ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

TRAFFIC COMPUTER STORAGE SYSTEM

โดย

วรกฤษณ์ ธีระรังสิกุล

WARAKRIT TEERARUNGSIKUL

อาจารย์ที่ปรึกษา

ดร.สิงหะ ฉวีสุข

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 2 ปีการศึกษา 2558

TRAFFIC COMPUTER STORAGE SYSTEM

WARAKRIT TEERARUNGSIKUL

A REPORT SUBMITTED IN PATIAL FULFILLMENT OF THE

REQUIREMENT OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2/2015

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

TRAFFIC COMPUTER STORAGE SYSTEM

นายวรกฤษณ์ ธีระรังสิกุล

รหัสประจำตัว 54660758

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาการศึกษาอิสระ 2 หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2 ปีการศึกษา 2558

..... อาจารย์ที่ปรึกษา

(ดร.สิงหะ ฉวีสุข)

..... กรรมการสอบ

(ดร.นล เปรมัษเฐียร)

หัวข้อ	ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์
นักศึกษา	นายวรกฤษณ์ ธีระรังสิกุล
รหัสนักศึกษา	54660758
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีสารสนเทศและการจัดการ
ปีการศึกษา	2558
อาจารย์ที่ปรึกษา	ดร.สิงหะ ฉวีสุข

บทคัดย่อ

รายงานฉบับนี้นำเสนอการออกแบบและพัฒนาระบบสารสนเทศเพื่อจัดเก็บข้อมูลจราจรคอมพิวเตอร์สำหรับบริษัทวุฒิศักดิ์คลินิก อินเตอร์กรุ๊ปจำกัด โดยมีวัตถุประสงค์ เพื่อใช้เก็บข้อมูลจราจรคอมพิวเตอร์ของพนักงานภายในองค์กร และเป็นเครื่องมือเพื่อใช้สร้างรายงาน วิเคราะห์พฤติกรรมการใช้งานระบบเครือข่ายของพนักงานภายในองค์กร ซึ่งส่งผลให้ผู้ดูแลระบบสามารถวิเคราะห์ปัญหาที่เกิดขึ้นภายในระบบเครือข่ายได้อย่างรวดเร็ว และสามารถตรวจสอบการใช้งานอินเทอร์เน็ตของพนักงานภายในองค์กรว่าใช้อย่างผิดวัตถุประสงค์หรือไม่

แนวทางในการศึกษา เริ่มจากศึกษาและวิเคราะห์ปัญหาที่เกิดขึ้นจากการปฏิบัติงานในปัจจุบัน ศึกษาความเป็นได้ของการพัฒนาระบบ ตลอดจนกำหนดความต้องการ วิเคราะห์และออกแบบระบบสารสนเทศนี้ โดยการออกแบบและพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ใช้รูปแบบของเว็บแอพพลิเคชันร่วมกับฐานข้อมูลเชิงสัมพันธ์ โดยระบบจะทำการเก็บข้อมูลจราจรคอมพิวเตอร์มาจากจุดต่อเชื่อมของเครือข่ายจากนั้นเปลี่ยนข้อมูลที่ได้ให้อยู่ในรูปแบบข้อมูลเชิงสัมพันธ์ และทำการแสดงผลผ่านเว็บเพจ โดยที่ผู้ดูแลระบบสามารถเรียกดูข้อมูลย้อนหลัง หรือข้อมูลเฉพาะที่ต้องการได้ เพื่อนำข้อมูลที่ได้ไปใช้วิเคราะห์ถึงปัญหาที่เกิดขึ้นในระบบเครือข่าย และสามารถนำไปใช้สนับสนุนการตัดสินใจของผู้บริหารเพื่อกำหนดนโยบายในการใช้งานอินเทอร์เน็ตของพนักงานในองค์กร

Title	TRAFFIC COMPUTER STORAGE SYSTEM
Student	Mr. Warakrit Teerarungsikul
Student ID	54660758
Degree	Master of Science
Program	Information Technology
Major	Information Technology Management
Academic	Year 2015
Advisor	Dr. Singha Chaveesuk

ABSTRACT

This report presents a design and development of the traffic computer storage system for Wuttisak Clinic Intergroup Co., Ltd. The objective is to collect employee computer traffic and is used to generate reports, Analyze usage behavior of employees within the enterprise network. As a result, administrators can analyze problems within the network quickly and monitor the employees in organization are used misuse internet or not.

The study approach in this thesis began with analyzing the problems with the current system and the possible system development, and identifying need. The system is designed and developed based on the relational database altogether with the web application. By designing and developing traffic computer storage system take the form of a web application with a relational database. The system will collect traffic computer data from network gateway then change the information provided in the form of relational data and rendering the webpage. The administrator can view historical data or specific data. It were used to analyze the problems in the network and can be used to support management decisions for determine employee's internet use policy

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

ภาพที่ หน้า

สารบัญรูป (ต่อ)

ภาพที่ หน้า

บทที่1

บทนำ

1.1 ความเป็นมา

ในปัจจุบันการส่งข้อมูลผ่านระบบเครือข่ายได้เพิ่มประสิทธิภาพในการทำงานให้กับองค์กรทั้งยังลดระยะเวลาในการทำงานลงอีกด้วยทางบริษัทวุฒิศักดิ์คลินิก อินเตอร์กรุ๊ปจำกัด จึงได้มีการนำการส่งข้อมูลผ่านระบบเครือข่ายมาใช้ในองค์กร เพื่อความสะดวกรวดเร็วในการปฏิบัติงานทางด้านต่าง ๆ

เนื่องจากในปัจจุบันได้มีปัญหาภัยคุกคามในเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็นการขโมยข้อมูล การโจมตี ทำลาย ทำให้เกิดความเสียหายต่างๆ จึงจำเป็นต้องมีการบันทึกข้อมูลจราจรคอมพิวเตอร์เพื่อพิสูจน์ตัวตนของผู้บุกรุก อีกทั้งยังสามารถนำไปใช้ในการสืบสวนและสอบสวนหาผู้กระทำความผิดมาลงโทษ และทางผู้บริหารของบริษัทวุฒิศักดิ์คลินิก อินเตอร์กรุ๊ปจำกัดมีความต้องการทราบถึงข้อมูลการใช้งานอินเทอร์เน็ตของพนักงานภายในบริษัทเนื่องจากการใช้งานอินเทอร์เน็ตเป็นไปอย่างแพร่หลายและยากต่อการควบคุม ซึ่งผู้บริหารต้องการให้พนักงานใช้อินเทอร์เน็ตเพื่อใช้ในการปฏิบัติงานที่ได้รับมอบหมายเท่านั้นจึงจำเป็นต้องมีรายงานการใช้งานอินเทอร์เน็ตของพนักงานแต่ละคนเพื่อรายงานให้ทางผู้บริหารได้ทราบด้วย

แต่ข้อมูลจราจรทางคอมพิวเตอร์นั้นถูกเก็บในลักษณะข้อมูลดิบ (Raw Data) ซึ่งยากต่อการนำไปวิเคราะห์และค้นหาปัญหาของระบบเครือข่ายจึงจำเป็นต้องพัฒนาระบบรายงานขึ้นมาควบคู่กับการเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วย เพื่อให้เห็นภาพรวมระบบปัจจุบัน แนวโน้มปัญหาและเพื่อกำหนดแผนการดูแลหรือพัฒนาระบบเครือข่ายให้เหมาะกับการใช้งานที่แท้จริง

1.2 วัตถุประสงค์ของโครงงาน

ระบบงานนี้พัฒนาขึ้นเพื่อใช้เก็บข้อมูลจราจรคอมพิวเตอร์ของพนักงานภายในบริษัท และเป็นเครื่องมือเพื่อใช้สร้างรายงาน และวิเคราะห์พฤติกรรมการใช้งานระบบเครือข่ายของพนักงานภายในองค์กร โดยมีวัตถุประสงค์ดังนี้

1.เพื่อจัดเก็บข้อมูลจราจรคอมพิวเตอร์ของพนักงานในบริษัท

2.เพื่อนำข้อมูลจราจรคอมพิวเตอร์ไปใช้วิเคราะห์ถึงพฤติกรรมการใช้งานระบบเครือข่ายของพนักงานในบริษัท

3.เพื่อนำพฤติกรรมการใช้งานระบบเครือข่ายของพนักงานที่ไม่เหมาะสมไปรายงานแก่ผู้บริหาร

1.3 ขอบเขตของโครงงาน

จากการศึกษาพฤติกรรมการส่งข้อมูลของพนักงานในบริษัท และจากโครงสร้างระบบเครือข่ายขององค์กร นำไปสู่การพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ เพื่อให้ระบบสามารถเก็บข้อมูลได้ครอบคลุม และลดปัญหาภัยคุกคามต่างๆ อีกทั้งยังช่วยทำให้การแก้ปัญหาในระบบเครือข่ายเป็นไปอย่างรวดเร็วยิ่งขึ้น โดยระบบแบ่งออกเป็น 3 ส่วน ดังนี้

1. การบันทึกการใช้งานของพนักงาน โดยที่ระบบจะต้องสามารถบันทึกการใช้งานของพนักงานได้ไม่น้อยกว่า 90 วัน เพื่อที่จะสามารถใช้อ้างอิงและสืบค้นภายหลังได้

2. การแสดงผลการใช้งานตามเวลาจริง (Real Time) ระบบจะต้องแสดงผลการใช้งานตามเวลาจริง (Real Time) ของพนักงานภายในองค์กรได้ เพื่อที่ทางผู้ดูแลระบบจะสามารถตรวจสอบหรือวิเคราะห์ถึงปัญหาที่เกิดขึ้นภายในองค์กรได้

3. การแสดงผลรายงานการใช้งานย้อนหลัง ระบบจะต้องสามารถแสดงผลรายงานการใช้งานของพนักงานย้อนหลัง เพื่อที่ทางผู้ดูแลระบบจะสามารถนำมาใช้วิเคราะห์ถึงปัญหาที่เกิดขึ้น และสามารถนำรายงานการใช้งานของพนักงานในองค์กรไปรายงานยังผู้บริหารได้

1.4 ประโยชน์ที่คาดว่าจะได้รับ

การพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์มีความคาดหมายถึงประโยชน์ที่จะได้รับดังนี้

1. ป้องกันหรือยืนยันตัวบุคคลที่กระทำในสิ่งที่ไม่สมควรในเครือข่ายขององค์กร

2. ลดปริมาณการใช้อินเทอร์เน็ตขององค์กรอย่างผิดวัตถุประสงค์

3. ความเร็วในการใช้งานอินเทอร์เน็ตขององค์กรเพิ่มมากขึ้น

4. ผู้ดูแลระบบและผู้บริหารสามารถจัดหานโยบายที่มีความเหมาะสมต่อการใช้งาน

5. ผู้ดูแลระบบเครือข่ายสามารถวิเคราะห์ปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว

ขั้นตอนการพัฒนาระบบ

1. ศึกษาความต้องการและความเป็นไปได้ของการพัฒนาระบบ

2. วิเคราะห์รายละเอียดต่างๆ ของระบบเครือข่ายในองค์กรว่าสามารถนำมาใช้กับระบบที่จะทำได้หรือไม่

3. ออกแบบโครงสร้างและฐานข้อมูลระบบ

4. พัฒนาระบบและจัดเก็บความรู้

5. ทำการติดตั้งและทดสอบระบบ

6. ตรวจสอบและควบคุมการทำงานของระบบ

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

การออกแบบและพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้ใช้แนวคิดในการพัฒนาในรูปแบบของเว็บแอพพลิเคชัน ซึ่งเป็นการแสดงผลบนหน้าเว็บเพจ โดยระบบจะทำการเก็บข้อมูลจราจรคอมพิวเตอร์มาจากจุดต่อเชื่อมของเครือข่ายจากนั้นเปลี่ยนข้อมูลที่ได้ให้อยู่ในรูปแบบข้อมูลเชิงสัมพันธ์ และทำการแสดงผลผ่านเว็บเพจ โดยการออกแบบและพัฒนาระบบได้นำหลักการทฤษฎีและเทคโนโลยีสาคัญที่เกี่ยวข้อง ดังต่อไปนี้

2.1 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ คือ การเก็บข้อมูลที่เกี่ยวข้องเฉพาะส่วนกำกับของข้อมูล (Message Header) ที่เกิดเหตุการณ์ขึ้นในการใช้งานอินเทอร์เน็ตหรือข้อมูลในการใช้งานระบบเครือข่าย เช่น บันทึกวันเวลา, หมายเลข IP ผู้ส่งข้อมูล, หมายเลข IP ผู้รับข้อมูล ซึ่งไม่ได้รวมไปถึงการจัดเก็บตัวข้อมูลหรือเนื้อความที่ผู้ใช้งานมีการรับส่งในขณะนั้นๆ เนื่องจากการกระทำดังกล่าวจะมีความผิดฐานละเมิดสิทธิส่วนบุคคล และ มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ถึงมาตรา 10 ที่ว่าด้วยเรื่องแอบดูข้อมูลโดยใช้โปรแกรมดักจับข้อมูลที่วิ่งผ่านเครือข่าย ดังนั้นในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นี้จึงไม่มีการเก็บตัวข้อมูลหรือเนื้อความที่ถูกส่ง จะมีเพียงการเก็บข้อมูลที่เกิดขึ้นในระบบคอมพิวเตอร์ ที่โปรแกรมหรืออุปกรณ์มีการสร้างขึ้นเพื่อบันทึกการทำงาน หรือที่เรียกว่า Log File เท่านั้น ซึ่งในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้จัดเก็บข้อมูลส่วนต่างๆดังต่อไปนี้

1. Host หมายถึง อุปกรณ์ที่ทำหน้าที่เป็นจุดต่อเชื่อมของเครือข่าย (Gateway) โดยระบบจะทำการบันทึกหมายเลข IP Address ว่า Log File นั้นส่งมาจาก Host ใด

2. Priority หมายถึง ระดับความอันตรายของพฤติกรรมในการใช้งานซึ่งโดยปกติแล้วจะมีทั้งหมด 8 ขั้น คือ Debug,Information,Notification,Warning,Error,Critical,Alert,Emergency โดยรายชื่อดังกล่าวไล่เรียงตามระดับความรุนแรง

3. Date/Time หมายถึง วันและเวลา ที่มีการส่ง Log File มายังระบบ

4. Message หมายถึง ข้อมูลที่เกี่ยวข้องเฉพาะส่วนกำกับของข้อมูล โดยข้อมูลในส่วนนี้จะมีเพียง หมายเลข IP ของผู้ส่ง, IP หรือชื่อ Domain ของผู้รับ, Port ที่ใช้ในการเชื่อมต่อเท่านั้น

โดยเมื่อนำข้อมูลส่วนต่างๆที่กล่าวมาข้างต้นมารวมกัน ผู้ดูแลระบบจะสามารถตรวจสอบพฤติกรรมในการใช้งานระบบเครือข่ายของพนักงานในองค์กรได้ เช่น ตรวจดูประวัติในการเข้าใช้งานเว็บไซต์ Facebook ของพนักงานย้อนหลังในระยะเวลา 7 วันที่ผ่านมา เป็นต้น ซึ่งกระบวนการดังกล่าวสามารถนำไปใช้วิเคราะห์ปัญหาที่เกิดขึ้นหรือนำไปใช้สนับสนุนการตัดสินใจของผู้บริหารเพื่อกำหนดนโยบายในการใช้งานอินเทอร์เน็ตของพนักงานในองค์กร เพื่อให้พนักงานในองค์กรทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.1.1 Syslog

Syslog เป็นมาตรฐานในการส่งข้อมูลจราจรคอมพิวเตอร์ในเครือข่ายอินเทอร์เน็ตโปรโตคอล (IP Network) โดยมีการทำงานแบบ ลูกข่าย และ แม่ข่าย (Client/Server) โดยที่ Syslog จะส่งข้อความที่เป็นตัวอักษรไปที่ผู้รับ โดยที่สามารถส่งผ่านได้ทั้งในโปรโตคอล UDP และ TCP ซึ่งในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นี้ ผู้พัฒนาได้ใช้โปรแกรม Syslog-ng เป็นโปรแกรมในการส่งข้อมูล Log File จาก Gateway มายังระบบ

2.2 การออกแบบฐานข้อมูล

เนื่องจากการที่ในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้นใช้ Syslog ในการส่งข้อมูล Log File จึงทำให้ข้อมูลที่ได้อยู่ในรูปแบบข้อมูลดิบ จึงจำเป็นต้องเปลี่ยนรูปแบบการจัดเก็บข้อมูลใหม่ เนื่องจากข้อมูลที่อยู่ในรูปแบบข้อมูลดิบไม่สามารถแสดงผลผ่านเว็บแอพพลิเคชั่น อีกทั้งยังไม่สามารถสืบค้นย้อนหลังหรือสืบค้นเฉพาะข้อมูลที่ต้องการได้ ซึ่งรายละเอียดของขั้นตอนการออกแบบฐานข้อมูลมีดังต่อไปนี้ (Captain, 2012)

