DNS PRIVACY

November 2019

EXECUTIVE SUMMARY

Internet access, both from smartphones and desktop computers, uses services to make browsing the web easier in a way that is transparent and convenient to the user. These services, known as the DNS protocol, involve the processing of data by third parties other than those that provide the services to be accessed. This processing could reveal browsing habits and geolocation information, and enables to generate profiles to be preserved indefinitely, and creates a serious risk to the privacy of users.

Despite the increase in Internet privacy awareness, the DNS protocol is probably the Great Ignored. This note identifies the privacy problems that the use of the DNS protocol may entail and the implications that the illegitimate processing of such data could have. In turn, it identifies the guarantees that can be implemented to manage these risks for both users and service providers in home and professional environments.

Keywords: Privacy, Internet, Confidentiality, Integrity, Authenticity, Encryption, Domains, GDPR, LOPDGDD, AEPD, UEET, DNS, TLS, HTTPS, DNSSEC, Innovation.

TABLE OF CONTENTS

I. INTRODUCTION

To allow users to enter in the browsers the names of the services they want to access, instead of a numerical code to identify servers on the Internet, the Domain Name System or DNS was developed.

When users browse the Internet, our devices perform constant queries through the DNS protocol to different machines in the network to determine the IP address to access. In this regard, instead of having to remember a number of up to twelve digits, it is possible to access, for example, the newspaper's website every morning by writing a commercial or easy-to-remember name. These queries are made transparently to the user by accessing certain servers, called DNS servers, which are configured on the network.

A DNS query includes an IP address that identifies the user and can geolocate who is browsing the Internet, and the name of the site to which users want to visit as well. Setting a unique identifier to certain browsing habits is then possible, which means profiling a user while providing the queries. For example, a person could be profiled according to their current political opinion based on the online sites used to be informed. Another example could be to deduce health problems depending on the types of forums, blog or websites in which users participate.

In the majority of cases, queries are communicated through the network and are not protected by, for example, encryption. In addition, when processing the request, some DNS servers may be configured to keep a record of these queries and use that data, not only legitimately to guarantee the security of the services[1], but for purposes other than the mere operation of the DNS system, in addition to being sensitive information that could be filtered to third parties.

An added problem in the event that the necessary guarantees are not adopted, is that the origin of the answers cannot be assured nor that the response has not been modified by a third party. Therefore, the use of DNS[2] spoofing techniques can make users browse websites that are not the ones they really want to visit, with the consequent risks to privacy: information theft, ransomware, etc.

This document focuses on the transversal[3] use of the DNS protocol in communications, emphasising the lack of security measures of the DNS protocol that can cause privacy problems, the improvements that have been adopted and the implications that illegitimate processing of such data may have.

[1] Recital 49 of the GDPR states: It is a legitimate interest of the data controller to process personal data to the extent strictly necessary and proportionate to guarantee the security of the network and of the information; that is to say, the capacity of a network or of an information system to resist, in a certain level of trust, accidental events or illicit or malicious actions that compromise the availability, authenticity, integrity and confidentiality of personal data kept or transmitted, and the security of related services offered by or accessible through these systems and networks, by public authorities, computer emergency response teams (CERT), computer security incident response teams (CSIRT), providers of electronic communications networks and services and providers of security technologies and services. This could include, for example, preventing unauthorised access to electronic communications networks and the malicious distribution of codes, and curbing "denial of service" attacks and damage to computer systems and electronic communications.

[2] DNS attacks: how they try to direct you to fake pages

[3] Transversal considering that all Internet services are accessed by using the DNS protocol

DNS has evolved in response to the need for communications security, so the (still slow) implementation of DNSSEC is providing the dimensions of integrity and authenticity. There are currently two proposals to enable confidentiality through the encryption of queries: DNS Over TLS and DNS Over HTTPS. These new security measures help to improve the level of privacy, but, as seen throughout this study, they do not guarantee it.

