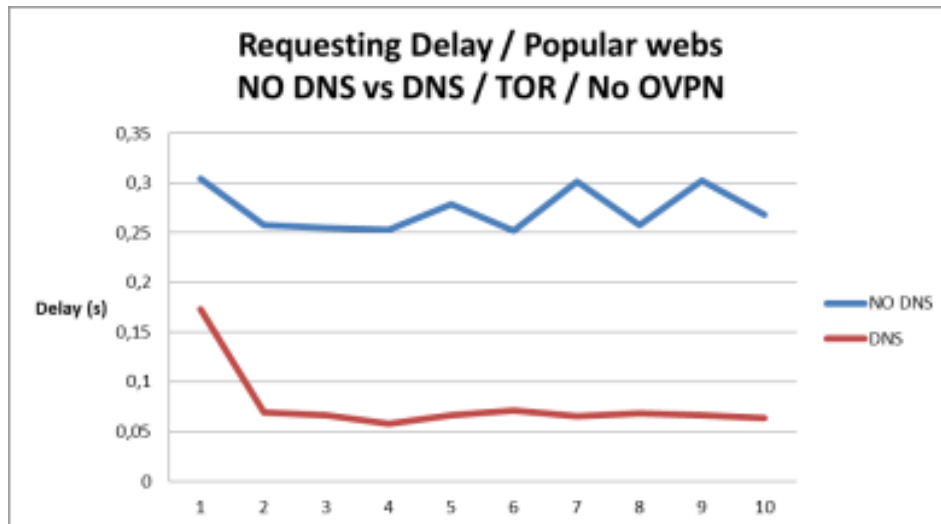


Chart 4-5 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

First conclusion comes from the stability of the DNS resolving without using a DNS server. It can be determine that the answering server is just at the endpoint of the TOR route. This means that the average time disabling DNS (Chart 4-5) is the duration of the TOR route crossing.

Secondly, tests have also exhibited that DNS masking presents a similar behaviour reducing the timing. Curl command has given less than the half time in readings (Chart 4-4). Moreover, TOR redirection holds itself still inside the limits established.

Lastly, DNS resolving is almost the same whether using TOR redirection or not what shows that DNS server into the Raspberry Pi 3 is working properly (Chart 4-6). Generalizing, test are returning good results so it is not necessary to dive into them passing directly to analyse next experiment gathered data.

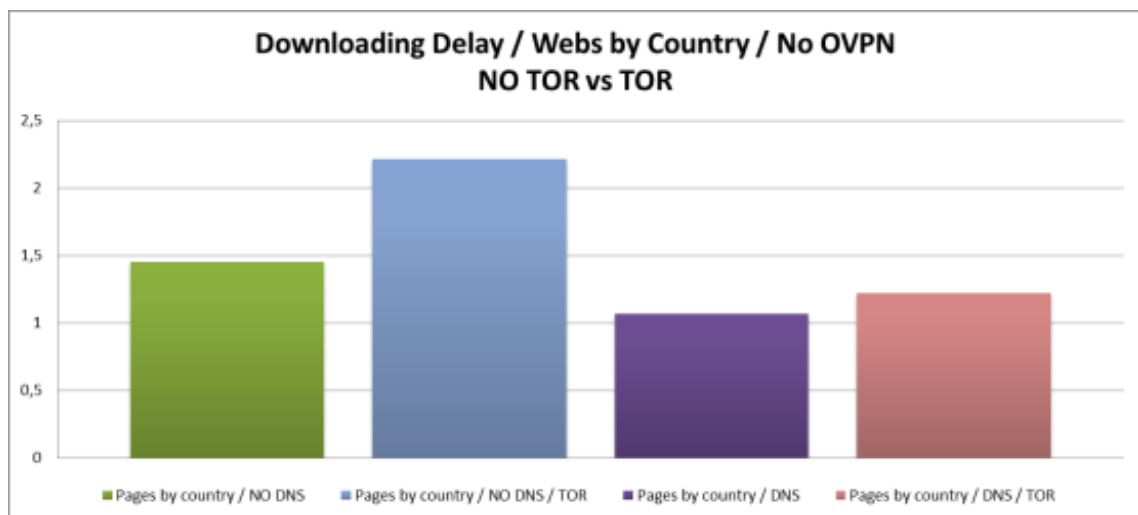


Chart 4-6 Bar Chart Requesting delay Clear access vs. TOR / DNS

4.1.5.4 With DNS, TOR & VPN

A punctual high peak is most likely an example of a TOR's route changing. Hotspot will cut or stop the communication and will adopt a new redirection way. Within this process packets will get lost and, if the system is able, it will resume the sending giving only place to a small delay (Table 4-3).

Downloading Delay / Webs by C		
DNS Server / TOR / OVP		
3°	4°	5°
2,375	3,533	3,6
2,939	2,14	2,242
3,305	3,003	2,137
2,389	2,164	2,642
3,852	13,558	4,678
3,12125	2,4356667	2,92475

Table 4-3 Changing TOR node example

Last experiment allows checking differences among configurations. Performance is adjusted to the expected one, delay increase proportional to the encryption, except from the last case. DNS server does not reduce it toward the case Raspberry Pi does not act as a server, when searching webpages hosted in distanced countries (Chart 4-7).

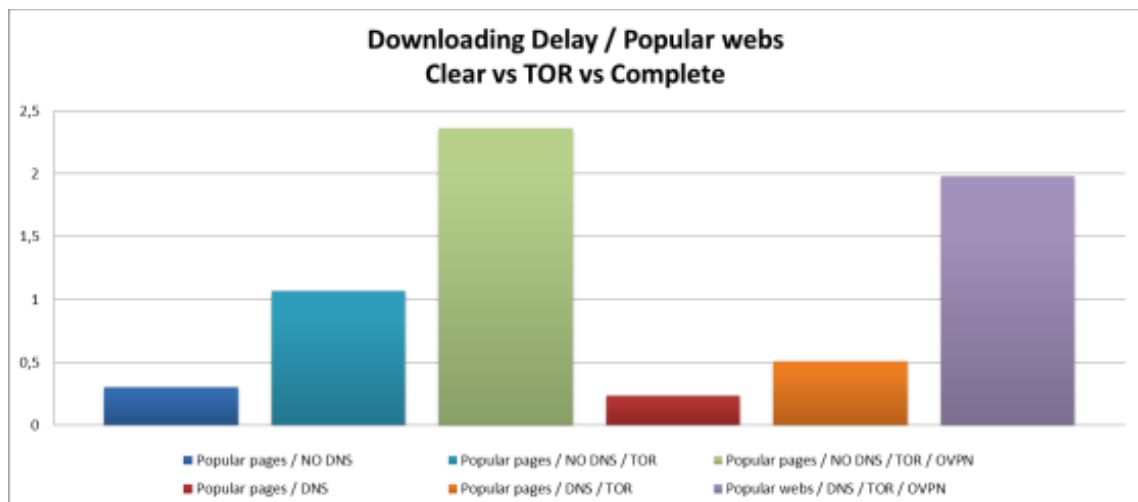


Chart 4-7 Bar Chart Downloading delay Clear access vs. TOR vs. TOR and OVPN

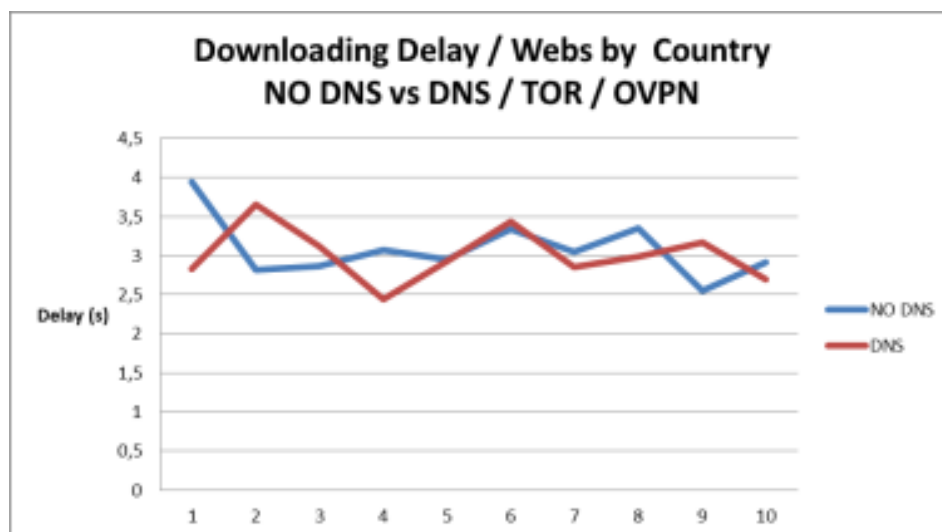


Chart 4-8 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN

TOR and clear configurations perform similarly regarding to DNS enabling. Thus, it should not be comprehensible an equal or even higher retard downloading delay for OpenVPN set (Chart 4-8). However, that is the reality, and is in tables where the reason could be found out (Table 4-4). Slowest flows correspond to farthest webpages so more tests are to be carried out to determine the cause.

<u>Downloading Delay / NO DNS vs DNS</u>			
Webs by Country / TOR / OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	2,1575	3,4729	-61%
South Africa Government	3,0994	2,7261	12%
Russia foreign ministry	2,8472	2,6723	6%
Argentinian afa	2,5119	2,7339	-9%
Rugby India	4,8007	4,07766667	15%
Average	3,08334	3,13657333	6%

Table 4-4 Downloading delay NO DNS vs. DNS / TOR and OVPN

Other great conclusion is that hotspot achieves objectives of fluency generating an enough rapid stream. Experience follows the patterns determined by Mrs Fui Hoon-Nah, Fiona. All the same, the three second retard is noticeable.

4.1.6 Most popular services and apps

Nowadays applications seek for interaction with the user to feed his interest, which explained why streaming data depends so much on the retard. Unlike the duration of a webpage downloading, interacting media cannot allow itself big peaks of delay. Tests will consist in measuring the latency and downloading and uploading speed while those programs are open (Figure 4-23).

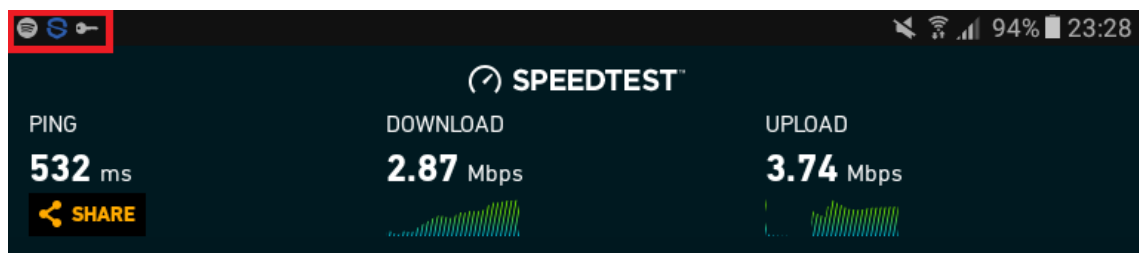


Figure 4-23 Screenshot of speed test while using OpenVPN and Spotify

Ping measures the continuous communication speed between two end points. Aiming that the user do not realise of the existence of any kind of retard, this must be less than 400 ms for live stream. Nevertheless, in certain media applications case, like YouTube or Netflix, average client bear spending a couple of minutes to acquire the data [107].

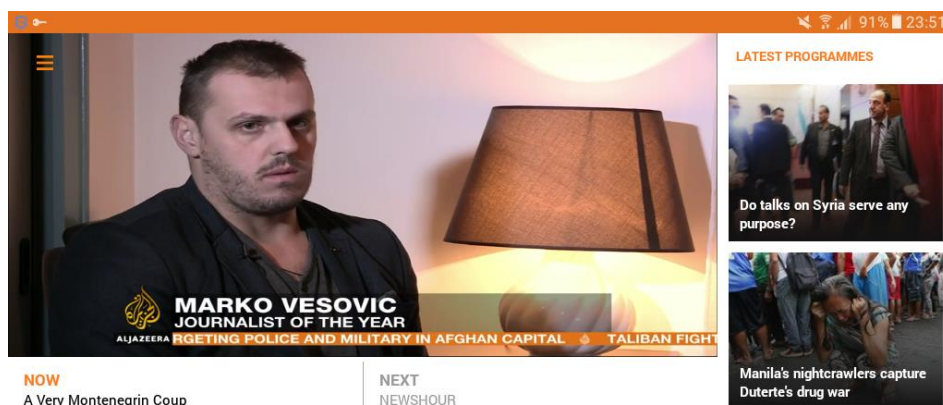


Figure 4-24 Screenshot of a live stream experiment while using OpenVPN

In Attached document VI: Popular services and applications test images of the experiments have been collected. Most impressive achievement is the capability of watching live stream media (Figure 4-24) without interruptions. In contrast, Netflix has been not able to pass login interface. The rest of the services have executed a similar experience that without the intermediate hotspot.

Subjected services are: Spotify audios, Facebook and Instagram navigation, Play Store downloading, YouTube clips, Whatsapp messaging, Aljazeera news app, Outlook service and Netflix. Among them YouTube's clips, Play Store's downloads or Whatsapp's messages, for instance, have responded inside parameters' boundaries, therefore, hotspot service has succeeded this test.

Is to be added that, during the realisation, incidentally, Google chrome browser happen to forbid navigation because of strange searching patterns. It has nothing to do with users' actions, but to TOR nodes activity. Google displays a warning, requesting users to prove they are not boots by simple tasks. Although it does not hinder the navigation, it could annoy clients.

4.1.7 Battery

Power consume fluctuates regarding the tasks asked to process, having no sense to assess battery life's expectancy by leaving it supplying the Raspberry until it runs out. In this study, battery's life will be analysed from a theoretical point of view:

$$W_{RPI} = V * A$$

Equation 4-1 Power

$$t = C / W_{RPI}$$

Equation 4-2 Life's expectancy

In accordance to Raspberry Pi Foundation typical bare-board active current consumption are 400mA for Raspberry Pi 3 and 330mA for the oldest version, with a maximum of 1.2A and 600mA respectively [108]. Calculations give the next results:

Device	Average consume (mA)	Maximum consume (mA)	Average battery's life expectancy	Minimum battery's life expectancy
Raspberry Pi 2	330	600	39 h 20 m	21 h 30 m
Raspberry Pi 3	400	1.2	32 h 30 m	10 h 40 m

Table 4-5 Raspberry Pi's battery's life expectancy

Results are by far favourable; not only have they enough capacity to power the hotspot, but also they are able to supply a third device for a reasonable period of time (Table 4-5). Due to the fact that it is heavy and bigger than the Raspberry Pi, a lighter one could be tested to get a handier tool.

4.2 Unable to test

Whether by the absence of resources or applications next features have not been tested and its functioning could not be checked:

- Defence against DDoS attacks
- Monitoring or sniffing inside the Raspberry Pi
- Monitoring or sniffing beyond TOR nodes

Assuming there could be leaks in them; some tips to avoid their inconveniences can be pointed out:

- **Defence against DDoS attacks**

Although it is highly unlikely, if ever it was produced, as hotspot has been designed portable, it would be solved simply disconnecting and searching for a new LAN access point which provides Internet connection.

- **Monitoring or sniffing inside the Raspberry Pi**

Firewall and antivirus control the net access to the hotspot, hence, as long as Raspberry Pi managing is denied and a safe and strong password is established this bug would be covered.

- **Monitoring or sniffing beyond the TOR nodes**

This compromise hinders the communication security and it is almost impossible to solve. Between the last TOR node and the webpage server the exchange of information is clear, so it is exposed to the breach analysis in Wireshark section (4.1.3.2).

As a matter of fact, if packets do not carry credential data it is impossible to associate the traffic with the user. However, hotspot will not act anymore as a safe redirecting device.

New dilemma will be if the whole system would be useful having security breaches into account. The point is that the amount of outgoing information of a TOR node could reach to unmanageable process levels for a human being.

For a specific victim a sniffer would not be able to determine what nodes are addressing either when. Sniffer should watch all of them, and even so, some credential should be needed to filter the traffic.

In case of executing a general monitoring, client conversations will be in danger. All the same, as mentioned, they would be one among thousands that would make them rejected if they did not carry valuable data.

In conclusion and owing to the fact that credentials are usually protected by the Secure Socket Layer and that every single file posted on Internet is susceptible of being seized is an acceptable leak. Nonetheless, it is advisable to check scope of application section (5.2).

4.3 Tests conclusions resume

Security, anonymity and speed tests have been passed successfully; nevertheless, it is recommendable to review its limits before deciding possible fields of application. Moreover, it should be subject to deeper tests to analyse specific possible bugs or fails.

4.3.1 Security

Mr Christopher M. Bishop in his book *Introduction to Computer Security* [109] defines the system security as the capability of a system “to start in an authorised state without entering in an unauthorised state (or nonsecure)”. This definition can be joined with Mr William Stallings’ one, recovered in his book *Cryptography and Network Security* [110], which emphasized the necessity of “automated tools for protecting files and other information stored on the computer became evident”. By those definitions, the Raspberry Pi hotspot would not be a secure system.

On one hand, ClamAV antivirus has not taken “automated” actions against the virus’ code. All the same, that does not mean it is useless as virus test was designed to check ClamAV. More dangerous experiments must be carried out and if it proved not being efficient there is a wide range of antivirus as the ones presented in section 2.4.7.

On the other hand, despite the fact that further TOR last node’s there were no encryption, its tests have returned positive results avoiding monitoring and packets seizing. TOR constitutes a strong shield in a local environment, for which it is designed. Not only will it provide security in public places, but it could be used as a fixed station in a home or personal network without compromising anonymity or speed aspects.

Summarizing, similarly to risks section (2.3.4), as hotspot cannot be considered totally safe, it would remain writing down a table making reference to danger levels and probabilities of an attack, to determine in which situations the hotspot will provide a service safe enough and what risks would be taken. It is not to be forgotten, as discussed in the introduction (1.1.1) that Internet is in constant evolution and at any moment could appear any application or code to break into the system. As a result, tests should be taken periodically to check out and to fix future leaks.

4.3.2 Anonymity

Concerning to the capability of the system to hide the real identity of the client, it would as long as users respect anonymous principles. Hotspot has nothing to do if real name or any credential data is intentionally release.

As discussed in anonymity section (4.1.4), in the same environment Raspberry Pi can be detected and distinguished, but not the devices connected to the subnet. Even though the subnet can be find out and is possible to determine the device that is generating that subnet, is almost impossible to get any piece of information about the workstation.

Thus, in order to maintain the anonymity warnings in Attached document I: Safety Measures must be followed.

4.3.3 Speed & Experience

As recovered in Navigation experience's sections (4.1.5), there have been realised a group of tests to analyse each part of the configuration. In order to display it in a clearer format, results are to be divided in the experiments where they have been deduced:

1. Clear access (Without TOR & Without OpenVPN)
 - Peaks are mostly caused by net saturation
 - A DNS server reduces the timing
 - Longer distances implies longer waiting periods
2. With DNS & TOR (Without OpenVPN)
 - TOR encryption increase the answering time.
 - DNS requesting is the same because communication between hotspot and workstation is not cipher.
3. With DNS, TOR & OpenVPN
 - New peaks in this case because of a TOR route change.
 - Timing grows again due to VPN encryption.
 - Popular pages decrease enormously their downloading speed due to their loading time within clear access is really low. Actually, they get an answering time closer to farther webpages, which have not suffered such impact.

These short conclusions come to define that encryption will slow down the whole process; nevertheless, DNS hotspot's server will keep the timing inside acceptable limits. Yet, a more important inference to point it out resides in the fact that the speed test has been carried out in a single LAN access. In other words, results are not absolute; instead, they are function of the maximum speed provided for a clear connection to the AP (access point).

Hence, readings in the Attached document XI: Downloading and Resolving delay Comparison are essential to forecast the speed provided by the Raspberry Pi from initial one. Complete configuration increases the download time around eight times for popular webpages and twice for the others. In the same way, TOR encryption speed is the half for popular and a similar one for the rest of the webpages.

As suggested in previous part, regarding what will the service be employed to and where will it do, the configuration could be modified to adapt itself to the characteristics of the LAN and the menace. Thus, if ever the connection were too slow, OpenVPN or TOR could be dispensable, and activating just one of them.

Incidentally, concerning to the differences between both Raspberry Pis performing as access point, apart from the fact that Raspberry Pi 2 has returned worst readings in general, the gap is not as big to discard one of them. Discrepancies among devices' features have had their effects within the experiments and a higher average was expectable for the oldest one. Consequently, is necessary an extra point to settle a better mini-computer to host the redirecting encryption code, supposing one of them will defeat the other. Here is where the necessity of an extra wireless adapter makes the difference by raising Raspberry Pi 2 hotspot cost and matching it to the newest one's cost (the average of a wireless adapter price is around 10£ and 12€ [111]). Therefore, Raspberry Pi 3 will stand out against its previous model and will be the right election for the hotspot that has been designed.

5 CONCLUSIONS AND FUTURE ADVANCES

5.1 Overview

In this last section, the results of the project will be reviewed to assess until what level objectives have been achieved and in what circumstances can the hotspot be employed. Summarizing initial aims, they consisted in: redirecting the traffic through the TOR net, providing security by means of firewalls, antiviruses and a virtual private network and, finally, the device designed must be portable.

Portability has been assured by a medium capacity battery. Principal inconveniences reside in its ergonomics; a notable size and the fact of having to transport an extra tool and having to charge it before using it. Best line of action to improve this part would be to incorporate a lighter battery and design a case which includes a space for it, similarly to a smartphone or a tablet.

Concerning to redirection and VPN encryption, they conceal the information through a row of keys successfully. Despite the TOR leaks discussed, the system can be considered safe as after the last TOR node, links will mostly be operated by national and official trustworthy telecommunication companies. Tests have shown that data obtained from the hotspot clients is not enough to discover the user without a huge knowledge on the field or the proper means; situations where hackers would be able just to identify the workstation because stolen packets are impossible to be decrypted without the key, not even the destination could be guessed.

In contrast, antivirus and firewall's test does not return such achievement. In spite of having detected the virus code, it has done nothing against it apart from warning the user. However, virus test has been a simple one just to determine whether antivirus was activated. Owing it has not been subjected to a proper test cannot be marked as useless, but neither as a safe device. At any rate, the wide range of available antiviruses at the market makes this problem a mishap. No antivirus has been designated to replace the current one due to a positive answer against Eicar virus has little meaning and a proper virus test involve many experiments which is out of this project.

Overall, Raspberry Pi hotspot accomplishes the objective it was designing for, a safe device which redirects the information through a communication tunnel on TOR net. Nevertheless, the consequences of a misemployment or an overestimation of its capabilities could compromise the security of the user. It is for this reason that possible fields of application must be emphasized. It would also be ideal that exhaustive tests would be carried out to assess entirely the limits of the hotspot.

5.2 Scope of application

During the development of the project have been commented some likely fields of employment like libraries or in conflict zones. Once the capabilities of the entire system have been studied, it is easier to select fitter scopes of application. TOR project offers a list of the kind of their user's profiles together with the principal reasons [112]:

Probability \ Damage	High	Medium	Low
High	Servicemen & Officers	Journalists	Activists
Medium	Business executives	Whistle-blowers	Bloggers
Low	IT Professionals	Normal people	High & low profile

Table 5-1 Users' profile and risks

– Green boxes

All the profiles included in these boxes (Table 5-1) are potential users of this hotspot. Their case does not suppose a potential threat, anyhow, a bad and unconscious employ of networks could endanger their security.

• Normal people

Reasons given for quotidian users are protecting themselves from irresponsible corporations and unscrupulous marketers and identity thieves. Another motivation is preventing children of potential cybercriminals. Regrettably, paedophilia is extended across Internet and infant innocence together with paedophile threats are the traps that drown them into this kind of criminals' game [113].

Using TOR redirection children identity will remain hiding against any kind of offender. Moreover, a deceiving paedophile method is based on youngsters' videos to make their victims think they are real and reliable people [114]. In this manner, it will also be more difficult for them to steal those media files.

• Bloggers

They usually employ TOR browser to avoid repression because of their posts. In case they use their real credentials, Raspberry Pi will prevent their real address of being found out and will cross through censorship walls.

• High and low profile

Either being in the public spotlight or in the shadow of the crowd an inaccurate comment can turn a worker into a jobless person. Nowadays companies control their employees' social networks accounts and, they can even admonish them following the enterprise rules. Important lawyers or politicians have also to take care with their words, portraying a good example of hotspot's predicted user.

– Yellow boxes

Yellow highlighted TOR user model (Table 5-1) is highly recommended to redirect their communications through the hotspot as their activities might entail hazards.

• Whistleblowers

Obviously, the level of danger assumed by a whistleblower depends on the disclosures that are going to be delivered. Their enemy also varies from official companies or governments to criminal syndicates. Wikileaks, one of the biggest sources of informants is constantly fed by TOR means [115] [116] [117].

- **Activists**

Human right activists labour is not as expose to repression than previous one but still involves a risk. People with enough power to protect their interests can harm physically activists or the public image of their organizations. If this power involves legal support the associations can be sued and sentenced to pay large sum of money.

- **IT Professionals**

In the source provided there are displayed a couple of reasons for IT professionals to use TOR. Basically, they refer to network security measures verifying and managing. It's mostly employ to reveal possible leaks and access to sensitive information. Thus, the danger lies on the delicateness of the documents to guard.

- **Orange boxes**

These people and organizations (Table 5-1) are not recommended to employ Raspberry Pi's redirection without testing hotspot weakest point in the field there are going to use it.

- **Journalists and their audience**

Out of biased newspapers and programmes there can be founded freelance reporters or Reporters without Borders who try to give voice to those people restrained by government's laws or silenced by local gangs. Besides, audience is afraid of being pigeonholed as revolutionaries for browsing other point of view.