1. พิจารณาข้อมูลนำเข้าและส่งออกของระบบ เพื่อวิเคราะห์ข้อมูลที่จำเป็นต้องจัดเก็บในฐานข้อมูล

2. วิเคราะห์โครงสร้างของแต่ละข้อมูลเพื่อพิจาณาถึงรูปแบบ ชนิดข้อมูล และค่าที่เป็นไปได้ของข้อมูลแต่ละตัว

3. วิเคราะห์เอนทิตีและแอตทริบิวต์ที่เป็นคุณลักษณะของแต่ละเอนทิตี

4. พิจารณาเงื่อนไขหรือรูปแบบการดำเนินการของธุรกิจ เพื่อกำหนดความสัมพันธ์ระหว่างเอนทิตี

5. สร้างแบบจำลองข้อมูลแสดงความสัมพันธ์ของแต่ละเอนทิตีทั้งหมดในระบบ โดยสามารถแบ่งแบบจำลองข้อมูลออกเป็น 3 ระดับ ดังนี้ (Coronel Morris, and Rob, 2011)

5.1 การออกแบบระดับแนวคิด เป็นแบบจำลองที่แสดงโครงสร้างโดยรวมของระบบฐานข้อมูล ประกอบด้วย เอนทิตี และความสัมพันธ์ระหว่างเอนทิตี ซึ่งสอดคล้องกับรูปแบบการดำเนินการของธุรกิจ โดยถูกนำเสนออยู่ในรูปแบบแผนภาพอีอาร์ การออกแบบระดับแนวคิดนี้จะไม่ขึ้นกับซอฟแวร์และฮาร์ดแวร์

5.2 การออกแบบระดับตรรกะ เป็นแบบจำลองที่นำการออกแบบระดับแนวคิดมาทำให้เป็นแบบจำลองข้อมูลเชิงตรรกะตามระบบจัดการฐานข้อมูลที่เลือกใช้ ซึ่งระบบจัดการจัดเก็บข้อมูลจราจรคอมพิวเตอร์เลือกใช้ระบบฐานข้อมูลมายเอสคิวแอล ดังนั้นจึงถือได้ว่า แบบจำลองระดับตรรกะขึ้นกับซอฟต์แวร์แต่ไม่ขึ้นกับฮาร์ดแวร์

5.3 การออกแบบระดับกายภาพ เป็นแบบจำลองเพื่อการนำไปพัฒนา จึงต้องคำนึงถึงซอฟต์แวร์ ฮาร์ดแวร์ รวมไปถึงเทคโนโลยีที่นำมาพัฒนาร่วมกับระบบฐานข้อมูล เพื่อพิจารณาวิธีการจัดเก็บหรือการเข้าถึงข้อมูลในฐานข้อมูล

6. ตรวจสอบความถูกต้องและปรับแก้แผนภาพอีอาร์ตามหลักการนอร์มัลไลเซชัน เพื่อให้ได้ฐานข้อมูลที่มีความความซ้ำซ้อนน้อยที่สุด และสามารถนำไปใช้ได้จริง โดยแผนภาพอีอาร์ของระบบจัดการบริการไอเอสพีนั้นจะปรับแก้แผนภาพตามหลักการนอร์มัลไลเซชันระดับ 3 เป็นอย่างน้อย

2.2.1 ระบบจัดการฐานข้อมูลมายเอสคิวแอล

ระบบจัดการฐานข้อมูลของโครงการนี้เลือกใช้มายเอสคิวแอล (MySQL) ซึ่งเป็นซอฟต์แวร์ประเภทซอฟต์แวร์ที่เปิดเผยคำสั่ง (Open Source) สำหรับจัดการฐานข้อมูลของระบบ เนื่องด้วยคุณสมบัติของมายเอสคิวแอล ดังนี้ (พร้อมเลิศ หล่อวิจิตร, 2550)

1. สามารถทำงานร่วมกับพีเอชพีสาหรับพัฒนาเว็บแอพพลิเคชัน

2. สนับสนุนการใช้งานบนระบบปฏิบัติการลีนุกซ์

3. สามารถทำงานร่วมกับอาปาเชเว็บเซิร์ฟเวอร์

4. รองรับชนิดข้อมูลประเภทต่าง ๆ

2.3 การพัฒนาเว็บแอพพลิเคชัน

ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์จะแสดงผลข้อมูลในรูปแบบไคลเอนท์-เซิร์ฟเวอร์ โดยผู้ดูแลระบบสามารถดูข้อมูลจราจรคอมพิวเตอร์ผ่านทางเว็บบราวเซอร์ ซึ่งเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาระบบนี้ ประกอบด้วย

1. เอชทีเอ็มแอล (HTML) ระบบในโครงการนี้ใช้ภาษาเอชทีเอ็มแอลเป็นพื้นฐานในการพัฒนาเว็บเพจโดยใช้ในการแสดงผลส่วนที่ไม่มีการเปลี่ยนแปลง หรือแม้กระทั่งการพัฒนาเว็บเพจด้วยภาษาสคริปต์ที่ประมวลผลฝั่งเซิร์ฟเวอร์ เช่น พีเอชพี ก็จำเป็นต้องใช้เอชทีเอ็มแอลช่วยในการแสดงผลในเว็บบราวเซอร์ เพราะเอชทีเอ็มแอลถือว่าเป็นภาษามาตรฐานในการแสดงผลในเว็บบราวเซอร์ทุกชนิด

2. พีเอชพี (PHP) คือ ภาษาในกลุ่มประมวลผลฝั่งเซิร์ฟเวอร์โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษาซีซึ่งใช้ในการพัฒนาเว็บแอพพลิเคชันประเภทที่สามารถตอบโต้กับผู้ใช้งานได้ โดยพีเอชพีจะใช้ในส่วนของการจัดเก็บหรือเรียกดูข้อมูลจากฐานข้อมูล

ด้วยลักษณะเด่นของพีเอชพีเมื่อเปรียบเทียบกับภาษาอื่น ๆ ในกลุ่มเดียวกัน พีเอชพีสามารถทำงานร่วมกับภาษาพื้นฐานในการพัฒนาเว็บเพจอย่างเอชทีเอ็มแอล โดยสามารถสอดแทรกลงไปได้ในทุกส่วนของเว็บเพจ อีกทั้งยังสามารถทำงานร่วมกับฐานข้อมูลมายเอสคิวแอล อาปาเชเว็บเซิร์ฟเวอร์ และระบบปฏิบัติการลีนุกซ์ได้อีกด้วย ดังนั้น ระบบนี้จึงใช้พีเอชพีในการพัฒนาระบบส่วนประมวลผล และแสดงผล (พร้อมเลิศ หล่อวิจิตร, 2550)

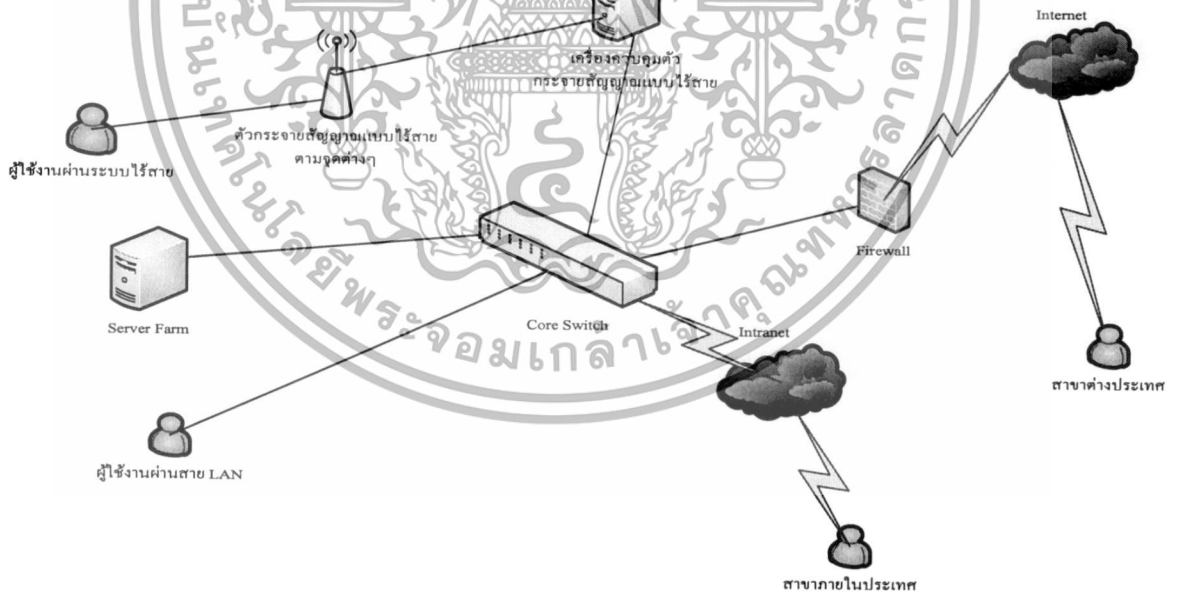
3. อาปาเชเว็บเซิร์ฟเวอร์ (Apache) คือ ซอฟต์แวร์ประเภทซอฟต์แวร์ที่เปิดเผยคำสั่งสำหรับให้บริการเว็บเซิร์ฟเวอร์ ทำหน้าที่จัดเก็บและให้บริการเว็บเพจแก่ผู้ใช้ อาปาเชเว็บเซอร์เวอร์สามารถทำงานได้บนระบบปฏิบัติการที่หลากหลาย รวมไปถึงลีนุกซ์ซึ่งเป็นระบบปฏิบัติการที่ใช้ในการติดตั้งระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ นอกจากนั้นอาปาเชยังสามารถใช้ได้กับภาษาในการพัฒนาเว็บแอพพลิเคชันซึ่งใช้พัฒนาระบบของโครงการนี้ ดังที่ได้กล่าวไว้ในตอนต้น อีกทั้งยังสนับสนุนการเชื่อมต่อกับระบบจัดการฐานข้อมูลมายเอสคิวแอลที่ใช้จัดเก็บข้อมูลในระบบ

บทที่ 3

การวิเคราะห์กระบวนการปฏิบัติงานปัจจุบัน

ในการพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์โดยการศึกษา วิเคราะห์พฤติกรรมการส่งข้อมูลผ่านระบบเครือข่ายของบุคลากรภายในองค์กร ทำให้ทราบถึงเส้นทางต่างๆที่ใช้ในการส่งข้อมูล ผู้พัฒนาจึงได้ทำการวิเคราะห์และออกแบบระบบจัดการการจราจรข้อมูลให้ครอบคลุมการส่งข้อมูลของบุคลากรในเส้นทางต่างๆ เพื่อให้เกิดประสิทธิภาพและลดปัญหาต่างๆในการส่งข้อมูลผ่านระบบเครือข่ายโดยมีรายละเอียดดังนี้

3.1 โครงสร้างภาพรวมของการส่งข้อมูลผ่านระบบเครือข่ายขององค์กร



ภาพที่ 3.1 แผนภาพแสดงการส่งข้อมูลผ่านระบบเครือข่าย

จากภาพที่ 3.1 แสดงการส่งข้อมูลผ่านระบบเครือข่ายจะเห็นได้ว่ามีเส้นทางการส่งข้อมูลผ่านระบบเครือข่ายทั้งหมด 5 เส้นทางดังต่อไปนี้

1. เส้นทางที่ใช้ติดต่อไปยังผู้ใช้งานผ่านสาย LAN

2. เส้นทางที่ใช้ติดต่อไปยังผู้ใช้งานผ่านระบบไร้สาย

3. เส้นทางที่ใช้ติดต่อไปยัง Server Farm

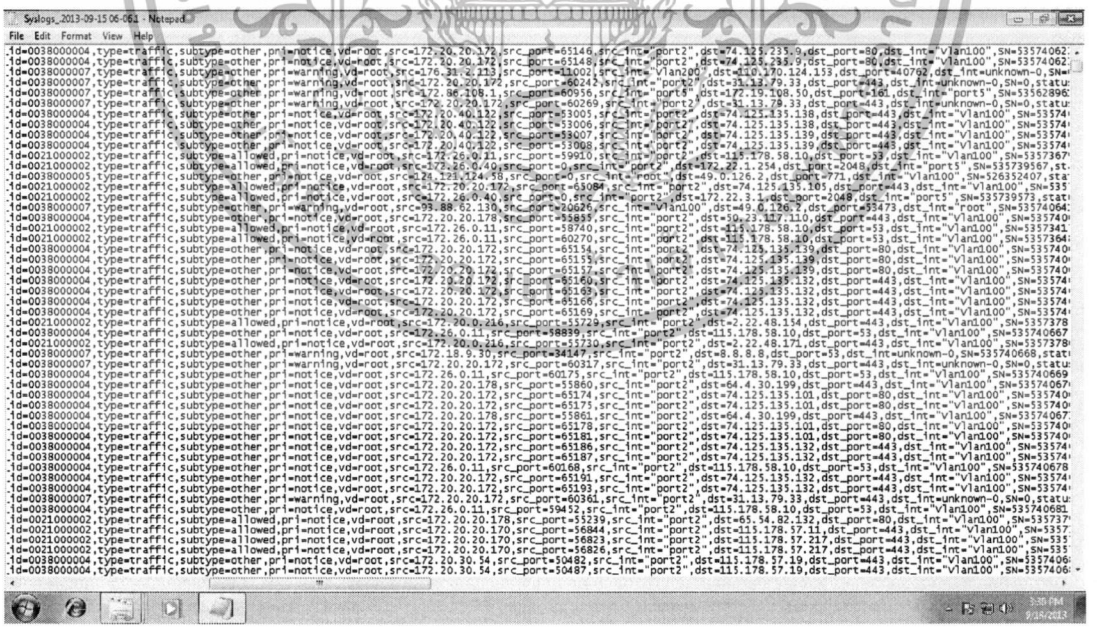
4. เส้นทางที่ใช้ติดต่อไปยังสาขาภายในประเทศ

5. เส้นทางที่ใช้ติดต่อไปยังสาขาต่างประเทศ

ซึ่งในการพัฒนาระบบระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้น จำเป็นที่จะต้องทำการออกแบบการโครงสร้างในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ใหม่ ซึ่งจะพูดถึงในบัทถัดไป

3.2 ระบบการจัดเก็บข้อมูลและการแสดงผลรายงานในปัจจุบัน

ในการส่งข้อมูลจราจรจาก Firewall นั้นข้อมูลจะถูกจัดเก็บไปยังเครื่องที่ทำการติดตั้งโปรแกรมที่ใช้ในการจัดเก็บ Syslog ซึ่งจะใช้สำหรับจัดเก็บข้อมูลดิบ <Raw File> ซึ่งรูปแบบในการจัดเก็บนั้นยากต่อการนำไปใช้งาน



ภาพที่ 3.2 ตัวอย่างข้อมูลดิบที่เก็บอยู่ใน Syslog server

3.3 ปัญหาของระบบงานปัจจุบัน

จากการศึกษาระบบการจัดเก็บข้อมูลและการแสดงผลรายงานในปัจจุบันแสดงให้เห็นถึงปัญหาหลายประการ ดังนี้

3.3.1 การสืบค้นข้อมูลย้อนหลัง

เนื่องจากระบบการจัดเก็บข้อมูลและการแสดงผลรายงานในปัจจุบันอยู่ในรูปแบบข้อมูลดิบ <Raw File> ซึ่งการแสดงผลรายงานดังกล่าวยากต่อการสืบค้นและนำไปวิเคราะห์ถึงปัญหาต่างๆที่เกิดขึ้น ซึ่งถือเป็นรูปของรายงานที่ไม่เหมาะสม เนื่องจากไม่สามารถนำไปใช้งานให้เกิดประโยชน์ได้จริง

3.3.2 การตรวจสอบการใช้งานตามเวลาจริง

เนื่องจากในระบบปัจจุบันไม่มีการแสดงผลการใช้งานตามเวลาจริง (Real Time) เมื่อเกิดปัญหาภายในระบบเครือข่ายขององค์กรจึงไม่สามารถวิเคราะห์ถึงปัญหาที่เกิดขึ้น และไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ภายในทันที ทำให้ส่งผลกระทบถึงหน่วยงานอื่นๆภายในองค์กร จึงอาจเป็นสาเหตุที่ทำให้องค์กรสูญเสียรายได้ในช่วงเวลาดังกล่าว

3.3.3 การแสดงผลเฉพาะข้อมูลที่ต้องการ

เนื่องจากระบบการจัดเก็บข้อมูลและการแสดงผลรายงานในปัจจุบันอยู่ในรูปแบบข้อมูลดิบ <Raw File> ซึ่งการแสดงผลรายงานดังกล่าวไม่สามารถแสดงผลออกมาในลักษณะรูปแบบของการสืบค้นสิ่งที่ต้องการได้ ทำให้ผู้ดูแลระบบไม่สามารถวิเคราะห์ถึงปัญหาที่เกิดขึ้นในอดีต ทำให้ยากต่อการหามาตรการที่จะใช้ป้องกันปัญหาที่จะเกิดขึ้นในอนาคตได้