II. PURPOSE AND RECIPIENTS

Since DNS is a transversal protocol in Internet services, privacy considerations must be taken into account by a large number of those involved, from software developers to network managers, DNS service providers themselves and Internet access providers.

The purpose of this technical note is to analyse the evolution of the Domain Name System protocol from the point of view of the implications on people's privacy, the way in which it is currently used, the risks that arise, the efforts being made to mitigate these risks and the implications that these changes could have on the privacy of users on the Internet. Likewise, recommendations to be considered in the selection of DNS services are included.

This technical note is within the strategic plan of the Agency, which promotes public awareness of the rights and guarantees that assist them in data protection affairs, with special attention to the protection of citizens with regard to the activities carried out in Internet, and aims to be an boost to initiatives that imply benefits in the privacy of people in the use of the Internet by the digital economy industry.

III. PRIVACY IMPLICATIONS OF THE DNS PROTOCOL

THE DNS PROTOCOL AND THE ASSOCIATED RISKS

The bases of the domain name protocol or DNS are initially established in 1983 by the IETF[4], being updated in 1987, specifying the way in which the IP addresses of Internet equipment will be resolved, as well as a distributed hierarchical domain names system where the domain owner, either on their own DNS servers or those appointed, will establish the relationship between domain names and IP addresses. These are known as authoritative DNS servers, which will be those that communicate with the DNS servers checked by client computers (PCs, mobile phones ...), called DNS resolvers.

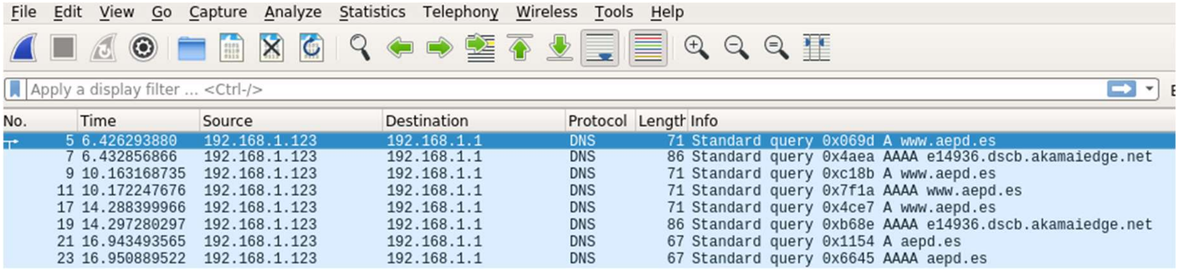
Subsequently, in order to provide security measures in the DNS protocol, the so-called security extensions or DNSSEC that use public key cryptography were incorporated, so that the integrity of the DNS response and its authenticity can be guaranteed. However, DNSSEC does not provide encryption mechanisms that enable the confidentiality of DNS communications. The reality is that the use of DNSSEC has not been extended as much as it was intended and its use on the Internet is very uneven.

On the other hand, the standard configuration in the local area networks uses the DHCP protocol to provide clients, at the operating system level, with information such as the IP address, gateway, network domain name and DNS servers that will check the device. Therefore, the network to which users are connected will set the DNS servers that are going to be looked up; that is, in home networks, it will normally be the operator who

[4] Internet Engineering Task Force

defines the DNS to use, while in corporate networks, administrators will decide if an own DNS server, that of the communications operator or any other public DNS is used.