Regarding if they are in war zone or in the middle of a conflict the danger grows substantially. As radio stations are captured by the most radical side between both parties in conflict the zone becomes perilous increasing the risk of highjack or assassination.

- **Business executives**

In this case TOR is seen as a method to break competition security as well as to keep strategies confidential. Many companies block IP addresses of their rivals preventing them from tracking important conversations or gathering intelligence. Provided that, TOR encryption would hide IP addresses deceiving defence methods, but would also protect information from being stolen.

- **Red boxes**

Lastly, the utilization of the device designed in this project is not advisable for professionals inside red boxes (Table 5-1). However, they would be the largest beneficiaries of a perfect functioning of Raspberry Pi's hotspot. Thus, this field should be interested in a polishing of this tool.

- **Law enforcement officers**

Sting operations and online surveillance need from anonymity software. TOR service can, not only protect field agents' identity, but let them act as offenders and surf some web sites closed to the general public.

- **Servicemen**

Hidden services' as well as military units deployed locations must remain conceal by a robust system. TOR, apart from the security provided, is able to facilitate a distributed service independent of national communications support, reducing the amount of resources expected to being deployed.

5.3 Development directions

Given the objectives of the project, the results of the tests and the scope of application exposed, likely directions of development are related to its ergonomic and to analyse its possible security bugs. Principal lines proposed are the followings:

- **Mainboard and Battery**

Even though Raspberry Pi is a small computer, its size, together with the battery, is quite big to transport a device that simply codifies clients' communication. Assuming the profiles discussed in previous section, people with low necessity of this tool would not bother themselves carrying it, while the ones with a huge require, cannot entirely rely on it.

Therefore, two lines of investigation are opened here: it is to be studied the possibility of installing the system in another mini-computer that only includes the hotspot's features and the analysis of a same powerful battery that accomplish the requirements but with a smaller size.

- **Configuration**

Many steps of the tutorial could be made it automatic by a script, like packets downloading and installation. An execute configuration file will facilitate greatly the process reducing the number of concepts to understand and becoming easy-to-use for newbies.

- **Certificates**

WinSCP is a safe method to transfer certificates; notwithstanding, only for Windows OS run stations, being a perilous and tedious process to shift them to other workstations. Therefore, would be an interesting line of advance to contemplate other types of certificates delivering like email or Bluetooth.

- **Shell**

As Raspberry Pi comes without a case, one has to been acquired. There are various types of cases, but currently none of them includes a space for the battery. Thus, it could be designed a specific case for the Raspberry Pi according its scope of application an including a comfortable transport of the battery and, moreover, the wireless adapter.

- **Security**

Despite the system has not returned bad results, its requirements seek for an impassable system with security measures that stop or remove any intended attack. Little or none leaks are expected from the system preventing users' credentials from being discovered. In this line, an in-depth study must be carried out to cover and fix all the possible bugs and gaps.

Summarizing, directions of improvement do not try to change the system, but to make the hotspot handier. From all of them the most important line of action is the exhaustive analysis of the system security to assure the achievement of its principal aim.

6 BIBLIOGRAPHY

- [1] S. Feruza Y. and T.-h. Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," *International of Multimedia and Ubiquitous Engineering*, vol. II, no. 2, pp. 17-18, 2007.
- [2] S. Feruza Y. and T.-h. Kim, "IT Security Review: Privacy, Protection, Acces Control, Assurance and System Secuirty," *International Journal of Multimedia and Ubiquitous Engineering*, vol. II, no. 2, pp. 18-21, 2007.
- [3] Braxmeier & Steinberger GbR, "Pixabay," [Online]. Available: <https://pixabay.com/>. [Accessed January and February 2017].
- [4] M. Kizza and Joseph, "Cyber Crimes and Hackers," in *Computer Network Security*, Chattanooga, TN, U.S.A., Springer Science & Business, 2005, pp. 141-149.
- [5] L. Van Wel and L. Royackers, "Ethical issues in web data mining," *Ethics and Information Technology*, vol. VI, no. 2, pp. 129-140, 2004.
- [6] P. Szor, "The Fascination of Malitious Code Analysis," in *The Art of Computer Virus Research and Defense*, Hagerstown, Pearson Education, 2005, pp. 58-65.
- [7] Dadax LTD, "Internet Live Stats," Worldometers, 26 February 2017. [Online]. Available: <http://www.internetlivestats.com/>. [Accessed 26 February 2017].
- [8] D. Gross, "Think you know the Web? Let's find out," *CNN*, pp. <http://edition.cnn.com/2014/11/26/tech/web/pew-survey-internet-knowledge/>, 2014 November 30.
- [9] A. Smith, "What Internet Users Know about Technology and the Web," Pew Research Center, Washington, 2014.
- [10] A. S. Tanenbaum and D. J. Wetherall, "Reference Models: The OSI Referenece Model," in *Computer Networks*, Boston, Pearson Education, Inc., 2011, pp. 41-48.
- [11] H. A. Seid, "Virtual Private Network". United States Patent 5.768.271, 16 June 1998.
- [12] Patni Computers Services, "Proceedings, Informing Science," June 2002. [Online]. Available:

- <http://www.proceedings.informingscience.org/IS2002Proceedings/papers/Bhiog058Secur.pdf>. [Accessed 31 January 2017].
- [13] SD-3C LLC, “SD Card,” SD-3C LLC, [Online]. Available: https://www.sdcard.org/downloads/formatter_4/. [Accessed 26 February 2017].
 - [14] GNU, “Source Force,” Open Source, [Online]. Available: <https://sourceforge.net/projects/win32diskimager/>. [Accessed 26 February 2017].
 - [15] Raspberry Pi Foundation, “Raspberry Pi Foundation,” [Online]. Available: <https://www.raspberrypi.org/downloads/raspbian/>. [Accessed 22 January 2017].
 - [16] S. Tatham, “Putty; Chiark Greenend,” 8 January 1999. [Online]. Available: <http://www.putty.org/>; <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. [Accessed 26 February 2017].
 - [17] RealVNC Ltd, “Real VNC,” RealVNC, 2002. [Online]. Available: <https://www.realvnc.com/>. [Accessed 26 February 2017].
 - [18] OpenVPN Technologies, Inc, “OpenVPN,” [Online]. Available: <https://openvpn.net/>. [Accessed 26 February 2017].
 - [19] Talos Group, “ClamAV,” [Online]. Available: <https://www.clamav.net/>. [Accessed 26 February 2017].
 - [20] Wireshark Team, “Wireshark,” Gerald Combs, 1998. [Online]. Available: <https://www.wireshark.org/>. [Accessed 26 February 2017].
 - [21] The Guardian, “The Guardian,” 6 June 2013. [Online]. Available: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. [Accessed 30 January 2017].
 - [22] The Tor project, Inc, “Tor project metrics,” [Online]. Available: <https://metrics.torproject.org/userstats-relay-country.html>. [Accessed 30 January 2017].
 - [23] C. Hoffman, “How to Geek,” 23 November 2015. [Online]. Available: <https://www.howtogeek.com/234233/whats-the-difference-between-a-modem-and-a-router/>. [Accessed 26 February 2017].
 - [24] What's my IP address, “What's my IP address,” [Online]. Available: <http://whatismyipaddress.com/router>. [Accessed 26 February 2017].
 - [25] Computer Hope, “Computer Hope,” [Online]. Available: <http://www.computerhope.com/jargon/r/router.htm>. [Accessed 26 February 2017].
 - [26] Wikimedia, “Wikimedia Commons,” [Online]. Available: https://commons.wikimedia.org/wiki/Main_Page. [Accessed January & February 2017].
 - [27] Technology Q&A, “Cisco,” Technology Q&A, 10 November 2014. [Online]. Available: <http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>. [Accessed 26 February 2017].
 - [28] Netsparker, “Now where,” Netsparker, September 2015. [Online]. Available: <https://n0where.net/how-does-it-work-iptables/>. [Accessed 26 February 2017].
 - [29] Raspberry Pi Foundation, “Raspberry Pi Foundation. Main Page,” Raspberry Pi Foundation, [Online]. Available: <https://www.raspberrypi.org/>. [Accessed 02 February 2017].

- [30] Raspberry Pi Foundation, "Raspberry Pi Foundation. Helping Videos.," 14 April 2015. [Online]. Available: <https://www.raspberrypi.org/help/videos/>. [Accessed 28 February 2017].
- [31] Raspberry Pi Foundation, "Raspberry Pi Foundation. Networking Lessons.," [Online]. Available: <https://www.raspberrypi.org/learning/networking-lessons/>. [Accessed 28 February 2017].
- [32] F. Jansson, "It's a clean machine.," 19 February 2013. [Online]. Available: <http://itsacleanmachine.blogspot.com.es/2013/02/wifi-access-point-with-raspberry-pi.html>. [Accessed 28 February 2017].
- [33] Adafruit Learning System, "Setting up a Raspberry Pi as a WiFi access point," [Online]. Available: <https://cdn-learn.adafruit.com/downloads/pdf/setting-up-a-raspberry-pi-as-a-wifi-access-point.pdf>. [Accessed 23 January 2017].
- [34] D. J. Barrett and R. E. Silverman, SSH, The Secure Shell: The Definitive Guide, Sebastopol: O'Reilly Media, Inc, 2001.
- [35] Microsoft Corporation, "Technet Microsoft," [Online]. Available: <https://technet.microsoft.com/en-us/library/cc959354.aspx>. [Accessed 06 February 2017].
- [36] USA Army, "Departament of the Army," USA Army Inteligence, [Online]. Available: <http://www.dami.army.pentagon.mil/site/TechSec/TEMPEST-Def.aspx>. [Accessed 07 February 2017].
- [37] Fuerzas Armadas de España, "Ejercito del Aire," Grupo de Transmisiones, [Online]. Available: <http://www.ejercitodelaire.mde.es/ea/pag?idDoc=E6A18D97A0F0A218C12570DD0042AB7A&idRef=5D263277D998F47BC1257459002696BA>. [Accessed 07 February 2017].
- [38] J. C. Ambrojo, "El país. Ciberpaís," Grupo Prisa. Ediciones El País S.L., 25 September 2003. [Online]. Available: http://elpais.com/diario/2003/09/25/ciberpais/1064457326_850215.html. [Accessed 07 February 2017].
- [39] Sans Institute, "SANS Institute," [Online]. Available: <https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981>. [Accessed 07 February 2017].
- [40] H. Tanaka, Information System Security, Berlin: Springer Berlin Heidelberg, 2007.
- [41] F. Xia, L. T. Yang, L. Wang and A. Vinel, "Internet of Things," *International Journal of Communication Systems*, no. 25, pp. 1101-1102, 2012.
- [42] Fibersystem AB, «Fibersystem AB,» [En línea]. Available: <https://www.fibersystem.se/emsec-electromagnetic-emanations/>. [Último acceso: 07 February 2017].
- [43] E. Williams, "Hackaday," 19 October 2015. [Online]. Available: <http://hackaday.com/2015/10/19/tempest-a-tin-foil-hat-for-your-electronics-and-their-secrets/>. [Accessed 08 February 2017].
- [44] A. Orebaugh, G. Ramírez, J. Burke, L. Pesce, M. Greg and J. Wright, Wireshark & Ethereal Network, Rockland, MA: Syngress Publishing, Inc, 2007.
- [45] A. S. Tanenbaum and D. J. Wetherall, "Network Security," in *Computer Networks*, Boston,

- Pearson Education, Inc., 2011, p. 860.
- [46] G. McDonald and O. Gavin, “Ransomware Growing Menace,” Symantec Corporation, Mountain View, 2012.
 - [47] C. Kang, "Megaupload shutdown raises new Internet-sharing fears," *The Washington Post*, pp. Web article: https://www.washingtonpost.com/business/technology/megaupload-shutdown-raises-new-internet-sharing-fears/2012/01/20/gIQATHRtEQ_story.html?utm_term=.4028ed5e66f3, 20 January 2012.
 - [48] S. Barker, “Security brief Corporation,” 06 July 2016. [Online]. Available: <https://securitybrief.co.nz/story/fourfold-increase-ransomware-attacks-against-android/>. [Accessed 09 February 2017].
 - [49] Dadax LTD, “Internet Live Stats: Internet Users,” Worldometers, 01 July 2016. [Online]. Available: <http://www.internetlivestats.com/internet-users/#trend>. [Accessed 10 February 2017].
 - [50] N. Woolf, "DDos attack that disrupted internet was largest of its kind in history, experts say," *The Guardian*, 26 October 2016.
 - [51] TKJ Media AB, “TkJ.se,” Spree AB, 5 August 2014. [Online]. Available: <http://blog.tkj.se/>. [Accessed 28 February 2017].
 - [52] Telegraph Media Group, “Top 10 worst computer viruses,” 18 March 2009. [Online]. Available: <http://www.telegraph.co.uk/technology/5012057/Top-10-worst-computer-viruses-of-all-time.html>. [Accessed 28 February 2017].
 - [53] Norton Team, “Norton,” 22 February 2016. [Online]. Available: https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html. [Accessed 28 February 2017].
 - [54] L. Keeler, “AOL,” 07 Decemeber 2016. [Online]. Available: <https://www.aol.com/article/news/2016/12/07/bizarre-and-viral-trends-captivated-millions-in-2016/21622739/>. [Accessed 28 February 2017].
 - [55] Augment, “Augment,” 20 June 2016. [Online]. Available: <http://www.augment.com/blog/interactive-media-newest-digital-marketing-trend/>. [Accessed 28 February 2017].
 - [56] Comigo, “Comigo,” 15 February 2015. [Online]. Available: <http://www.comigo.com/blog/the-2-most-important-interactive-features-pay-tv-operators-should-offer-today/>. [Accessed 28 February 2017].
 - [57] B. Parmar, “Hindustan Times,” 20 October 2016. [Online]. Available: <http://www.hindustantimes.com/business-news/this-is-how-3-2-million-debit-cards-in-india-were-compromised/story-BHsFrKK076cHYu4SRx2VjN.html>. [Accessed 28 February 2017].
 - [58] S. Cobb, “We Live Security,” 24 October 2016. [Online]. Available: <http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>. [Accessed 28 February 2017].
 - [59] Russia Today, “Russia Today,” 22 October 2016. [Online]. Available: <https://www.rt.com/viral/363778-internet-things-ddos-attack/>. [Accessed 28 February 2017].
 - [60] S. Thielman, “The Guardian,” 25 October 2016. [Online]. Available:

- <https://www.theguardian.com/technology/2016/oct/25/ddos-cyber-attack-dyn-internet-of-things>. [Accessed 28 February 2017].
- [61] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. LV, no. 1, pp. 74-81, 2012.
 - [62] D. Chyi, "Flickr," 13 July 2007. [Online]. Available: <https://www.flickr.com/photos/blogjunkie/796739866>. [Accessed 08 February 2017].
 - [63] T. Fox-Brewster, "Londoners give up eldest children in public Wi-Fi security horror show," *The guardian*, 29 September 2014.
 - [64] The Tor Project, Inc, "Tor Project," [Online]. Available: <https://www.torproject.org/about/overview.html.en>. [Accessed 22 January 2017].
 - [65] Cyberops, "Cyberops," [Online]. Available: https://cyberops.com.au/wp-content/uploads/2016/08/2000px-Onion_diagram.svg_-250x250.png. [Accessed 22 January 2017].
 - [66] The Tor Project, Inc, "Transproxy Project," March 2016. [Online]. Available: <https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxyLeaks>. [Accessed 12 February 2017].
 - [67] SSL Shopper, "Verisign," 26 October 2016. [Online]. Available: https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml. [Accessed 04 February 2017].
 - [68] Adafruit Learning System, "Adafruit," [Online]. Available: <https://learn.adafruit.com/onion-pi/overview>. [Accessed 22 January 2017].
 - [69] OpenVPN Technologies, Inc, "OpenVPN," 2002. [Online]. Available: <https://openvpn.net/index.php/open-source/documentation/howto.html>. [Accessed 04 February 2017].
 - [70] M. Feilner, Building and Integrating Virtual Private Networks, Birmingham (UK): Packt Publishing Ltd., 2006.
 - [71] Verisign, "SSL Shopper," SSL Shopper, 15 May 2007. [Online]. Available: <https://www.sslshopper.com/what-is-ssl.html>. [Accessed 05 February 2017].
 - [72] N. Sullivan, "Cloud Flare," 24 June 2015. [Online]. Available: <https://blog.cloudflare.com/content/images/2015/06/illustrations-ssl-blog-june-2015-03.png>. [Accessed 10 February 2017].
 - [73] T. Hayajneh, S. Khasawneh, B. Jamil and A. Itradat, "Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications," in *SECURWARE 2012: The Sixth International Conference on Emerging Security Information*, Zarqa, Jordan, 2012.
 - [74] F. Keikkila, "IEEE Security & Privacy," in *SecureWorld Expo 2005*, Deaborn, 2005.
 - [75] S. Wong, "Database Leet Upload," 20 May 2003. [Online]. Available: <http://www.leetupload.com/database/Misc/Papers/WIRELESS/SHELF/paper1109.pdf>. [Accessed 10 February 2017].
 - [76] R. Mobili, "Wi-Fi Protected Setup (WPS)," Universita Degli Studi di Napoli Federico II, Naples, 2014.

- [77] Sophos Ltd., “Sophos,” [Online]. Available: <https://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-linux.aspx>. [Accessed 10 February 2017].
- [78] Comodo Group, Inc., “Comodo Group,” [Online]. Available: https://www.comodo.com/home/internet-security/antivirus-for-linux.php?track=8223#bottom_free_download. [Accessed 10 February 2017].
- [79] Ubuntu Community, “Ubuntu Forums. Firewall,” 20 June 2013. [Online]. Available: <https://help.ubuntu.com/community/Firewall>. [Accessed 10 February 2017].
- [80] Ubuntu Community, “Ubuntu Forums. UFW,” 2015 May 27. [Online]. Available: <https://help.ubuntu.com/community/UFW>. [Accessed 10 February 2017].
- [81] J. Jung, E. Sit, H. Balakrishnan and R. Morris, “DNS performance and the effectiveness of caching,” *IEEE/ACM Transactions on Networking*, vol. X, no. 5, pp. 589-603, 2002.
- [82] M. Brain and S. Crawford, “How Stuff Works: How Domain Name Servers Work,” 01 April 2000. [Online]. Available: <http://computer.howstuffworks.com/dns.htm>. [Accessed 28 February 2017].
- [83] Raspbian community, “Raspbian,” [Online]. Available: <https://www.raspbian.org/RaspbianImages>. [Accessed 22 January 2017].
- [84] Raspberry Pi Foundation, “Raspberry Pi Forums,” 23 January 2016. [Online]. Available: <https://www.raspberrypi.org/forums/viewtopic.php?f=66&t=133691>. [Accessed 11 February 2017].
- [85] N. West and J. Pujol García, *Operation Garbo: The Personal Story of the Most Successful Spy of World War II*, Biteback Publishing, 2011.
- [86] Linux Community, “Linux commands,” July 2005. [Online]. Available: http://linuxcommand.org/man_pages/chmod1.html. [Accessed 11 February 2017].
- [87] Tor Project, Inc, “Tor project,” [Online]. Available: <https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy>. [Accessed 28 January 2017].
- [88] The Tor Project, Inc, “Isolating proxy project,” 2014. [Online]. Available: <https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO/IsolatingProxy>. [Accessed 12 February 2017].
- [89] Whonix, “Whonix Forums,” Decemeber 2014. [Online]. Available: <https://forums.whonix.org/t/whonix-raspberry-pi/723>. [Accessed 12 February 2017].
- [90] Whonix Community, “Whonix Build in Debian Configuration,” [Online]. Available: https://www.whonix.org/wiki/Dev/Build_Documentation/Physical_Isolation. [Accessed 12 February 2017].
- [91] The Tor project, Inc, “Check Tor,” Tor Project, Inc, [Online]. Available: <https://check.torproject.org/>. [Accessed 07 February 2017].
- [92] J. Aragon, “Jonah Aragon,” 10 April 2014. [Online]. Available: <https://sys.jonaharagon.com/2016/05/12/setting-up-an-openvpn-server-on-a-raspberry-pi-2-part-12/>. [Accessed 02 February 2017].
- [93] Talos Group, “ClamAV,” [Online]. Available: <https://www.clamav.net/documents/installing-clamav>. [Accessed 14 February 2017].

- [94] F. Ceratto, "Debian Wiki," Public Interest, Inc, 21 January 2016. [Online]. Available: <https://wiki.debian.org/HowTo/dnsmasq>. [Accessed 15 February 2017].
- [95] S. Monk, "Adafruit Learning System," 04 May 2015. [Online]. Available: <https://learn.adafruit.com/adafruit-raspberry-pi-lesson-7-remote-control-with-vnc/installing-vnc>. [Accessed 28 February 2017].
- [96] RS Components Ltd., "RS Components Ltd.," Raspberry Pi Foundation, 11 February 2017. [Online]. Available: <http://uk.rs-online.com/web/generalDisplay.html?id=raspberrypi>. [Accessed 02 March 2017].
- [97] European Institute for Computer Anti-Virus Research, "EICAR," Trivent Media & Design, 01 May 2003. [Online]. Available: <http://www.eicar.org/86-0-intended-use.html>. [Accessed 02 March 2017].
- [98] rtCamp Solutions, "Easy Engine," [Online]. Available: <https://easyengine.io/tutorials/mail/server/testing/antivirus/>. [Accessed 02 March 2017].
- [99] M. Febrero and Borja, "Instituto Nacional de Ciberseguridad de España S.A.," Plan Avanza2, Febrero 2011. [Online]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf. [Accessed 21 February 2017].
- [100] Cyberware Ltd., "Cyber Air," [Online]. Available: <http://www.cyberair.co.uk/support/windows/sharing-internet-connection-to-other-devices-via-ethernet-cable>. [Accessed 03 March 2017].
- [101] K. Eaton, "Fast Company," Fast Company & Inc, 15 March 2012. [Online]. Available: <https://www.fastcompany.com/1825005/how-one-second-could-cost-amazon-16-billion-sales>. [Accessed 20 February 2017].
- [102] J. White, "Linkedin," Linkedin, 12 November 2012. [Online]. Available: <https://www.linkedin.com/pulse/20141112210153-68335342-top-3-business-failures-due-to-slow-internet>. [Accessed 20 February 2017].
- [103] F. Fui-Hoon Nah, "A study on tolerable waiting time: how long are Web users willing to wait?," in *Behaviour & Information Technology*, Rolla, Missouri, Tom Stewart, 2007, pp. 153-163.
- [104] SimilarWeb LTD 2017, "SimilarWeb," 01 January 2017. [Online]. Available: <https://www.similarweb.com/top-websites>. [Accessed 20 February 2017].
- [105] Moz, Inc, "The Moz," 26 January 2017. [Online]. Available: <https://moz.com/top500>. [Accessed 20 February 2017].
- [106] Alexa Internet, Inc, "Alexa," 20 February 2017. [Online]. Available: <http://www.alexa.com/topsites>. [Accessed 20 February 2017].
- [107] W. Zhang, Q. Zheng, H. Li and F. Tian, "An overlay multicast protocol for live streaming and delay-guaranteed interactive media," *Journal of Network and Computer Applications*, vol. XXXV, no. 1, pp. 20-28, 2012.
- [108] Raspberry Pi Foundation, "Raspberry Pi Foundation. FAQs.," [Online]. Available: <https://www.raspberrypi.org/help/faqs/#powerReqs>. [Accessed 03 March 2017].

- [109] C. M. Bishop, Introduction to Computer Security, Boston: Addison-Wesley, 2004.
- [110] W. Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, New Jersey: Prentice Hall, 2005.
- [111] Amazon.com, Inc, “Amazon,” 04 March 2017. [Online]. Available: https://www.amazon.com/s/ref=nb_sb_noss?url=node%3D13983791&field-keywords=raspberry+pi+wireless+adapter. [Accessed 04 March 2017].
- [112] The Tor Project, Inc, “The Tor Project, Inc. Tor users,” [Online]. Available: <https://www.torproject.org/about/torusers.html.en>. [Accessed 04 March 2017].
- [113] M. Murgia, “The Telegraph,” 21 June 2016. [Online]. Available: <http://www.telegraph.co.uk/technology/2016/06/20/children-as-young-as-one-fall-prey-to-paedophiles-using-internet/>. [Accessed 04 March 2017].
- [114] A. Frei, N. Erenay, V. Dittmann and M. Graf, “Paedophilia on the Internet - a study of 33 convicted offenders in the Canton of Lucerne,” Psychiatrische Klinik, Lucerne, 2005.
- [115] E. Lozano, A. Joyce, R. Schiemann, A. Ting and D. Yahyavi, “Online Whistleblowing,” in *Wikileaks & Whistleblowing: Digital Information leakage and its impact on society*, Stanford, Stanford University, 2010-2011, p. 4.
- [116] G. Smith, “The Huffington Post,” 18 July 2013. [Online]. Available: http://www.huffingtonpost.com/2013/07/18/tor-snowden_n_3610370.html. [Accessed 04 March 2017].
- [117] Anonymous France, “Anonymous France,” 06 January 2016. [Online]. Available: <https://www.anonymous-france.eu/wikileaks-submission-platform.html>. [Accessed 04 March 2017].
- [118] M. Long, “Make use of,” 15 December 2016. [Online]. Available: <http://www.makeuseof.com/tag/free-linux-antivirus-programs/>. [Accessed 10 February 2017].
- [119] Linux Community, “Linux Forums,” 31 October 2016. [Online]. Available: <http://www.linuxforums.org/forum/debian-linux/208556-need-antivirus-raspbian.html>. [Accessed 10 February 2017].
- [120] Raspberry Pi Foundation, “Raspberry Pi Foundation,” 05 February 2015. [Online]. Available: <https://www.raspberrypi.org/forums/viewtopic.php?f=91&t=98775>. [Accessed 10 February 2017].
- [121] OpenVPN Technologies, Inc, “OpenVPN,” [Online]. Available: <https://openvpn.net/index.php/access-server/docs/admin-guides/183-how-to-connect-to-access-server-from-a-mac.html>. [Accessed 13 February 2017].
- [122] Jefatura del Estado Español, “I. Disposiciones generales,” in *Ley Orgánica 15/1999, de 13 de diciembre, de Prtección de Datos de Carácter Personal*, Madrid, Boletín Oficial del Estado Español, 1999, p. Title 2: Articles 5 y 6.
- [123] P. W. Stallings, Network and Internetwork security principles and practice, New Jersey: Prentice Hall, 1995.
- [124] A. KS, “Hongkiat,” 27 January 2017. [Online]. Available: <http://www.hongkiat.com/blog/do-donts-tor-network/>. [Accessed 28 February 2017].