3.4 แนวทางการแก้ปัญหา

เนื่องจากปัญหาที่เกิดขึ้นในปัจจุบันมีสาเหตุมาจากระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการแสดงผลข้อมูลเป็นหลักจึงต้องมีการพัฒนาระบบสารสนเทศขึ้นเพื่อให้เอื้อต่อกระบวนการจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการแสดงผล และสามารถเพิ่มประสิทธิภาพในการสืบค้นข้อมูลการใช้งานระบบเครือข่ายของพนักงานในองค์กร ตรวจสอบและวิเคราะห์ถึงปัญหาการส่งข้อมูลภายในองค์กร รวมถึงสามารถนำไปใช้วิเคราะห์ถึงปัญหาและออกมาตรการเพื่อป้องกันปัญหาที่จะเกิดขึ้นในอนาคตให้ดียิ่งขึ้น โดยออกแบบให้ระบบครอบคลุมกระบวนการ การจัดเก็บ

ข้อมูลจราจรคอมพิวเตอร์ในปัจจุบัน และปรับปรุงการแสดงผลรายงานการใช้งานระบบเครือข่ายของพนักงานในองค์กร ทั้งนี้เพื่อลดเวลาในการวิเคราะห์และแก้ไขปัญหาที่เกิดจากการส่งข้อมูลในระบบเครือข่าย ป้องกันการเกิดปัญหาในระบบเครือข่ายที่จะเกิดขึ้นในอนาคต เพิ่มความสะดวกรวดเร็วในการสืบค้นข้อมูลการใช้งานระบบเครือข่ายของพนักงานในองค์กร นอกจากนั้นยังสามารถสร้างรายงานการใช้งานระบบเครือข่ายของพนักงานภายในองค์กรเพื่อนำไปให้ผู้บริหารใช้ประกอบการตัดสินใจในการออกมาตรการการใช้งานระบบเครือข่ายในองค์กรได้ ซึ่งการวิเคราะห์และออกแบบระบบใหม่จะได้กล่าวถึงในบทถัดไป

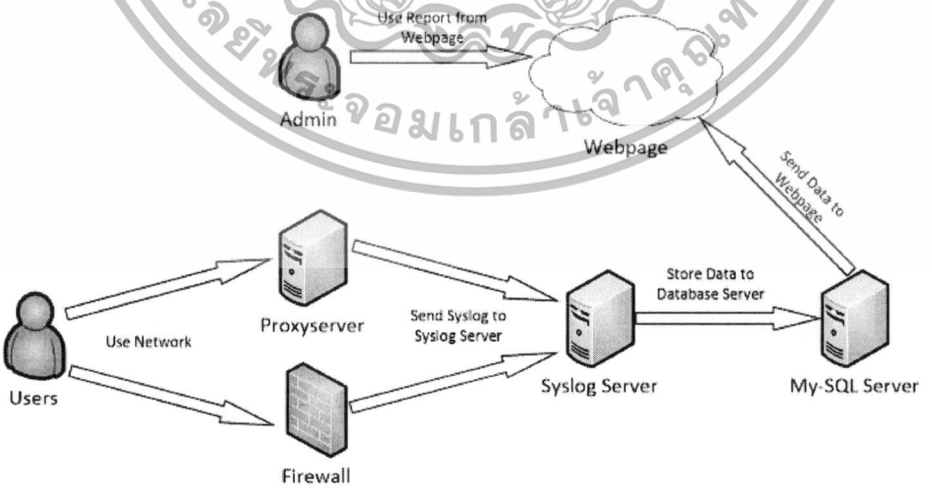
บทที่ 4

การวิเคราะห์และออกแบบระบบใหม่

จากการศึกษาและวิเคราะห์การทำงานของระบบปัจจุบัน จะเห็นได้ว่าข้อมูลจราจรคอมพิวเตอร์ที่ได้ยากต่อการนำไปวิเคราะห์และใช้งาน จึงจำเป็นต้องใช้การจัดเก็บข้อมูลในฐานข้อมูลและทำการแสดงผลในรูปแบบของเว็บเพจ ซึ่งการจัดเก็บข้อมูลและแสดงผลดังกล่าวจะทำให้ง่ายต่อการสืบค้นและวิเคราะห์ถึงปัญหาที่เกิดขึ้น โดยมีรายละเอียดดังนี้

4.1 โครงสร้างรวมของระบบ

สำหรับระบบระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้น จะทำการเก็บข้อมูลจราจรคอมพิวเตอร์มาจากจุดต่อเชื่อมของเครือข่าย (Gateway) ซึ่งในโครงสร้างของระบบการจัดเก็บข้อมูลนั้นจะมี Gateway ทั้งหมด 2 จุด (Node) ซึ่งในที่ละ Node นั้น จะทำการเก็บข้อมูลจราจรคอมพิวเตอร์ในส่วนของตนเอง แล้วจึงทำการส่งข้อมูลจราจรคอมพิวเตอร์มารวมกันที่ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยระบบจะทำการจัดเก็บข้อมูลและส่งต่อไปยังฐานข้อมูลโดยระบบนี้จะใช้ MySQL เป็นตัวจัดการฐานข้อมูล และนำออกมาแสดงผลในรูปแบบของเว็บเพจ ซึ่งทำให้ผู้ดูแลระบบได้ใช้เพื่อวิเคราะห์ข้อมูล โดยผู้ดูแลระบบสามารถเข้าถึงการแสดงผลข้อมูลได้ด้วยอุปกรณ์ที่รองรับการทำงานเว็บแอพพลิเคชั่น ซึ่งส่วนประกอบของระบบงานมีการสรุปเป็นยูสเคสไดอะแกรม ไดอะแกรมแสดงลำดับการทำงาน และพจนานุกรมข้อมูล ดังนี้

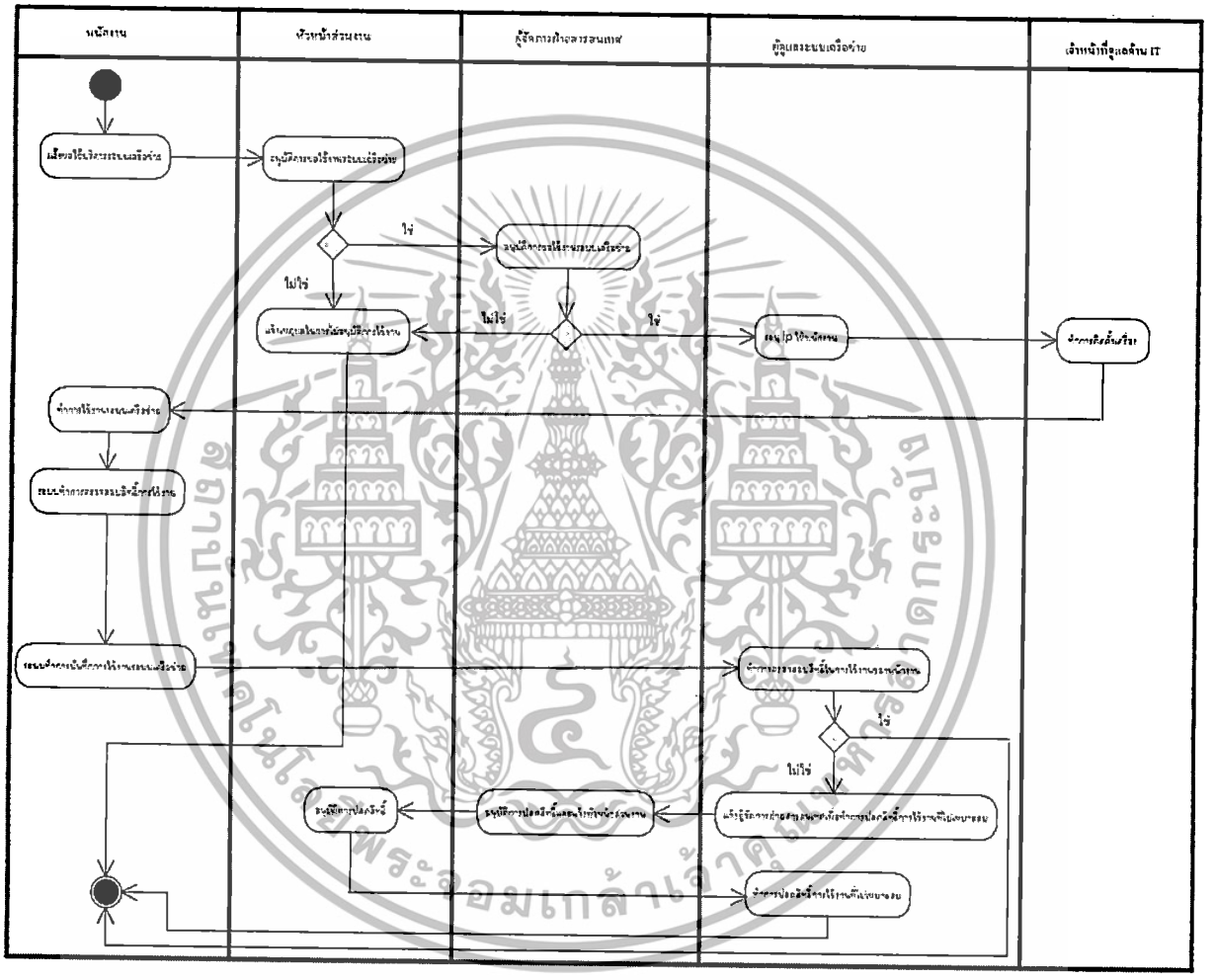


ภาพที่ 4.1 โครงสร้างภาพรวมของระบบ

4.2 แอกทิวิตีไดอะแกรม

การวิเคราะห์และออกแบบระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยอาศัยเครื่องมือในการจำลองแบบด้วย ยูเอ็มแอล แสดงรายละเอียดของระบบเพื่อช่วยสื่อสารกับผู้เกี่ยวข้องให้เข้าใจ

กระบวนการทำงาน โดยใช้แผนภาพแอกทิวิตีไดอะแกรม ดังภาพที่ 4.2 เป็นการแสดงกระบวนการทำงาน โดยสัมพันธ์กับหน้าที่ของแต่ละส่วนงาน โดยมีรายละเอียดดังนี้



ภาพที่ 4.2 แอกทิวิตีไดอะแกรมแสดงขั้นตอนการใช้งานระบบเครือข่ายของพนักงาน

4.3 ยูสเคสไดอะแกรม

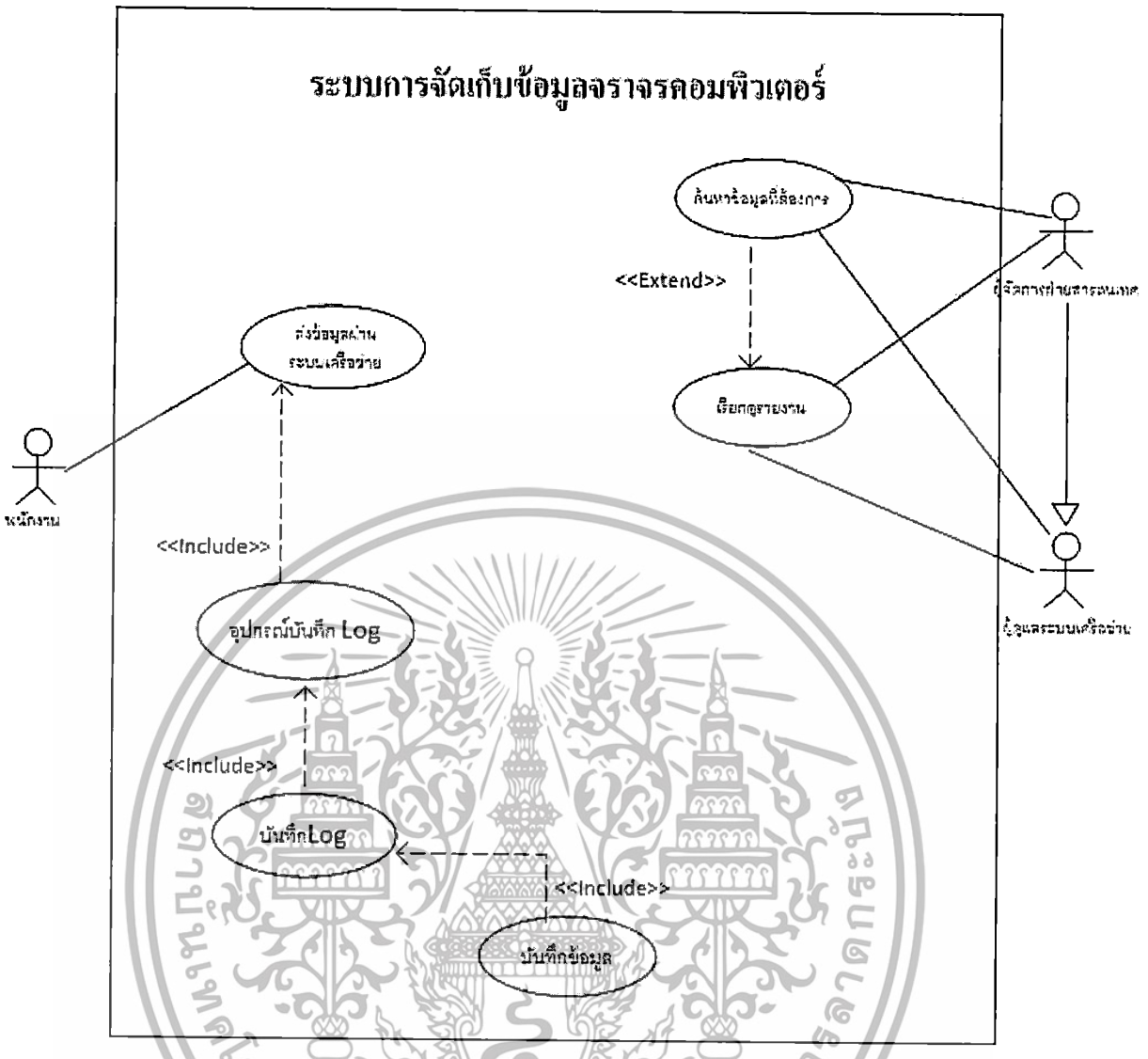
การวิเคราะห์และออกแบบระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยอาศัยเครื่องมือในการจำลองแบบด้วย ยูเอ็มแอล แสดงรายละเอียดของระบบเพื่อช่วยสื่อสารกับผู้เกี่ยวข้องให้เข้าใจกระบวนการทำงาน โดยใช้แผนภาพ ยูสเคสไดอะแกรม ดังรูปที่ 4.3 เป็นการแสดงแอกเตอร์ที่เข้ามาใช้ระบบ และใช้ยูสเคสใดของระบบ โดยมีรายละเอียดดังนี้

1. **พนักงาน** คือ บุคลากรทุกคนในองค์กร เมื่อบุคลากรในองค์กรมีการส่งข้อมูลผ่านระบบเครือข่าย จุดต่อเชื่อมของเครือข่าย (Gateway) จะทำการตรวจสอบสิทธิ์ในการใช้งานและส่งข้อมูลจราจรคอมพิวเตอร์เป็นข้อมูลดิบไปยังเครื่องบันทึกข้อมูล

2. **ผู้จัดการฝ่ายสารสนเทศ** คือ บุคลากรที่มีหน้าที่ตรวจสอบรายงานการใช้งานระบบเครือข่ายเพื่อนำไปวิเคราะห์และกำหนดนโยบายการใช้งานระบบเครือข่ายให้กับบุคลากรในองค์กร

3. **ผู้ดูแลระบบเครือข่าย** คือบุคลากรที่มีหน้าที่กำหนดสิทธิ์ในการใช้งานเครือข่ายให้กับพนักงานทุกงานทุกคนในองค์กร โดยการกำหนดสิทธิ์นี้เพื่อสนองนโยบายการใช้งานระบบเครือข่ายที่ได้รับมอบหมายจากผู้จัดการฝ่ายสารสนเทศ และกำหนดว่าข้อมูลส่วนไหนในข้อมูลดิบมีความจำเป็นต้องใช้ในรายงาน และมีหน้าที่ตรวจสอบรายงานการใช้งานอินเทอร์เน็ต เพื่อนำไปวิเคราะห์ถึงปัญหาที่เกิดจากการส่งข้อมูลในระบบเครือข่าย

แผนภาพแสดง ผู้เกี่ยวข้อง กับระบบต่าง ๆ ของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และตารางรายละเอียดการทำงานของแต่ละยูสเคส