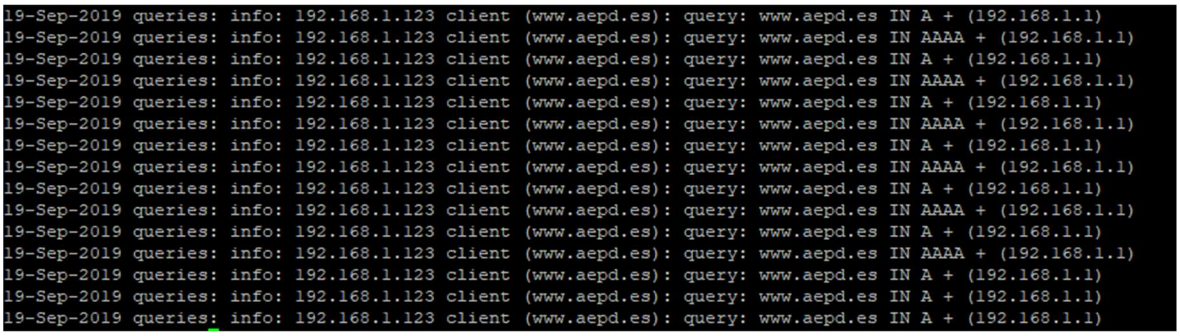
When browsing the Internet from a device to different web sites, the first thing the device needs to know is the IP address that corresponds to the name of the site written in the browser. These queries are sent (and forwarded) without encryption (fig. 1) through the different elements of the network and are processed by the DNS servers[5]. This procedure is particularly vulnerable in open wifis or guest networks and entails two differentiated confidentiality risks.



No.	Time	Source	Destination	Protocol	Length	Info
5	6.426293880	192.168.1.123	192.168.1.1	DNS	71	Standard query 0x069d A www.aepd.es
7	6.432856866	192.168.1.123	192.168.1.1	DNS	86	Standard query 0x4aea AAAA e14936.dscb.akamaiedge.net
9	10.163168735	192.168.1.123	192.168.1.1	DNS	71	Standard query 0xc18b A www.aepd.es
11	10.172247676	192.168.1.123	192.168.1.1	DNS	71	Standard query 0x7f1a AAAA www.aepd.es
17	14.288399966	192.168.1.123	192.168.1.1	DNS	71	Standard query 0x4ce7 A www.aepd.es
19	14.297280297	192.168.1.123	192.168.1.1	DNS	86	Standard query 0xb68e AAAA e14936.dscb.akamaiedge.net
21	16.943493565	192.168.1.123	192.168.1.1	DNS	67	Standard query 0x1154 A aepd.es
23	16.950889522	192.168.1.123	192.168.1.1	DNS	67	Standard query 0x6645 AAAA aepd.es

Figure 1. Network traffic in DNS query.

On the one hand, DNS queries can be intercepted on the network and thus can be read and processed by a third party. On the other hand, DNS servers can record information from the queries (Figure 2) of each device when the user browses the Internet or uses other services on the network.



```
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN AAAA + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
19-Sep-2019 queries: info: 192.168.1.123 client (www.aepd.es): query: www.aepd.es IN A + (192.168.1.1)
```

Figure 2. Registration of a DNS server.

DNS OVER TLS AND DNS OVER HTTPS

To provide confidentiality in DNS queries, different alternatives have been developed, including DNS over TLS (DoT) and DNS over HTTPS (DoH). Both solutions are designed to mitigate the risk that DNS queries can be intercepted, and if they are that the information is illegible, contributing to improve confidentiality.

Recently, the DNS over HTTPS or DoH protocol has been defined as a draft. Therefore, users can take advantage of functionalities present in HTTP, such as compression, redirection, and encryption of DNS queries through TLS. The latter, TLS, is the protocol currently used to encrypt the HTTPS communications of browsers. In this regard, DNS queries become HTTPS queries between client and server. Firstly, this would entail a

[5] Those established as shown in the previous section

relevant improvement in the privacy of communications, since this prevents third parties from knowing the DNS queries made by any device.

A third party that analyses the network traffic generated by a browser with DoH enabled (Figure 3), will only identify standard HTTPS communications made through port 443 TCP. DoH queries will be masked among the rest of the communications with a secure website.

In order to use DoH DNS servers that accept queries based on that protocol must be accessed. In the definition of DoH, it is established that DoH servers can be selected manually (in a simplified way as if it were the address of a website) or can be further provided through DHCP or similar protocols.