- [125] J. Mieres, “Buenas prácticas en seguridad informática,” ESET, 2009.
- [126] N. Lord, “Digital Guardian,” 01 February 2017. [Online]. Available: <https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe>. [Accessed 28 February 2017].
- [127] Malaysia Computer Emergency Response Team, “My Cert,” [Online]. Available: http://www.cybersecurity.my/data/content_files/11/616.pdf. [Accessed 28 February 2017].

I. ATTACHED DOCUMENT I: SAFETY MEASURES

I. General measures³⁰

- Install antivirus and firewall
- Use start-up passwords and PINs and change them periodically
- Create passwords longer than 8 characters, based on a phrase and alternating symbols:
A practical example will be:
Member of the Order of the British Empire = M3m83r0f_0rD3r_BE
- Set filtering rules and do not open suspicious ones
- Back up device data
- Download only from trustworthy websites
- Use https webpages
- Block GPS location and net triangulation
- Use recovery lost devices applications
- Enable Wi-Fi and Bluetooth hiding settings
- Apply storage encryption
- Keep your system updated

II. Anonymous measures³¹

- Use TOR hotspot and OpenVPN
- Disable all automatic updates while using TOR
- Delete and disable cookies
- Do not use personal accounts or give personal data
- Do not use P2P programs

III. Protection measures³¹

- Use TOR with OpenVPN
- Do not use P2P
- The rest of the encryption measures can be omitted

³⁰ Sources are: [1] Jorge Mieres, “Buenas prácticas en seguridad informática”, ESET, 2009. [2] Nate Lord, “Digital Guardian”, 01 February 2017. [Online]. Available: <https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe> [Accessed 28 February 2017]. [3] Malaysia Computer Emergency Response Team, “My Cert”, [Online]. Available: http://www.cybersecurity.my/data/content_files/11/616.pdf [Accessed 28 February 2017].

³¹ Source is: [4] Ashutosh KS, “Hongkiat”, 27 January 2017. [Online]. Available: <http://www.hongkiat.com/blog/don-donts-tor-network/> [Accessed 28 February 2017].

II. ATTACHED DOCUMENT II: FLOW DIAGRAMS

I. General Flow Diagram

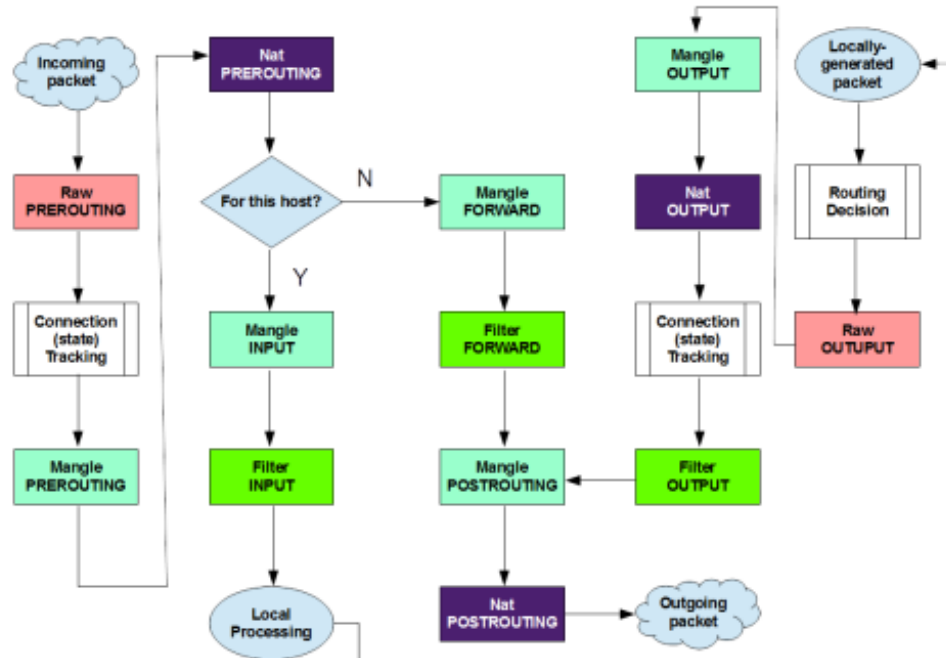


Figure II-1 General Flow Diagram

II. UFW Flow Diagram

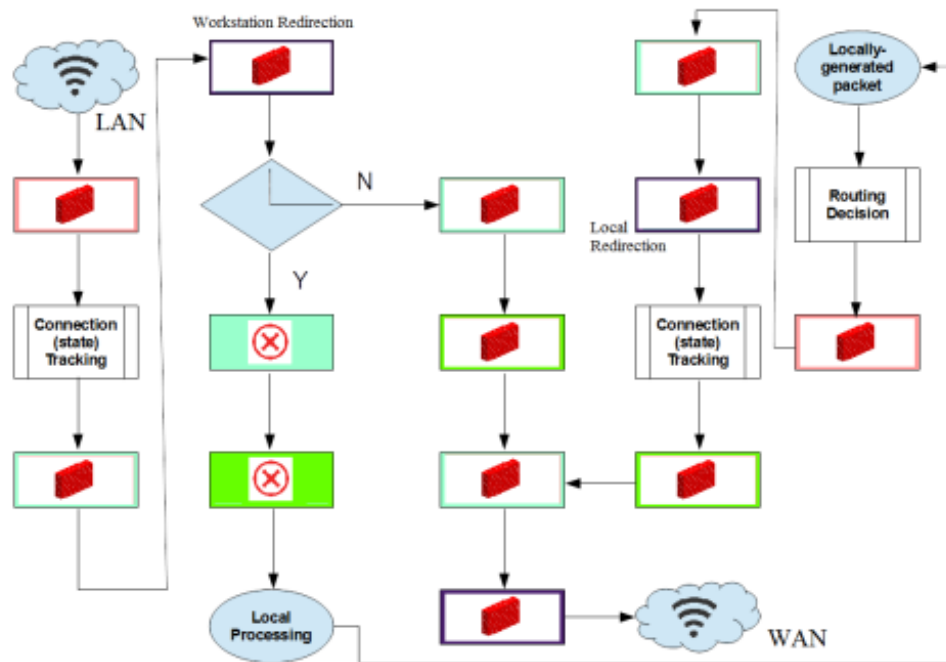


Figure II-2 UFW Flow Diagram

III. TOR Flow Diagram

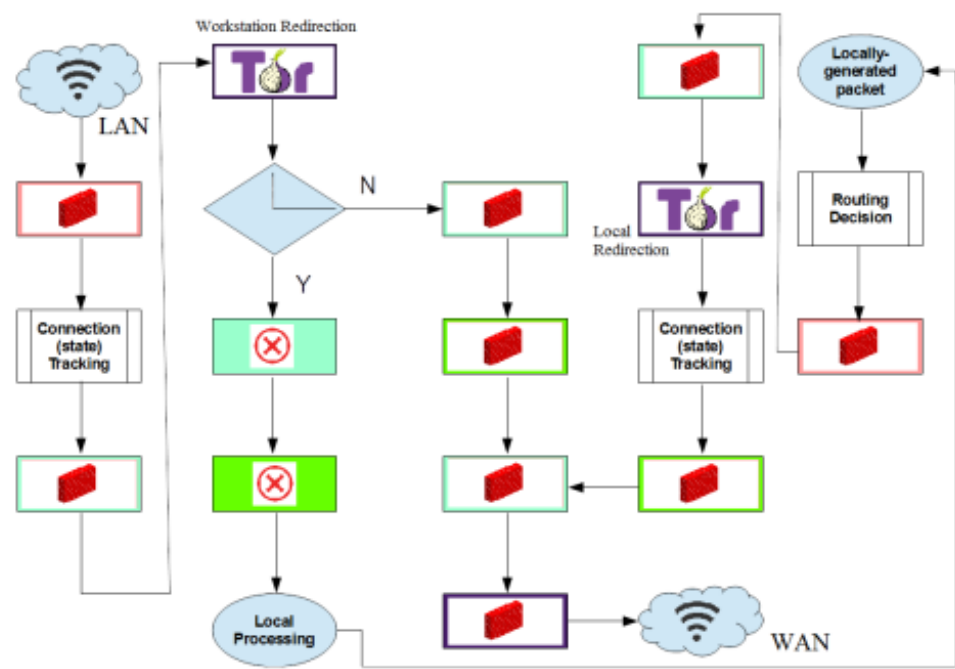


Figure II-3 TOR Flow Diagram

IV. OpenVPN Diagram Flow

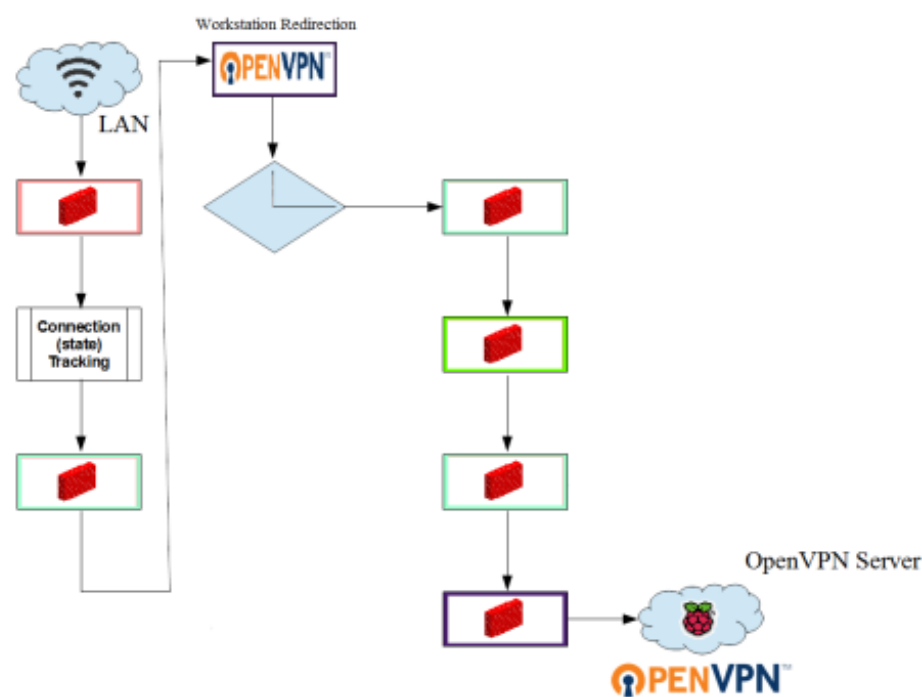


Figure II-4 OpenVPN Diagram Flow

V. OpenVPN and TOR Diagram Flow

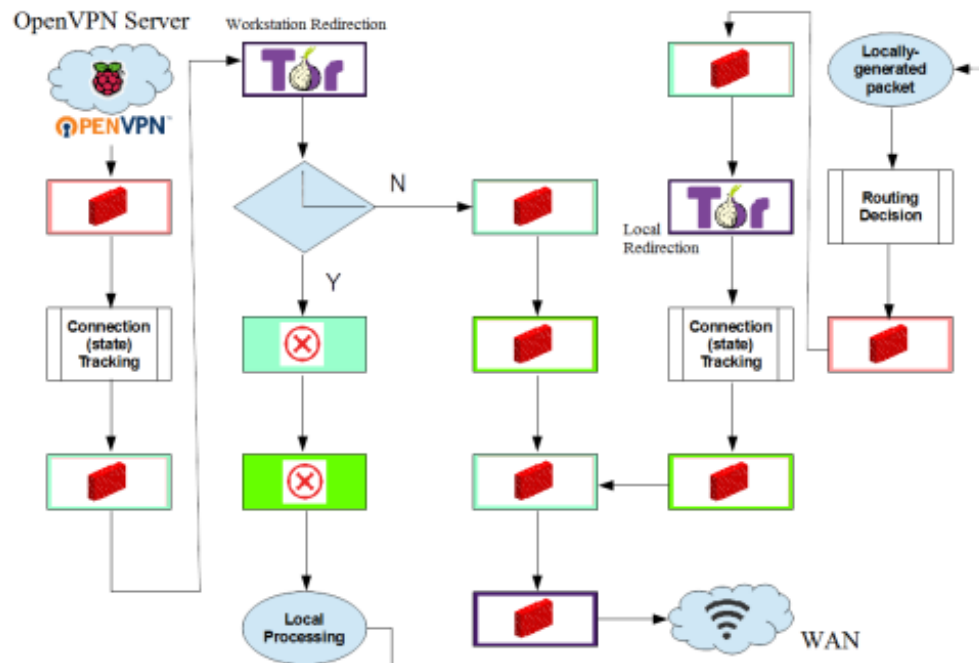


Figure II-5 OpenVPN and TOR Diagram Flow

III. ATTACHED DOCUMENT III: CLIENTS GENERATOR

I. Clients generator file

Create a file which contains the following to generate clients' certificates faster:

- **sudo su**
- **cd /etc/openvpn/easy-rsa/keys/**
- **nano /etc/openvpn/easy-rsa/keys/clientgenerator.sh**³²
Type the next script.

```
#!/bin/bash
# Default Variable Declarations
DEFAULT="client.ovpn"
FILEEXT=".ovpn"
CRT=".crt"
KEY=".key"
CA="ca.crt"
TA="ta.key"
NAME="${1}"

if [ -z "${NAME}" ]; then
    # Ask for a Client name
    echo "Please enter an existing Client Name:"
    read NAME
fi

#1st Verify that client's Public Key Exists
if [ ! -f $NAME$CRT ]; then
    echo "[ERROR]: Client Public Key Certificate not found: $NAME$CRT"
    exit
fi
echo "Client's cert found: $NAME$CRT"

#Then, verify that there is a private key for that client
if [ ! -f $NAME$KEY ]; then
```

³² Based on Mr Eric Jodoin MakeOpenVPN.sh file, from Mr Jonah Aragon "Setting Up OpenVPN on a Raspberry Pi 2" tutorial, hosted in "<https://gist.github.com/coolaj86/4120d90e57d1d01cd59f#file-makeopenvpn-sh>"

```
    echo "[ERROR]: Client Private Key not found: $NAME$KEY"
    exit
fi
echo "Client's Private Key found: $NAME$KEY"

#Confirm the CA public key exists
if [ ! -f $CA ]; then
    echo "[ERROR]: CA Public Key not found: $CA"
    exit
fi
echo "CA public Key found: $CA"

#Confirm the tls-auth ta key file exists
if [ ! -f $TA ]; then
    echo "[ERROR]: tls-auth Key not found: $TA"
    exit
fi
echo "tls-auth Private Key found: $TA"

#Ready to make a new .opvn file - Start by populating with the default file
cat $DEFAULT > $NAME$FILEEXT

#Now, append the CA Public Cert
echo "<ca>" >> $NAME$FILEEXT
cat $CA >> $NAME$FILEEXT
echo "</ca>" >> $NAME$FILEEXT

#Next append the client Public Cert
echo "<cert>" >> $NAME$FILEEXT
cat $NAME$CRT | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' >>
$NAME$FILEEXT
echo "</cert>" >> $NAME$FILEEXT

#Then, append the client Private Key
echo "<key>" >> $NAME$FILEEXT
cat $NAME$KEY >> $NAME$FILEEXT
```

```
echo "</key>" >> $NAME$FILEEXT
```

#Finally, append the TA Private Key

```
echo "<tls-auth>" >> $NAME$FILEEXT
```

```
cat $TA >> $NAME$FILEEXT
```

```
echo "</tls-auth>" >> $NAME$FILEEXT
```

```
echo "Done! $NAME$FILEEXT Successfully Created."
```

Save and close.

– **Chmod 700 clientgenerator.sh**

II. Generating clients

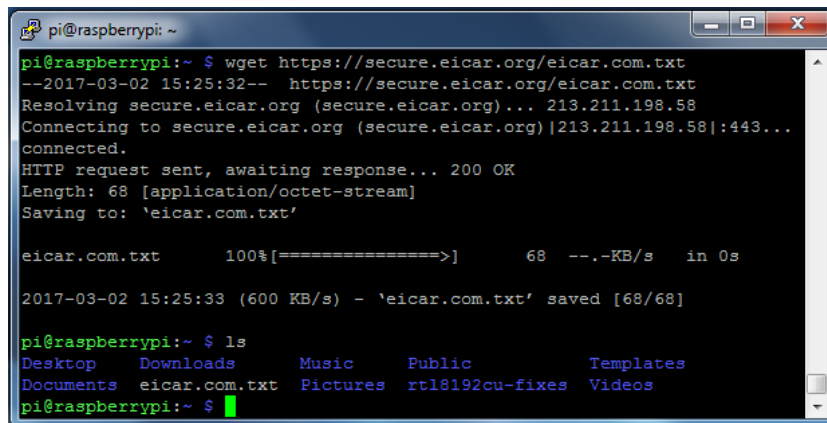
Type the following commands to create new clients' certificates:

- **sudo su**
- **cd /etc/openvpn/easy-rsa/keys/**
- **./build-key-pass Client1³³**
- **./clientgenerator.sh**

The name requested must be the same introduced in the previous command.

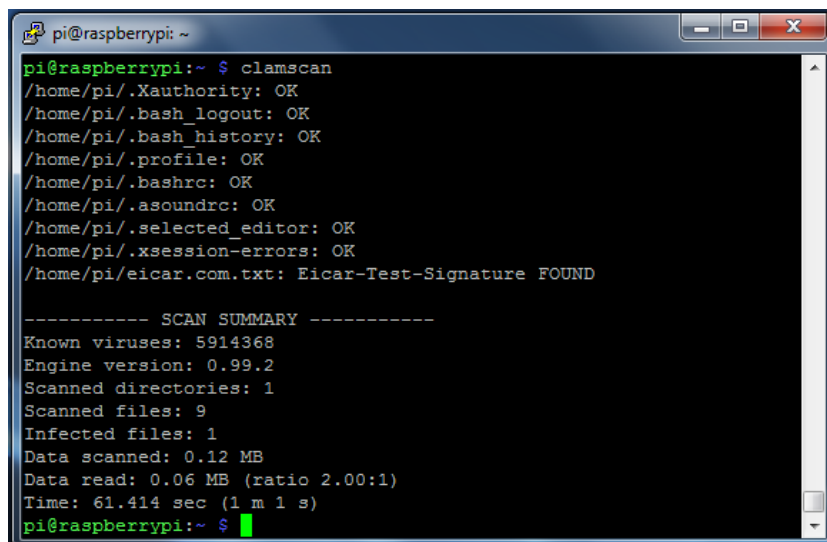
³³ "Client1" can be changed for any name for the user's certificate.

IV. ATTACHED DOCUMENT IV: VIRUS TEST



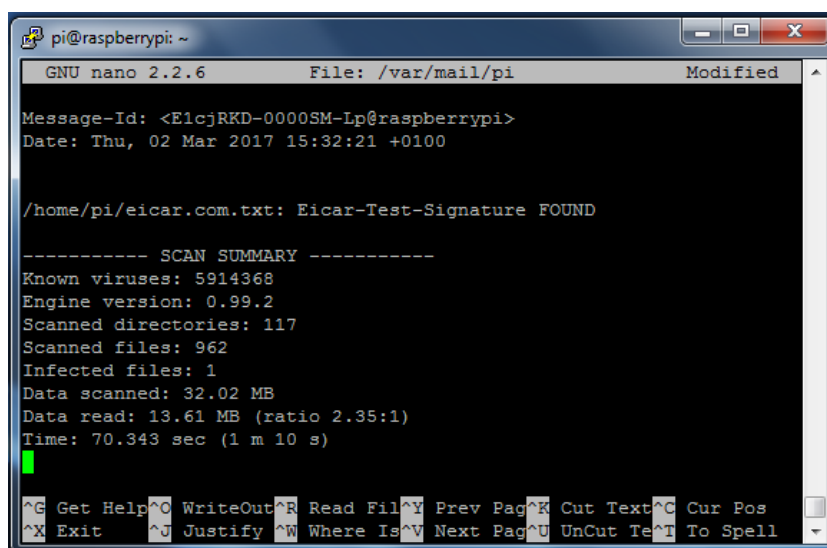
```
pi@raspberrypi: ~  
pi@raspberrypi:~$ wget https://secure.eicar.org/eicar.com.txt  
--2017-03-02 15:25:32-- https://secure.eicar.org/eicar.com.txt  
Resolving secure.eicar.org (secure.eicar.org)... 213.211.198.58  
Connecting to secure.eicar.org (secure.eicar.org)[213.211.198.58]:443...  
connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 68 [application/octet-stream]  
Saving to: 'eicar.com.txt'  
  
eicar.com.txt      100%[=====>]          68  --.-KB/s   in 0s  
  
2017-03-02 15:25:33 (600 KB/s) - 'eicar.com.txt' saved [68/68]  
  
pi@raspberrypi:~$ ls  
Desktop  Downloads  Music      Public     Templates  
Documents eicar.com.txt Pictures  rtl8192cu-fixes Videos  
pi@raspberrypi:~$
```

Figure IV-1 Screenshot downloading Eicar's virus



```
pi@raspberrypi:~$ clamscan  
/home/pi/.Xauthority: OK  
/home/pi/.bash_logout: OK  
/home/pi/.bash_history: OK  
/home/pi/.profile: OK  
/home/pi/.bashrc: OK  
/home/pi/.asoundrc: OK  
/home/pi/.selected_editor: OK  
/home/pi/.xsession-errors: OK  
/home/pi/eicar.com.txt: Eicar-Test-Signature FOUND  
  
----- SCAN SUMMARY -----  
Known viruses: 5914368  
Engine version: 0.99.2  
Scanned directories: 1  
Scanned files: 9  
Infected files: 1  
Data scanned: 0.12 MB  
Data read: 0.06 MB (ratio 2.00:1)  
Time: 61.414 sec (1 m 1 s)  
pi@raspberrypi:~$
```

Figure IV-2 Screenshot of a scan executed



```
pi@raspberrypi: ~  
GNU nano 2.2.6      File: /var/mail/pi      Modified  
  
Message-Id: <E1cjRKD-0000SM-Lp@raspberrypi>  
Date: Thu, 02 Mar 2017 15:32:21 +0100  
  
/home/pi/eicar.com.txt: Eicar-Test-Signature FOUND  
  
----- SCAN SUMMARY -----  
Known viruses: 5914368  
Engine version: 0.99.2  
Scanned directories: 117  
Scanned files: 962  
Infected files: 1  
Data scanned: 32.02 MB  
Data read: 13.61 MB (ratio 2.35:1)  
Time: 70.343 sec (1 m 10 s)  
  
^G Get Help ^O WriteOut ^R Read Fil ^Y Prev Pag ^K Cut Text ^C Cur Pos  
^X Exit    ^J Justify ^W Where Is ^V Next Pag ^U UnCut Te ^T To Spell
```

Figure IV-3 Screenshot of a pi's mail checking

V. ATTACHED DOCUMENT V: WIRESHARK TEST

I. First Wireshark test

File

Name: C:\Users\Usuario\Desktop\TFG\Test\Wireshark\First.pcapng
Length: 3028 kB
Format: Wireshark/... – pcapng
Encapsulation: Ethernet

Time

First packet: 2017-02-16 17:17:51
Last packet: 2017-02-16 17:18:19
Elapsed: 00:00:27

Capture

Hardware: Unknown
OS: 64-bit Windows 7 Service Pack 1, build 7601
Application: Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)

Interfaces

<u>Interface</u>	<u>Dropped packets</u>	<u>Capture filter</u>	<u>Link type</u>	<u>Packet size limit</u>
\Device\NPF_{65EA4DFB-7A7A-4513-8DE1-38246D5EF4A8}	Unknown	None	Ethernet	262144 bytes

Statistics

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	3351	3351 (100.0%)	N/A
Time span, s	27.997	27.997	N/A
Average pps	119.7	119.7	N/A
Average packet size, B	870.5	870.5	N/A
Bytes	2917944	2917944 (100.0%)	0
Average bytes/s	104 k	104 k	N/A
Average bits/s	833 k	833 k	N/A

Packet	Summary	Group	Protocol	Count
⚠ Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	4
⚠ Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	7
⚠ Warning	No response seen to ICMP request	Sequence	ICMP	7
⚠ Warning	Connection reset (RST)	Sequence	TCP	51
⚠ Warning	BER: Dissector for OID not implemented. Contact Wireshar...	Undecoded	SSL	4
ℹ Note	This session reuses previously negotiated keys (Session res...	Sequence	SSL	1
ℹ Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	7
ℹ Note	This frame is a (suspected) retransmission	Sequence	TCP	26
ℹ Note	This frame is a (suspected) fast retransmission	Sequence	TCP	2
ℹ Note	Duplicate ACK (#9)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#8)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#7)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#6)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#5)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#4)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#3)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#24)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#23)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#22)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#21)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#20)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#2)	Sequence	TCP	2
ℹ Note	Duplicate ACK (#19)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#18)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#17)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#16)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#15)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#14)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#13)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#12)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#11)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#10)	Sequence	TCP	1
ℹ Note	Duplicate ACK (#1)	Sequence	TCP	8
💬 Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP	12