ภาพที่ 4.3 ยูสเคสไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ยูสเคสของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ซึ่งแสดงรายละเอียดการทำงานของระบบ ดังต่อไปนี้

1. ยูสเคสส่งข้อมูลผ่านระบบเครือข่าย คือ กระบวนการ การใช้งานส่งข้อมูลผ่านระบบเครือข่ายของบุคลากรทุกคนในองค์กร เช่น การใช้งานอินเทอร์เน็ต,การส่ง E-Mail,การติดต่อสื่อสารกับเครื่องแม่ข่ายในระบบต่างๆขององค์กร

2. ยูสเคสอุปกรณ์บันทึก Log คือ กระบวนการบันทึกข้อมูลจราจรคอมพิวเตอร์ของจุดต่อเชื่อมของเครือข่าย (Gateway) ซึ่งในโครงสร้างของระบบการจัดเก็บข้อมูลนั้นจะมี Gateway ทั้งหมด 2 จุด (Node) ซึ่งในที่ละ Node นั้น จะทำการเก็บข้อมูลจราจรคอมพิวเตอร์ในส่วนของตนเอง ซึ่ง Gateway ดังกล่าวจะมีการบันทึกข้อมูลจราจรคอมพิวเตอร์โดยอัตโนมัติ

3. **ยูสเคสบันทึก Log** คือ กระบวนการส่งข้อมูล Log จากจุดเชื่อมต่อของเครือข่ายมายังเครื่องบันทึกข้อมูลจราจรคอมพิวเตอร์ โดยกระบวนการดังกล่าวระบบจะทำการบันทึกข้อมูลโดยอัตโนมัติ โดยใช้โปรแกรม syslog-ng เป็นโปรแกรมเรียกเก็บข้อมูล Log จาก Gateway

4. **ยูสเคสบันทึกข้อมูล** คือ กระบวนการบันทึกข้อมูลให้อยู่ในรูปแบบข้อมูลเชิงสัมพันธ์ที่ได้จากเครื่องบันทึกข้อมูลจราจรคอมพิวเตอร์ลงไปในฐานข้อมูล โดยในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้นใช้ MySQL Server เป็นฐานข้อมูลของระบบ โดยระบบจะทำการบันทึกข้อมูลโดยอัตโนมัติ โดยใช้โปรแกรม syslog-ng เป็นโปรแกรมในการเพิ่มข้อมูลลงไปในฐานข้อมูล

5. **ยูสเคสเรียกดูรายงาน** คือ กระบวนการที่ผู้ดูแลระบบเครือข่ายหรือผู้จัดการฝ่ายสารสนเทศทำการเรียกดูรายงานข้อมูลจราจรคอมพิวเตอร์ผ่านระบบแบบการใช้งานตามเวลาจริง เพื่อใช้หาสาเหตุของปัญหาที่เกิดขึ้น ณ ปัจจุบัน โดยระบบจะแสดงผลข้อมูลจราจรคอมพิวเตอร์ผ่านเว็บเพจ

6. **ยูสเคสค้นหาข้อมูลที่ต้องการ** คือ กระบวนการที่ผู้ดูแลระบบเครือข่ายหรือผู้จัดการฝ่ายสารสนเทศทำการเรียกดูรายงานข้อมูลจราจรคอมพิวเตอร์ผ่านตัวกรองข้อมูลที่ต้องการ เช่น ต้องการดูข้อมูลย้อนหลัง 1 สัปดาห์ข้อพนักงานที่ใช้งานเว็บไซต์ facebook เป็นต้น

ยูสเคสไดอะแกรมที่แสดงไว้ข้างต้น มีรายละเอียดขั้นตอนการทำงานในแต่ละยูสเคส ซึ่งอธิบายเป็นตารางรายละเอียดของยูสเคสและหน้าจอการทำงานระบบ ดังนี้

ตารางที่ 4.1 รายละเอียดการทำงานของยูสเคส ส่งข้อมูลผ่านระบบเครือข่าย

ชื่อยูสเคส	ยูสเคสส่งข้อมูลผ่านระบบเครือข่าย	ID : 1
จุดประสงค์	ส่งข้อมูลผ่านระบบเครือข่าย	
รายละเอียดโดยสังเขป	กระบวนการ การใช้งานส่งข้อมูลผ่านระบบเครือข่ายของบุคลากรทุกคนในองค์กร เช่น การใช้งานอินเทอร์เน็ต,การส่ง E-Mail,การติดต่อสื่อสารกับเครื่องแม่ข่ายในระบบต่างๆขององค์กร	
แอกเตอร์	พนักงาน	
ยูสเคสที่เกี่ยวข้อง		
ผู้เกี่ยวข้องอื่น	-	
เงื่อนไขเริ่มต้น	พนักงานมีสิทธิ์ในการใช้งาน	
เงื่อนไขภายหลัง	จุดต่อเชื่อมของเครือข่าย (Gateway) บันทึกข้อมูลการใช้งานของพนักงาน	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
1. ทำการใช้งานอินเทอร์เน็ต	1.1 ตรวจสอบสิทธิ์ในการใช้งาน 1.2 Gateway บันทึกข้อมูลการใช้งาน	

ตารางที่ 4.2 รายละเอียดการทำงานของยูสเคส อุปกรณ์บันทึก Log

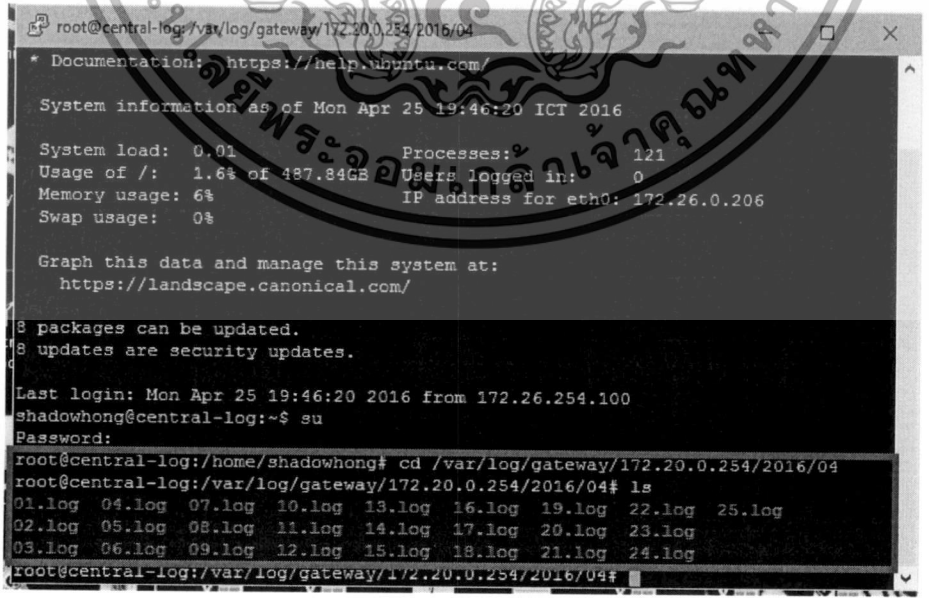
ชื่อยูสเคส	ยูสเคสอุปกรณ์บันทึก Log	ID : 2
จุดประสงค์	บันทึกข้อมูลการจราจรโดยจุดต่อเชื่อมของเครือข่าย (Gateway)	
รายละเอียดโดยสังเขป	กระบวนการบันทึกข้อมูลการจราจรคอมพิวเตอร์ของจุดต่อเชื่อมของเครือข่าย (Gateway) ซึ่งอุปกรณ์ Gateway จะทำการบันทึกข้อมูลของพนักงานโดยอัตโนมัติ	
แอกเตอร์	-	
ยูสเคสที่เกี่ยวข้อง	Include : ส่งข้อมูลผ่านระบบเครือข่าย	
ผู้เกี่ยวข้องอื่น	พนักงาน	
เงื่อนไขเริ่มต้น	มีการส่งข้อมูลผ่านระบบเครือข่ายจากพนักงาน	
เงื่อนไขภายหลัง	ส่งข้อมูลจราจรคอมพิวเตอร์ไปยังเครื่องบันทึกข้อมูล	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
-	1. ตรวจสอบอุปกรณ์ที่จะทำการส่งข้อมูลจราจรคอมพิวเตอร์มายังระบบ	

```
035 device_id=FG600B3910601035 log_id=0038000007 type=traffic subtype=other pri=
warning vd=root src=116.211.0.90 src_port=48200 src_int="Vlan100" dst=49.0.126.7
9 dst_port=8080 dst_int="Vlan100" SN=19459498 status=deny policyid=0 dst_country
="Thailand" src_country="China" service=8080/tcp proto=6 duration=0 sent=0 rcvd=
0 msg="Denied by forward policy check"
Apr 25 19:43:59 172.20.0.254 date=2016-04-25 time=19:44:06 devname=FG600B3910601
035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=
notice vd=root src=172.19.109.20 src_port=51657 src_int="port5" dst=172.26.0.11
dst_port=53 dst_int="port2" SN=19459499 status=start policyid=37 dst_country="Re
served" src_country="Reserved" service=DNS proto=17 duration=0 sent=0 rcvd=0
Apr 25 19:43:59 172.20.0.254 date=2016-04-25 time=19:44:06 devname=FG600B3910601
035 device_id=FG600B3910601035 log_id=0038000007 type=traffic subtype=other pri=
warning vd=root src=116.211.0.90 src_port=48200 src_int="Vlan100" dst=49.0.126.5
9 dst_port=3128 dst_int="Vlan100" SN=19459500 status=deny policyid=0 dst_country
="Thailand" src_country="China" service=SQUID proto=6 duration=0 sent=0 rcvd=0 m
sg="Denied by forward policy check"
Apr 25 19:43:59 172.20.0.254 date=2016-04-25 time=19:44:06 devname=FG600B3910601
035 device_id=FG600B3910601035 log_id=0021000002 type=traffic subtype=allowed pr
i=notice vd=root src=172.20.60.32 src_port=52169 src_int="port2" dst=13.107.5.80
 dst_port=80 dst_int="Vlan100" SN=19458131 status=accept policyid=56 dst_country
="United States" src_country="Reserved" dir_disp=org tran_disp=snat tran_sip=49.
0.126.2 tran_sport=59725 service=HTTP proto=6 duration=71 sent=132 rcvd=132 sent
_pkt=3 rcvd_pkt=3
Apr 25 19:43:59 172.20.0.254 date=2016-04-25 time=19:44:06 devname=FG600B3910601
```

ภาพที่ 4.4 ตัวอย่างการบันทึกข้อมูลการจราจร โดยจุดต่อเชื่อมของเครือข่าย (Gateway)

ตารางที่ 4.3 รายละเอียดการทำงานของยูสเคส บันทึก Log

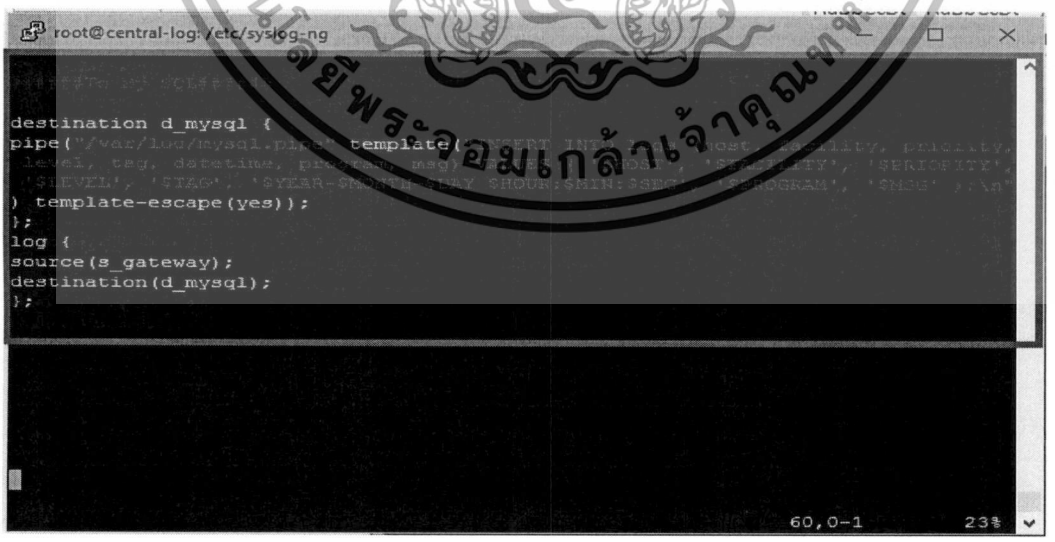
ชื่อยูสเคส	ยูสเคสบันทึก Log	ID : 3
จุดประสงค์	บันทึกข้อมูลจราจรคอมพิวเตอร์จาก Gateway มายังระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์	
รายละเอียดโดยสังเขป	บันทึกข้อมูลการจราจรคอมพิวเตอร์ที่ได้จากจุดต่อเชื่อมของเครือข่าย (Gateway) ลงไปเก็บยังเครื่องแม่ข่ายโดยแยกเก็บตาม อุปกรณ์,ปี,เดือน ,วัน ของข้อมูล	
แอกเตอร์	-	
ยูสเคสที่เกี่ยวข้อง	Include : อุปกรณ์บันทึก Log	
ผู้เกี่ยวข้องอื่น	-	
เงื่อนไขเริ่มต้น	มีการบันทึกข้อมูลการจราจรโดยจุดต่อเชื่อมของเครือข่าย	
เงื่อนไขภายหลัง	บันทึกข้อมูลที่ได้ลงไปยังฐานข้อมูล	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
-	1. บันทึกข้อมูลจราจรคอมพิวเตอร์ที่ได้จาก Gateway	



ภาพที่ 4.5 ตัวอย่างการบันทึกข้อมูลจราจรคอมพิวเตอร์จาก Gateway มายังเครื่องแม่ของระบบ

ตารางที่ 4.4 รายละเอียดการทำงานของยูสเคส บันทึกข้อมูล

ชื่อยูสเคส	ยูสเคสบันทึกข้อมูล	ID : 4
จุดประสงค์	บันทึกข้อมูลจราจรคอมพิวเตอร์ให้อยู่ในรูปแบบข้อมูลเชิงสัมพันธ์	
รายละเอียดโดยสังเขป	เนื่องจากข้อมูลจราจรคอมพิวเตอร์ที่ได้จากจุดต่อเชื่อมของเครือข่าย (Gateway) อยู่ในรูปแบบ Syslog ซึ่งรูปแบบดังกล่าวไม่สามารถนำมาแสดงเป็นรายงานหรือสืบค้นโดยตรงได้จึงต้องทำการเปลี่ยนรูปแบบข้อมูลดังกล่าวและบันทึกลงฐานข้อมูลก่อน จึงจะสามารถนำไปใช้งานได้	
แอกเตอร์	-	
ยูสเคสที่เกี่ยวข้อง	บันทึก Log	
ผู้เกี่ยวข้องอื่น	-	
เงื่อนไขเริ่มต้น	บันทึกข้อมูลจราจรคอมพิวเตอร์จาก Gateway มายังเครื่องแม่ของระบบ	
เงื่อนไขภายหลัง	แปลงผลที่ได้ไปยังหน้าแสดงรายงานของระบบ	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
-	1. ทำการเพิ่มข้อมูลที่ได้จาก log ของอุปกรณ์ gateway ไปยังฐานข้อมูล	



ภาพที่ 4.6 คำสั่งที่ใช้ในการส่งข้อมูลจราจรคอมพิวเตอร์ให้อยู่ในรูปแบบข้อมูลเชิงสัมพันธ์

ตารางที่ 4.5 รายละเอียดการทำงานของยูสเคส เรียกดูรายงาน

ชื่อยูสเคส	ยูสเคสเรียกดูรายงาน	ID : 7
จุดประสงค์	ดูรายงานข้อมูลจราจรคอมพิวเตอร์แบบ Real-time	
รายละเอียดโดยสังเขป	เรียกดูรายงานจราจรคอมพิวเตอร์ของพนักงานในองค์กรแบบการใช้งานตามเวลาจริง (Real-time) เพื่อตรวจสอบถึงปัญหาที่เกิดขึ้นในระบบเครือข่ายโดยผู้จัดการฝ่ายสารสนเทศหรือผู้ดูแลระบบเครือข่าย	
แอกเตอร์	ผู้จัดการฝ่ายสารสนเทศ , ผู้ดูแลระบบเครือข่าย	
ยูสเคสที่เกี่ยวข้อง	-	
ผู้เกี่ยวข้องอื่น	พนักงาน	
เงื่อนไขเริ่มต้น	มีการใช้งานระบบเครือข่ายจากพนักงานในองค์กร	
เงื่อนไขภายหลัง	-	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
1. เลือก เมนู Watch เพื่อดูรายงานการใช้งานตามเวลาจริง (Real-time)	1. แสดงรายงานจราจรคอมพิวเตอร์ของพนักงานในองค์กรแบบการใช้งานตามเวลาจริง (Real-time)	