Source	Destination	dst port	Protocol	Length	Info
192.168.1.123	104.16.248.249	443	TLSv1.2	111	Application Data
192.168.1.123	104.16.248.249	443	TLSv1.2	141	Application Data
104.16.248.249	192.168.1.123	34860	TCP	60	443 → 34860 [ACK] Seq=1 Ack=145 Win=32 Len=0
104.16.248.249	192.168.1.123	34860	TLSv1.2	272	Application Data
104.16.248.249	192.168.1.123	34860	TLSv1.2	85	Application Data
192.168.1.123	104.16.248.249	443	TCP	54	34860 → 443 [ACK] Seq=145 Ack=250 Win=1452 Len=0
192.168.1.123	104.16.248.249	443	TLSv1.2	111	Application Data
192.168.1.123	104.16.248.249	443	TLSv1.2	148	Application Data
104.16.248.249	192.168.1.123	34860	TCP	60	443 → 34860 [ACK] Seq=250 Ack=296 Win=32 Len=0
104.16.248.249	192.168.1.123	34860	TLSv1.2	408	Application Data
104.16.248.249	192.168.1.123	34860	TLSv1.2	85	Application Data
192.168.1.123	104.16.248.249	443	TCP	54	34860 → 443 [ACK] Seq=296 Ack=635 Win=1452 Len=0

Figure 3. Traffic network query DNS over HTTPS

Some web browsers have chosen to use DoH. For example, Firefox allows users to enable it under the browser options (Figure 4) and plans to set it as default settings. However, since these are settings established by the browser, they will only be effective on the DNS requests made by the browser itself, not affecting other browsers or applications on the device that access the Internet.

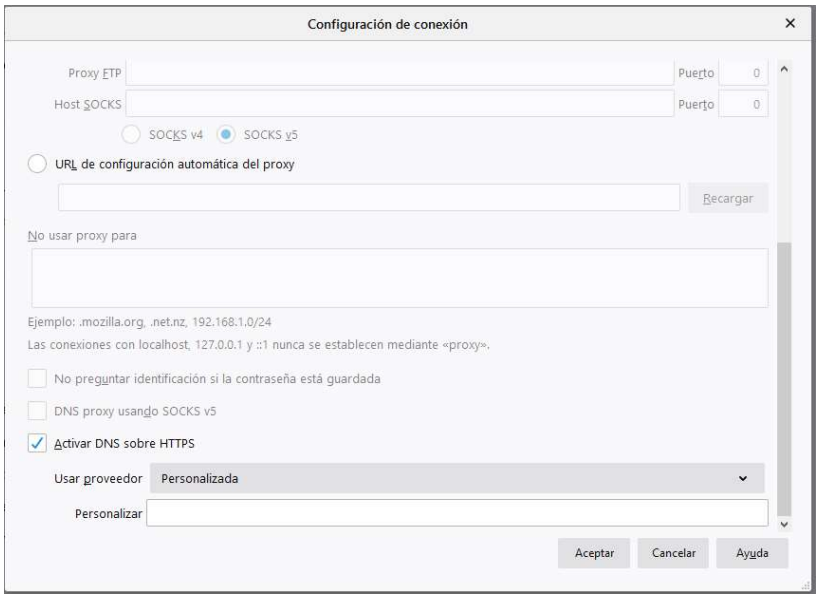


Figure 4. DoH settings in Firefox.

Although Firefox allows users to set the DoH server freely, activating this option sets the default Cloudflare server (Figure 5), which stores the queries made for 24 hours, as reported on its website.

Figure 5. Default DoH provider in Firefox

To avoid connectivity problems, in case Firefox cannot resolve the addresses through DoH, it detects a parental control system or business DNS settings, it will make an unencrypted query to the DNS servers established at the operating system level a Multicast query DNS (Figure 6).