Figure V-1 Screenshot of packets seized during first test (1/3)

Packet	Summary	Group	Protocol	Count
💬 Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP	12
💬 Chat	HTTP/1.1 206 Partial Content\r\n	Sequence	HTTP	1
💬 Chat	HTTP/1.1 200 OK\r\n	Sequence	HTTP	64
💬 Chat	GET /51.2885-19/s150x150/16585454_1111380455634877_6...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16465149_234141486995135_67...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16464471_1733046910249294_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16464140_381649522191800_10...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16230935_918182051617691_76...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16230855_707718756056555_51...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16230728_1115876348520943_5...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16229457_157962241368455_83...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16123814_1774068212915344_6...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16123569_1706207189690027_4...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/16123402_367256766975608_25...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/15275629_1768406326745829_7...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/15251655_437749916613280_10...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/15046957_590208421158038_66...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/14704983_349480665401653_26...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/13731320_1362771400431743_8...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/13628295_164416970631962_39...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/13573459_1694544740807038_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/12292615_958609527551594_99...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/11909367_1646466128930076_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-19/s150x150/11363800_193092554415447_74...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s640x640/e15/16789118_11581337309708...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c84.0.472.472/16585144_25...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c72.0.591.591/16789876_18...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c30.0.1019.1019/16789401_...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c155.0.769.769/16465073_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c129.0.462.462/16465038_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c114.0.851.851/16464394_1...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c111.0.858.858/16583806_4...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c101.0.467.467/16788901_2...	Sequence	HTTP	1
💬 Chat	GET /51.2885-15/s240x240/e35/c0.96.768.768/16789310_85...	Sequence	HTTP	1

Figure V-2 Screenshot of packets seized during first test (2/3)

Packet	Summary	Group	Protocol	Count
▷ Chat	GET /t51.2885-15/s240x240/e35/c0.124.1080.1080/16789695...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/c0.109.1080.1080/16788901...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16788737_13028374697705...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16788578_18968959838671...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16788410_23090557398300...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585649_17509818652305...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585530_16782850924700...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585528_18679837068105...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585270_28949503813481...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585225_26699306039684...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16585166_17988768583236...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16584988_73163036033702...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16584919_12537290580677...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16583849_18356304033698...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16583826_10905638677565...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16583664_14328407603477...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16583473_37809901257560...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16583288_18397680129569...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16465875_12289400604948...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16465514_10835422817563...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16465071_18103115625411...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/16464263_17156113334207...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e35/14591118_25544954156514...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/c236.0.607.607/16790183_1...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/c140.0.360.360/16788824_1...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/c139.0.361.361/16789734_2...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/16790054_17330033670149...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/16789200_18880775480703...	Sequence	HTTP	1
▷ Chat	GET /t51.2885-15/s240x240/e15/16465561_22119337501878...	Sequence	HTTP	1
▷ Chat	GET /t50.2886-16/16783708_1255973697813809_5825225639...	Sequence	HTTP	3
▷ Chat	Connection establish request (SYN): server port 80	Sequence	TCP	6
▷ Chat	Connection establish request (SYN): server port 443	Sequence	TCP	6
▷ Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	6
▷ Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	7

Figure V-3 Screenshot of packets seized during first test (3/3)

II. Second Wireshark test³⁴

File

Name: C:\Users\Usuario\Desktop\TFG\Test\Wireshark\Second.pcapng
Length: 8542 kB
Format: Wireshark/... – pcapng
Encapsulation: Ethernet

Time

First packet: 2017-02-16 17:24:27
Last packet: 2017-02-16 17:24:59
Elapsed: 00:00:31

Capture

Hardware: Unknown
OS: 64-bit Windows 7 Service Pack 1, build 7601
Application: Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{65EA4DFB-7A7A-4513-8DE1-38246D5EF4A8}	Unknown	none	Ethernet	262144 bytes

³⁴ Similar captured distribution than in first section (First Wireshark test).

Statistics

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	9725	9725 (100.0%)	N/A
Time span, s	31.609	31.609	N/A
Average pps	307.7	307.7	N/A
Average packet size, B	845.5	845.5	N/A
Bytes	8221510	8221510 (100.0%)	0
Average bytes/s	260 k	260 k	N/A
Average bits/s	2080 k	2080 k	N/A

III. Third Wireshark test

File

Name:	C:\Users\Usuario\Desktop\TFG\Test\Wireshark\Third.pcapng
Length:	14 MB
Format:	Wireshark/... – pcapng
Encapsulation:	Ethernet

Time

First packet:	2017-02-16 22:29:19
Last packet:	2017-02-16 22:36:25
Elapsed:	00:07:06

Capture

Hardware:	Unknown
OS:	64-bit Windows 7 Service Pack 1, build 7601
Application:	Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)

Interfaces

<u>Interface</u>	<u>Dropped packets</u>	<u>Capture filter</u>	<u>Link type</u>	<u>Packet size limit</u>
\Device\NPF_{65EA4DFB-7A7A-4513-8DE1-38246D5EF4A8}	0 (0 %)	None	Ethernet	262144 bytes

Statistics

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	18231	18231 (100.0%)	N/A
Time span, s	426.331	426.331	N/A
Average pps	42.8	42.8	N/A
Average packet size, B	739.5	739.5	N/A
Bytes	13475236	13475236 (100.0%)	0
Average bytes/s	31 k	31 k	N/A
Average bits/s	252 k	252 k	N/A

Packet	Summary	Group	Protocol	Count
Warning	Previous segment not captured (common at capture start)	Sequence	TCP	40
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	3
Warning	Connection reset (RST)	Sequence	TCP	14
Note	Duplicate ACK (#1)	Sequence	TCP	30
Note	Duplicate ACK (#2)	Sequence	TCP	26
Note	Duplicate ACK (#3)	Sequence	TCP	24
Note	Duplicate ACK (#4)	Sequence	TCP	21
Note	Duplicate ACK (#5)	Sequence	TCP	18
Note	Duplicate ACK (#6)	Sequence	TCP	16
Note	Duplicate ACK (#7)	Sequence	TCP	15
Note	Duplicate ACK (#8)	Sequence	TCP	12
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	13
Note	This frame is a (suspected) retransmission	Sequence	TCP	378
Note	Duplicate ACK (#9)	Sequence	TCP	8
Note	Duplicate ACK (#10)	Sequence	TCP	7
Note	Duplicate ACK (#11)	Sequence	TCP	7
Note	Duplicate ACK (#12)	Sequence	TCP	5
Note	Duplicate ACK (#13)	Sequence	TCP	5
Note	Duplicate ACK (#14)	Sequence	TCP	4
Note	Duplicate ACK (#15)	Sequence	TCP	3
Note	Duplicate ACK (#16)	Sequence	TCP	3
Note	Duplicate ACK (#17)	Sequence	TCP	2
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	18
Note	"Time To Live" != 255 for a packet sent to the Local Netwo...	Sequence	IPv4	3
Note	Dissector for QUIC Tag MIDS (Unknown) code not implem...	Undecoded	QUIC	29
Note	Dissector for QUIC Tag STTL (Unknown) code not implem...	Undecoded	QUIC	14
Note	Truncated Tag Length...	Malformed	QUIC	14
Note	Duplicate ACK (#18)	Sequence	TCP	1
Chat	TCP window update	Sequence	TCP	97
Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP	312
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	24
Chat	Connection finish (FIN)	Sequence	TCP	374

Figure V-4 Screenshot of packets seized during third test

IV. Fourth Wireshark test

File

Name: C:\Users\Usuario\Desktop\TFG\Test\Wireshark\Fourth.pcapng
 Length: 29 MB
 Format: Wireshark/... – pcapng
 Encapsulation: Ethernet

Time

First packet: 2017-02-16 23:14:52
 Last packet: 2017-02-16 23:18:08
 Elapsed: 00:03:16

Capture

Hardware: Unknown
 OS: 64-bit Windows 7 Service Pack 1, build 7601
 Application: Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)

Interfaces

<u>Interface</u>	<u>Dropped packets</u>	<u>Capture filter</u>	<u>Link type</u>	<u>Packet size limit</u>
\Device\NPF_{65EA4DFB-7A7A-4513-8DE1-38246D5EF4A8}	206 (0.6 %)	none	Ethernet	262144 bytes

Statistics

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	34004	34004 (100.0%)	N/A
Time span, s	196.313	196.313	N/A
Average pps	173.2	173.2	N/A
Average packet size, B	826.5	826.5	N/A
Bytes	28116144	28116144 (100.0%)	0
Average bytes/s	143 k	143 k	N/A
Average bits/s	1145 k	1145 k	N/A

Severity	Summary	Group	Protocol	Count
Warning	Connection reset (RST)	Sequence	TCP	1
Warning	ACKed segment that wasn't captured (common at capture...	Sequence	TCP	11
Warning	Previous segment not captured (common at capture start)	Sequence	TCP	9
Warning	Ignored Unknown Record	Protocol	SSL	30
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1
Note	"Time To Live" != 255 for a packet sent to the Local Netwo...	Sequence	IPv4	2
Note	This frame is a (suspected) retransmission	Sequence	TCP	16
Note	Duplicate ACK (#1)	Sequence	TCP	5
Note	Duplicate ACK (#2)	Sequence	TCP	4
Note	Duplicate ACK (#3)	Sequence	TCP	4
Note	Duplicate ACK (#4)	Sequence	TCP	3
Note	Duplicate ACK (#5)	Sequence	TCP	2
Note	Duplicate ACK (#6)	Sequence	TCP	2
Note	Duplicate ACK (#7)	Sequence	TCP	2
Note	Duplicate ACK (#8)	Sequence	TCP	2
Note	Duplicate ACK (#9)	Sequence	TCP	2
Note	Duplicate ACK (#10)	Sequence	TCP	2
Note	Duplicate ACK (#11)	Sequence	TCP	2
Note	Duplicate ACK (#12)	Sequence	TCP	2
Note	Duplicate ACK (#13)	Sequence	TCP	2
Note	Duplicate ACK (#14)	Sequence	TCP	2
Note	Duplicate ACK (#15)	Sequence	TCP	2
Note	Duplicate ACK (#16)	Sequence	TCP	2
Note	Duplicate ACK (#17)	Sequence	TCP	1
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	1
Chat	TCP window update	Sequence	TCP	270
Chat	Connection finish (FIN)	Sequence	TCP	15
Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP	24
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	13

Figure V-5 Screenshot of packets seized during fourth test

V. Fifth Wireshark test

File

Name:	C:\Users\Usuario\Desktop\TFG\Test\Wireshark\Fifth.pcapng
Length:	11 MB
Format:	Wireshark/... – pcapng
Encapsulation:	Unknown

Time

First packet:	2017-02-16 23:18:23
Last packet:	2017-02-16 23:20:59
Elapsed:	00:00:36

Capture

Hardware:	Unknown
OS:	64-bit Windows 7 Service Pack 1, build 7601
Application:	Dumpcap (Wireshark) 2.2.4 (v2.2.4-0-gcc3dc1b)

Interfaces

<u>Interface</u>	<u>Dropped packets</u>	<u>Capture filter</u>	<u>Link type</u>	<u>Packet size limit</u>
\\Device\\NPF_{65EA4DFB-7A7A-4513-8DE1-38246D5EF4A8}	Unknown	none	Ethernet	262144 bytes

Statistics

<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	13273	13273 (100.0%)	N/A
Time span, s	36.136	36.136	N/A
Average pps	367.3	367.3	N/A
Average packet size, B	863.5	863.5	N/A
Bytes	11454979	11454979 (100.0%)	0
Average bytes/s	316 k	316 k	N/A
Average bits/s	2535 k	2535 k	N/A

Severity	Summary	Group	Protocol	Count
▷ Note	"Time To Live" != 255 for a packet sent to the Local Netwo...	Sequence	IPv4	5
▷ Note	This frame is a (suspected) retransmission	Sequence	TCP	2
▷ Chat	TCP window update	Sequence	TCP	218
▷ Chat	NOTIFY * HTTP/1.1\r\n	Sequence	SSDP	144
▷ Chat	Connection finish (FIN)	Sequence	TCP	2
▷ Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	12

Figure V-6 Screenshot of packets seized during fifth test

VI. ATTACHED DOCUMENT VI: POPULAR SERVICES AND APPLICATIONS TEST

I. Streaming media (Spotify)

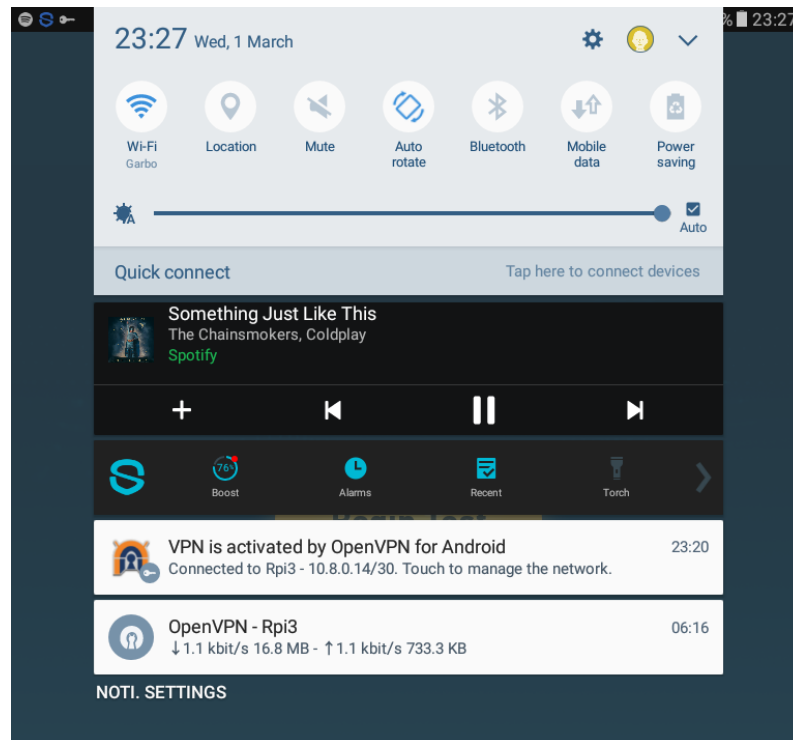


Figure VI-1 Screenshot of Spotify test

II. Social Networks' applications (Facebook)

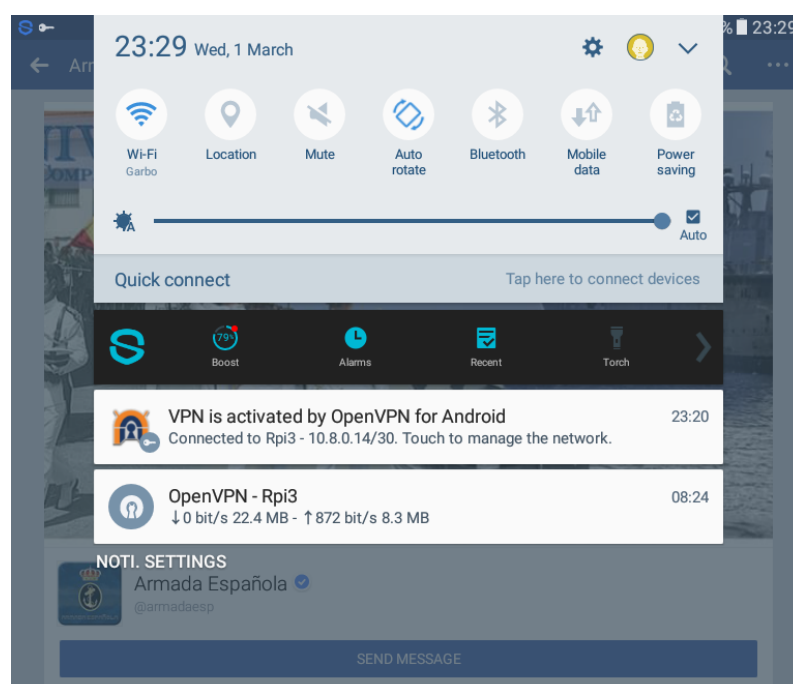


Figure VI-2 Screenshot of Facebook test

III. Streaming media Social Networks (Instagram)

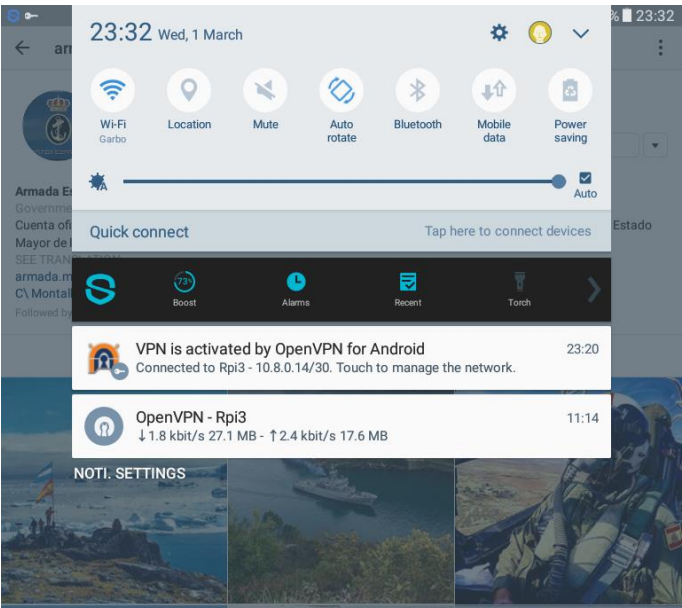


Figure VI-3 Screenshot of Instagram test

IV. Download manager (Play Store)

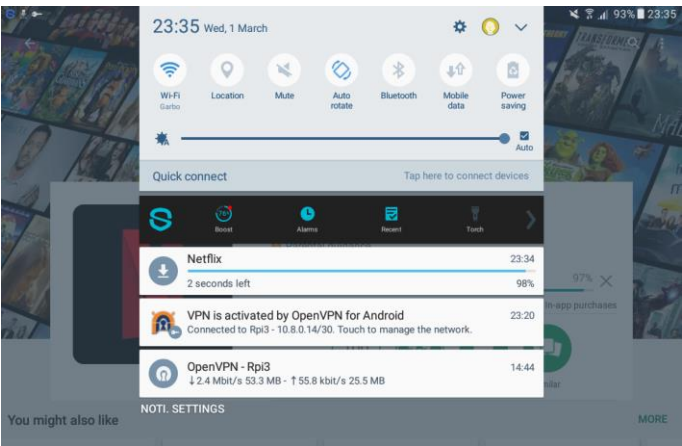


Figure VI-4 Screenshot of Play Store test

V. Streaming media (YouTube)

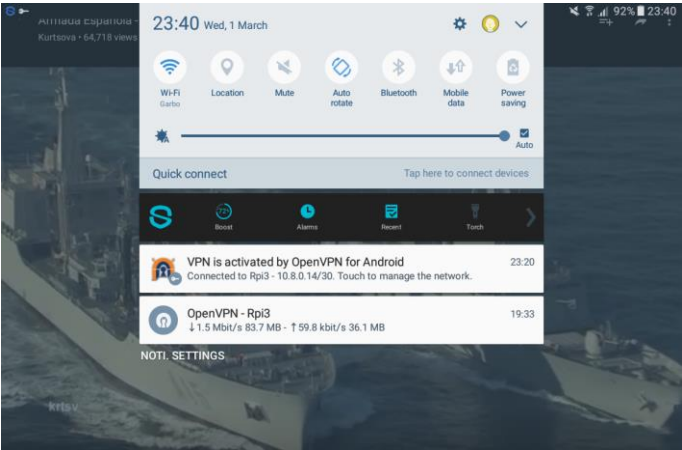


Figure VI-5 Screenshot of YouTube test

VI. News broadcasting applications (Al Jazeera News)

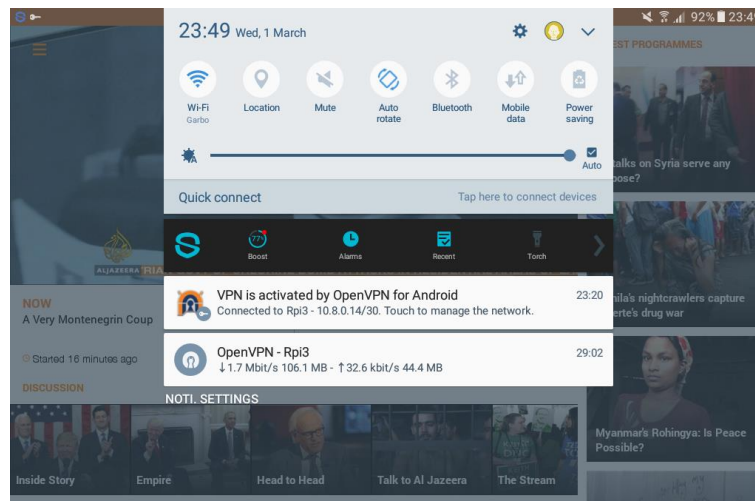


Figure VI-6 Screenshot of Al Jazeera News application test

VII. Outlook

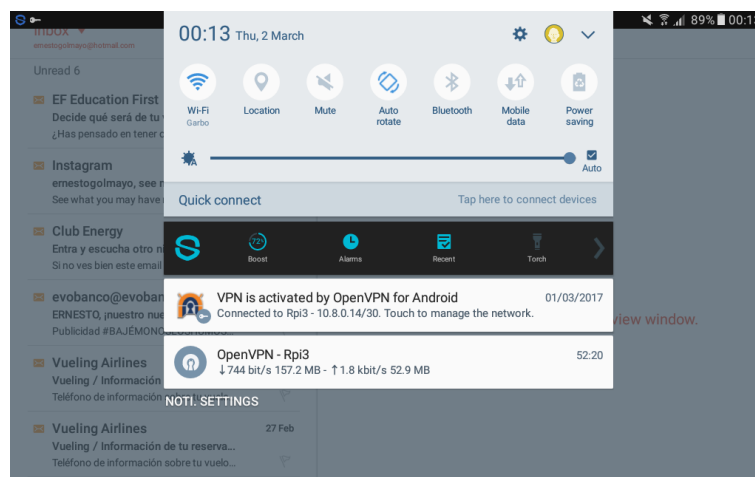


Figure VI-7 Screenshot of Outlook test

VIII. Messenger applications (Whatsapp)

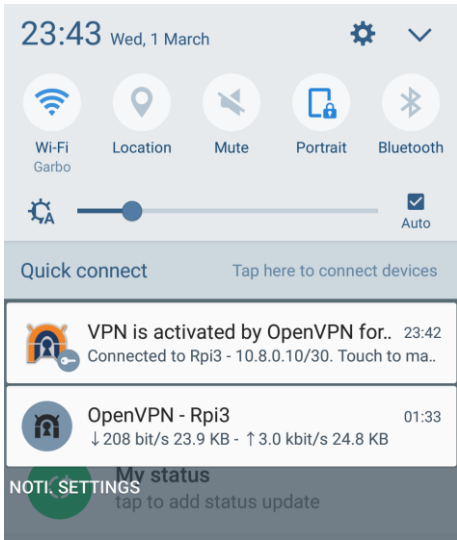


Figure VI-8 Screenshot of Whatsapp test

IX. Summary of popular services and applications test³⁵

SPEEDTEST™				
7 RESULTS				
TYPE	TIME	DOWNLOAD	UPLOAD	PING
📶	02/03/2017 00:13	2.91	2.69	622
📶	01/03/2017 23:51	1.66	2.72	638
📶	01/03/2017 23:40	1.53	3.16	187
📶	01/03/2017 23:35	3.00	3.27	138
📶	01/03/2017 23:32	3.29	2.59	180
📶	01/03/2017 23:29	2.78	4.51	532
📶	01/03/2017 23:27	2.87	3.74	532

Figure VI-9 Screenshot of popular services and applications test's summary

³⁵ Whatsapp test was carried out on a different station and it is not included in the summary.