WUTTISAK LOG

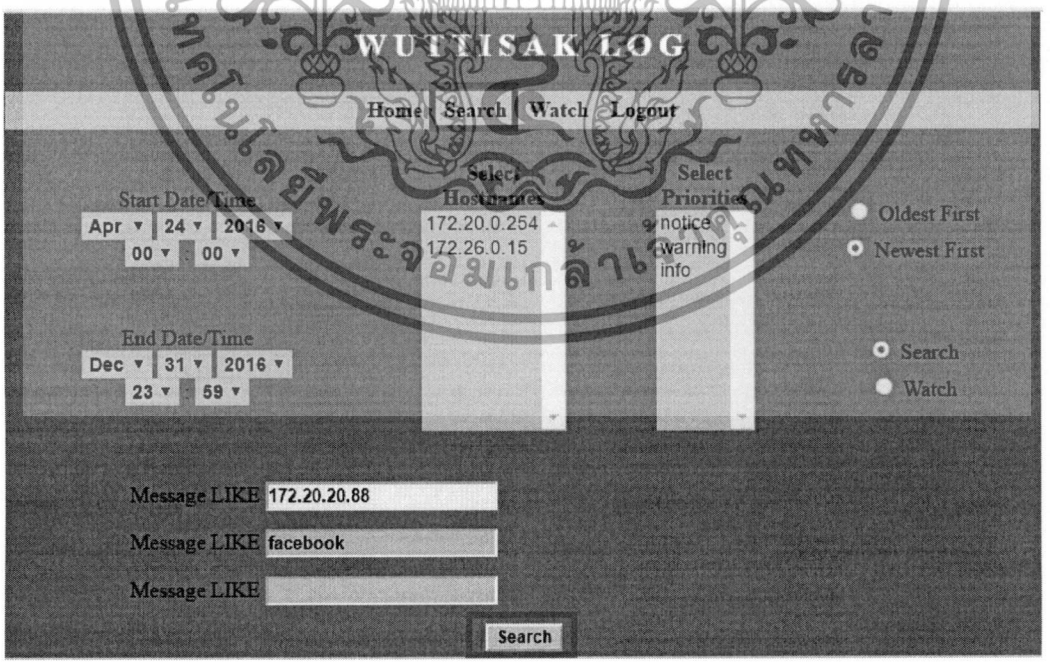
Home Search Watch Logout

Host	Program	Priority	Facility	Date/Time	Message
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61229 src_int="port2" dst=65.55.37.104 dst_port=25 dst_int="Vlan100" SN=21960334 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=21417 service=SMTP proto=6 duration=0 sent=0 rcvd=0
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61228 src_int="port2" dst=207.115.36.21 dst_port=25 dst_int="Vlan100" SN=21960333 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=63912 service=SMTP proto=6 duration=0 sent=0 rcvd=0
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0021000002 type=traffic subtype=allowed pri=notice vd=root src=172.20.10.53 src_port=60940 src_int="port2" dst=212.54.58.11 dst_port=25 dst_int="Vlan100" SN=21959315 status=accept policyid=56 dst_country="Netherlands" src_country="Reserved" dir_disp=org tran_disp=snat tran_sip=49.0.126.2 tran_sport=9352 service=SMTP proto=6 duration=23 sent=212 rcvd=317 sent_pkt=5 rcvd_pkt=4
172.20.0.254	date=2016-04-26	warning	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000007 type=traffic subtype=other pri=warning vd=root src=172.22.11.1 src_port=137 src_int="port5" dst=255.255.255.255 dst_port=137 dst_int="root" SN=21960332 status=deny policyid=0 dst_country="Reserved" src_country="Reserved" service=137/udp proto=17 duration=0 sent=0 rcvd=0 msg="iprope_in_check() check failed, drop"
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61227 src_int="port2" dst=98.138.112.34 dst_port=25 dst_int="Vlan100" SN=21960330 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=54703 service=SMTP proto=6 duration=0 sent=0 rcvd=0

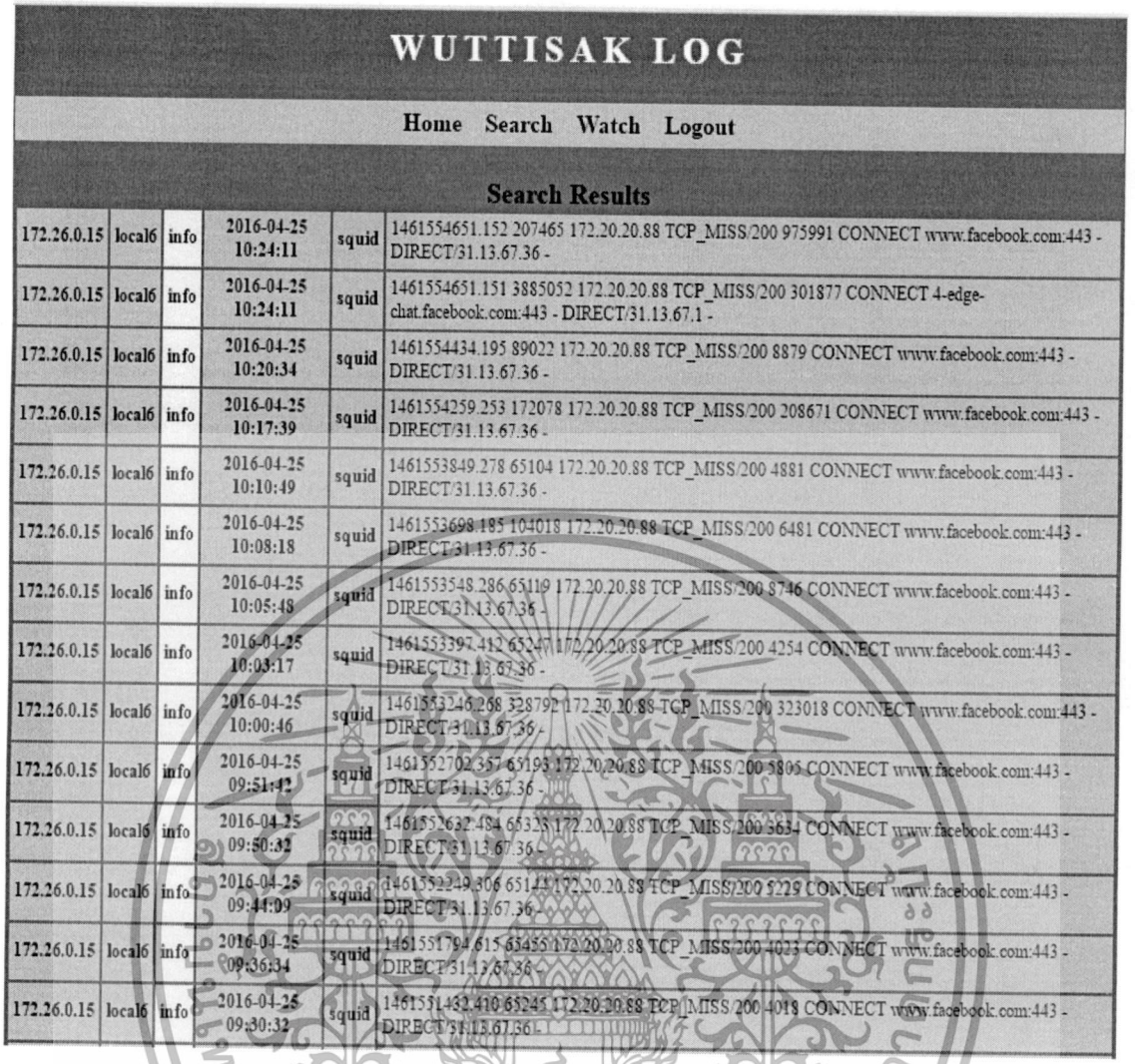
ภาพที่ 4.7 หน้าจอเรียกดูรายงาน

ตารางที่ 4.6 รายละเอียดการทำงานของยูสเคส ค้นหาข้อมูลที่ต้องการ

ชื่อยูสเคส	ยูสเคสค้นหาข้อมูลที่ต้องการ	ID : 8
จุดประสงค์	ค้นหาข้อมูลจราจรคอมพิวเตอร์ที่ต้องการจากระบบ	
รายละเอียดโดยสังเขป	เรียกดูข้อมูลจราจรคอมพิวเตอร์ที่ต้องการจากรายงาน โดยค้นหาเฉพาะข้อมูลที่ต้องการ เช่น เรียกดูรายงานการใช้งานเว็บไซต์ Facebook ในช่วงเวลา 1 สัปดาห์ที่ผ่านมา	
แอกเตอร์	ผู้จัดการฝ่ายสารสนเทศ , ผู้ดูแลระบบเครือข่าย	
ยูสเคสที่เกี่ยวข้อง	เรียกดูรายงาน	
ผู้เกี่ยวข้องอื่น	-	
เงื่อนไขเริ่มต้น	-	
เงื่อนไขภายหลัง	แสดงผลข้อมูลตามการสืบค้น	
ขั้นตอนการทำงาน		
แอกเตอร์	**ระบบ**	
1. เลือก เมนู Search 2. ใส่ข้อมูลที่ต้องการแล้วกด ปุ่ม Search	1. แสดงรายละเอียดหน้าจอค้นหาข้อมูล 2. ระบบทำการแสดงผลการค้นหา	



ภาพที่ 4.8 หน้าจอค้นหาข้อมูล



WUTTISAK LOG

Home Search Watch Logout

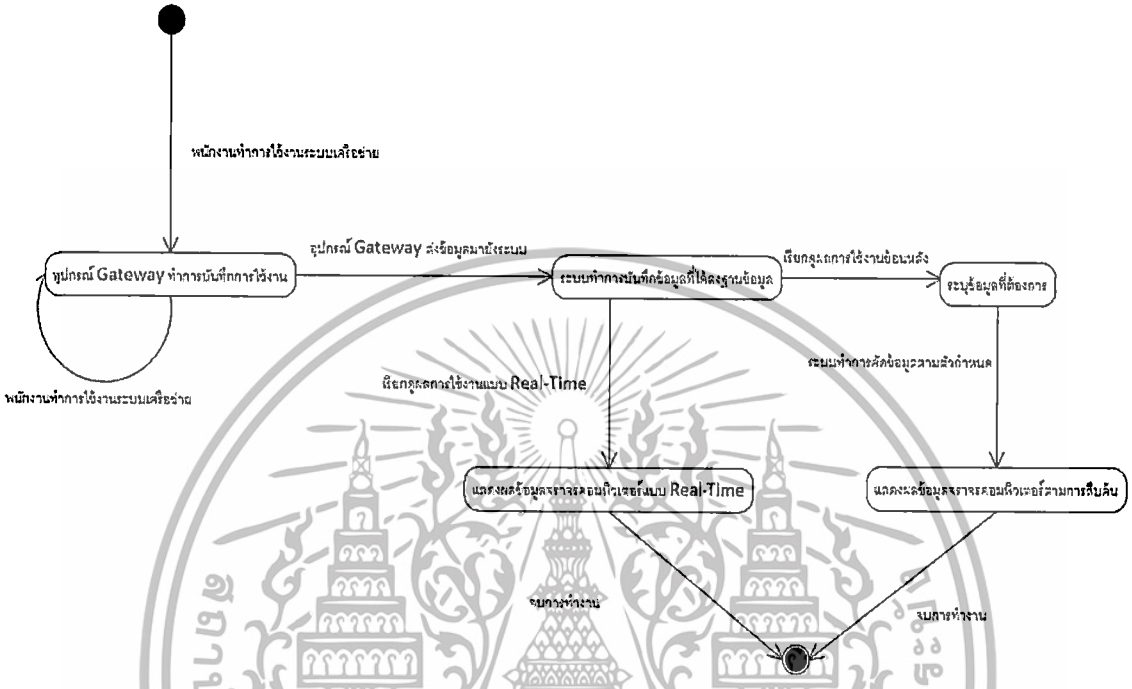
Search Results

172.26.0.15	local6	info	2016-04-25 10:24:11	squid	1461554651.152 207465 172.20.20.88 TCP_MISS/200 975991 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:24:11	squid	1461554651.151 3885052 172.20.20.88 TCP_MISS/200 301877 CONNECT 4-edge-chat.facebook.com:443 - DIRECT/31.13.67.1 -
172.26.0.15	local6	info	2016-04-25 10:20:34	squid	1461554434.195 89022 172.20.20.88 TCP_MISS/200 8879 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:17:39	squid	1461554259.253 172078 172.20.20.88 TCP_MISS/200 208671 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:10:49	squid	1461553849.278 65104 172.20.20.88 TCP_MISS/200 4881 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:08:18	squid	1461553698.185 104018 172.20.20.88 TCP_MISS/200 6481 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:05:48	squid	1461553548.286 65119 172.20.20.88 TCP_MISS/200 8746 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:03:17	squid	1461553397.412 65247 172.20.20.88 TCP_MISS/200 4254 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:00:46	squid	1461553246.268 328792 172.20.20.88 TCP_MISS/200 323018 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:51:42	squid	1461552702.357 65193 172.20.20.88 TCP_MISS/200 5805 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:50:32	squid	1461552632.484 65323 172.20.20.88 TCP_MISS/200 3634 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:44:09	squid	1461552249.306 65143 172.20.20.88 TCP_MISS/200 5229 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:36:34	squid	1461551794.615 65455 172.20.20.88 TCP_MISS/200 4033 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:30:32	squid	1461551432.410 65245 172.20.20.88 TCP_MISS/200 4018 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -

ภาพที่ 4.9 หน้าจอแสดงผลการค้นหา

4.4 สเตทชาร์ตไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

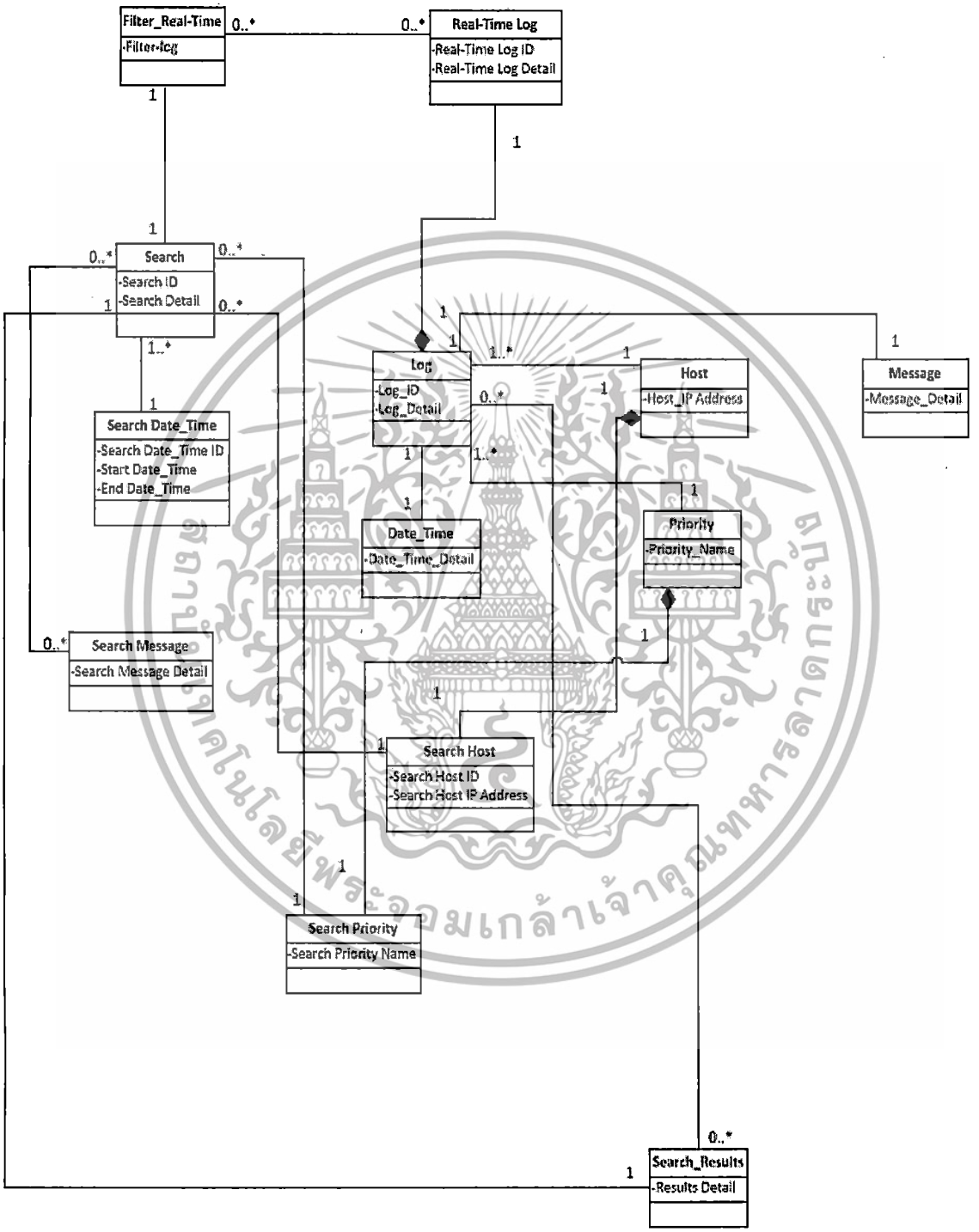
ความสัมพันธ์ของอ๊อบเจกต์ ของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์



