ระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์

COMPUTER TRAFFIC DATA MANAGEMENT SYSTEM

โดย

ธนวรรณ อัศวธนบดี

THANAWAN ASSAVATHANABODEE

อาจารย์ที่ปรึกษา

รศ.ดร. โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคฤดูร้อน ปีการศึกษา 2551

COMPUTER TRAFFIC DATA MANAGEMENT SYSTEM

THANAWAN ASSAVATHANABODEE

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

SUMMER/ 2008

หัวข้อ	ระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์
นักศึกษา	นางสาวธนวรรณ อัศวธนบดี
รหัสนักศึกษา	50066508
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2551
อาจารย์ที่ปรึกษา	รศ.ดร. โชติพัชร์ ภรณวลัย

บทคัดย่อ

ระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data Management System) เป็นระบบที่พัฒนาขึ้นมา เพื่อช่วยให้ "ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)" สามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้สอดคล้องตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ ประกาศกระทรวง ICT เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ. ศ. 2550 โดยในโครงการพัฒนาระบบงานนี้ ได้ออกแบบให้ทำงานในรูปแบบของ Web Application เพื่อให้ง่ายต่อการบริหารจัดการการเก็บรวบรวมจราจรจากเครื่องแม่ข่ายต่างๆ ตามที่พรบ.กำหนด อันได้แก่ Mail Server , Web Server , Proxy Server , FTP Server รวมถึงง่ายต่อการสืบค้นข้อมูลจราจรที่จัดเก็บในฐานข้อมูล โดยสามารถบอกได้ว่า บุคคลใดในองค์กร มีการกระทำใด ที่เครื่อง IP Address อะไร และ ณ เวลาใด ทั้งนี้เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์นั้น สามารถนำมาใช้ประโยชน์ในการสืบสวน สอบสวน หาผู้กระทำความผิดตามพระราชบัญญัติฯ ได้อย่างรวดเร็ว

Title	Computer Traffic Data Management System
Student	Ms. Thanawan Assavathanabodee
Student ID.	50066508
Degree	Master of Science
Program	Information Science
Academic Year	2008
Advisor	Assoc.Prof .Dr. Chtipat Pornavalai

ABSTRACT

Computer Traffic Data Management System is a system that has been developed to assist the Access Service Provider to store computer traffic data log to be in line with the laws and regulations regarding computer crime Act B.E. 2007, and the announcement of Ministry of ICT regarding the code of conduct of storing computer traffic data log for provider 2007. In which the development project has been design to work in form of Web Application that made it convenient for managing and storing Computer Traffic Data Log from each server according to the Act. Namely Mail Server, Web Server, Proxy Server, FTP Server, along with convenient of searching computer traffic data log that is stored in the database. Moreover to be able to tell who in the organization has done what to which IP Address and when. All this together for the computer traffic data log can be brought to beneficial use in investigating and finding the person responsible for their crime against the act in a short time.

กิตติกรรมประกาศ

การพัฒนาระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์ สามารถสำเร็จลุล่วงเป็นอย่างดี เนื่องจากคณาจารย์ทุกท่านที่ได้ถ่ายทอดความรู้ในการศึกษาครั้งนี้ โดยเฉพาะอย่างยิ่ง ขอขอบพระคุณ อาจารย์ โชติพัชร์ ภรณวลัย ที่เสนอขอบเขตการพัฒนาระบบงาน และคอยให้คำปรึกษาในเรื่องการพัฒนาระบบงาน เพื่อให้โครงงานครั้งนี้เสร็จสมบูรณ์

ขอขอบคุณ นายนุชา เสาสี รุ่น IS23.2 , นายอำนวย อุทัยรังษี , นายปฏิญญา สังฆพร , นายชัยพฤกษ์ วัฒนาการ ซึ่งเป็นรุ่นพี่และเพื่อนที่ทำงาน บริษัทแอดวานซ์ อินโฟร์ เซอร์วิส จำกัด มหาชน ที่ให้คำปรึกษาในเรื่องการทำงานผ่านเครือข่ายต่างๆ

ขอขอบคุณนายนวกิจ ลีลาอุดมลิปี ที่ช่วยให้คำปรึกษาในเรื่องการเขียนเว็บแอพพลิเคชัน

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณบิดา มารดา และครอบครัวของข้าพเจ้าที่คอยให้กำลังใจ และให้การสนับสนุนในทุก ๆ เรื่อง ในการศึกษาตลอดมาจนปริญญานิพนธ์นี้สำเร็จลุล่วงไปได้ด้วยดี

คุณค่าและประโยชน์อันพึงมาจากโครงงานพัฒนาระบบงานฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ธนวรรณ อัศวธนบดี

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

รูปที่ หน้า

สารบัญภาพ (ต่อ)