Source	Destination	Info
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question
192.168.1.123	224.0.0.251	Standard query 0x0000 A www.consultadnserronea.local, "QM" question

Figure 6. Query Multicast DNS.

For its part, Google plans to incorporate DoH for version 78 of its Chrome browser, which, as indicated, will experimentally incorporate the possibility of choosing the following DoH service providers: Cleanbrowsing, Cloudflare, DNS.SB, Google, OpenDNS, Quad9.

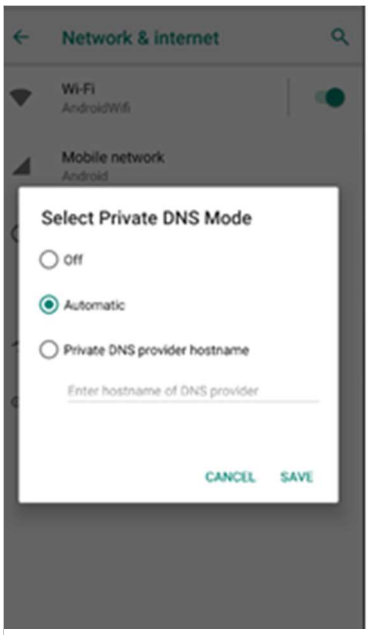


Figure 7. Selection of private DNS on Android.

DNS over TLS, or DoT, is another alternative that implements the encryption capabilities provided by TLS over the DNS protocol, so that a standard DNS query is encrypted with TLS and sent to a server set to answer DoT. At the network level, the DoT server must be listening on port 853 TCP where the client will make the requests. BIND is the most widespread DNS server today, and allows users to set it as a DoT server easily.

As for mobile devices, from Android 9 it is possible to natively set the DNS servers that the Smartphone will use regardless of the network in which it is connected. At the moment the Microsoft and Apple systems do not have this option without resorting to third-party software.

IV. CONCLUSIONS

For more than 35 years the DNS protocol has been one of the pillars of the use of the Internet and data networks in general, facilitating browsing the web without having to remember a numerical address such as the IP address.

Despite the increase in concern and awareness about privacy on the Internet, the DNS protocol is probably the Greatest Ignored. However, as we have seen, the information collected through this service can have a relevant impact on the privacy of people because, through the queries that have been made to the DNS server, it is possible to know in detail the browsing habits and profile the owner of a device.

Like most Internet protocols, DNS was defined without regard to security, subsequently developing measures to ensure the integrity and authenticity of the response such as DNSSEC and more recently measures to ensure confidentiality such as DoT and DoH.

The incorporation of these solutions can be a great advance for the privacy of communications especially in unreliable networks, but they are not exempt from some limitations that must be overcome when the technology is mature and its implementation is wider:

- Currently, only web browsers implement DoH, so the rest of the queries made by the applications of the equipment and OS continue to be performed without encrypting the communication. DoT is not yet implemented natively on most devices.
- The implementation of DoH in fallback mode in the browser means that, in some cases, the requests will continue to be made through the traditional DNS protocol, with the uncertainty of not knowing which request has been made encrypted and which has not.
- Although users can easily establish DoH servers through the settings of their browser, which a priori is an advantage for their privacy, this option should be carefully analysed, since it can lead to choosing a provider that has servers in countries outside of the EEA and/or that use the query records for purposes other than to exclusively provide the DNS service resulting in possible processing activities subject to the GDPR. This last consideration is not exclusive to DoH and DoT, but can also be extended to the original DNS.
- By allowing queries to other DNS servers other than those already defined by the operating system and tunnelled through HTTPS, DoH will make it easier for malware to avoid detection mechanisms.
- DoH can give a false sense of security, since it is possible to identify the use of DNS queries through HTTPS with different techniques such as TLS fingerprinting, identifying the destination if it corresponds to a DoH server or analysing HTTPS unencrypted traffic

As recommendations to the industry and the rest of the agents involved, each in its corresponding area of action, the following lines of action are proposed:

- Promote and facilitate greater implementation of DNSSEC, activating it in all DNS, both resolvers and authoritative.