ภาพที่ 4.10 สเตทชาร์ตไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

4.5 คลาสไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

คลาสที่นำเสนอ ความสัมพันธ์ของคลาสหลัก ของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์



ภาพที่ 4.11 คลาสไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

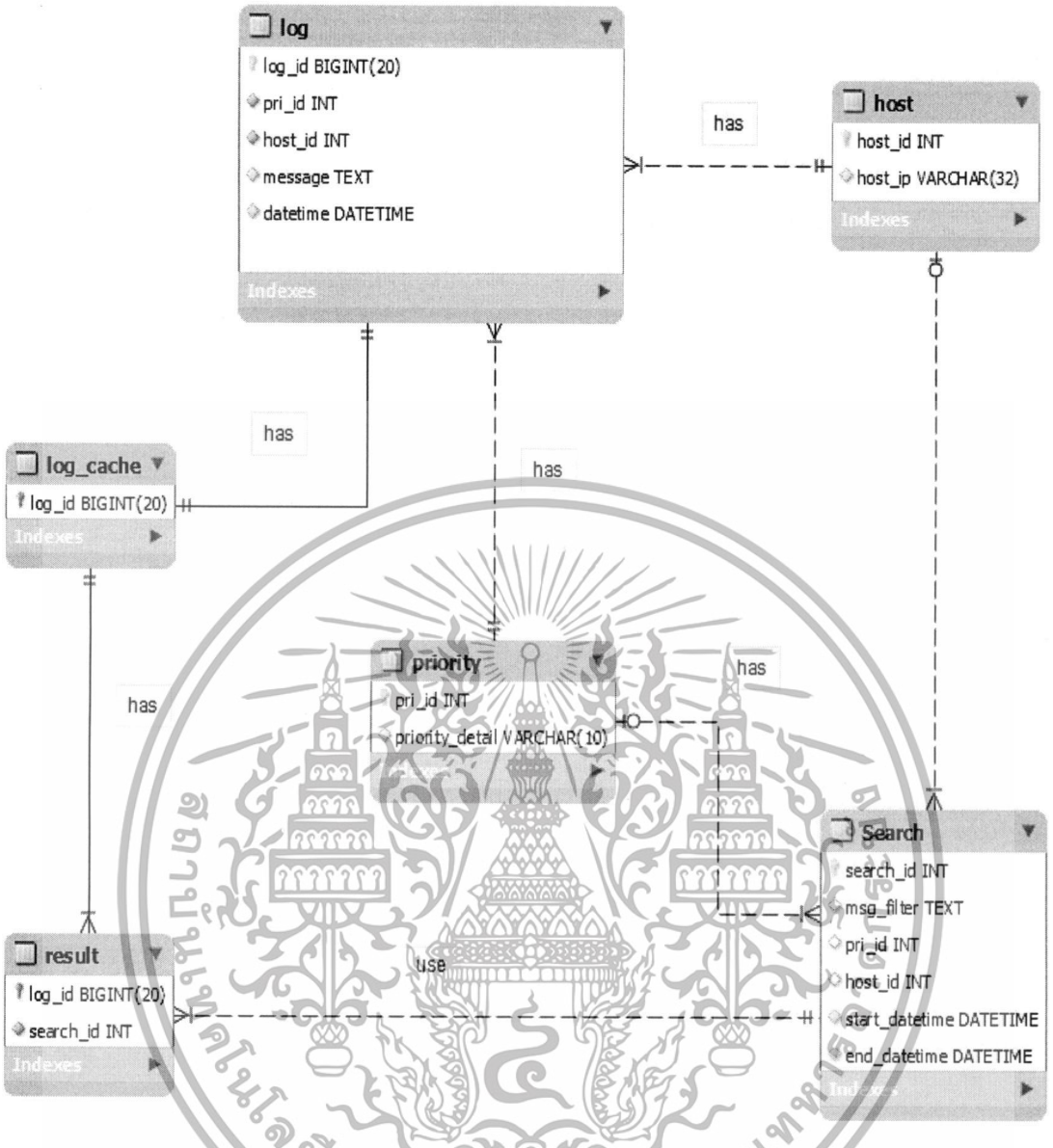
4.6 การออกแบบระบบฐานข้อมูล

เริ่มการออกแบบโดยใช้ แบบจำลองข้อมูล (Data Model) ที่เป็นการจาลองข้อมูลที่เกิดขึ้นทั้งหมดในระบบ พร้อมทั้งจำลองความสัมพันธ์ระหว่างข้อมูลที่เกิดขึ้น โดยใช้แผนภาพแสดงความสัมพันธ์ระหว่างข้อมูล (Entity Relationship Diagram: E-R Diagram)

ฐานข้อมูลเชิงสัมพันธ์ (Relation Model) เป็นการจัดเก็บข้อมูลที่มีโครงสร้างเลียนแบบตารางในการเก็บข้อมูล โดยข้อมูลที่เก็บอยู่ในรูปแบบตารางจะมีชื่อเรียกเพื่ออ้างถึงเวลาต้องการข้อมูลในตารางนั้น และนำข้อมูลมาใช้ได้โดยใช้คลาสที่ทำหน้าที่ปรับปรุงข้อมูล โดยใช้ ภาษาเอสคิวแอล (SQL) เป็นส่วนโปรแกรมจัดการ เพิ่ม/ลบ/ปรับปรุง ข้อมูลทั้งหมด

แบบจำลองข้อมูลของระบบแสดงให้เห็นความสัมพันธ์ระหว่างข้อมูลหลักของระบบจัดการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ซึ่งแสดงให้เห็นในภาพที่ 4.12 มีรายละเอียดของข้อมูลดังต่อไปนี้

1. log คือ ข้อมูลจราจรคอมพิวเตอร์ที่ได้มีทำการส่งผ่านระบบเครือข่ายโดยข้อมูลจะถูกเก็บไว้เพื่อสืบค้นย้อนหลัง
2. host คือ ข้อมูลที่ใช้ระบุว่าข้อมูลจราจรคอมพิวเตอร์ส่งมาจากที่ใด
3. priority คือ ระดับความอันตรายของพฤติกรรมในการใช้งานซึ่งโดยปกติแล้วจะมีทั้งหมด 8 ขั้น คือ Debug,Information,Notification,Warning,Error,Critical,Alert,Emergency โดยรายชื่อดังกล่าวไล่เรียงตามระดับความรุนแรง
4. log_cache คือ ข้อมูลจราจรคอมพิวเตอร์ที่ได้ผ่านกระบวนการเก็บข้อมูลลง cache table ของระบบแล้ว และพร้อมที่จะนำไปแสดงผลแบบ Real-Time เนื่องจากระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้นมีการบันทึกข้อมูลจำนวนมากและการแสดงผลของระบบเป็นการเรียกข้อมูลซ้ำๆอย่างต่อเนื่อง เพื่อทำให้แสดงผลเสมือน Real-Time การเรียกใช้งานในลักษณะนี้ผ่านฐานข้อมูลโดยตรงจะทำให้การแสดงผลใช้เวลานาน
5. search คือ เอนทิตีที่ใช้เก็บค่าตัวกรองสำหรับการสืบค้นข้อมูลจราจรตามที่ต้องการ
6. result คือ เอนทีตีที่ใช้เก็บค่าการแสดงผลที่ได้จากการสืบค้น (ระบบจะนำมาใช้เมื่อมีการแสดงผลแบบ Real-Time ผ่านเงื่อนไขตัวกรอง)



ภาพที่ 4.12 คลาสไดอะแกรมของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

จากแผนภาพแสดงความสัมพันธ์ข้อมูลของรูปที่ 4.12 จะมีการเก็บชนิดข้อมูล แสดงในตาราง พจนานุกรมตารางที่ 4.7-4.12

ตารางที่ 4.7 รายละเอียดตาราง log

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
log_id	BIGINT(20)	รหัสข้อมูลจราจรคอมพิวเตอร์	PK	Y	
host_id	INT	รหัส Gateway	FK	Y	host
pri_id	INT	รหัส ระดับความอันตราย	FK	Y	priority
message	TEXT	ข้อความที่ส่งมาจาก Gateway	-	Y	
datetime	INT	วันเวลาที่ส่งข้อมูล	-	Y	

ตารางที่ 4.8 รายละเอียดตาราง host

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
host_id	INT	รหัส Gateway	PK	Y	
host_ip	VARCHAR(32)	หมายเลข IP อุปกรณ์ Gateway	-	Y	

ตารางที่ 4.9 รายละเอียดตาราง priority

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
pri_id	INT	รหัส ระดับความอันตราย	PK	Y	
priority_detail	VARCHAR(10)	ชื่อระดับความอันตราย	-	Y	

ตารางที่ 4.10 รายละเอียดตาราง log_cache

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
log_id	BIGINT(20)	รหัสข้อมูลจราจรคอมพิวเตอร์	PK,FK	Y	log

ตารางที่ 4.11 รายละเอียดตาราง search

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
search_id	INT	รหัสในการค้นหา	PK	Y	
host_id	INT	รหัส Gateway	FK	N	host
pri_id	INT	รหัส ระดับความอันตราย	FK	N	priority
msg_filter	TEXT	ข้อความที่ต้องการค้นหา		N	
start_datetime	DATETIME	เวลาเริ่มต้นในการค้นหา		Y	
end_datetime	DATETIME	เวลาสุดท้ายในการค้นหา		Y	

ตารางที่ 4.12 รายละเอียดตาราง result

ชื่อแอตทริบิวต์	ชนิดข้อมูล	คำอธิบาย	คีย์	ค่าไม่ว่าง	ตารางที่อ้างถึง
log_id	BIGINT(20)	รหัสข้อมูลจราจรคอมพิวเตอร์	PK,FK	Y	log_cache,log
search_id	INT	รหัสในการค้นหา	FK	Y	search

บทที่ 5

การออกแบบส่วนต่อประสานกับผู้ใช้

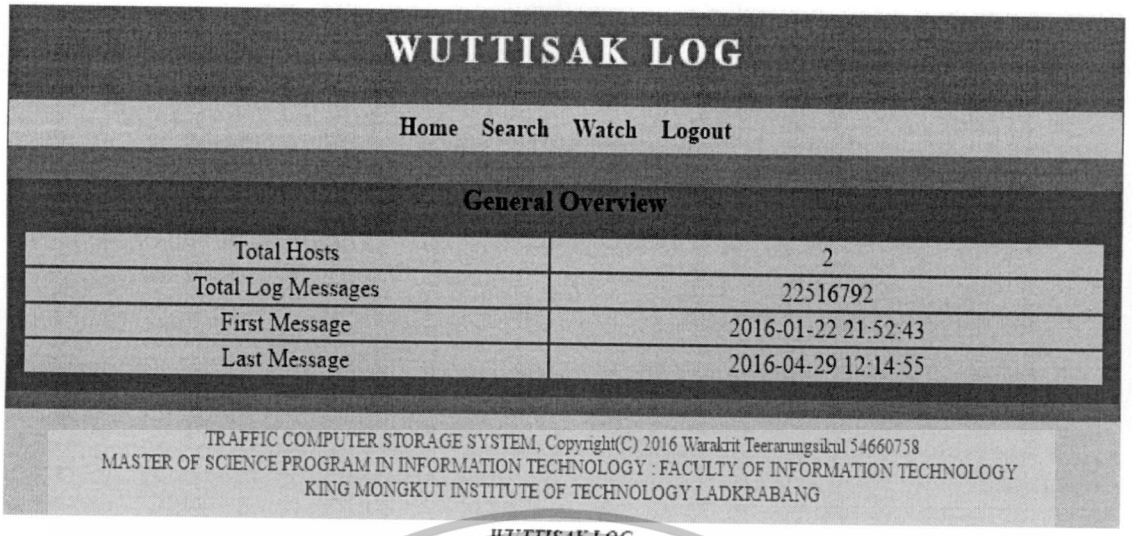
จากการออกแบบระบบระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ เพื่อนำระบบไปประยุกต์ใช้กับการทำงานโดยต่อประสานกับผู้ใช้ ในบทนี้จึงกล่าวถึงการใช้งานระบบในส่วนงานต่าง ๆ ดังต่อไปนี้

5.1 หน้าจอเข้าสู่ระบบ

ในการเริ่มต้นการใช้งานระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ซึ่งพัฒนาส่วนต่อประสานกับผู้ใช้โดยใช้ภาษา PHP ในการพัฒนา ผู้ใช้สามารถเข้าใช้ระบบโดยเข้าใช้งานผ่านเว็บบราวเซอร์ โดยสามารถเข้าผ่าน ip address ของเครื่อง Server ของระบบ เมื่อเริ่มเข้าไปจะเจอหน้า Log in ดังภาพที่ 5.1

ภาพที่ 5.1 หน้าจอ Login ในการเข้าใช้งานระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

จากภาพที่ 5.1 ให้ผู้ใช้กรอกชื่อผู้ใช้งานที่ช่องแรก และรหัสผ่านที่ช่องที่สอง จากนั้นเลือกที่ปุ่ม Login เพื่อเข้าสู่ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ จากนั้นจะเข้าสู่หน้าแรกของระบบดังแสดงในภาพที่ 5.2



ภาพที่ 5.2 หน้าจอแรกของระบบหลังจากเข้าใช้งานระบบ

จากภาพที่ 5.2 จะเห็น ว่าเมื่อผู้ใช้งานเข้ามาในระบบจะพบสถานะเบื้องต้นของระบบซึ่งประกอบไปด้วย

1. **Total Hosts** หมายถึงจำนวนอุปกรณ์ Gateway ที่ทำการส่งข้อมูลจราจรคอมพิวเตอร์มายังระบบ
2. **Total Log Messages** หมายถึงจำนวนข้อมูลจราจรคอมพิวเตอร์ทั้งหมดที่ส่งมายังฐานข้อมูล
3. **Fist Message** หมายถึงวันและเวลาที่ข้อมูลจราจรคอมพิวเตอร์ข้อมูลแรกถูกส่งเข้ามายังระบบ
4. **Last Message** หมายถึงวันและเวลาล่าสุดที่ข้อมูลจราจรคอมพิวเตอร์ถูกส่งเข้ามายังระบบ

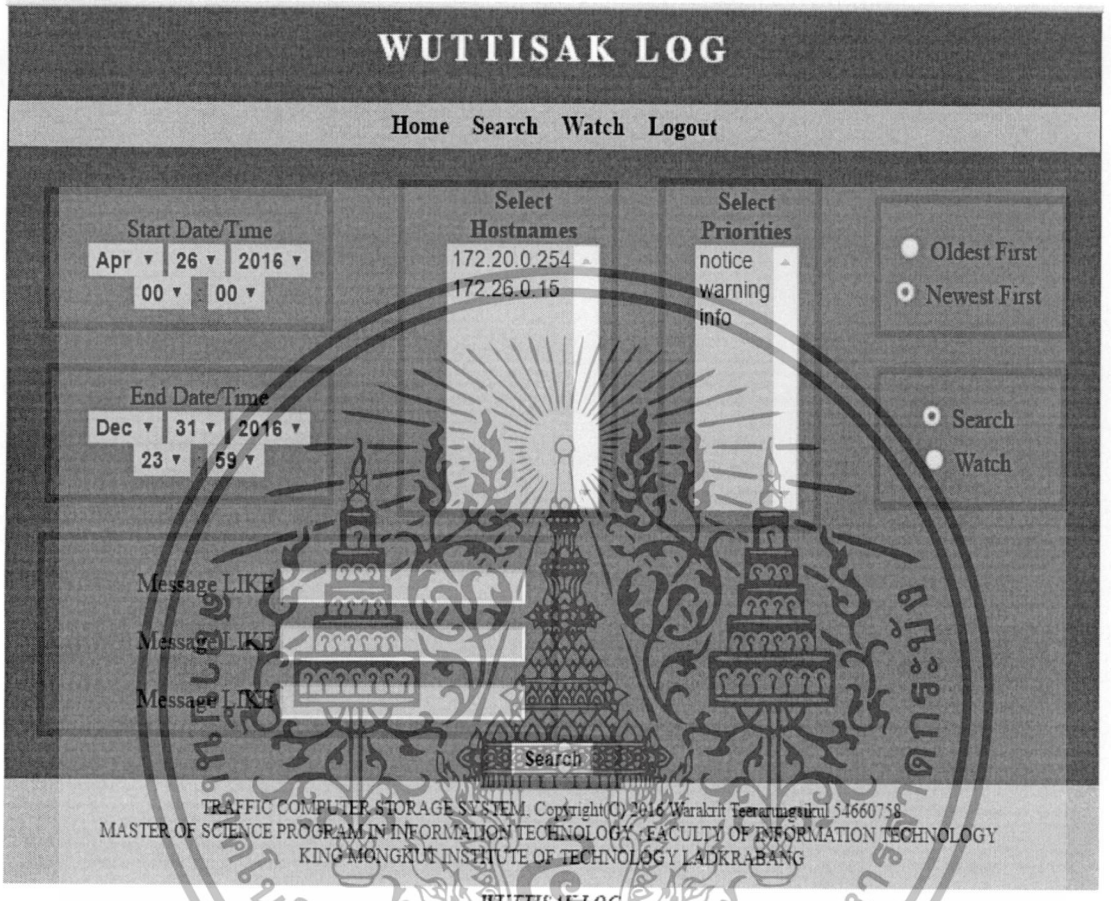
และมีเมนูในการใช้งานทั้งหมด 4 เมนูดังนี้