VII. ATTACHED DOCUMENT VII: DOWNLOADING AND RESOLVING DELAY CHARTS CLEAR ACCESS

I. Readings without DNS Server

Downloading Delay / Popular webs												
No DNS Server / No TOR / No OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	0,225	0,201	0,201	0,201	0,216	0,186	0,202	0,203	0,181	0,201	0,2017	
Youtube	0,299	0,308	0,209	0,281	0,217	0,221	0,203	0,292	0,101	0,281	0,2412	
Facebook	0,314	0,262	0,236	0,286	0,387	0,244	0,246	0,32	0,307	0,343	0,2945	
Wikipedia	0,33	0,18	0,181	0,565	0,308	0,2	0,308	0,18	0,201	0,18	0,2633	
Amazon	0,58	0,559	0,565	0,58	0,581	0,619	0,396	0,834	0,601	0,578	0,5893	
Twitter	0,301	0,292	0,363	0,355	0,342	0,404	0,345	0,342	0,339	0,319	0,3402	
Linkedin	0,292	0,327	0,37	0,328	0,31	0,292	0,291	0,266	0,263	0,271	0,301	
Instagram	0,215	0,195	0,308	0,21	0,237	0,28	0,195	0,213	0,231	0,248	0,2332	
Yahoo	0,286	0,264	0,267	0,256	0,275	0,307	0,24	0,275	0,252	0,262	0,2684	
Average	0,3157778	0,2875556	0,3	0,3402222	0,3192222	0,3058889	0,2695556	0,325	0,2751111	0,2981111	0,30364444	

Table VII-1 Downloading delay readings NO DNS / NO TOR / NO OVPN / Clear access

Requesting Delay / Popular webs												
No DNS Server / No TOR / No OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	0,139	0,116	0,099	0,117	0,105	0,109	0,128	0,089	0,101	0,112	0,1115	
Youtube	0,146	0,165	0,139	0,106	0,125	0,151	0,111	0,127	0,123	0,171	0,1364	
Facebook	0,103	0,109	0,106	0,082	0,112	0,101	0,092	0,113	0,121	0,103	0,1042	
Wikipedia	0,217	0,254	0,115	0,177	0,127	0,129	0,081	0,105	0,09	0,083	0,1378	
Amazon	0,095	0,087	0,087	0,092	0,097	0,103	0,112	0,096	0,09	0,093	0,0952	
Twitter	0,116	0,076	0,084	0,118	0,108	0,084	0,091	0,08	0,111	0,103	0,0971	
LinkedIn	0,136	0,087	0,134	0,128	0,114	0,091	0,121	0,099	0,135	0,116	0,1161	
Instagram	0,178	0,141	0,114	0,113	0,086	0,101	0,084	0,117	0,119	0,107	0,116	
Yahoo	0,105	0,078	0,082	0,102	0,085	0,094	0,111	0,089	0,093	0,115	0,0954	
Average	0,1372222	0,1236667	0,1066667	0,115	0,1065556	0,107	0,1034444	0,1016667	0,1092222	0,11144444	0,11218889	

Table VII-2 Requesting delay readings NO DNS / NO TOR / NO OVPN / Clear access

Downloading Delay / Webs by Country												
No DNS / No TOR / No OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
New Zealand Navy	1,857	1,83	2,275	1,859	1,406	2,39	1,865	2,014	1,883	1,843	1,9222	
South Africa Government	1,418	1,409	2,057	1,898	1,816	1,716	1,325	1,825	1,383	1,425	1,6272	
Russia foreign ministry	0,432	0,375	0,444	0,412	0,354	0,376	0,401	0,435	0,387	0,394	0,401	
Argentinian afa	1,425	1,183	1,172	1,01	1,395	1,009	1,05	1,001	0,833	0,941	1,1019	
Rugby India	3,492	3,54	3,612	3,588	2,214	0,987	1,095	0,908	1,453	1,059	2,1948	
Average	1,7248	1,6674	1,912	1,7534	1,437	1,2956	1,1472	1,2366	1,1878	1,1324	1,44942	

Table VII-3 Downloading delay readings NO DNS / NO TOR / NO OVPN / Clear access

Requesting Delay / Webs by Country												
No DNS Server / No TOR / No OVPN												
Web / Delay	First	Second	Third	Fourth	Fifth	Sixth	Seventh	Eight	Ninth	Tenth	Average	
New Zealand Navy	0,443	0,451	0,416	0,416	0,439	0,111	0,088	0,089	0,11	0,439	0,3002	
South Africa Government	0,314	0,313	0,293	0,104	0,135	0,101	0,107	0,131	0,126	0,108	0,1732	
Russia foreign ministry	0,129	0,127	0,13	0,108	0,126	0,091	0,096	0,0109	0,133	0,117	0,10679	
Argentinian afa	0,305	0,319	0,306	0,306	0,085	0,1	0,294	0,104	0,105	0,104	0,2028	
Rugby India	0,13	0,106	0,138	0,837	0,139	0,133	0,862	1,106	0,862	0,077	0,439	
Average	0,2642	0,2632	0,2566	0,3542	0,1848	0,1072	0,2894	0,28818	0,2672	0,169	0,244398	

Table VII-4 Requesting delay readings NO DNS / NO TOR / NO OVPN / Clear access

II. Readings with DNS Server

Downloading Delay / Popular webs											
DNS Server / No TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,234	0,135	0,11	0,169	0,129	0,124	0,142	0,135	0,165	0,137	0,148
Youtube	0,257	0,211	0,259	0,16	0,149	0,16	0,15	0,185	0,167	0,167	0,1865
Facebook	0,308	0,312	0,247	0,218	0,24	0,269	0,188	0,282	0,263	0,211	0,2538
Wikipedia	0,248	0,183	0,201	0,84	0,212	0,224	0,211	0,195	0,196	0,207	0,2085556
Amazon	0,384	0,369	0,328	0,373	0,437	0,368	0,377	0,438	0,508	0,358	0,394
Twitter	0,336	0,287	0,267	0,265	0,282	0,281	0,345	0,271	0,299	0,276	0,2909
Linkedin	0,336	0,198	0,202	0,219	0,206	0,2	0,2	0,218	0,224	0,224	0,2227
Instagram	0,316	0,28	0,161	0,151	0,195	0,153	0,167	0,141	0,342	0,162	0,2068
Yahoo	0,181	0,147	0,151	0,262	0,193	0,147	0,205	0,15	0,166	0,169	0,1771
Average	0,2888889	0,246875	0,221875	0,227125	0,23125	0,222375	0,2225	0,233125	0,2705	0,21775	0,23822639

Table VII-5 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access

Requesting Delay / Popular webs											
DNS Server / No TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,123	0,094	0,088	0,088	0,08	0,065	0,073	0,077	0,07	0,078	0,0836
Youtube	0,168	0,06	0,058	0,08	0,091	0,07	0,066	0,064	0,071	0,088	0,0816
Facebook	0,161	0,07	0,059	0,055	0,073	0,062	0,063	0,069	0,057	0,072	0,0741
Wikipedia	0,135	0,086	0,077	0,07	0,059	0,074	0,064	0,061	0,078	0,065	0,0769
Amazon	0,123	0,092	0,068	0,064	0,071	0,073	0,062	0,057	0,069	0,069	0,0748
Twitter	0,106	0,059	0,061	0,08	0,059	0,061	0,071	0,077	0,067	0,099	0,074
Linkedin	0,141	0,082	0,092	0,06	0,06	0,057	0,063	0,088	0,089	0,073	0,0805
Instagram	0,136	0,084	0,06	0,069	0,084	0,059	0,066	0,064	0,071	0,073	0,0766
Yahoo	0,107	0,083	0,059	0,06	0,078	0,06	0,063	0,081	0,077	0,065	0,0733
Average	0,1333333	0,078889	0,0691111	0,0695556	0,0727778	0,0645556	0,0656667	0,0708889	0,0721111	0,0757778	0,07726667

Table VII-6 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access

Downloading Delay / Webs by Country											
DNS Server / No TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	1,881	1,686	1,358	1,373	1,638	1,328	1,666	1,334	1,395	1,471	1,513
South Africa Government	1,116	1,751	1,185	1,132	1,182	1,39	1,707	1,151	1,198	1,19	1,3002
Russia foreign ministry	0,385	0,306	0,325	0,33	0,324	0,332	0,326	0,313	0,325	0,319	0,3285
Argentinian afa	1,04	0,798	0,892	0,994	0,911	0,925	0,841	1	0,891	0,963	0,9255
Rugby India	2,438	1,115	1,44	1,071	1,395	1,059	1,052	1,085	1,074	0,893	1,2622
Average	1,372	1,1312	1,04	0,98	1,09	1,0068	1,1184	0,9766	0,9766	0,9672	1,06588

Table VII-7 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access

Requesting Delay / Webs by Country											
DNS Server / No TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	0,441	0,084	0,059	0,1	0,084	0,059	0,062	0,074	0,081	0,092	0,1136
South Africa Government	0,144	0,085	0,06	0,059	0,072	0,079	0,06	0,082	0,061	0,072	0,0774
Russia foreign ministry	0,137	0,077	0,078	0,06	0,08	0,06	0,061	0,077	0,063	0,057	0,075
Argentinian afa	0,125	0,084	0,082	0,083	0,06	0,083	0,075	0,069	0,059	0,071	0,0791
Rugby India	0,491	0,084	0,062	0,084	0,062	0,069	0,077	0,077	0,08	0,093	0,1179
Average	0,2676	0,0828	0,0682	0,0772	0,0716	0,07	0,067	0,0758	0,0688	0,077	0,0926

Table VII-8 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access

III. No DNS vs. DNS

<u>Downloading Delay / NO DNS vs DNS</u>			
Popular webs / No TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	0,2017	0,148	27%
Youtube	0,2412	0,1865	23%
Facebook	0,2945	0,2538	14%
Wikipedia	0,2633	0,2085556	21%
Amazon	0,5893	0,394	33%
Twitter	0,3402	0,2909	14%
Linkedin	0,301	0,2227	26%
Instagram	0,2332	0,2068	11%
Yahoo	0,2684	0,1771	34%
Average	0,3036444	0,2320395	23%

Table VII-9 Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN

<u>Requesting Delay / NO DNS vs DNS</u>			
Popular webs / No TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	0,1115	0,0836	25%
Youtube	0,1364	0,0816	40%
Facebook	0,1042	0,0741	29%
Wikipedia	0,1378	0,0769	44%
Amazon	0,0952	0,0748	21%
Twitter	0,0971	0,074	24%
Linkedin	0,1161	0,0805	31%
Instagram	0,116	0,0766	34%
Yahoo	0,0954	0,0733	23%
Average	0,1121889	0,0772667	30%

Table VII-10 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access

<u>Downloading Delay / NO DNS vs DNS</u>			
Webs by Country / No TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	1,9222	1,513	21%
South Africa Government	1,6272	1,3002	20%
Russia foreign ministry	0,401	0,3285	18%
Argentinian afa	1,1019	0,9255	16%
Rugby India	2,1948	1,2622	42%
Average	1,44942	1,06588	24%

Table VII-11 Downloading delay readings DNS / NO TOR / NO OVPN / Clear access

<u>Requesting Delay / NO DNS vs DNS</u>			
Webs by Country / No TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	0,3002	0,1136	62%
South Africa Government	0,1732	0,0774	55%
Russia foreign ministry	0,10679	0,075	30%
Argentinian afa	0,2028	0,0791	61%
Rugby India	0,439	0,1179	73%
Average	0,244398	0,0926	56%

Table VII-12 Requesting delay readings DNS / NO TOR / NO OVPN / Clear access

IV. Line Charts

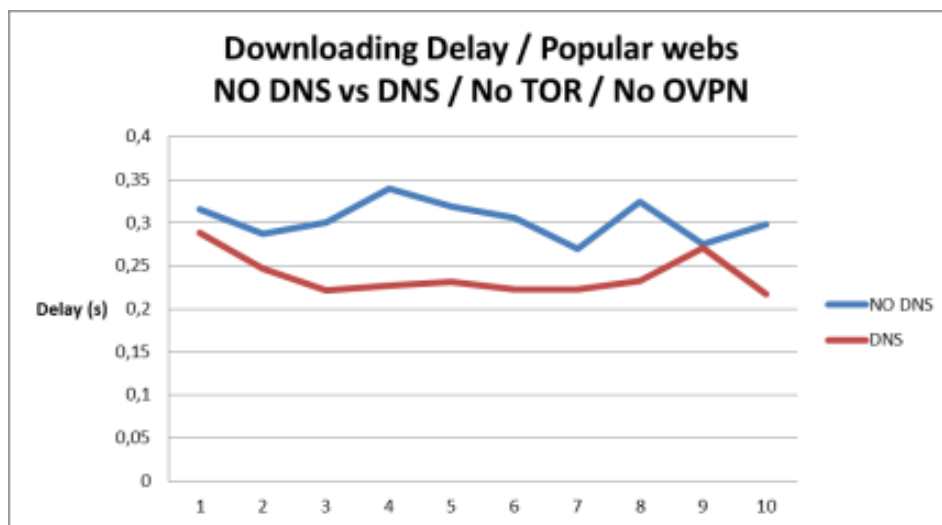


Chart VII-1 Line Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN

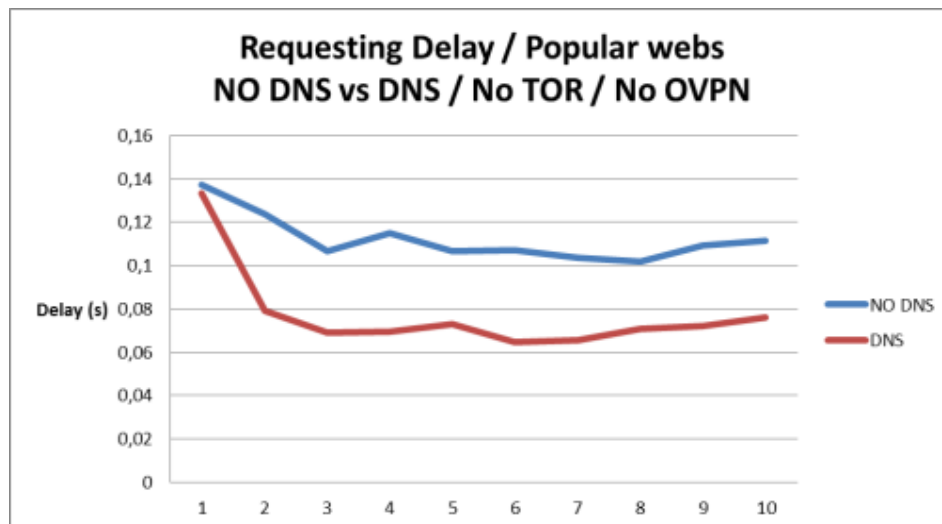


Chart VII-2 Line Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN

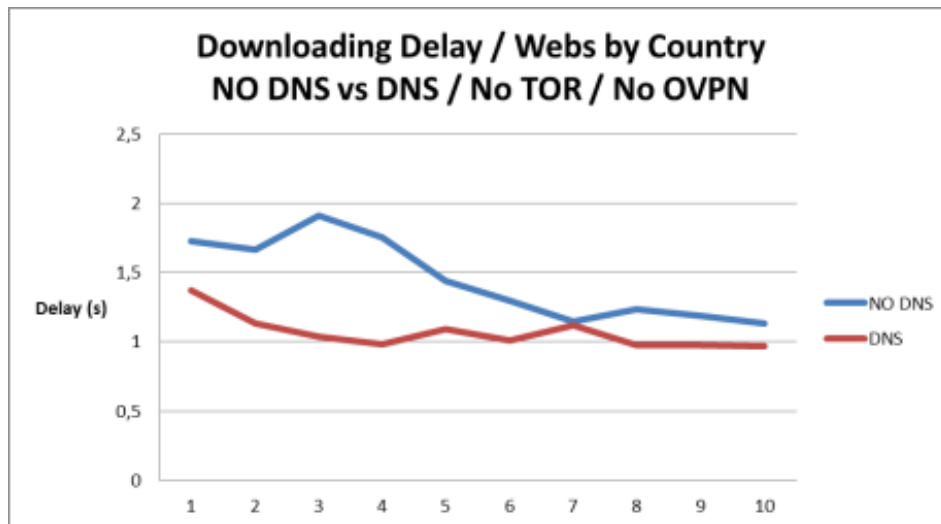


Chart VII-3 Line Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN

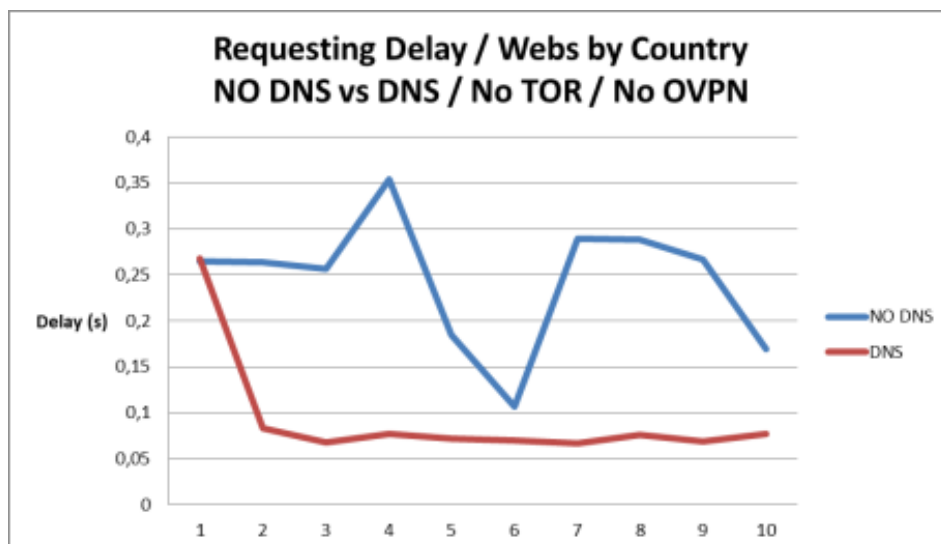


Chart VII-4 Line Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN

V. Bar Charts

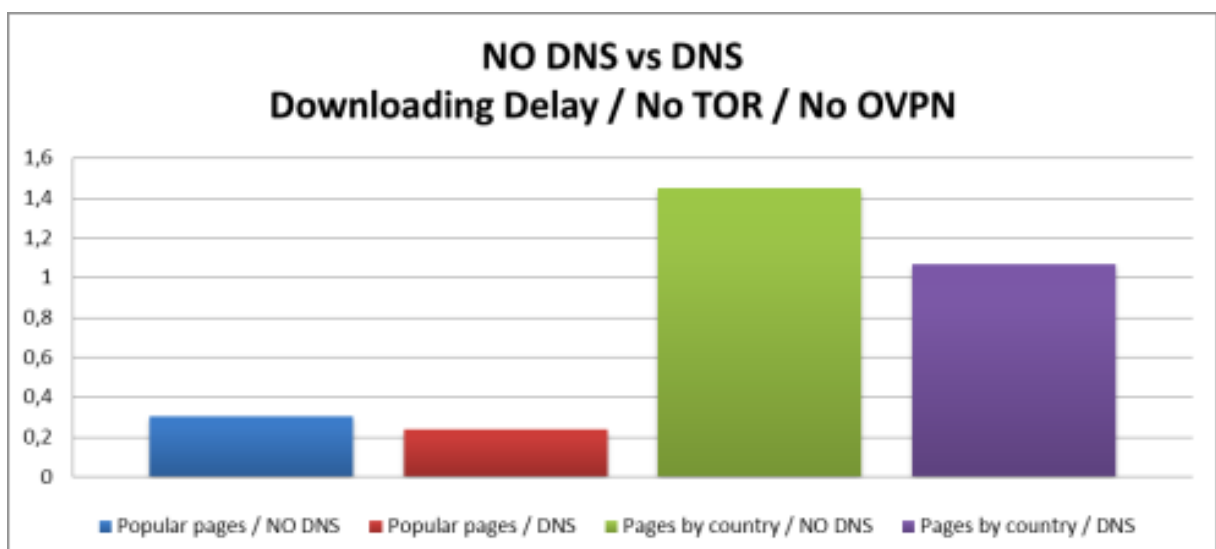


Chart VII-5 Bar Chart Downloading delay NO DNS vs. DNS / NO TOR / NO OVPN

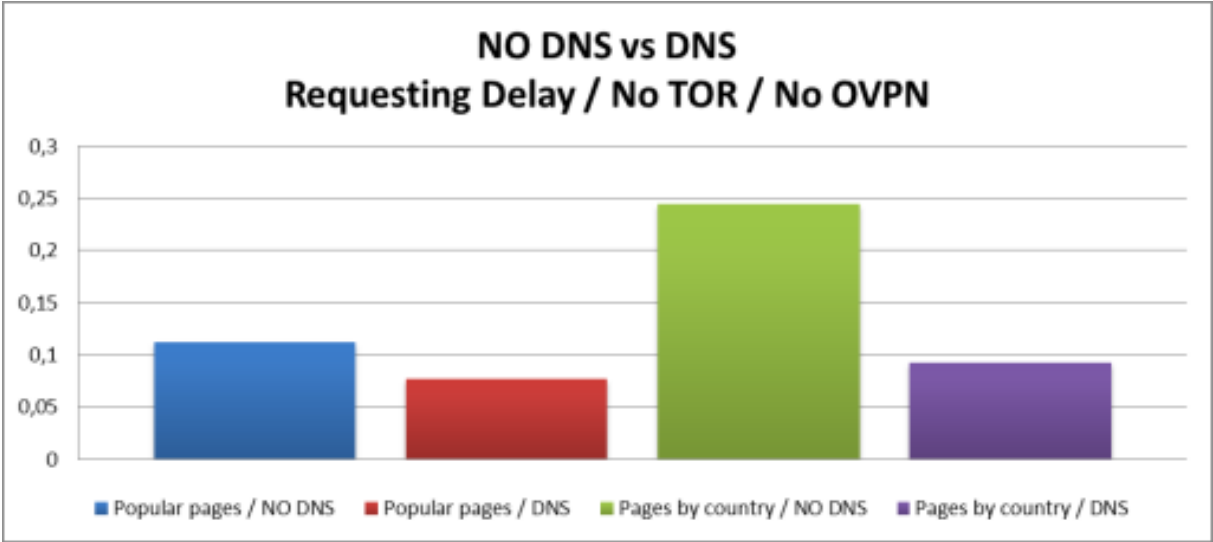


Chart VII-6 Bar Chart Requesting delay NO DNS vs. DNS / NO TOR / NO OVPN

VIII. ATTACHED DOCUMENT VIII: DOWNLOADING AND RESOLVING DELAY CHARTS TOR REDIRECTION

I. Readings without DNS Server

Downloading Delay / Popular webs											
No DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,64	0,624	0,608	1,487	0,986	0,966	1,053	1,026	0,911	0,787	0,9088
Youtube	1,831	0,884	0,872	1,885	1,884	0,864	0,852	0,876	0,862	0,857	1,1667
Facebook	1,161	1,199	0,831	1,17	0,974	1,179	0,938	0,912	0,927	0,95	1,0241
Wikipedia	1,04	0,746	1,113	0,759	1,09	0,999	1,998	1,007	2,01	2,08	1,2842
Amazon	0,824	0,833	0,761	0,75	0,748	1,095	0,842	0,828	0,808	0,831	0,832
Twitter	0,904	0,909	0,913	0,914	0,939	0,917	0,897	0,901	0,917	0,939	0,915
Linkedin	0,998	0,997	0,999	1,683	1,56	1,595	1,626	1,63	1,607	1,691	1,4386
Instagram	0,98	0,971	1,007	0,967	1,054	0,976	0,984	0,975	0,972	0,999	0,9885
Yahoo	0,957	1,175	0,959	0,973	0,965	1,514	0,974	0,961	0,97	0,95	1,0398
Average	1,0372222	0,9264444	0,8958889	1,1764444	1,1333333	1,1227778	1,1293333	1,0128889	1,10933333	1,12044444	1,06641111

Table VIII-1 Downloading delay readings NO DNS / NO OVPN / TOR Redirection

Requesting Delay / Popular webs											
No DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,18	0,257	0,25	0,256	0,254	0,245	0,238	0,26	0,263	0,239	0,2442
Youtube	0,267	0,247	0,245	0,279	0,27	0,241	0,27	0,278	0,279	0,28	0,2656
Facebook	0,65	0,274	0,238	0,252	0,294	0,266	0,278	0,275	0,271	0,27	0,3068
Wikipedia	0,334	0,255	0,246	0,273	0,26	0,243	0,625	0,258	0,244	0,251	0,2989
Amazon	0,253	0,264	0,269	0,256	0,256	0,245	0,261	0,254	0,648	0,264	0,297
Twitter	0,269	0,26	0,271	0,234	0,256	0,262	0,277	0,265	0,264	0,277	0,2635
Linkedin	0,255	0,259	0,262	0,239	0,264	0,259	0,257	0,255	0,255	0,255	0,256
Instagram	0,277	0,252	0,256	0,253	0,397	0,264	0,257	0,231	0,252	0,305	0,2744
Yahoo	0,25	0,253	0,259	0,236	0,254	0,246	0,249	0,246	0,246	0,272	0,2511
Average	0,3038889	0,2578889	0,2551111	0,2531111	0,2783333	0,2523333	0,3013333	0,258	0,30244444	0,26811111	0,273055556

Table VIII-2 Requesting delay readings NO DNS / NO OVPN / TOR Redirection

Downloading Delay / Webs by Country											
No DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	3,397	2,848	2,316	2,399	2,324	2,079	2,051	2,062	2,305	2,101	2,3882
South Africa Government	1,696	1,706	1,687	1,674	1,708	1,709	1,653	1,653	1,702	1,738	1,6926
Russia foreign ministry	10,995	0,864	0,887	0,886	0,906	0,888	0,958	0,851	0,868	0,878	0,887333333
Argentinian afa	1,404	1,811	1,409	1,396	1,6	1,374	1,415	1,367	1,371	1,422	1,4569
Rugby India	2,88	4,207	4,107	3,452	3,681	3,227	3,117	3,639	4,627	3,411	3,6348
Average	4,0744	2,2872	2,0812	1,9614	2,0438	1,8554	1,8388	1,9144	2,1746	1,91	2,21412

Table VIII-3 Downloading delay readings NO DNS / NO OVPN / TOR Redirection

Requesting Delay / Webs by Country											
No DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	1,151	0,253	0,358	0,265	0,252	0,251	0,25	0,277	0,257	0,25	0,3564
South Africa Government	0,41	0,27	0,248	0,226	0,238	0,249	0,248	0,226	0,238	0,249	0,2602
Russia foreign ministry	0,241	0,225	0,224	0,225	0,235	0,215	0,341	0,228	0,215	0,229	0,2378
Argentinian afa	0,646	0,242	0,251	0,234	0,246	0,248	0,239	0,245	0,243	0,234	0,2828
Rugby India	0,551	0,214	0,254	0,241	0,236	0,228	0,284	0,208	0,26	0,261	0,2737
Average	0,5998	0,2408	0,267	0,2382	0,2414	0,2382	0,2724	0,2368	0,2426	0,2446	0,28218

