BORANG PENGESAHAN STATUS TESIS*

JUDUL: MONITORING DNS TRAFFIC THROUGH GOOGLE MAPS

SESI PENGAJIAN: 2012/2013

Saya NORFARAHANI BINTI JUSOH

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
_____	TIDAK TERHAD	

_____ _____

(TANDATANGAN PENULIS) (TANDATANGAN PENYELIA)

Alamat tetap: NO 491, KG JAMBU BONGKOK,21610, MARANG , TERENGGANU

Nama Penyelia: PROF MADYA DR. MOHD. FAIZAL BIN ABDOLLAH

Tarikh: _____ Tarikh: _____

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

DECLARATION

I hereby declare that this project report entitled

MONITORING DNS TRAFFIC THROUGH GOOGLE MAPS

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date: 27-AUGUST-2013

(NORFARAHANI BINTI JUSOH)

SUPERVISOR : _____ Date: 27-AUGUST-2013

(PROF. MADYA DR. MOHD. FAIZAL BIN ABDOLLAH)

MONITORING DNS TRAFFIC THROUGH GOOGLE MAPS

NORFARAHANI BINTI JUSOH

This report is submitted in partial fulfilment of the requirements for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2013

DEDICATION

I dedicated this thesis to my beloved mother Esah binti Salleh, and my family who always been at my side and always supporting me. I hope that this achievement will complete the dream that you had for me all those many years ago. I also dedicated this thesis to my friends who always helping me.

In memory of

My beloved late father, Jusoh bin Sulaiman and my brother, Mohd Fadhli bin Jusoh.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank God for his blessings. Because of Him I was able to finish this thesis without any obstacles. Thank Him for the gift of life, health, and all life opportunities.

Then, my special gratitude goes to my supervisor, Dr Mohd. Faizal Abdollah. Thanks for your guidance I was able to stay focused, structured and motivated. Because of your patience with reading over and over, several drafts that I send to you, I got and learn so much from your comments and that helped me a lot into doing my best. Thank you for everything and may God bless you abundantly.

I would also like to thank to my family for their support and always encourage me to be the best. Because of them, I am here on the first place.

I would also thank to my friends especially Laili Munawaroh and Munirah Mohd. Aris for being so supportive, for helping me survive all the stress from this year and not letting me give up.

Finally, I also place on record, my sense of gratitude to one and all who directly or indirectly, have lent their helping hand in this thesis.

ABSTRACT

The main focus of this paper is to develop DNS monitoring tool that can monitor DNS traffic by using Google Maps. As known the growth of network, DNS will have the risk to be attacked by malicious attack and DNS spoofing. The problem that related with Google Maps today is it does not embedded with the function that can monitor global DNS network traffic. The main objective of this project is to establish the DNS monitoring tool using Google Maps function by adding DNS network traffic monitoring map. In this project, the methodology that used is based on System Development Life Cycle (SDLC) approaches. This project is followed SDLC model because it is included an implementation of system. The implementation of this project starts by register into Google Maps API to obtain the API Key. This API Key will used to create a new Google Maps. The packet of DNS form UTeM will be captured using Wireshark by filtering at port 53. Then, all the data will imported into Google Fusion Table. The data will be visualized into map form. In the end of this project, a map that can monitor DNS traffic can be developed and used by administrator to detect any anomaly behaviors that happened in the DNS traffic.

ABSTRAK

Fokus utama kajian ini adalah untuk membangunkan alat pemantauan DNS yang boleh memantau trafik DNS dengan menggunakan Peta Google. Seperti yang diketahui dengan berkembangnya rangkaian internet, DNS turut berisiko untuk diserang oleh serangan berniat jahat serta penipuan DNS. Masalah yang berkaitan dengan Peta Google hari ini adalah ia tidak dilengkapkan dengan fungsi yang boleh memantau rangkaian trafik DNS di seluruh dunia. Objektif utama projek ini adalah untuk mewujudkan alat pemantauan DNS menggunakan fungsi Peta Google dengan menambah rangkaian trafik bagi DNS pada peta pemantauan. Dalam projek ini, metodologi yang digunakan adalah berdasarkan pendekatan Pembangunan Kitaran Hidup (SDLC). Projek ini dibuat mengikut model SDLC kerana ia merupakan pelaksanaan sistem. Pelaksanaan projek ini bermula dengan mendaftar ke dalam Google Maps API untuk mendapatkan Kunci API. Kunci API ini akan digunakan untuk membuat Peta Google baru. Paket DNS daripada UTeM akan ambil menggunakan Wireshark dan ditapis di port 53. Kemudian, semua data akan diimport ke dalam Jadual Fusion Google. Data yang ditukar ke dalam bentuk peta. Pada akhir projek ini, peta yang boleh memantau lalu lintas DNS dapat dibangunkan dan digunakan oleh penyelaras untuk mengesan apa-apa tingkah laku luar biasa yang berlaku dalam trafik DNS.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	Application Programming Interface
CSV	Comma Separate Values
DFD	Data Flow Diagram
DNS	Domain Name System
ERD	Entity-Relationship Diagram
HTML	Hypertext Markup Language
SDLC	System Development Life Cycle
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator

CHAPTER I

INTRODUCTION

1.1 Introduction

DNS are abbreviation that stands for Domain Name System. Based on (SearchNetworking, 2005) the function of DNS is to translate Internet domain and host names into IP address. DNS will convert the address of requested website into IP address of the web server that hosting those sites. DNS is very important because it will make a user-friendly name that is easier to learn and remember compared to numeric addresses. DNS monitoring tools is the tools that are used to monitor the DNS traffic and to capture the traffic. The examples of software that can used to monitor traffic are Wireshark and TCPdump which is a free-source packet analyser.

The main focus of this project is to develop DNS monitoring tool using Google Maps. As known, Google is one of the most popular web search engines that are

widely used today. (Davis, 2012) discussed in Google Secret that instead of web search, Google also develop many applications. One of the famous applications that are introduced by Google today is Google Maps. Google Maps offers a tone of useful mapping services by using the satellite. Even thought many functions of Google Maps have been introduced, but the Google Maps that can be used to monitor DNS traffic around world is not implemented yet.

1.2 Background

Based on (Webopedia, 2013), Domain Name System (DNS) functions in translating the internet domain and host names into IP address. Meanwhile, Google Maps is one of the applications that are introduced by Google. Other functions of Google Maps are to search for address, traffic conditions, and driving directions. However, the disadvantages of Google Maps are it cannot be used to monitor the DNS network traffic. So, this project will disclose the relation between DNS and Google Maps. This project is focusing on monitor the DNS network traffic through Google Maps. As the implementation, the samples of packets that flow in UTeM are captured using Wireshark at and then filtered the port 53 which is the DNS port. Later, the data of DNS packet that captured will be imported into Google Fusion Table and will visualize into maps. Google Maps API is used to modify and form an advanced map mashups with personal data which is DNS data that are being captured by using Wireshark to create the Google Maps that can show the global DNS traffic. Then, use Hypertext Markup Language (HTML) and JavaScript to make the route between the source, Destination and UTeM. Some methodologies will be carried out to make sure the objective can be achieve which are project planning, requirement analysis, project design, implementation, testing, maintenance and documentation. At the end of this project, a Google Maps will able to view the DNS traffic. This map can be used by administrator to detect the location of unauthorized people who access the server.

1.3 Research Problem

Presently, DNS have become one of the essential services that must have in the network communication as the advanced of the internet. As the growth of network, DNS will have the risk to be attacked by malicious attack and DNS spoofing. Based on the background of this project, the problems of this research were identified as stated in the Table 1.1.

Table 1.1: Research Problem for Google Maps with DNS network traffic monitor

No	Problem Statement
RP1	The existing software that can monitor DNS traffic only works to capture and analyse network, do not have the function that can display the DNS traffic around the world.
RP2	As the growth of network, DNS will have the risk to be attacked.

From the Table 1.1, there are two problems that are identified in this research. The first problem is the existing software that is available only works to capture and analyse network. It does not have the speciality to display the DNS traffic around the world. The second problem is as the growth of the network that used today, DNS have the higher risk to be attacked.

1.4 Research Question

Research questions are the general statement for the objectives of the study. In this project, the research question will state the studies that are related about Google Maps and DNS traffic monitor. This project is proposed to discover about the DNS traffic that can be monitor through Google Maps. The research questions about this project are stated in the Table 1.2.

Table 1.2: Research Question for Google Maps with DNS network traffic monitor

RP	RQ	Research Question
RP1	RQ1	What is the current software that can be used to monitor DNS traffic and what is the function of Google Maps?
RP2	RQ2	How to make sure DNS traffic flow is secured?

The questions in this project are obtained based on the research problem in Table 1.1. The first question is what is the current software that can be used to monitor DNS traffic and what is the function of Google Maps. The second question is how to make sure DNS traffic flow is secure.

1.5 Research Objective

From the research question in Table 1.2, the research objectives were obtained. The main objectives of this project is to enhance the function of Google Maps so that it DNS network traffic around the world can be monitor through the Google Maps. Other objectives for this project are stated in the Table 1.3.

Table 1.3: Research Objectives for Google Maps with DNS network traffic monitor

RP	RQ	RO	Research Objectives
RP1	RQ1	RO1	To study about the way to monitor DNS network traffic and the function of Google Maps.
RP2	RQ2	RO2	To develop the DNS monitoring tool using Google Maps function by adding the DNS network traffic monitoring map.
RP2	RQ2	RO2	To test and validate the function of Google Maps with DNS network traffic.

There are three objectives that will be achieved in the end of this project. The first objective is to study about the way to monitor DNS network traffic and the function of Google Maps. The second objective is to develop the DNS monitoring tools using Google Maps by adding the DNS network traffic monitoring map. The last objective is to test and validate the function of Google Maps with DNS network traffic.