1. **Home** เป็นคำสั่งที่ให้ผู้ใช้งานกลับมายังหน้าแรกของระบบ
2. **Search** เป็นคำสั่งเพื่อเข้าสู่หน้าจอค้นหาข้อมูลจราจรคอมพิวเตอร์ที่ต้องการ
3. **Watch** เป็นคำสั่งที่ใช้ดูข้อมูลจราจรคอมพิวเตอร์ตามเวลาจริง (Real-Time)
4. **Logout** เป็นคำสั่งที่ให้ผู้ใช้งานทำการออกจากระบบ

ซึ่งรายละเอียดการใช้งานเมนูต่าง ๆ มีดังนี้

5.2 หน้าจอค้นหาข้อมูล

ในการเข้าสู่หน้าจอการค้นหาข้อมูลให้ผู้ใช้งานทำการเลือกที่เมนู Search จะพบเมนูในการเลือกการค้นหาดังภาพที่ 5.3



ภาพที่ 5.3 แสดงหน้าจอค้นหาข้อมูลจราจรคอมพิวเตอร์

จากภาพที่ 5.3 จะเห็นว่ามีตัวกรองที่สามารถใช้ในการหาข้อมูลได้ดังต่อไปนี้

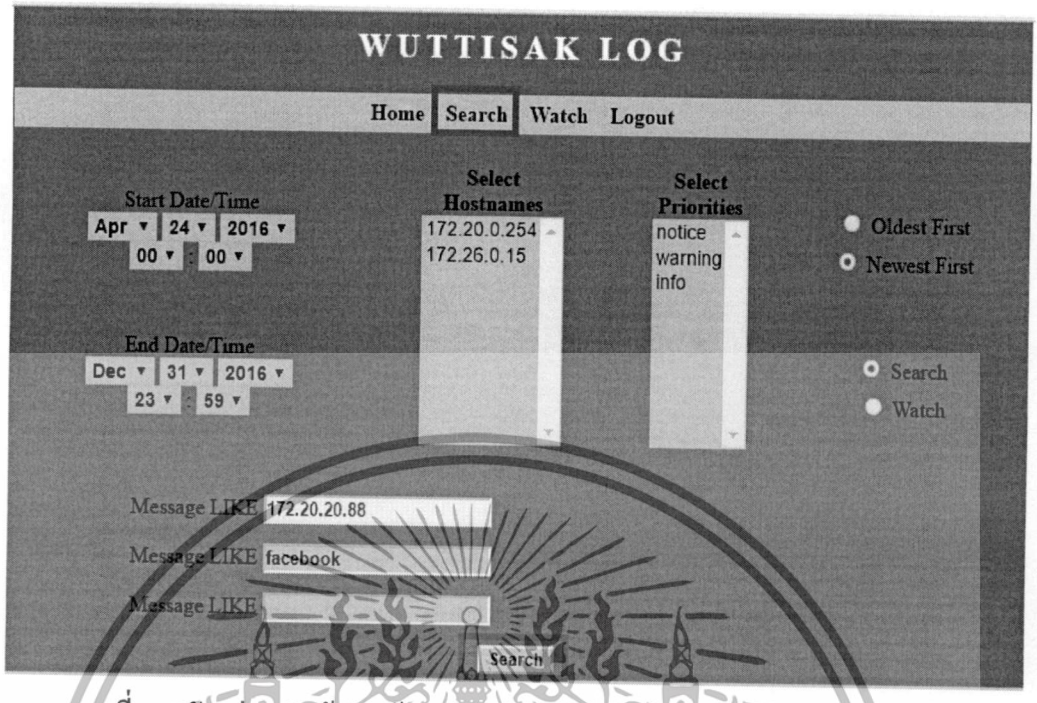
1. เมนู Start Date/Time หมายถึงช่วงเวลาเริ่มต้นที่จะให้แสดงผลของข้อมูลจราจรคอมพิวเตอร์
2. เมนู End Date/Time หมายถึงช่วงเวลาสิ้นสุดที่จะให้แสดงผลของข้อมูลจราจรคอมพิวเตอร์
3. เมนู Select Hostnames หมายถึงเลือกว่าจะดูข้อมูลที่ส่งมาจากจุดเชื่อมต่อ (Gateway) ตัวไหน ซึ่งในระบบที่ใช้งานปัจจุบันมี Gateway 2 ตัว คือ 172.20.0.254 ซึ่งเป็น Firewall ของระบบเครือข่ายซึ่งจะส่งข้อมูลภัยคุกคามที่ส่งมาจากข้างนอกหรือคนในองค์กรพยายามจะส่งออกไป แต่เนื่องจากข้อมูลจราจรคอมพิวเตอร์ของอุปกรณ์ดังกล่าวไม่มีมีการเปลี่ยน

หมายเลข ip ปลายทางเป็นชื่อเว็บไซต์ในการเก็บข้อมูลจราจรคอมพิวเตอร์ จึงจำเป็นต้องใช้ Proxy Server มาเป็นตัวช่วยในการระบุเว็บไซต์ปลายทางที่พนักงานในองค์กรใช้งาน ซึ่ง Proxy Server นี้มี ip address คือ 172.26.0.15 ดังแสดงในภาพที่ 5.3 ซึ่งหากไม่ทำการเลือก Hostname ระบบจะแสดงผลการส่งข้อมูลจาก Gateway ทั้ง 2 ตัว

4. เมนู Select Priorities หมายถึงเลือกระดับความอันตรายของพฤติกรรมในการใช้งานซึ่งโดยปกติแล้วจะมีทั้งหมด 8 ขั้น คือ Debug,Information,Notification,Warning,Error,Critical,Alert,Emergency โดยรายชื่อดังกล่าวไล่เรียงตามระดับความรุนแรง ซึ่งจากภาพที่ 5.3 จะพบเพียง 3 ขั้นคือ notice ,warning และ info เนื่องจากในการค้นหาข้อมูลของระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์นั้นจะแสดงการค้นหาเฉพาะระดับขั้นที่เคยมีการส่ง Log มาจาก Gateway เท่านั้น ซึ่งหากไม่มีการเลือกระดับ Priorities ระบบจะทำการแสดงผลทุก Priorities
5. เมนู Oldest Fist และ Newest First เป็นเมนูที่ให้เลือกว่าต้องการแสดงข้อมูลที่เก่าที่สุดก่อนหรือแสดงข้อมูลที่ใหม่ที่สุดก่อน
6. เมนู Search และ Watch เป็นคำเมนูที่ให้เลือกว่าจะดูตามการค้นหาแบบต่อเนื่องตามเวลาจริง (Watch) หรือเพียงแค่แสดงรายงานถึงช่วงเวลาที่ผู้ใช้กดปุ่ม Search เท่านั้น
7. เมนู Message LIKE เป็นเมนูที่ใช้กรองข้อความที่ต้องการที่จะค้นหาเช่น ใส่ ip address ของพนักงานที่ต้องการค้นหาในช่องที่ 1 และใส่คำว่า facebook ในช่องที่ 2 ผลลัพธ์ที่ได้จะแสดงออกมาเฉพาะการส่งข้อมูลจาก ip ที่เราค้นหาไปยังเว็บไซต์ facebook ซึ่ง ip address ของพนักงานในองค์กรจะถูกจัดเก็บเป็นเอกสารตั้งแต่ทางฝ่ายเทคโนโลยีสารสนเทศเป็นคนติดตั้งเครื่อง และทำการล็อคสิทธิ์พนักงานให้ไม่สามารถเปลี่ยน ip เองได้ โดยการให้พนักงานในองค์กรทำการ Join Domain และใช้กฎ Group Policy ที่ทำการประกาศโดย active directory ขององค์กร

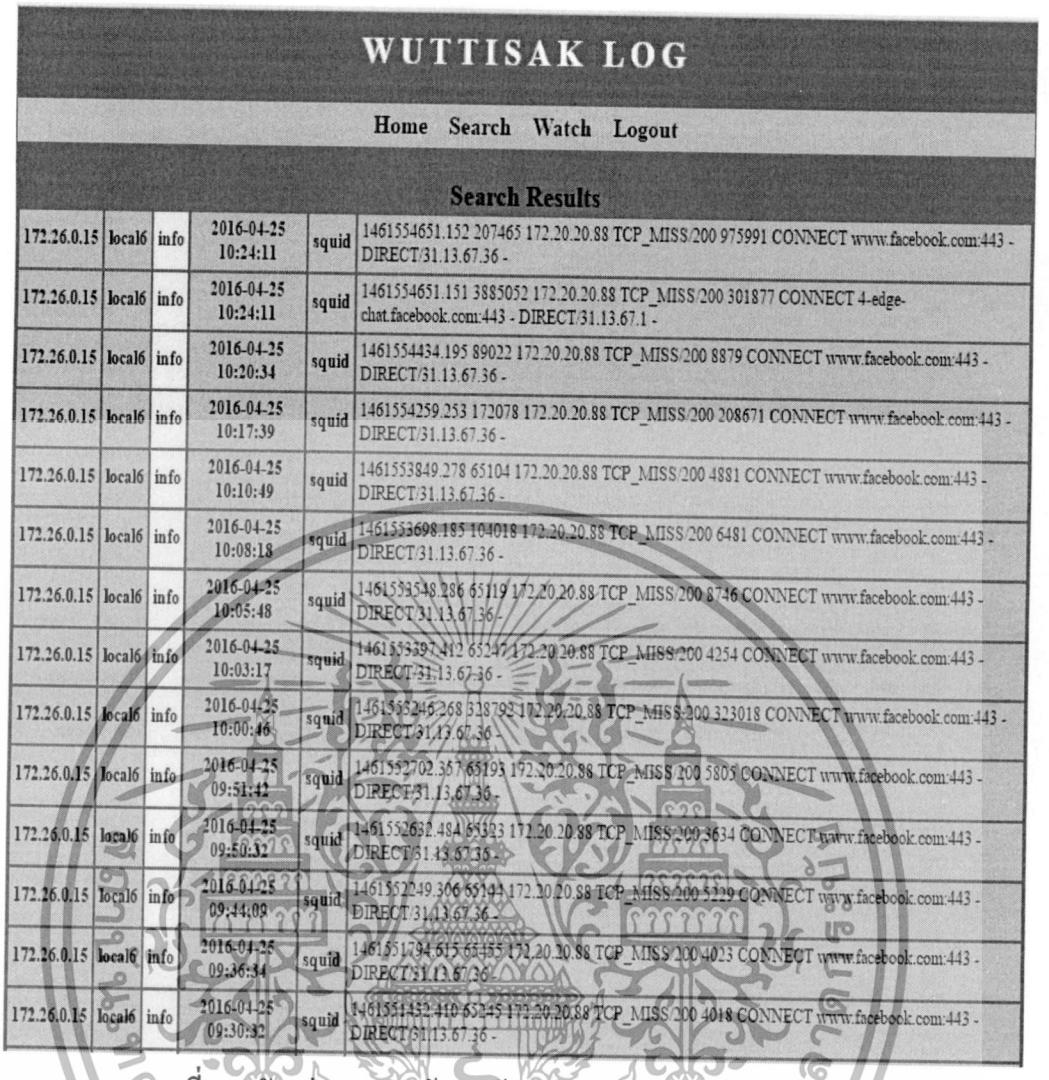
	A	B	C	D	E	F	G	H	I	J
109	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณแจ็ค)	1	04-0015-11-0089-00163	04-0014-11-0180-00819	CHK_CLI10	172.20.30.39	
110	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณปอ)	1	04-0024-11-0137-00587	04-0014-11-0189-00822	CHK_CLI11	172.20.30.30	
111	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณฝ้าย)	1	04-0024-11-0133-00583	04-0014-11-0122-00811	CHK_CLI12	172.20.30.31	
112	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณตุ๊กตา)	1	04-0024-11-0135-00585	04-0014-11-0121-00310	CHK_CLI13	172.20.30.32	
113	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณปอ)	1	04-0015-11-0092-00166	04-0014-11-0132-00321	CHK_CLI14	172.20.30.33	
114	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณอร)	1	04-0024-11-0136-00586	04-0014-11-0118-00307	CHK_CLI15	172.20.30.34	
115	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณมิ้ค)	1	04-0015-11-0083-00157	04-0014-11-0134-00323	CHK_CLI16	172.20.30.35	
116	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณบิ๋น)	1	04-0015-11-0084-00158	04-0014-11-0128-00317	CHK_CLI17	172.20.30.36	
117	3		ฝ่ายเซ็ตเกอร์					CHK_CLI18	172.20.30.37	
118	3	CPU	ฝ่ายเซ็ตเกอร์	checker (คุณจ๋า)	1	04-0015-11-0159-00283	CMYS 0124 (รหัสเก่า)	CHK_CLI19	172.20.30.38	
119	3		ฝ่ายเซ็ตเกอร์					CHK_CLI20	172.20.30.39	
120	3		ฝ่ายเซ็ตเกอร์					CHK_CLI21	172.20.30.40	
121										
122	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณแอน-ผู้จัดการฝ่ายบริหารค่าตอบแทน)	1	04-0015-11-0001-00075	04-0014-11-0024-00213	HR_CLI1	172.20.30.50	
123	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณแนท)	1	04-0024-11-0121-00571	04-0014-11-0108-00297	HR_CLI2	172.20.30.51	
124	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณส่ม)	1	04-0024-11-0031-00481	04-0014-10-0171-00186	HR_CLI3	172.20.30.52	
125	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณแพปปี)	1	04-0024-11-0132-00582	04-0014-11-0117-00306	HR_CLI4	172.20.30.53	
126	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณกวาง)	1	04-0024-11-0129-00579	04-0014-11-0110-00299	HR_CLI5	172.20.30.54	
127	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณแอ๋)	1	04-0015-11-0076-00150	04-0014-11-0185-00874	HR_CLI6	172.20.30.55	
128	3	CPU	ฝ่ายทรัพยากรบุคคล	HR (คุณลาล่า)	1	04-0024-11-0124-00574	04-0014-10-0105-00121	HR_CLI7	172.20.30.56	
129	3		ฝ่ายทรัพยากรบุคคล	(คุณเดียร์)	1	04-0015-11-0138-00212	04-0014-11-0028-00217	HR_CLI8	172.20.30.57	

ภาพที่ 5.4 ตัวอย่างเอกสารการบันทึก ip address ของพนักงานในองค์กร



ภาพที่ 5.5 ตัวอย่างการค้นหาข้อมูลในระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

จากภาพที่ 5.5 ผู้ใช้งานต้องการหาข้อมูลจราจรคอมพิวเตอร์ของหมายเลข ip address 172.20.20.88 โดยค้นหาเฉพาะการส่งข้อมูลไปยังโดเมน facebook โดยค้นหาทุกระดับ Priorities และให้แสดงผลข้อมูลโดยเริ่มตั้งแต่วันที่ 24 เมษายน ถึงปัจจุบัน (หาก End Date เกินวันที่ ณ ปัจจุบัน ระบบจะทำการค้นหาจนถึงปัจจุบัน) โดยเลือกรูปแบบการค้นหาเป็น Search ซึ่งได้ผลการค้นหาตามภาพที่ 5.6