Table VIII-4 Requesting delay readings NO DNS / NO OVPN / TOR Redirection

II. Readings with DNS Server

Downloading Delay / Popular webs											
DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,966	0,411	0,307	0,326	0,34	0,427	0,397	0,328	0,388	0,363	0,4253
Youtube	0,553	0,361	0,358	0,322	0,325	0,33	0,385	0,354	0,366	0,433	0,3787
Facebook	0,684	0,363	0,325	0,364	0,391	0,379	0,402	0,365	0,369	0,322	0,3964
Wikipedia	0,632	0,491	0,415	0,474	0,396	0,415	0,405	0,604	1,388	0,466	0,5686
Amazon	0,718	0,722	0,493	0,56	0,742	0,648	0,78	0,606	0,611	0,715	0,6595
Twitter	0,735	0,733	0,503	0,677	0,541	0,827	0,567	0,523	0,495	0,592	0,6193
Linkedin	0,621	0,452	0,426	0,49	0,473	0,443	0,54	0,404	0,422	0,527	0,4798
Instagram	0,66	1,377	0,436	0,458	0,442	0,428	0,43	0,46	0,639	0,409	0,5739
Yahoo	0,462	0,456	0,441	0,47	0,457	0,463	0,449	0,494	0,405	0,443	0,454
Average	0,6701111	0,61375	0,407875	0,458875	0,45625	0,487125	0,48825	0,4555	0,58475	0,478375	0,510086111

Table VIII-5 Downloading delay readings DNS / NO OVPN / TOR Redirection

Requesting Delay / Popular webs											
DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
Google	0,172	0,08	0,08	0,079	0,06	0,081	0,07	0,08	0,066	0,077	0,0845
Youtube	0,174	0,056	0,056	0,056	0,056	0,08	0,079	0,074	0,08	0,056	0,0767
Facebook	0,189	0,083	0,056	0,056	0,079	0,08	0,056	0,056	0,058	0,08	0,0793
Wikipedia	0,225	0,055	0,079	0,055	0,055	0,055	0,055	0,079	0,073	0,056	0,0787
Amazon	0,162	0,082	0,08	0,056	0,056	0,079	0,079	0,076	0,056	0,07	0,0796
Twitter	0,166	0,055	0,076	0,055	0,056	0,055	0,079	0,055	0,056	0,067	0,072
Linkedin	0,162	0,079	0,056	0,056	0,079	0,076	0,057	0,056	0,08	0,055	0,0756
Instagram	0,15	0,055	0,055	0,056	0,08	0,078	0,055	0,077	0,059	0,055	0,072
Yahoo	0,16	0,079	0,056	0,056	0,073	0,055	0,056	0,063	0,072	0,055	0,0725
Average	0,1733333	0,0693333	0,066	0,0583333	0,066	0,071	0,0651111	0,0684444	0,06666667	0,06344444	0,076766667

Table VIII-6 Requesting delay readings DNS / NO OVPN / TOR Redirection

Downloading Delay / Webs by Country											
DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	1,863	1,554	1,794	1,536	1,49	2,506	1,672	1,741	1,658	1,545	1,7359
South Africa Government	2,628	1,086	1,31	1,186	1,143	1,109	1,36	1,189	1,14	1,694	1,3845
Russia foreign ministry	0,569	0,439	0,396	0,399	0,443	0,522	0,695	0,569	0,468	0,439	0,4939
Argentinian afa	0,891	0,74	0,721	0,789	0,763	0,765	0,883	0,779	0,734	0,72	0,7785
Rugby India	1,312	2,099	1,365	1,28	1,279	1,897	1,923	2,06	2,087	1,71	1,7012
Average	1,4526	1,1836	1,1172	1,038	1,0236	1,3598	1,3066	1,2676	1,2174	1,2216	1,2188

Table VIII-7 Downloading delay readings DNS / NO OVPN / TOR Redirection

Requesting Delay / Webs by Country											
DNS Server / TOR / No OVPN											
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average
New Zealand Navy	0,788	0,08	0,08	0,08	0,079	0,071	0,08	0,056	0,056	0,056	0,1426
South Africa Government	0,337	0,079	0,079	0,066	0,055	0,055	0,069	0,056	0,079	0,056	0,0931
Russia foreign ministry	0,465	0,078	0,08	0,056	0,056	0,055	0,077	0,057	0,056	0,056	0,1036
Argentinian afa	0,368	0,0860,079	0,067	0,059	0,077	0,055	0,055	0,079	0,055	0,079	0,099333333
Rugby India	0,549	0,079	0,076	0,056	0,056	0,081	0,076	0,055	0,055	0,057	0,114
Average	0,5014	0,079	0,0764	0,0634	0,0646	0,0634	0,0714	0,0606	0,0602	0,0608	0,11012

Table VIII-8 Requesting delay readings DNS / NO OVPN / TOR Redirection

III. No DNS vs. DNS

<u>Downloading Delay / NO DNS vs DNS</u>			
Popular webs / TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	0,9088	0,4253	53%
Youtube	1,1667	0,3787	68%
Facebook	1,0241	0,3964	61%
Wikipedia	1,2842	0,5686	56%
Amazon	0,832	0,6595	21%
Twitter	0,915	0,6193	32%
Linkedin	1,4386	0,4798	67%
Instagram	0,9885	0,5739	42%
Yahoo	1,0398	0,454	56%
Average	1,0664111	0,5061667	51%

Table VIII-9 Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

<u>Requesting Delay / NO DNS vs DNS</u>			
Popular webs / TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	0,2442	0,0845	65%
Youtube	0,2656	0,0767	71%
Facebook	0,3068	0,0793	74%
Wikipedia	0,2989	0,0787	74%
Amazon	0,297	0,0796	73%
Twitter	0,2635	0,072	73%
Linkedin	0,256	0,0756	70%
Instagram	0,2744	0,072	74%
Yahoo	0,2511	0,0725	71%
Average	0,2730556	0,0767667	72%

Table VIII-10 Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

<u>Downloading Delay / NO DNS vs DNS</u>			
Webs by Country / TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	2,3882	1,7359	27%
South Africa Government	1,6926	1,3845	18%
Russia foreign ministry	0,8873333	0,4939	44%
Argentinian afa	1,4569	0,7785	47%
Rugby India	3,6348	1,7012	53%
Average	2,0119667	1,2188	38%

Table VIII-11 Table IV 10 Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

<u>Requesting Delay / NO DNS vs DNS</u>			
Webs by Country / TOR / No OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	0,3564	0,1426	60%
South Africa Government	0,2602	0,0931	64%
Russia foreign ministry	0,2378	0,1036	56%
Argentinian afa	0,2828	0,0993333	65%
Rugby India	0,2737	0,114	58%
Average	0,28218	0,1105267	61%

Table VIII-12 Table IV 10 Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

IV. Line Charts

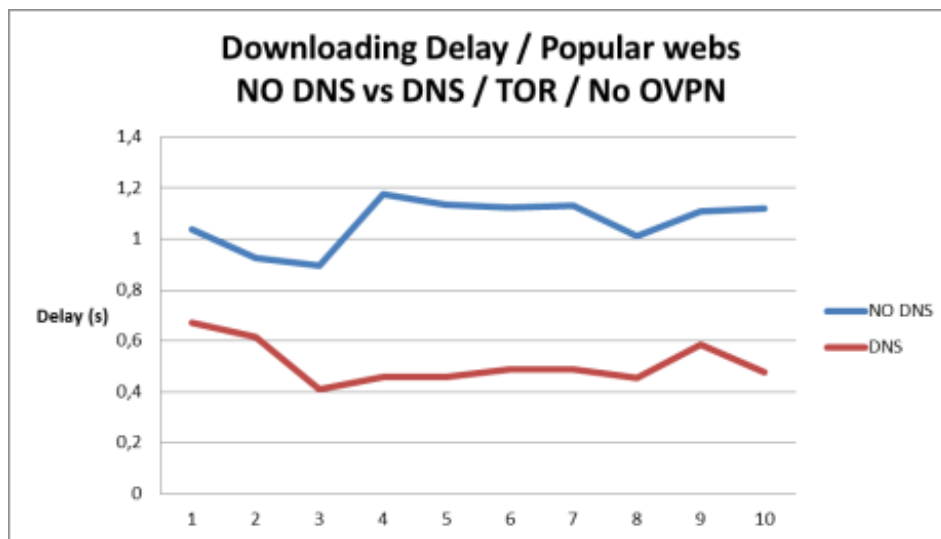


Chart VIII-1 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

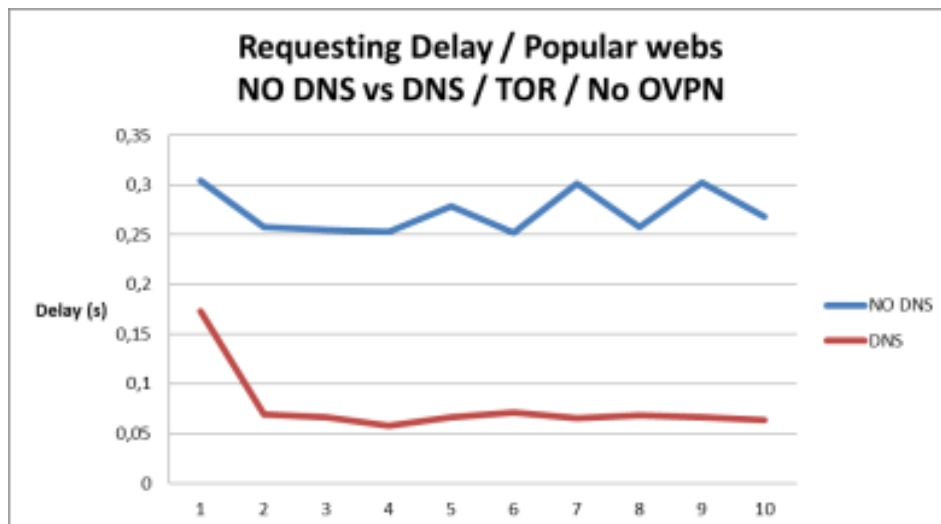


Chart VIII-2 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

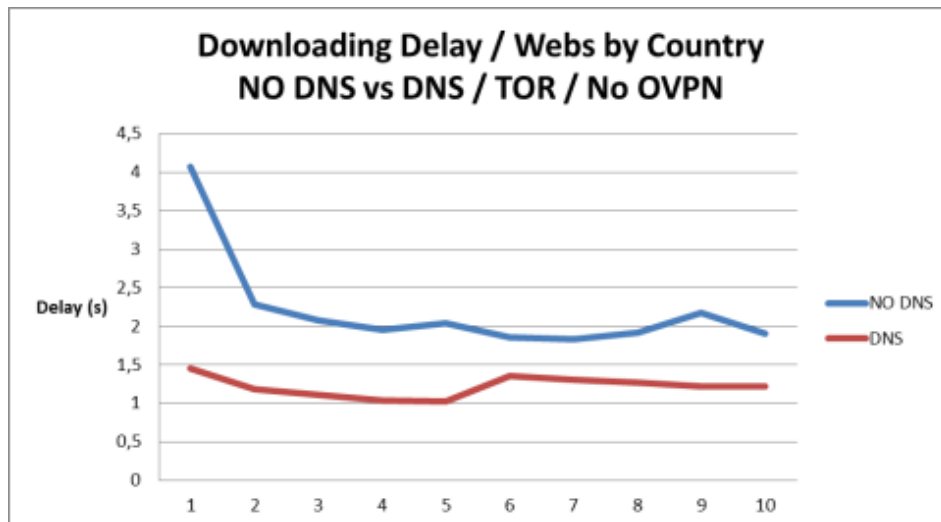


Chart VIII-3 Line Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

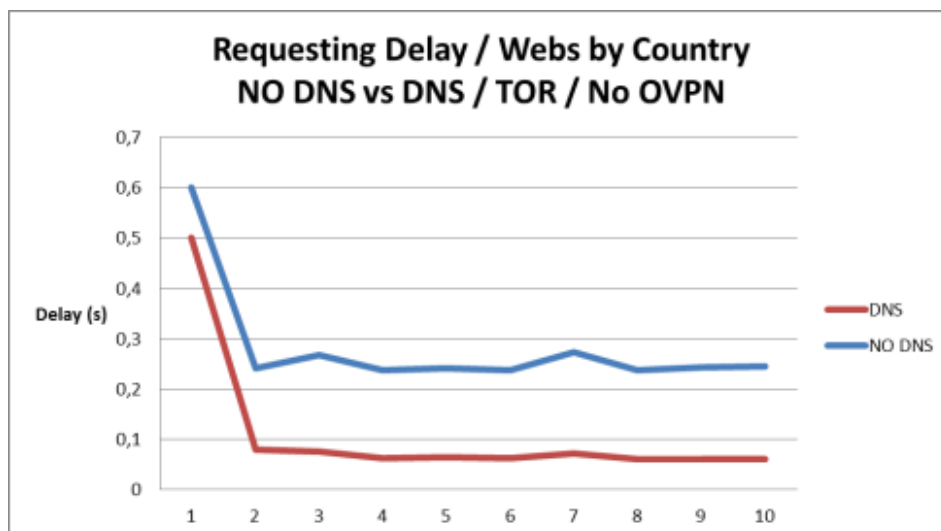


Chart VIII-4 Line Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

V. Bar Charts

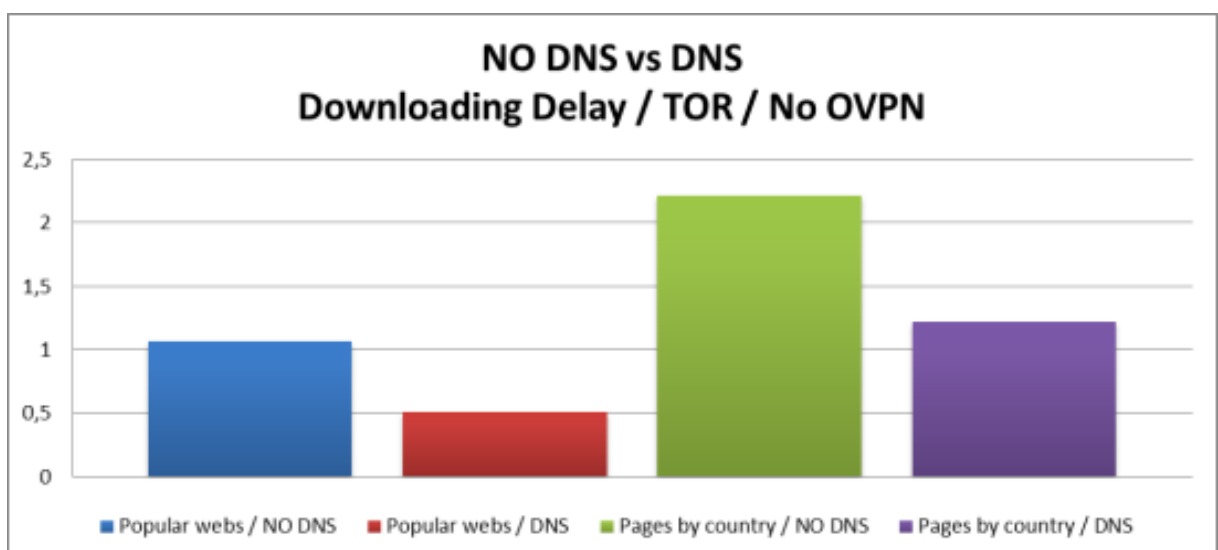


Chart VIII-5 Bar Chart Downloading delay NO DNS vs. DNS / NO OVPN / TOR Redirection

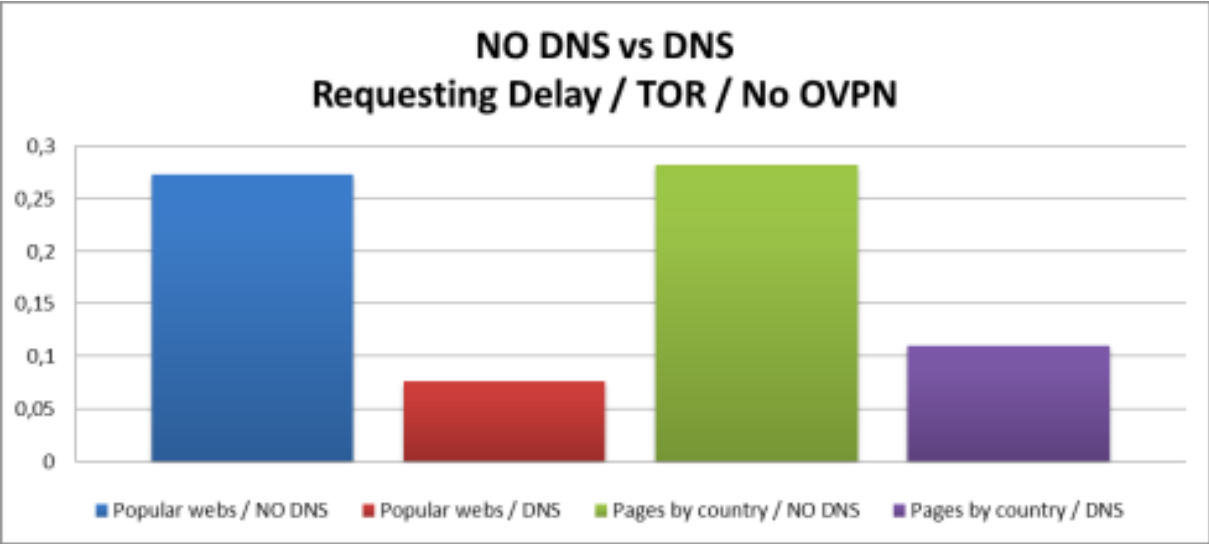


Chart VIII-6 Bar Chart Requesting delay NO DNS vs. DNS / NO OVPN / TOR Redirection

IX. ATTACHED DOCUMENT IX: DOWNLOADING AND RESOLVING DELAY CHARTS TOR AND OVPN

I. Readings without DNS Server

Downloading Delay / Popular webs												
No DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°		Average
Google	2,354	1,637	1,575	2,377	1,645	1,314	1,58	1,365	1,702	2,673		1,8222
Youtube	2,225	2,244	2,595	2,523	2,465	2,595	2,545	2,194	3,549	2,655		2,559
Facebook	3,217	2,335	2,665	2,395	2,399	2,426	2,462	2,416	2,465	2,289		2,5069
Wikipedia	3,112	2,249	2,137	2,152	3,76	2,47	2,209	3,218	2,141	2,227		2,5675
Amazon	2,242	3,706	2,456	4,315	2,615	2,124	2,083	2,267	2,167	2,202		2,6177
Twitter	1,982	3,61	2,348	2,115	2,265	2,098	2,135	2,434	4,092	3,238		2,6317
LinkedIn	2,32	2,764	2,604	2,354	2,282	2,22	2,65	2,407	2,265	2,238		2,4104
Instagram	2,206	2,421	2,478	2,362	2,41	2,989	2,969	2,222	2,554	2,294		2,4905
Yahoo	1,493	1,242	1,224	1,615	2,36	1,202	1,181	1,205	2,395	2,561		1,6478
Average	2,3501111	2,4675556	2,2313333	2,4675556	2,4667778	2,1597778	2,2015556	2,192	2,5922222	2,4863333		2,36152222

Table IX-1 Downloading delay readings NO DNS / TOR and OVPN

Requesting Delay / Popular webs												
No DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°		Average
Google	0,564	0,655	0,62	0,675	0,548	0,667	0,607	1,285	0,607	0,579		0,6807
Youtube	0,926	0,355	1,379	0,653	0,369	0,991	1,06	0,869	0,489	0,688		0,7779
Facebook	1,324	1,572	1,205	1,053	0,834	0,436	0,94	0,478	0,387	0,546		0,8775
Wikipedia	0,9	0,58	0,335	0,404	0,906	2,268	0,33	0,913	0,327	0,34		0,55944444
Amazon	1,773	1,517	1,595	0,462	1,35	0,61	1,088	1,064	1,491	1,926		1,2876
Twitter	1,278	0,626	0,355	0,788	1,189	0,613	1,113	0,922	1,008	0,902		0,8794
LinkedIn	1,291	0,75	0,942	2,621	0,894	0,36	1,156	1,895	0,615	1,397		1,1921
Instagram	1,433	0,925	1,488	1,059	0,524	1,125	1,302	0,541	0,851	0,36		0,9608
Yahoo	0,707	0,327	0,328	0,321	0,509	0,375	1,288	0,752	0,327	0,371		0,5305
Average	1,1328889	0,8118889	0,9163333	0,8928889	0,7914444	0,647125	0,9871111	0,9687778	0,678	0,7898889		0,86163472

Table IX-2 Requesting delay readings NO DNS / TOR and OVPN

Downloading Delay / Webs by Country												
No DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°		Average
New Zealand Navy	3,21	2,706	1,878	2,637	1,543	1,683	1,778	2,695	1,867	1,578		2,1575
South Africa Government	3,689	2,59	2,591	2,496	2,615	3,445	4,388	2,349	3,437	3,394		3,0994
Russia foreign ministry	2,872	1,622	3,095	2,574	3,014	4,405	3,232	2,64	2,685	2,333		2,8472
Argentinian afa	3,432	1,783	1,737	3,044	2,999	1,716	1,89	3,993	1,766	2,759		2,5119
Rugby India	6,495	5,38	5,015	4,579	4,586	5,409	3,919	5,076	3,017	4,531		4,8007
Average	3,9396	2,8162	2,8632	3,066	2,9514	3,3316	3,0414	3,3506	2,5544	2,919		3,08334

Table IX-3 Downloading delay readings NO DNS / TOR and OVPN

Requesting Delay / Webs by Country												
No DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°		Average
New Zealand Navy	0,632	0,344	0,776	0,324	0,334	0,31	0,319	1,003	0,349	0,388		0,4779
South Africa Government	2,251	2,05	1,124	2,119	1,29	0,855	2,152	1,75	0,564	0,59		1,4745
Russia foreign ministry	0,851	1,27	1,274	1,974	1,125	1,055	1,046	0,894	2,274	0,661		1,2424
Argentinian afa	2,769	1,253	0,865	1,403	0,837	0,995	1,625	0,315	0,879	0,434		1,1375
Rugby India	1,664	0,932	0,631	1,172	0,423	0,659	1,118	1,357	0,335	0,918		0,9209
Average	1,6334	1,1698	0,934	1,3984	0,8018	0,7748	1,252	1,0638	0,8802	0,5982		1,05064

Table IX-4 Requesting delay readings NO DNS / TOR and OVPN

II. Readings with DNS Server

Downloading Delay / Popular webs												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	2,291	2,206	1,21	1,457	2,471	2,183	2,253	2,472	2,49	2,615	2,1648	
Youtube	2,175	1,144	1,191	1,185	1,22	2,412	2,285	1,042	2,276	2,28	1,721	
Facebook	2,816	2,6	2,677	2,489	2,538	2,481	2,535	2,562	1,322	2,198	2,4218	
Wikipedia	3,085	1,384	1,048	0,974	0,988	1,169	1,01	2,283	1,114	1,008	1,4063	
Amazon	1,382	1,395	2,651	1,23	1,293	2,547	3,256	1,22	1,046	1,085	1,7105	
Twitter	2,933	3,907	3,119	3,114	2,067	2,363	1,058	2,527	1,118	2,26	2,4466	
Linkedin	2,376	2,189	2,614	3,866	2,143	2,748	1,506	2,029	2,178	0,963	2,2612	
Instagram	2,096	2,042	2,052	2,192	1,459	1,888	0,931	1,321	2,229	2,107	1,8317	
Yahoo	1,3	4,292	1,233	1,228	2,268	1,169	0,992	1,006	1,271	1,517	1,6276	
Average	2,2726667	2,108375	2,07025	2,063375	1,772375	2,223875	1,85425	1,932	1,721625	1,8145	1,98332917	

Table IX-5 Downloading delay readings DNS / TOR and OVPN

Requesting Delay / Popular webs												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	0,991	0,06	0,083	0,087	0,085	0,088	0,082	0,065	0,072	0,085	0,1698	
Youtube	0,51	0,06	0,082	0,082	0,059	0,06	0,077	0,075	0,072	0,059	0,1136	
Facebook	0,551	0,086	0,084	0,083	0,059	0,075	0,089	0,06	0,082	0,082	0,1251	
Wikipedia	1,094	0,072	0,06	0,084	0,06	0,084	0,059	0,076	0,063	0,074	0,1726	
Amazon	0,459	0,084	0,059	0,083	0,075	0,06	0,073	0,067	0,099	0,059	0,1118	
Twitter	0,452	0,089	0,078	0,064	0,094	0,06	0,061	0,076	0,06	0,06	0,1094	
Linkedin	0,671	0,081	0,061	0,083	0,07	0,073	0,089	0,061	0,074	0,066	0,1329	
Instagram	0,747	0,085	0,094	0,092	0,069	0,083	0,07	0,069	0,06	0,086	0,1455	
Yahoo	0,598	0,086	0,081	0,069	0,074	0,082	0,075	0,06	0,06	0,071	0,1256	
Average	0,6747778	0,0781111	0,0757778	0,0807778	0,0716667	0,0738889	0,075	0,0676667	0,07133333	0,07133333	0,13403333	

Table IX-6 Requesting delay readings DNS / TOR and OVPN

Downloading Delay / Webs by Country												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
New Zealand Navy	3,805	4,671	2,375	3,533	3,6	3,736	2,489	3,972	3,728	2,82	3,4729	
South Africa Government	3,048	3,633	2,939	2,14	2,242	2,234	3,209	3,356	2,221	2,239	2,7261	
Russia foreign ministry	2,122	2,124	3,305	3,003	2,137	2,912	2,386	3,137	3,383	2,214	2,6723	
Argentinian afa	2,757	3,014	2,389	2,164	2,642	4,623	2,047	2,132	2,42	3,151	2,7339	
Rugby India	3,408	5,851	3,852	13,558	4,678	3,987	3,769	3,321	4,651	3,182	4,07766667	
Average	2,83375	3,6555	3,12125	2,4356667	2,92475	3,439	2,85275	2,9865	3,16875	2,6965	3,05249167	

