**NTNU – Trondheim**
Norwegian University of
Science and Technology

# Title

**Terje Kristoffer Skow**

Submission date: November 2015
Responsible professor: Than Van Do, ITEM
Supervisor: Hai Ngyuen, Telenor Research

Norwegian University of Science and Technology
Department of Telematics

## Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of

the original language. There is no need for special content, but the length of words should match the language.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

# Preface

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

# Contents

# List of Figures

# List of Tables

# List of Algorithms

# List of Acronyms

**DNS** Domain Name System.

**DPI** Deep Packet Inspection.

**TTL** Time to live.

**VPN** Virtual Private Network.

# Chapter 1
# DNS

## 1.1 Introduction

Domain Name System (DNS) is an important part for the internet. It was designed and standardized in the mid and late 1980s as the previous system `HOST.TXT` was headed for and encountering problems [MD88], but has since been updated and configured many times. DNS needed to be able maintain a fast response time as the database grew larger, this was solved by using a hierarchical set up. This means that each layer only has a limited information and sends the request to a new server until it reaches the correct server, called `name server`. It started with one root server, which has expanded to 13 today. The each layer of the hierarchy is called a zone, and it delegates the responsibility for underlying zones delimited by the `dot` in the request name. When a request for `ntnu.no` goes through DNS it starts in the root zone, where it sent down the hierarchy to the `.no` zone.

consists of many distributed databases The main function of DNS is to translate domain names to IP addresses.

mostly used to translate a domain name to an IP address which the network use to route http traffic

This type of lookup receive an `'A'` record if the IP is an ipv4 address and `'AAAA'` if it's an ipv6 address. `'CNAME'` is also a much used response. it returns the correct domain name for the 'A' lookup, e.g. if you want to go to aftenposten.no, you could write ap.no the DNS then respond with a CNAME response containing aftenposten.no which automatically trigger a new request for aftenposten.no which give an 'A' response containing the ipv4 address. There are over 30 different record types in the DNS. Every one has their different purpose and therefore different maximum size on the payload. DNS mostly use UDP on port 53, but could also use TCP on the same port. TCP is used when the payload is over 512 bytes or if there is a zone transfer.

DNS is build as a hierarchical system where each level sends you along until you have reached the correct server. The internet has 13 root servers, and a lookup in the system is backwards. The easiest way to explain this is with an example. If you request `some.test.example.com` the first request will be to the root server which will look up the IP-address of the server that controls the .com domain. Next the .com server looks up who controls the example.com domain, and the example.com server finds the DNS server of test.example.com. At last the test.example.com DNS server returns the IP-address of some.test.example.com. Since this process takes a long time, most responses has a Time to live (TTL) which is how long the router should use the given IP-address as a response to requests for that domain.

Normally a DNS server in an enterprise does not send requests directly to the internet, but use an internal DNS server instead. If you are the owner of the authoritative server for a domain, you can control the responses. This is what a DNS tunnel exploits, which will be explained more in the next section.

# Chapter 2
# DNS Tunneling

## 2.1 DNS Tunneling

DNS tunneling was first used by people who exploited that DNS was not monitored in network you had to pay to use, e.g. hotels and cafés. It was used as an Virtual Private Network (VPN) tunnel. In later years it has been discovered that in enterprises the DNS are not monitored as much as other traffic on the network. People has therefore figured out that it is a good way to ex filtrate data in secure networks. DNS could also be used for a "command and control" attack, where commands are sent over DNS.

The way DNS works it that if you control the authoritative DNS server for a domain you can easily send commands.

With the increase of smartphones it has been discovered that DNS tunneling could again be used as the it started, to use the network without having to pay for it. Carriers can not start charging for regular queries since just regular use of a the internet produces a lot of DNS traffic. Which an user would not see and it would be hard for the carrier to explain for an user what he has been charged for.

# Chapter 3
# DNS Tunneling Detection

There has been done some research in detecting DNS tunneling over the years, but as it is still a problem no one has found a solution that is cost efficient. The best way for detecting tunnels is still Deep Packet Inspection (DPI) which is slows down the DNS requests as the amount of requests increase. DPI looks into each request and response for payload information which can indicate a DNS tunnel. For instance if requests maximizes the size of the labels and the overall name it should be looked at [Far13], this since tunnels would try to minimize the number of packages and maximize speed. Looking at the hostname should also be an indication since regular DNS names is dictionary words or have some meaning, while an encoded name would be meaningless. Traffic analysis is the other main alternative to detecting tunnels. Looking at volume, frequency and other attributes of DNS traffic could give indication of a tunnel. Earlier research has covered different techniques, looking at the volume of DNS traffic from a IP address or the volume of DNS traffic to a specific domain [Far13]. The overarching way of detecting tunnels with traffic analysis is looking for anomalies and stand out cases.

### 3.0.1 Traffic analysis

Data that is tunnelled through DNS is normally limited to 512 bytes per request, which leads to clients to send and receive lots of requests and responses. If the server should have the possibility to send data to the client will the client have to constantly send requests to get the data as a response from the server. All this leads to lots of DNS traffic which is not similar to normal use.

# Chapter 4
# Conclusion

# References

[Far13] Greg Farnham. Detecting dns tunneling. *InfoSec Reading Room*, 2013.

[MD88] P. Mockapetris and K. J. Dunlap. Development of the domain name system. In *Symposium Proceedings on Communications Architectures and Protocols*, SIGCOMM '88, pages 123–133, New York, NY, USA, 1988. ACM.