- Promote and facilitate the widespread use of DNS queries encrypted with any of the methods mentioned at the operating system level without the need to resort to third-party software.
- DNS service providers must inform about the terms and conditions of use of the service, including the applicable legal basis in case of storing and/or processing the data of the queries, as well as the rest of the information related to possible processing activities subject to the GDPR.
- In the case of Internet access companies that provide their clients with access to third-party DNS servers, they must ensure that they select providers that meet the requirements of the GDPR, choosing those DNS services that offer sufficient guarantees that make possible that the rights of the interested parties are guaranteed by data processing.

Finally, it should be highlighted that the data processed by the DNS server is collected for a specific processing, to provide the domain name resolution service, and that any other type of additional processing, in particular the communication of said data for other purposes such as user profiling implies serious implications for privacy. In this case, there would be a processing of personal data from which its legal basis must be identified, the user must be informed, the exercise of the rights of the user must be guaranteed and compliance with the GDPR in its entirety must be guaranteed. Otherwise, it would be an illegitimate processing of that personal data.

V. BIBLIOGRAPHY

[1] Liu, C. and Albitz, P. (2009). *DNS and BIND*. O'Reilly Media, Inc.

[2] Deckelmann, S. (2019). *What's next in making Encrypted DNS-over-HTTPS the Default – Future Releases*. [online] Future Releases. Available at: https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

[3] McManus, P. (2019). *Improving DNS Privacy in Firefox – Firefox Nightly News*. [online] Firefox Nightly News. Available at: https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

[4] Chromium Blog. (2019) *Experimenting with same-provider DNS-over-HTTPS upgrade*. [online] Available at: https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html

[5] Bradbury, D. (2019). *Mozilla increases browser privacy with encrypted DNS*. [online] Naked Security. Available at: https://nakedsecurity.sophos.com/2019/09/10/mozilla-increases-browser-privacy-with-encrypted-dns/

[6] Hunter, M. (2019). *Encrypted DNS Could Help Close the Biggest Privacy Gap on the Internet. Why Are Some Groups Fighting Against It?*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2019/09/encrypted-dns-could-help-close-biggest-privacy-gap-Internet-why-are-some-groups

[7] GitHub. (2019) *folbricht/routedns*. [online] Available at: https://github.com/folbricht/routedns

[8] ag, u. (2019) *ungleich blog - Mozilla's new DNS resolution is dangerous*. [online] Ungleich.ch. Available at: https://ungleich.ch/en-us/cms/blog/2018/08/04/mozillas-new-dns-resolution-is-dangerous/

[9] Dnscrypt.info. (2019) *Home page of the DNSCrypt project [DNS security]*. [online] Available at: https://dnscrypt.info/protocol/

[10] Tools.ietf.org. (2019) *RFC 7858 - Specification for DNS over Transport Layer Security (TLS)*. [online] Available at: https://tools.ietf.org/html/rfc7858

[11] Tools.ietf.org. (2019) *RFC 8484 - DNS Queries over HTTPS (DoH)*. [online] Available at: https://tools.ietf.org/html/rfc8484

[12] Simplednscrypt.org. (2019) *Simple DNSCrypt*. [online] Available at: https://simplednscrypt.org/

[13] Hashed Out by The SSL Store™. (2019) *What is the difference between DNS over TLS & DNS over HTTPS?*. [online] Available at: https://www.thesslstore.com/blog/dns-over-tls-vs-dns-over-https/

[14] Kb.isc.org. (2019) *DNS over TLS - BIND 9*. [online] Available at: https://kb.isc.org/docs/aa-01386

[15] Android Developers. (2019) *Distribution dashboard | Android Developers*. [online] Available at: https://developer.android.com/about/dashboards

[16] Sans.org. (2019) *SANS Institute: Reading Room - DNS Issues*. [online] Available at: https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160