Table IX-7 Downloading delay readings DNS / TOR and OVPN

Requesting Delay / Webs by Country												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
New Zealand Navy	0,598	0,086	0,081	0,069	0,074	0,082	0,075	0,06	0,06	0,071	0,1256	
South Africa Government	0,563	0,083	0,083	0,067	0,077	0,072	0,066	0,081	0,08	0,071	0,1243	
Russia foreign ministry	0,781	0,094	0,06	0,06	0,063	0,062	0,06	0,072	0,06	0,061	0,1373	
Argentinian afa	0,798	0,078	0,082	0,06	0,07	0,072	0,069	0,073	0,087	0,083	0,1472	
Rugby India	1,183	0,096	0,066	0,072	0,084	0,06	0,088	0,073	0,068	0,084	0,1874	
Average	0,7846	0,0874	0,0744	0,0656	0,0736	0,0696	0,0716	0,0718	0,071	0,074	0,14436	

Table IX-8 Requesting delay readings DNS / TOR and OVPN

III. No DNS vs. DNS

<u>Downloading Delay / NO DNS vs DNS</u>			
Popular webs / TOR / OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	1,8222	2,1648	-19%
Youtube	2,559	1,721	33%
Facebook	2,5069	2,4218	3%
Wikipedia	2,5675	1,4063	45%
Amazon	2,6177	1,7105	35%
Twitter	2,6317	2,4466	7%
Linkedin	2,4104	2,2612	6%
Instagram	2,4905	1,8317	26%
Yahoo	1,6478	1,6276	1%
Average	2,36152222	1,95461111	15%

Table IX-9 Downloading delay NO DNS vs. DNS / TOR and OVPN

<u>Requesting Delay / NO DNS vs DNS</u>			
Popular webs / TOR / OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
Google	0,6807	0,1698	75%
Youtube	0,7779	0,1136	85%
Facebook	0,8775	0,1251	86%
Wikipedia	0,55944444	0,1726	69%
Amazon	1,2876	0,1118	91%
Twitter	0,8794	0,1094	88%
Linkedin	1,1921	0,1329	89%
Instagram	0,9608	0,1455	85%
Yahoo	0,5305	0,1256	76%
Average	0,86066049	0,13403333	83%

Table IX-10 Requesting delay NO DNS vs. DNS / TOR and OVPN

<u>Downloading Delay / NO DNS vs DNS</u>			
Webs by Country / TOR / OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	2,1575	3,4729	-61%
South Africa Government	3,0994	2,7261	12%
Russia foreign ministry	2,8472	2,6723	6%
Argentinian afa	2,5119	2,7339	-9%
Rugby India	4,8007	4,07766667	15%
Average	3,08334	3,13657333	6%

Table IX-11 Downloading delay NO DNS vs. DNS / TOR and OVPN

Requesting Delay / NO DNS vs DNS			
Webs by Country / TOR / OVPN			
Web / Relation	NO DNS	DNS	Delay Decrease (%)
New Zealand Navy	0,4779	0,1256	74%
South Africa Government	1,4745	0,1243	92%
Russia foreign ministry	1,2424	0,1373	89%
Argentinian afa	1,1375	0,1472	87%
Rugby India	0,9209	0,1874	80%
Average	1,05064	0,14436	84%

Table IX-12 Requesting delay NO DNS vs. DNS / TOR and OVPN

IV. Line Charts

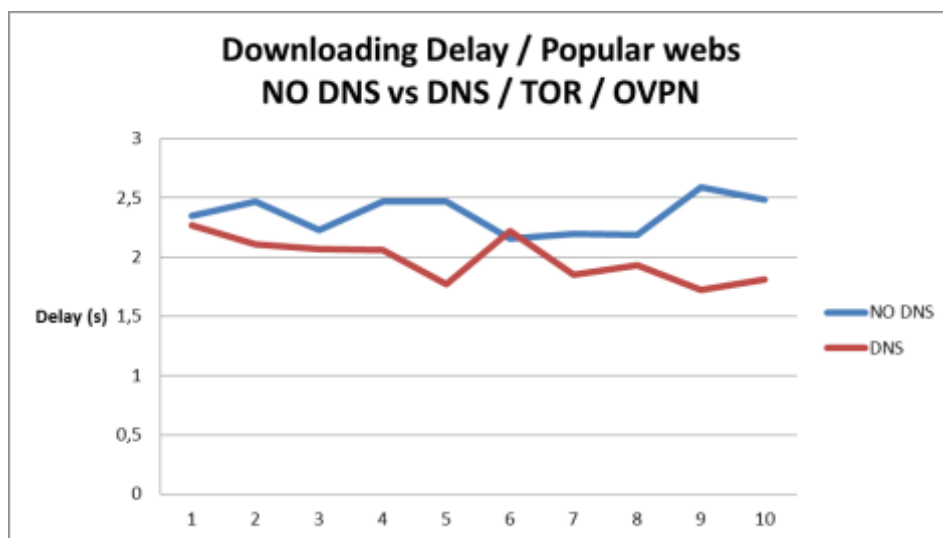


Chart IX-1 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN

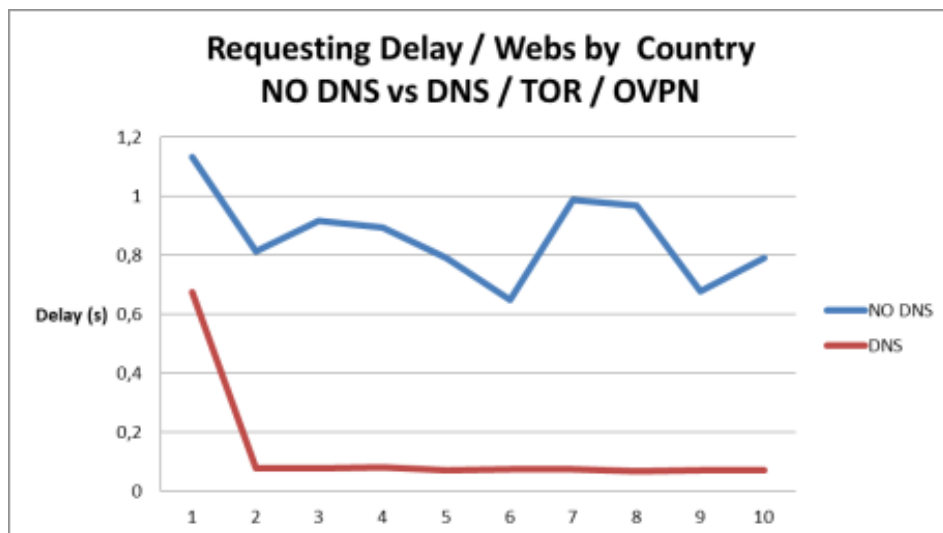


Chart IX-2 Line Chart Requesting delay NO DNS vs. DNS / TOR and OVPN

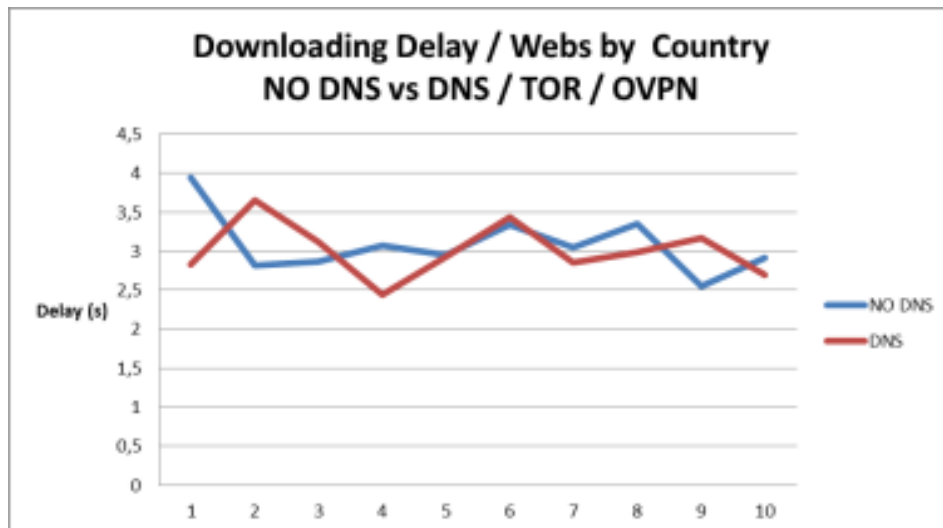


Chart IX-3 Line Chart Downloading delay NO DNS vs. DNS / TOR and OVPN

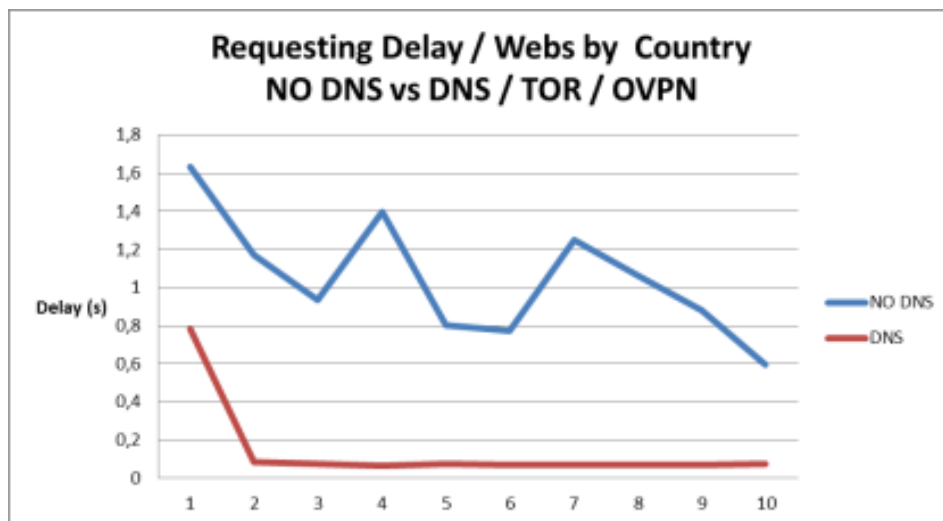


Chart IX-4 Line Chart Requesting delay NO DNS vs. DNS / TOR and OVPN

V. Bar Charts

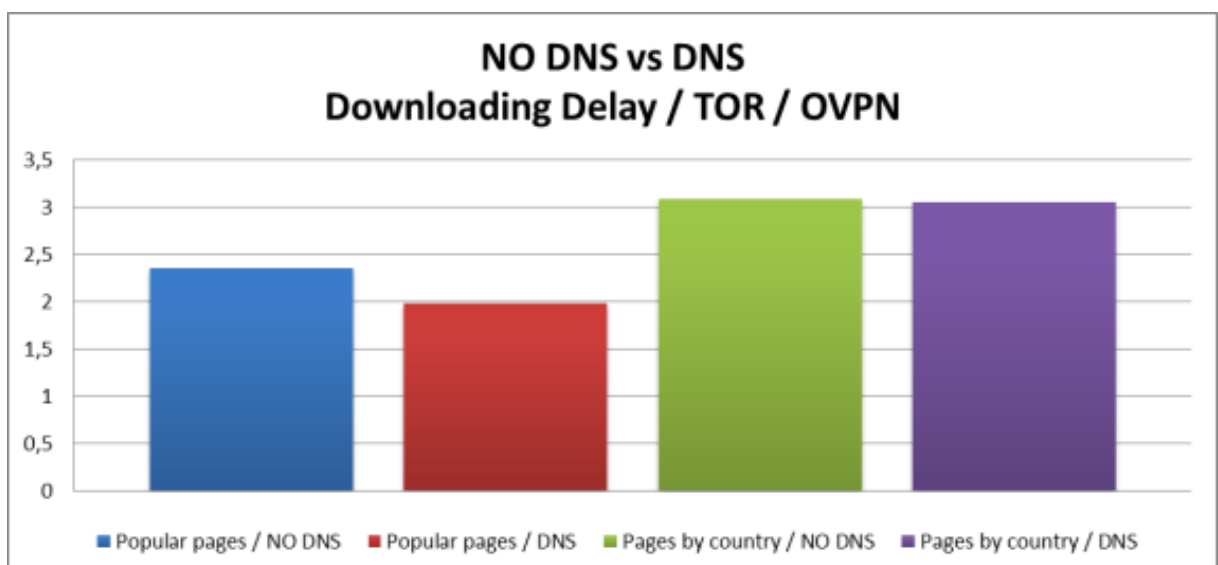


Chart IX-5 Bar Chart Downloading delay NO DNS vs. DNS / TOR and OVPN

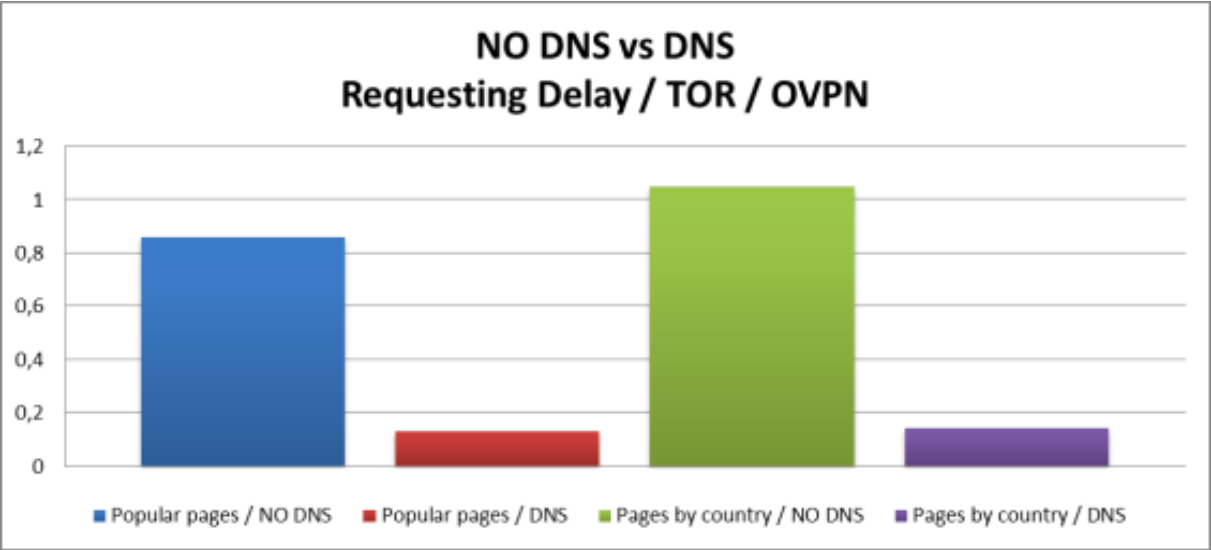


Chart IX-6 Bar Chart Requesting delay NO DNS vs. DNS / TOR and OVPN

X. ATTACHED DOCUMENT X: DOWNLOADING AND RESOLVING DELAY RASPBERRY PI 2

I. DNS, TOR and OVPN activated

<u>Downloading Delay / Popular webs / Rpi 2</u>												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	3,663	2,847	1,564	2,111	1,525	3,593	1,899	2,467	2,687	2,533	2,4889	
Youtube	3,164	3,841	3,116	2,791	1,873	1,496	1,849	1,941	1,678	1,518	2,3267	
Facebook	3,101	2,194	2,321	2,222	2,457	2,645	2,194	2,217	2,761	2,416	2,4528	
Wikipedia	2,941	2,648	2,677	2,511	1,649	1,515	1,481	1,649	1,115	1,547	1,9733	
Amazon	2,11	1,384	1,563	1,464	1,773	1,912	1,495	1,152	1,188	1,067	1,5108	
Twitter	2,844	3,262	2,359	2,846	2,125	2,017	1,635	1,497	1,549	1,649	2,1783	
LinkedIn	3,589	1,081	1,645	1,791	2,156	2,582	1,968	2,167	2,537	4,31	2,3826	
Instagram	3,104	2,697	1,964	2,491	1,645	1,647	1,451	1,994	1,682	1,771	2,0446	
Yahoo	3,629	2,948	2,336	2,154	2,599	2,132	2,169	2,225	2,268	2,57	2,503	
Average	3,12722	2,49425	2,15113	2,27838	1,90038	2,17588	1,7465	1,8855	1,89963	2,10138	2,176022	

Table X-1 Downloading delay readings NO DNS / TOR and OVPN / Raspberry Pi 2

<u>Requesting Delay / Popular webs / RPi 2</u>												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
Google	1,011	0,069	0,061	0,082	0,079	0,08	0,066	0,089	0,092	0,081	0,171	
Youtube	0,666	0,082	0,078	0,078	0,078	0,064	0,071	0,075	0,07	0,069	0,1331	
Facebook	0,491	0,088	0,099	0,089	0,081	0,077	0,068	0,068	0,061	0,064	0,1186	
Wikipedia	0,992	0,088	0,077	0,075	0,074	0,072	0,077	0,075	0,078	0,077	0,1685	
Amazon	0,516	0,076	0,083	0,091	0,084	0,081	0,079	0,066	0,061	0,064	0,1201	
Twitter	0,466	0,066	0,069	0,068	0,067	0,089	0,084	0,091	0,098	0,09	0,1188	
LinkedIn	0,582	0,094	0,086	0,089	0,081	0,078	0,071	0,072	0,071	0,07	0,1294	
Instagram	0,861	0,071	0,075	0,076	0,074	0,061	0,069	0,084	0,078	0,073	0,1522	
Yahoo	0,511	0,091	0,084	0,086	0,081	0,081	0,081	0,084	0,068	0,071	0,1238	
Average	0,67733	0,08056	0,07911	0,08156	0,07767	0,07589	0,074	0,07822	0,07522	0,07322	0,137278	

Table X-2 Requesting delay readings NO DNS / TOR and OVPN Raspberry Pi 2

<u>Downloading Delay / Webs by Country / RPi 2</u>												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
New Zealand Navy	3,451	3,472	4,167	3,67	2,891	2,846	3,3	3,445	3,511	3,699	3,4452	
South Africa Government	3,861	3,498	3,614	3,322	2,647	2,95	2,471	2,678	2,734	3,042	3,0817	
Russia foreign ministry	3,422	2,781	3,163	2,48	2,587	2,797	2,629	2,781	2,751	2,151	2,7542	
Argentinian afa	3,119	2,696	2,617	2,229	2,138	2,986	2,63	3,002	2,975	2,946	2,7338	
Rugby India	4,827	3,542	3,173	3,847	3,737	3,946	4,258	3,498	4,09	3,816	3,876333	
Average	3,736	3,1978	3,3468	3,1096	2,8	3,105	3,0576	3,0808	3,2122	3,1308	3,111508	

Table X-3 Downloading delay readings NO DNS / TOR and OVPN / Raspberry Pi 2

<u>Requesting Delay / Webs by Country / RPi 2</u>												
DNS Server / TOR / OVPN												
Web / Delay	1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	Average	
New Zealand Navy	1,022	0,091	0,071	0,077	0,078	0,08	0,099	0,076	0,073	0,089	0,1756	
South Africa Government	0,716	0,073	0,072	0,078	0,079	0,079	0,086	0,08	0,076	0,073	0,1412	
Russia foreign ministry	0,834	0,08	0,08	0,076	0,079	0,073	0,075	0,069	0,077	0,079	0,1522	
Argentinian afa	0,943	0,076	0,073	0,071	0,071	0,077	0,071	0,073	0,075	0,074	0,1604	
Rugby India	0,853	0,081	0,073	0,083	0,071	0,08	0,079	0,073	0,074	0,078	0,1545	
Average	0,8736	0,0802	0,0738	0,077	0,0756	0,0778	0,082	0,0742	0,075	0,0786	0,15678	

Table X-4 Requesting delay readings NO DNS / TOR and OVPN / Raspberry Pi 2

XI. ATTACHED DOCUMENT XI: DOWNLOADING AND RESOLVING DELAY COMPARISON

I. Clear Access vs. TOR Tables

Downloading Delay / NO TOR vs TOR			
Popular webs / DNS Server / No OVPN			
Web / Relation	NO TOR	TOR	Delay Increase (T/NT)
Google	0,148	0,4253	2,87
Youtube	0,1865	0,3787	2,03
Facebook	0,2538	0,3964	1,56
Wikipedia	0,20855556	0,5686	2,73
Amazon	0,394	0,6595	1,67
Twitter	0,2909	0,6193	2,13
Linkedin	0,2227	0,4798	2,15
Instagram	0,2068	0,5739	2,78
Yahoo	0,1771	0,454	2,56
Average	0,23203951	0,506166667	2,18

Table XI-1 Downloading delay Clear access vs. TOR / DNS

Requesting Delay / NO TOR vs TOR			
Popular webs / DNS Server / No OVPN			
Web / Relation	NO TOR	TOR	Delay Increase (T/NT)
Google	0,0836	0,0845	1,01
Youtube	0,0816	0,0767	0,94
Facebook	0,0741	0,0793	1,07
Wikipedia	0,0769	0,0787	1,02
Amazon	0,0748	0,0796	1,06
Twitter	0,074	0,072	0,97
Linkedin	0,0805	0,0756	0,94
Instagram	0,0766	0,072	0,94
Yahoo	0,0733	0,0725	0,99
Average	0,07726667	0,076766667	0,99

Table XI-2 Requesting delay Clear access vs. TOR / DNS

Downloading Delay / NO DNS vs DNS			
Webs by Country / DNS Server / No OVPN			
Web / Relation	NO TOR	TOR	Delay Increase (T/NT)
New Zealand Navy	1,513	1,7359	1,15
South Africa Government	1,3002	1,3845	1,06
Russia foreign ministry	0,3285	0,4939	1,50
Argentinian afa	0,9255	0,7785	0,84
Rugby India	1,2622	1,7012	1,35
Average	1,06588	1,2188	1,18

Table XI-3 Downloading delay Clear access vs. TOR / DNS

Requesting Delay / NO TOR vs TOR			
Webs by Country / DNS Server / No OVPN			
Web / Relation	NO TOR	TOR	Delay Increase (T/NT)
New Zealand Navy	0,1136	0,1426	1,26
South Africa Government	0,0774	0,0931	1,20
Russia foreign ministry	0,075	0,1036	1,38
Argentinian afa	0,0791	0,099333333	1,26
Rugby India	0,1179	0,114	0,97
Average	0,0926	0,110526667	1,21