WUTTISAK LOG

Home Search Watch Logout

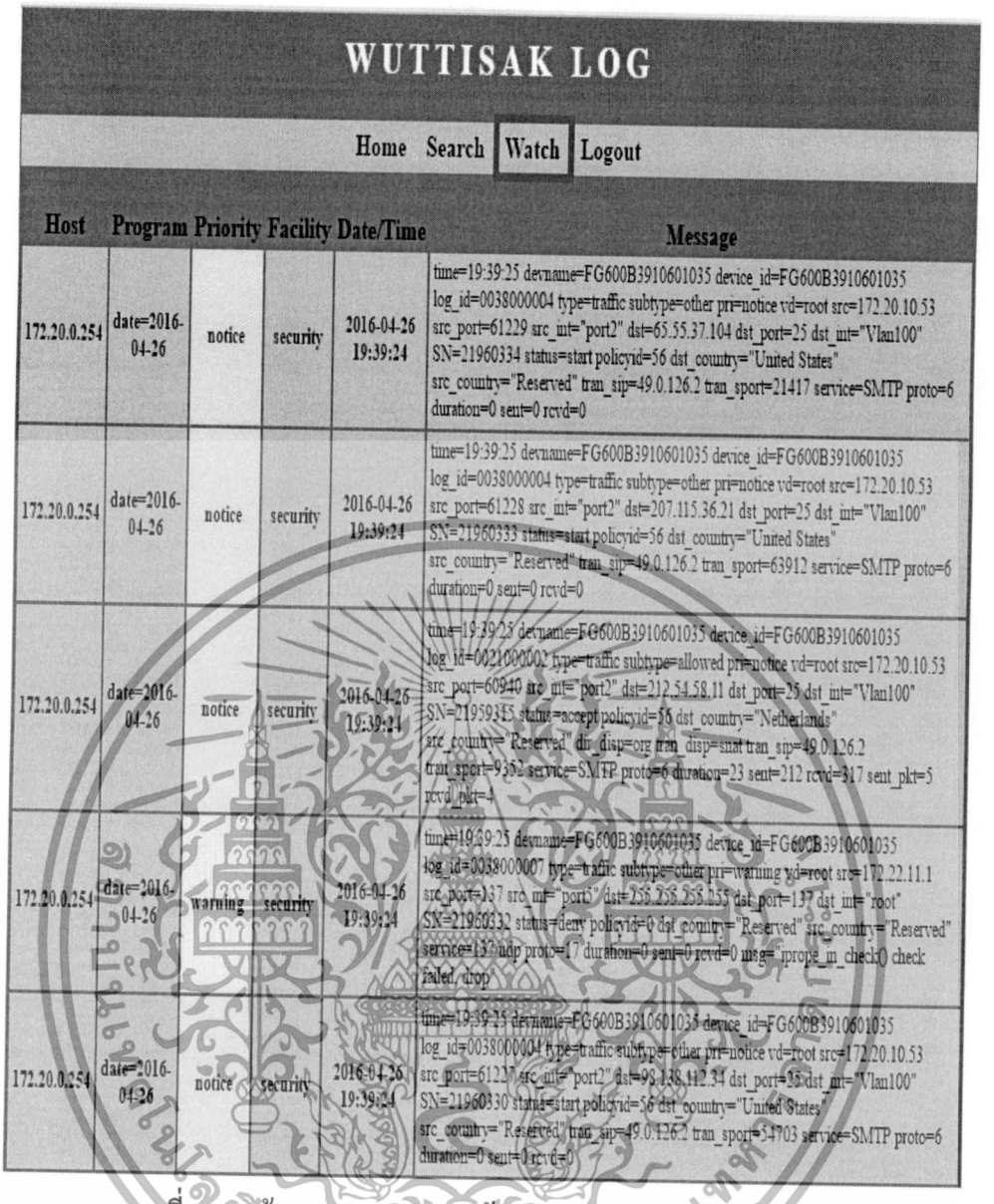
Search Results

172.26.0.15	local6	info	2016-04-25 10:24:11	squid	1461554651.152 207465 172.20.20.88 TCP_MISS/200 975991 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:24:11	squid	1461554651.151 3885052 172.20.20.88 TCP_MISS/200 301877 CONNECT 4-edge-chat.facebook.com:443 - DIRECT/31.13.67.1 -
172.26.0.15	local6	info	2016-04-25 10:20:34	squid	1461554434.195 89022 172.20.20.88 TCP_MISS/200 8879 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:17:39	squid	1461554259.253 172078 172.20.20.88 TCP_MISS/200 208671 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:10:49	squid	1461553849.278 65104 172.20.20.88 TCP_MISS/200 4881 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:08:18	squid	1461553698.185 104018 172.20.20.88 TCP_MISS/200 6481 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:05:48	squid	1461553548.286 65119 172.20.20.88 TCP_MISS/200 8746 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:03:17	squid	1461553397.412 65247 172.20.20.88 TCP_MISS/200 4254 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 10:00:46	squid	1461553246.268 328793 172.20.20.88 TCP_MISS/200 323018 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:51:42	squid	1461552702.367 65193 172.20.20.88 TCP_MISS/200 5805 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:50:32	squid	1461552632.484 65323 172.20.20.88 TCP_MISS/200 3634 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:44:09	squid	1461552249.306 65193 172.20.20.88 TCP_MISS/200 5229 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:36:34	squid	1461551794.615 65455 172.20.20.88 TCP_MISS/200 4023 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -
172.26.0.15	local6	info	2016-04-25 09:30:32	squid	1461551432.410 65245 172.20.20.88 TCP_MISS/200 4018 CONNECT www.facebook.com:443 - DIRECT/31.13.67.36 -

ภาพที่ 5.6 ตัวอย่างผลการค้นหาข้อมูลจราจรคอมพิวเตอร์จากระบบ

5.3 หน้าจอดูข้อมูลคอมพิวเตอร์ตามเวลาจริง (Real-Time)

ในส่วนของการดูข้อมูลจราจรคอมพิวเตอร์ตามเวลาจริงนั้นผู้ใช้งานต้องการเลือกที่เมนู Watch จากนั้นระบบจะทำการประมวลผลข้อมูลจราจรคอมพิวเตอร์ที่เข้ามา และระบบจะทำการแสดงผลข้อมูลจราจรคอมพิวเตอร์ตามเวลาจริง (Real-time) ซึ่งจะทำให้เห็นข้อมูล Log เข้ามาเรื่อยๆตามการใช้งานของพนักงานในองค์กร



WUTTISAK LOG

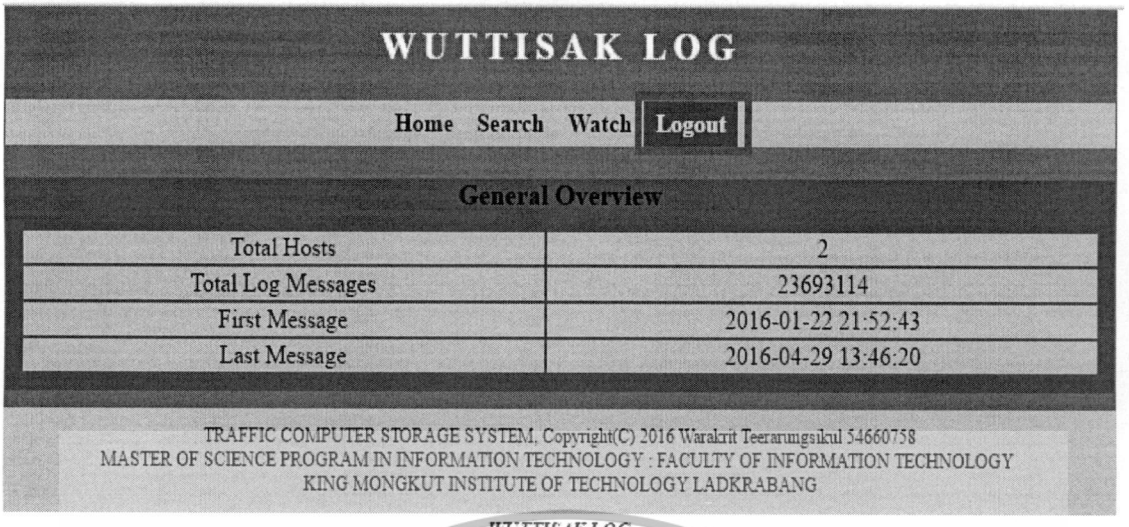
Home Search Watch Logout

Host	Program	Priority	Facility	Date/Time	Message
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61229 src_int="port2" dst=65.55.37.104 dst_port=25 dst_int="Vlan100" SN=21960334 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=21417 service=SMTP proto=6 duration=0 sent=0 rcvd=0
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61228 src_int="port2" dst=207.115.36.21 dst_port=25 dst_int="Vlan100" SN=21960333 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=63912 service=SMTP proto=6 duration=0 sent=0 rcvd=0
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0021000002 type=traffic subtype=allowed pri=notice vd=root src=172.20.10.53 src_port=60940 src_int="port2" dst=212.54.58.11 dst_port=25 dst_int="Vlan100" SN=21959335 status=accept policyid=56 dst_country="Netherlands" src_country="Reserved" dir_disp=org tran_disp=snat tran_sip=49.0.126.2 tran_sport=9352 service=SMTP proto=6 duration=23 sent=212 rcvd=317 sent_pkt=5 rcvd_pkt=4
172.20.0.254	date=2016-04-26	warning	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000007 type=traffic subtype=other pri=warning vd=root src=172.22.11.1 src_port=137 src_int="port5" dst=255.255.255.255 dst_port=137 dst_int="root" SN=21960332 status=deny policyid=0 dst_country="Reserved" src_country="Reserved" service=137/udp proto=17 duration=0 sent=0 rcvd=0 msg="iprope_in_check() check failed, drop"
172.20.0.254	date=2016-04-26	notice	security	2016-04-26 19:39:24	time=19:39:25 devname=FG600B3910601035 device_id=FG600B3910601035 log_id=0038000004 type=traffic subtype=other pri=notice vd=root src=172.20.10.53 src_port=61237 src_int="port2" dst=98.138.112.34 dst_port=25 dst_int="Vlan100" SN=21960330 status=start policyid=56 dst_country="United States" src_country="Reserved" tran_sip=49.0.126.2 tran_sport=54703 service=SMTP proto=6 duration=0 sent=0 rcvd=0

ภาพที่ 5.7 หน้าจอแสดงผลการดูข้อมูลจราจรคอมพิวเตอร์ตามเวลาจริง

5.4 เมนู Logout

เมื่อผู้ใช้งานต้องการออกจากระบบการจัดเก็บข้อมูลจราจรให้เลือกที่เมนู Logout ที่อยู่มุมบนขวาของหน้าจอ ดังแสดงตามภาพที่ 5.8



ภาพที่ 5.8 ภาพตัวอย่างในการ Logout ออกจากระบบ

บทที่ 6

บทสรุป

บทนี้เป็นบทสุดท้ายของโครงงานที่ได้เริ่มจัดทำตั้งแต่ต้นจนเริ่มนำไปทดสอบใช้งาน เพื่อสรุปข้อมูลของโครงการที่ดำเนินการ ว่าพบปัญหาในการพัฒนาระบบในส่วนใด มีข้อเสนอแนะและแนวทางพัฒนาระบบเพิ่มเติมต่อไป

6.1 บทสรุปของการดำเนินโครงการ

จากจุดประสงค์ที่จะพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์เพื่อใช้จัดเก็บข้อมูลจราจรคอมพิวเตอร์ของพนักงานในองค์กร ซึ่งจากเดิมข้อมูลจราจรที่ได้ถูกจัดเก็บในรูปแบบของข้อมูลดิบ ซึ่งไม่สามารถนำไปใช้งานหรือวิเคราะห์ถึงปัญหาที่เกิดขึ้นได้ อีกทั้งไม่สามารถเรียกดูรายงานตามเวลาจริงหรือสืบค้นการใช้งานย้อนหลังได้ เมื่อมีการพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ขึ้น ทำให้สามารถจัดเก็บข้อมูลจราจรที่ได้มาดีขึ้น สามารถเก็บข้อมูลได้นานถึง 90 วัน ตามกฎหมายกำหนด อีกทั้งมีการจัดการข้อมูลที่ได้มาให้อยู่ในฐานข้อมูลเชิงสัมพันธ์จึงทำให้สามารถสืบค้นข้อมูลที่ต้องการผ่านตัวกรอง หรือดูรายงานตามเวลาจริงได้อีกด้วย ทำให้ผู้ดูแลระบบเครือข่ายสามารถแก้ปัญหาที่เกิดขึ้นหรือสามารถตอบสนองนโยบายในการใช้งานอินเทอร์เน็ตที่ทางผู้บริหารต้องการได้ ซึ่งการตอบสนองนโยบายดังกล่าวทำให้พนักงานในองค์กรทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

6.2 ข้อจำกัดของการพัฒนาระบบ

จากเริ่มพัฒนาระบบจนถึงระบบเริ่มทดสอบใช้งานพบปัญหาในการพัฒนาระบบคือ รูปแบบของการส่งข้อมูลจราจรคอมพิวเตอร์ของอุปกรณ์แต่ละตัวไม่เหมือนกัน ทำให้ผู้พัฒนาต้องทดสอบการส่งข้อมูลจราจรคอมพิวเตอร์แล้วทำการสั่งการให้ระบบส่งค่าที่ได้ลงไปในฐานข้อมูลซึ่งอุปกรณ์บางชนิดไม่รองรับการส่งค่าต่างๆไปยังฐานข้อมูล เช่น อุปกรณ์ของ Cisco ถ้าเป็นอุปกรณ์ในส่วนของการ Routing รูปแบบ Log ของ Syslog ที่ได้จะมีเพียงค่าสถานะของ Interface ของอุปกรณ์เท่านั้น เช่นมี Log แจ้งว่า Interface ของอุปกรณ์มีสถานะ Down หรือ UP ซึ่งข้อมูลที่ได้ไม่สามารถนำไปใช้งานต่อให้เกิด

ประโยชน์ได้และอุปกรณ์บางชนิดไม่มีการเก็บค่า Domain ปลายทาง ซึ่งอุปกรณ์จะทำการส่งค่า Destination มาเป็นหมายเลข ip address ซึ่งยากต่อการพัฒนาระบบ

ปัญหาอีกข้อที่พบคือความช้าในการดึงข้อมูลจากฐานข้อมูลมาแสดงผลหรือสืบค้น เนื่องจากฐานข้อมูลมีขนาดใหญ่และมีการเก็บข้อมูลจำนวนมาก เนื่องจากมีข้อมูลเข้าระบบตลอดเวลา แม้ว่าจะลองพยายามใช้เทคนิคต่างๆเพื่อช่วยเพิ่มความเร็วในการดึงข้อมูลแล้วก็ตาม แต่ก็ยังไม่ได้ผลที่น่าพอใจนัก

6.3 ข้อเสนอแนะและแนวทางในการพัฒนาระบบเพิ่มเติม

แนวทางในการพัฒนาระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์เพิ่มเติม คือ ในระบบที่ได้ทำมานั้น การระบุผู้ใช้ในองค์กรยังจำเป็นต้องนำ ip address ที่ได้มาเทียบกับเอกสารอยู่ ซึ่งเป็นการทำงานซ้ำซ้อนอีกทั้งยังมีโอกาสผิดพลาดอีกด้วย หากตัวระบบสามารถจัดเก็บชื่อพนักงานบริษัท หรือ ระบบสามารถเชื่อมต่อกับ Active Directory ซึ่งมีระบบนี้อยู่แล้วในองค์กรจะทำให้ลดความซ้ำซ้อนของการทำงานหรือลดความผิดพลาดลงได้

และในปัจจุบันในมีโครงสร้างรูปแบบใหม่ๆที่ใช้ในการเก็บข้อมูลจราจรคอมพิวเตอร์ หากสามารถพัฒนาให้ระบบมีการทำงานที่รวดเร็วขึ้นได้ก็จะสะดวกต่อผู้ดูแลระบบเครือข่ายมากยิ่งขึ้น

บรรณานุกรม

พร้อมเลิศ หล่อวิจิตร. 2550. **คู่มือเรียน PHP และ MySQL สาหรับผู้เริ่มต้น**. กรุงเทพฯ : โปรวิชั่น.

Captain, F.A. 2012 . **Six-Step Relational Database Design.** Seattle, WA : Create Space.

Coronel, C., Morris , S., and Rob, P. 2011. **Database System : Design, Implementation and Management**. 9th ed. Boston, MA : Cengage Learning.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายวรกฤษณ์ ธีระรังสิกุล
ที่อยู่	49 ซอยเทวัญ 3 ต.ปากน้ำโพ อ.เมืองฯ จ.นครสวรรค์ 60000
ประวัติการศึกษา	2551 วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ ม.เทคโนโลราชมงคลธัญบุรี
ประสบการณ์การทำงาน	
พ.ศ. 2555-ปัจจุบัน	วิศวกรระบบเครือข่าย บริษัท วุฒิศักดิ์ อินเตอร์กรุ๊ป จำกัด
พ.ศ. 2554-2555	เจ้าหน้าที่ดูแลระบบเครือข่าย สำนักงานปลัดกระทรวงอุตสาหกรรม
พ.ศ. 2552-2554	นักวิชาการคอมพิวเตอร์ คณะพาณิชยศาตร์และการบัญชี ม.ธรรศาสตร์
พ.ศ. 2551-2552	พนักงานไอที บริษัท มิราม่าเซอร์วิส จำกัด