1.6 Project Scope

From (SearchCIO, 2012), determining and documenting a project goals, deliverable, tasks, costs and deadlines are a part of the project scope. In this project, Wireshark are chosen as software that used to analyse and capture the DNS network traffic compared to Tcpdump. Based on (http://en.wikipedia.org), the advantages of Wireshark are the data that display can refine using a display filter. The data in the Wireshark can be captured from the live network connection. Other than that, the live data can be read from many types of network. The captured network data also can be displayed in the form of GUI or command line.

Another scope of this project is the period of the DNS network traffic that will be captured. The sample of DNS network traffic from UTeM will be captured by using Wireshark. All the traffic will be analyse at the port 53 which is the port for DNS services. This port functioned to convert domain name into the form of IP address and use User Datagram Protocol (UDP) for transport layer.

Hence, to integrate the data into maps form, Google Maps API version 3 are used. This is the latest version of Google Maps API that is available. It used JavaScript and HTML code to write the coding, faster compared to previous version and can supported by mobile devices.

1.7 Project Contribution

Project contribution defined as what is the advantage of this project to the people after it was successfully implemented. By implementing the DNS monitoring traffic through Google Maps, the flow of DNS traffic around the world can be monitored. Administrator can use Google Maps to detect any abnormal behaviour that happened when the traffic flow at the DNS server is congested.

1.8 Expected Output

The expected output is the final result that was expected in the end of this project. The output for this project is DNS monitoring tool using Google Maps can be successfully developed. This maps can be used to monitor DNS network traffic that are that flow and access into DNS.

1.9 Report Organization

1.9.1 Introduction

This chapter will introduce about DNS and Google Maps. The general background about DNS network traffic monitor through Google Maps is discussed here. The problem statement, scope, and expected output of the project are explained in this chapter.

1.9.2 Literature Review

In this chapter, the previous work that are related with DNS monitoring, DNS traffic analysis, directory public, Google Maps API, and detection of abnormal behaviour of DNS traffic are explained. Then, all of the information will analyse and the benefits from the implementation of DNS traffic network monitor through Google Maps are stated. The new solution for this project is proposed at the end of this chapter.

1.9.3 Methodology

For this chapter, the methodology that used in this project is using System Development Live Cycle (SDLC) because this project is assumed as system development. The milestone and Gantt chart are included in this chapter.

1.9.4 Design and Implementation

The software and hardware that used to develop this project are explained in this chapter. For this project, Wireshark are used to capture the packet and analyse it. Other than that, Google Maps API version 3 is used to create Google Maps that can monitor DNS network traffic around the world. The DFD, ERD and flow chart will used to display the flow of implementation in this chapter. The sample result for Google Maps that can display DNS traffic network will describe.

1.9.5 Testing and Analysis

This chapter will discuss the method and steps that are used to analyse the Google Maps to make sure it can function properly. If there are some errors occur, this project will refer to SDLC to fix the problem.

1.9.6 Conclusion

For this chapter, the conclusion and suggestion for the further work based on the overall results are explained here.

1.10 Conclusion

As the conclusion, the general background of this project is explained in this chapter. The introduction that discussed the introduction and general process also has been clarified in this chapter. The problems that occur regarding the topics, objectives scope and the expected output of this project are state. The next chapter will explained about the literature review and previous work that related to this project.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

This chapter will discuss about the sources that are related with capturing the DNS for global traffic. All of the resources are obtained from internet, books, journals, articles and webpage that are relevant with the project title. Literature review is the research of the previous project and it can give a better understand about the method that was proposed.

2.2 Facts and Finding

2.2.1 DNS Monitoring

Based on (IBM, 2013), DNS monitoring is a techniques that used to monitor the DNS service in the network. The aim of DNS monitor is to find the information of the hosts. The DNS monitor can be configured by look up the address or the hostnames of the target hosts. Then, DNS

monitor will measure the services performances by collecting the search results and the response time in the log files. There is two ways to monitor the DNS which are by using IP address lookup or by using hostname lookup.

i. IP address lookup

By using this way, the client will make the request of IP address by using host name. If the address is found, it will return it to client while if the address if failed to search, it will send a message that contains the failed search. The client will retry to configure if the request times out and it will create failed event if there is no retries left. Table 2.1 below shows some information that need to monitor DNS.

Table 2.1: Components to monitor DNS traffic
for Google Maps with DNS network traffic monitor

Components	Description
IP Address of DNS Server	The IP address of the DNS server that want to monitor.
Port Number of DNS Server	The default port number that is used for DNS is port 53.
Host Address	The hostname or domain name that want to be solved.
Monitor IP Address	IP address of the target domain to be solved.

Table source: (IBM, 2013)

ii. Hostname lookup

Hostname lookup will need to provide the IP address that will be resolved into hostname compared to IP address lookup that need to provide hostname to be solved into IP address.