Table XI-4 Requesting delay Clear access vs. TOR / DNS

II. Clear Access vs. TOR Bar Charts

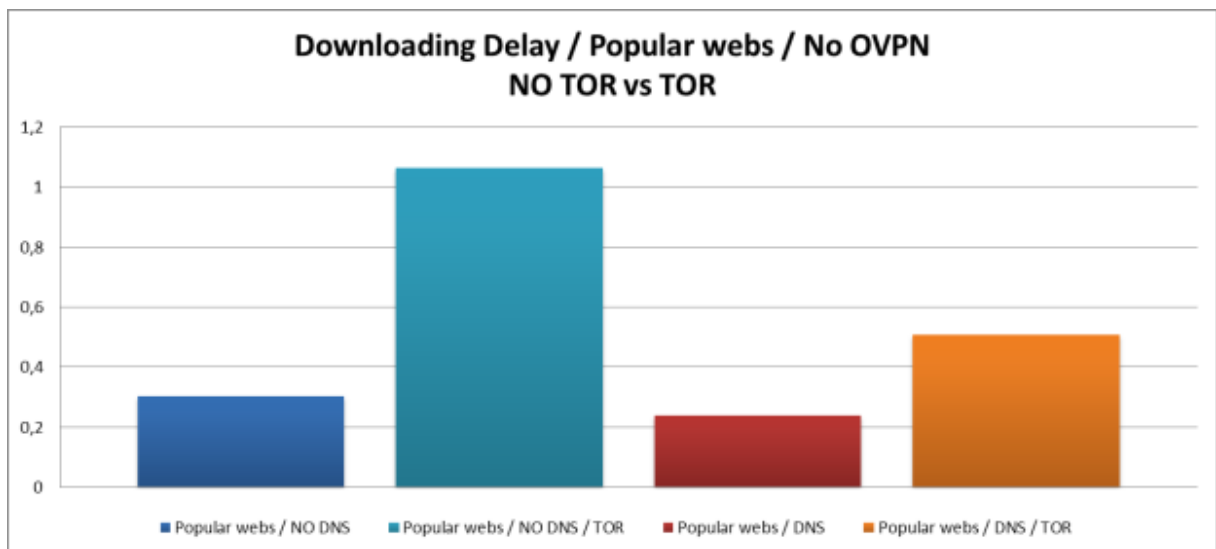


Chart XI-1 Bar Chart Downloading delay Clear access vs. TOR / DNS

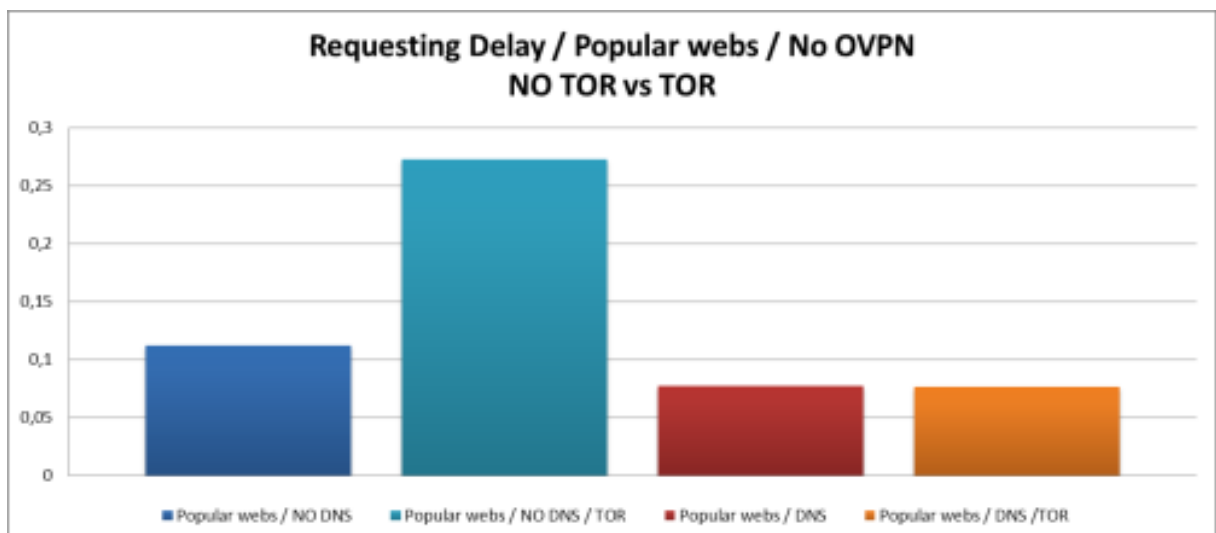


Chart XI-2 Bar Chart Requesting delay Clear access vs. TOR / DNS

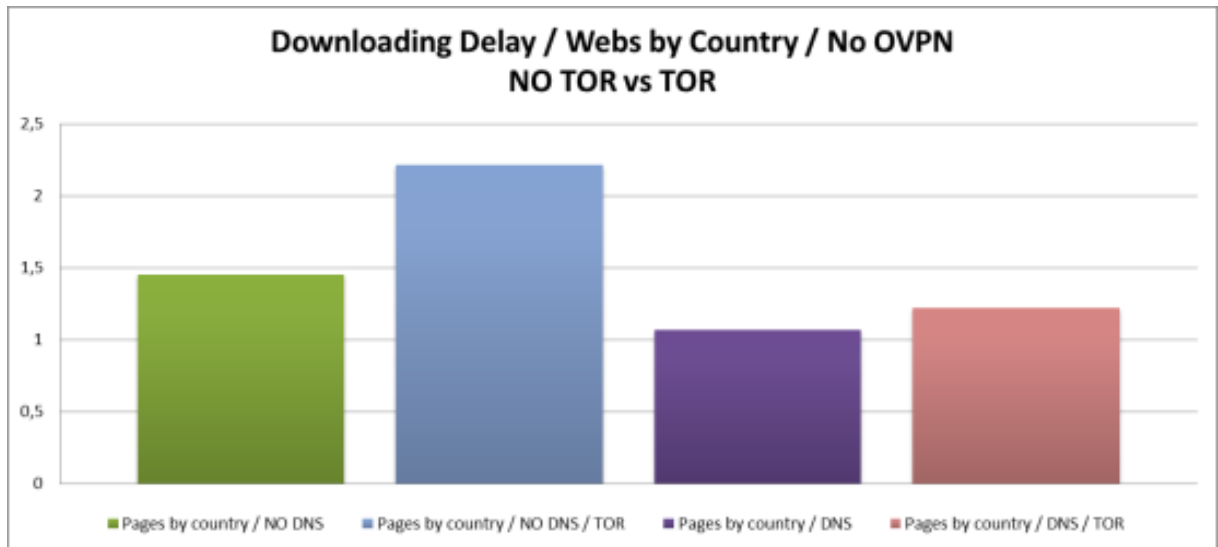


Chart XI-3 Bar Chart Downloading delay Clear access vs. TOR / DNS

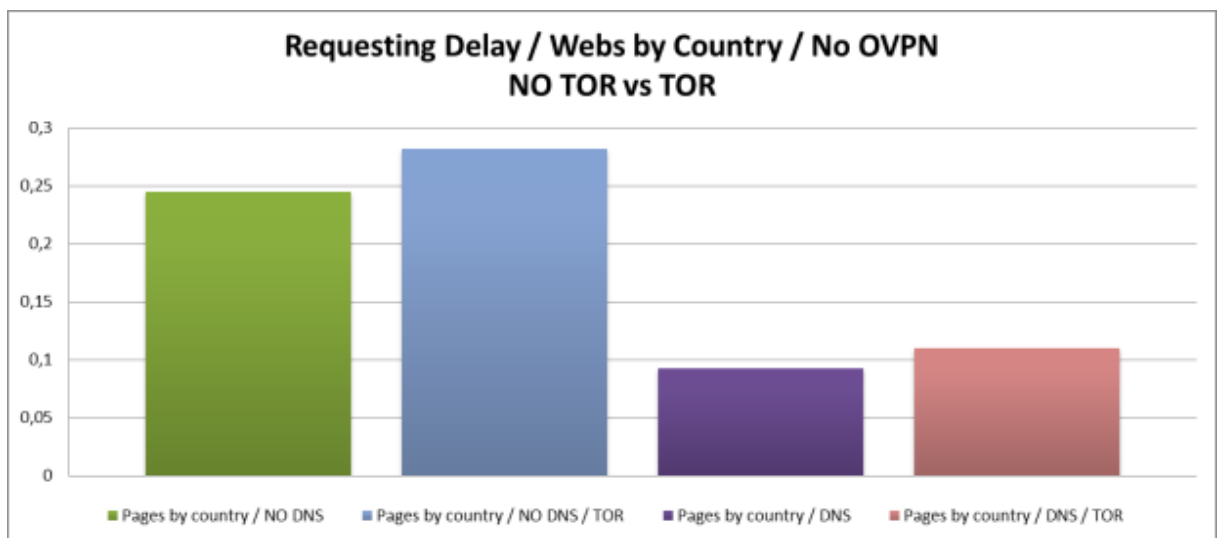


Chart XI-4 Bar Chart Requesting delay Clear access vs. TOR / DNS

III. Clear Access vs. TOR and OVPN

Downloading Delay / Clear vs Complete			
Popular webs / DNS Server / TOR / OVPN			
Web / Relation	Clear	Complete	Delay Increase (Cl/Cp)
Google	0,148	2,1648	14,63
Youtube	0,1865	1,721	9,23
Facebook	0,2538	2,4218	9,54
Wikipedia	0,2085556	1,4063	6,74
Amazon	0,394	1,7105	4,34
Twitter	0,2909	2,4466	8,41
Linkedin	0,2227	2,2612	10,15
Instagram	0,2068	1,8317	8,86
Yahoo	0,1771	1,6276	9,19
Average	0,2320395	1,954611111	8,42

Table XI-5 Downloading delay Clear access vs. TOR and OVPN / DNS

<u>Requesting Delay / Clear vs Complete</u>			
Popular webs / DNS Server / TOR / OVPN			
Web / Relation	Clear	Complete	Delay Increase (Cl/Cp)
Google	0,0836	0,1698	2,03
Youtube	0,0816	0,1136	1,39
Facebook	0,0741	0,1251	1,69
Wikipedia	0,0769	0,1726	2,24
Amazon	0,0748	0,1118	1,49
Twitter	0,074	0,1094	1,48
Linkedin	0,0805	0,1329	1,65
Instagram	0,0766	0,1455	1,90
Yahoo	0,0733	0,1256	1,71
Average	0,0772667	0,134033333	1,73

Table XI-6 Requesting delay Clear access vs. TOR and OVPN / DNS

<u>Downloading Delay / Clear vs Complete</u>			
Webs by Country / DNS Server / TOR / OVPN			
Web / Relation	Clear	Complete	Delay Increase (Cl/Cp)
New Zealand Navy	1,513	3,4729	2,30
South Africa Government	1,3002	2,7261	2,10
Russia foreign ministry	0,3285	2,6723	8,13
Argentinian afa	0,9255	2,7339	2,95
Rugby India	1,2622	4,077666667	3,23
Average	1,06588	3,136573333	2,64

Table XI-7 Downloading delay Clear access vs. TOR and OVPN / DNS

<u>Requesting Delay / Clear vs Complete</u>			
Webs by Country / DNS Server / TOR / OVPN			
Web / Relation	Clear	Complete	Delay Increase (Cl/Cp)
New Zealand Navy	0,1136	0,1256	1,11
South Africa Government	0,0774	0,1243	1,61
Russia foreign ministry	0,075	0,1373	1,83
Argentinian afa	0,0791	0,1472	1,86
Rugby India	0,1179	0,1874	1,59
Average	0,0926	0,14436	1,60

Table XI-8 Requesting delay Clear access vs. TOR and OVPN / DNS

IV. TOR vs. TOR and OVPN

<u>Downloading Delay / TOR vs Complete</u>			
Popular webs / DNS Server / TOR			
Web / Relation	TOR	Complete	Delay Increase (T/Cp)
Google	0,4253	2,1648	5,09
Youtube	0,3787	1,721	4,54
Facebook	0,3964	2,4218	6,11
Wikipedia	0,5686	1,4063	2,47
Amazon	0,6595	1,7105	2,59
Twitter	0,6193	2,4466	3,95
Linkedin	0,4798	2,2612	4,71
Instagram	0,5739	1,8317	3,19
Yahoo	0,454	1,6276	3,59
Average	0,506166667	1,954611111	3,86

Table XI-9 Downloading delay TOR vs. TOR and OVPN / DNS

<u>Requesting Delay / TOR vs Complete</u>			
Popular webs / DNS Server / TOR			
Web / Relation	TOR	Complete	Delay Increase (T/Cp)
Google	0,0845	0,1698	2,01
Youtube	0,0767	0,1136	1,48
Facebook	0,0793	0,1251	1,58
Wikipedia	0,0787	0,1726	2,19
Amazon	0,0796	0,1118	1,40
Twitter	0,072	0,1094	1,52
Linkedin	0,0756	0,1329	1,76
Instagram	0,072	0,1455	2,02
Yahoo	0,0725	0,1256	1,73
Average	0,076766667	0,134033333	1,74

Table XI-10 Requesting delay TOR vs. TOR and OVPN / DNS

<u>Downloading Delay / TOR vs Complete</u>			
Webs by Country / DNS Server / TOR			
Web / Relation	TOR	Complete	Delay Increase (T/Cp)
New Zealand Navy	1,7359	3,4729	2,00
South Africa Government	1,3845	2,7261	1,97
Russia foreign ministry	0,4939	2,6723	5,41
Argentinian afa	0,7785	2,7339	3,51
Rugby India	1,7012	4,077666667	2,40
Average	1,2188	3,136573333	2,47

Table XI-11 Downloading delay TOR vs. TOR and OVPN / DNS

<u>Requesting Delay / TOR vs Complete</u>			
Webs by Country / DNS Server / TOR			
Web / Relation	TOR	Complete	Delay Increase (T/Cp)
New Zealand Navy	0,1426	0,1256	0,88
South Africa Government	0,0931	0,1243	1,34
Russia foreign ministry	0,1036	0,1373	1,33
Argentinian afa	0,099333333	0,1472	1,48
Rugby India	0,114	0,1874	1,64
Average	0,110526667	0,14436	1,33

Table XI-12 Requesting delay TOR vs. TOR and OVPN / DNS

V. Clear Access vs. TOR vs. TOR and OVPN Bar Charts

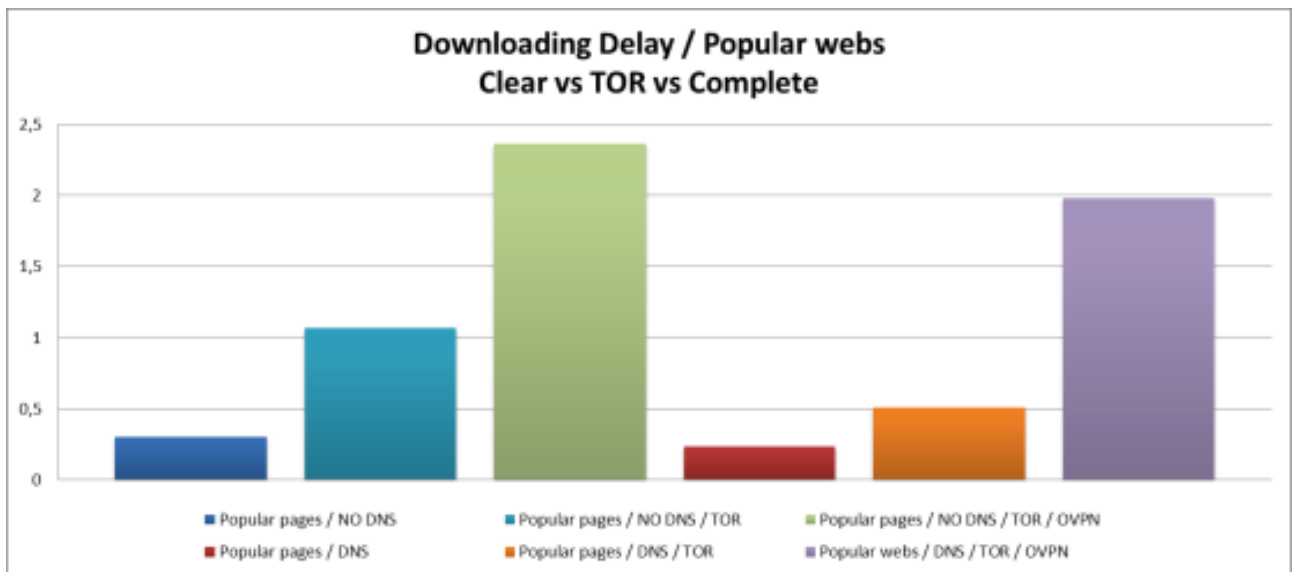


Chart XI-5 Bar Chart Downloading delay Clear access vs. TOR vs. TOR and OVPN

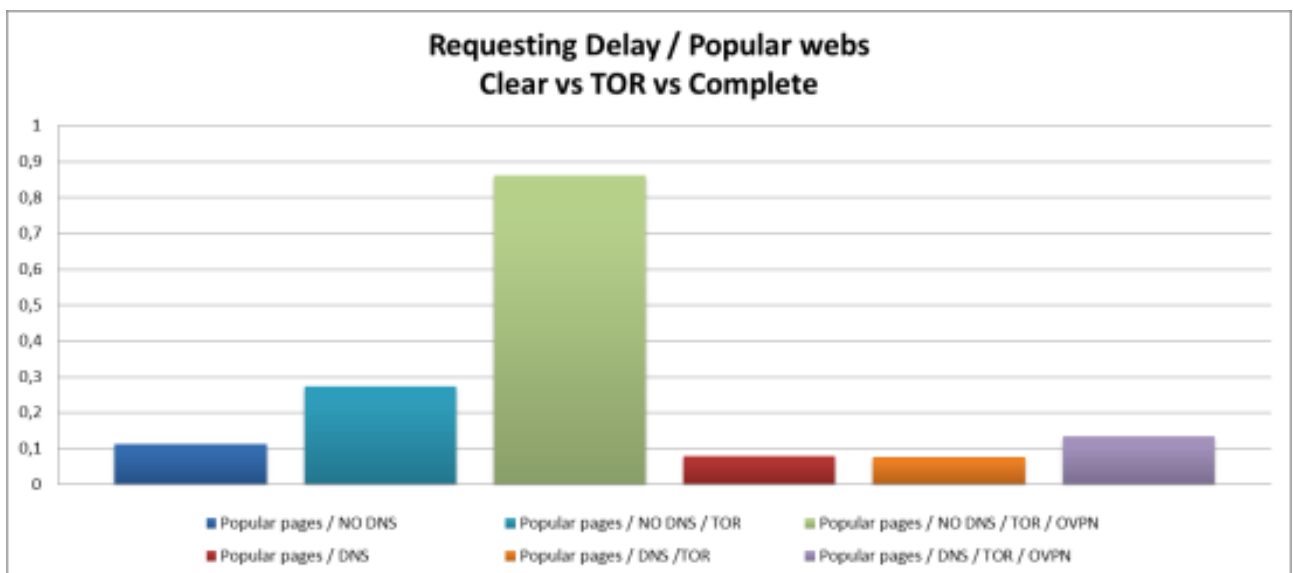


Chart XI-6 Bar Chart Requesting delay TOR vs. TOR and OVPN / DNS

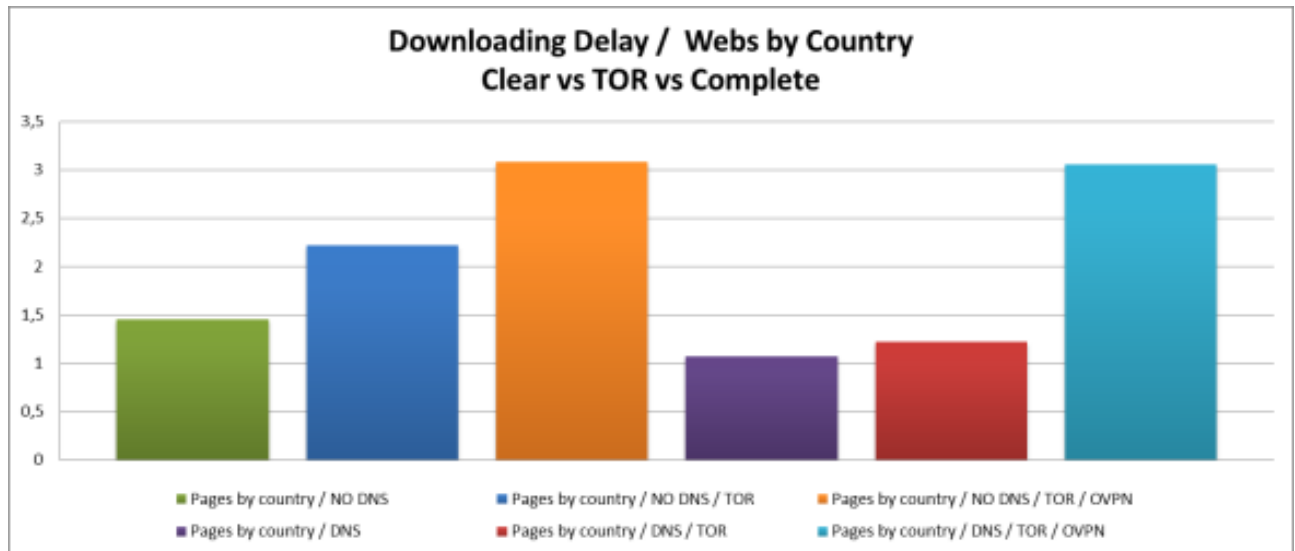


Chart XI-7 Bar Chart Downloading delay TOR vs. TOR and OVPN / DNS

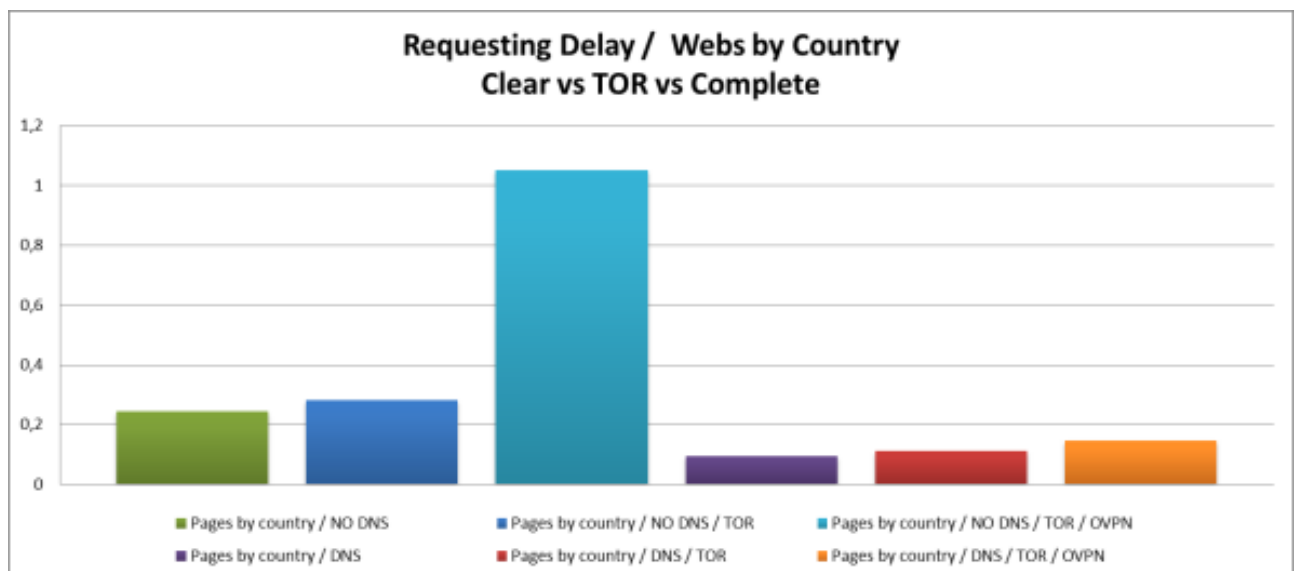


Chart XI-8 Bar Chart Requesting delay TOR vs. TOR and OVPN / DNS

VI. Raspberry Pi 2 vs. Raspberry Pi 3

Downloading Delay / RPi 3 vs RPi 2			
Popular webs / DNS Server / TOR / OVPN			
Web / Relation	RPi 3	RPi 2	Delay Increase (RPi2/RPi3)
Google	2,1648	2,4889	1,15
Youtube	1,721	2,3267	1,35
Facebook	2,4218	2,4528	1,01
Wikipedia	1,4063	1,9733	1,40
Amazon	1,7105	1,5108	0,88
Twitter	2,4466	2,1783	0,89
Linkedin	2,2612	2,3826	1,05
Instagram	1,8317	2,0446	1,12
Yahoo	1,6276	2,503	1,54
Average	1,95461	2,20678	1,13

Table XI-13 Downloading delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS

<u>Requesting Delay / RPi 3 vs RPi 2</u>			
Popular webs / DNS Server / TOR / OVPN			
Web / Relation	RPi 3	RPi 2	Delay Increase (RPi2/RPi3)
Google	0,1698	0,171	1,01
Youtube	0,1136	0,1331	1,17
Facebook	0,1251	0,1186	0,95
Wikipedia	0,1726	0,1685	0,98
Amazon	0,1118	0,1201	1,07
Twitter	0,1094	0,1188	1,09
Linkedin	0,1329	0,1294	0,97
Instagram	0,1455	0,1522	1,05
Yahoo	0,1256	0,1238	0,99
Average	0,13403	0,13728	1,03

Table XI-14 Requesting delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS

<u>Downloading Delay / RPi 3 vs RPi 2</u>			
Webs by Country / DNS Server / TOR / OVPN			
Web / Relation	RPi 3	RPi 2	Delay Increase (RPi2/RPi3)
New Zealand Navy	3,4729	3,4452	0,99
South Africa Government	2,7261	3,0817	1,13
Russia foreign ministry	2,6723	2,7542	1,03
Argentinian afa	2,7339	2,7338	1,00
Rugby India	4,07767	3,87633	0,95
Average	3,13657	3,17825	1,02

Table XI-15 Downloading delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS

<u>Requesting Delay / RPi 3 vs RPi 2</u>			
Webs by Country / DNS Server / TOR / OVPN			
Web / Relation	RPi 3	RPi 2	Delay Increase (RPi2/RPi3)
New Zealand Navy	0,1256	0,1756	1,40
South Africa Government	0,1243	0,1412	1,14
Russia foreign ministry	0,1373	0,1522	1,11
Argentinian afa	0,1472	0,1604	1,09
Rugby India	0,1874	0,1545	0,82
Average	0,14436	0,15678	1,11

Table XI-16 Requesting delay Raspberry Pi 2 vs. Raspberry Pi 3/ DNS

VII. Distance Analysis

Distance to Central Europe (Vienna)			
City	km	NM	Distance / Time curl (speed)
Wellington	18141	9795	6473
Cape Town	13995	7556	5811
Moscow	1670	901	2742
Buenos Aires	11803	6373	6886
New Dehli	5561	3002	2378

Table XI-17 Distance to Europe's centre

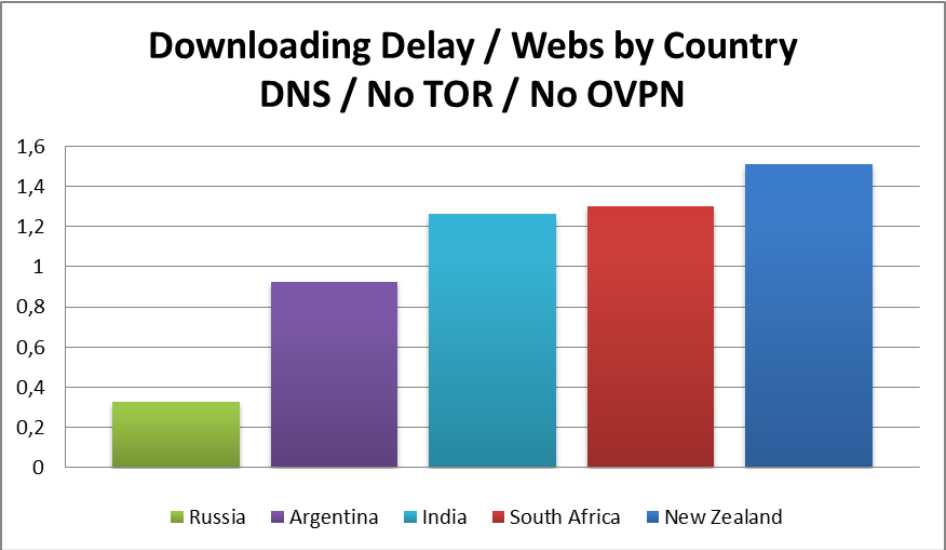


Chart XI-9 Bar Chart delay vs. Distance