รูปที่ หน้า

สารบัญภาพ (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ด้วยในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เริ่มเข้าไปมีบทบาทและทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มขยายวงกว้าง และทวีความรุนแรงเพิ่มมากขึ้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ประกาศลงในราชกิจจานุเบกษา เมื่อวันที่ 18 มิถุนายน 2550 และให้มีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นไป พระราชบัญญัติฉบับนี้มีวัตถุประสงค์ เพื่อต้องการลดปัญหาการก่ออาชญากรรมทางคอมพิวเตอร์ โดยให้องค์กรหรือผู้ให้บริการต่างๆ มีการบันทึกข้อมูลที่เป็นประโยชน์ต่อการแกะรอยหาผู้กระทำความผิดทางคอมพิวเตอร์ ซึ่งได้มีการกำหนดหน้าที่ของผู้ให้บริการในการจัดเก็บข้อมูลของผู้ใช้บริการไว้ว่า ผู้ให้บริการจะต้องจัดเก็บข้อมูลจราจร (Traffic Data) และ Log อื่น ๆ ของระบบที่เกี่ยวข้องให้มีความน่าเชื่อถือ ไม่มีบุคคลใดสามารถเปลี่ยนแปลงหรือแก้ไขข้อมูลดังกล่าวได้ และจะต้องสามารถระบุตัวตนของผู้ใช้งานได้ เพื่อใช้สำหรับติดตามหาตัวผู้กระทำผิด ไม่น้อยกว่า 90 วัน แต่ไม่เกิน 1 ปี โดยบังคับให้ผู้ให้บริการต้องมีข้อมูลจราจร (Traffic Data) พร้อมสามารถตรวจสอบได้ ตั้งแต่วันที่ 22 สิงหาคม 2551 เป็นต้นไป อีกทั้งอุปกรณ์ที่บันทึกข้อมูลนั้นจะต้องมีระบบเวลาที่น่าเชื่อถือตามมาตรฐานสากล โดยหากผู้ให้บริการใดไม่ปฏิบัติต้องระวางโทษปรับไม่เกิน 5 แสนบาท

ดังนั้น จึงได้มีการจัดทำระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อประโยชน์ในการนำข้อมูลจราจรนั้น มาใช้ในการตรวจสอบหาผู้กระทำความผิด ตามวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นอกจากนี้ยังช่วยให้ผู้ดูแลระบบสามารถบริหารจัดการ และสืบค้นข้อมูลจราจรในเบื้องต้นได้ ผ่านทาง Web Browser

1.2 วัตถุประสงค์

1.2.1 เพื่อรวบรวมจัดเก็บข้อมูลจราจร (Traffic Data) และรักษาความปลอดภัยบนระบบเครือข่ายโดยมีการจัดเก็บเป็นแบบรวมศูนย์กลาง เพื่อให้ง่ายต่อการค้นหาและบริหารจัดการ

1.2.2 เพื่อให้การจัดเก็บข้อมูลจราจรถูกต้อง และเป็นไปตามพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.2.3 เพื่อเพิ่มความสะดวกแก่ผู้ดูแลระบบ ในการวิเคราะห์การใช้งานคอมพิวเตอร์และเครือข่าย

1.2.4 เพื่อให้สามารถระบุตัวบุคคลของผู้ใช้งานเซอร์วิสต่างๆ ได้ และบอกได้ว่า ใคร ทำอะไร ที่ไหน เมื่อไร

1.3 ขอบเขตของโครงงาน

1.3.1 ออกแบบและพัฒนา Computer Traffic Data Management Web Application

1.3.2 ออกแบบและพัฒนาระบบเครือข่าย เพื่อสนับสนุนการทำงานของระบบ

1.3.3 ออกแบบและจัดทำฐานข้อมูลที่เกี่ยวข้อง เพื่อสนับสนุนการทำงานของระบบ

1.3.4 สร้างข้อมูลจราจรจากการใช้งานเซอร์วิสต่างๆ เพื่อสนับสนุนการทำงานของระบบ

1.4 วิธีการดำเนินงาน

1.4.1 ศึกษาแนวทางปฏิบัติในการจัดเก็บข้อมูลจราจรให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.4.2 ศึกษาการทำงานและติดตั้งเครื่องแม่ข่ายต่างๆ ได้แก่ Active Directory , FTP Server , DHCP Server , Mail Server , Proxy Server , Web Server

1.4.3 ศึกษาข้อมูลและรูปแบบของ Log ประเภทต่างๆ ที่จัดเก็บในแต่ละเซอร์วิส

1.4.4 ศึกษาวิธีการใช้เครื่องมือที่ใช้ในการส่งข้อมูล Log ไปยังเครื่องคอมพิวเตอร์อื่น

1.4.5 ศึกษาวิธีการใช้เครื่องมือที่ใช้ในการรับข้อมูล Log จากเครื่องคอมพิวเตอร์อื่น

1.4.6 ศึกษาวิธีการใช้เครื่องมือ LogParser ที่ใช้ในการจัดเก็บข้อมูล Log ลงในฐานข้อมูล

1.4.7 ออกแบบฐานข้อมูล SQL Server สำหรับจัดเก็บข้อมูลจราจร

1.4.8 ทำการติดตั้งเครื่องแม่ข่ายต่างๆ และส่งข้อมูลจากเครื่องแม่ข่ายต่างๆ ไปไว้ที่เครื่องกลาง (Centralized Log Server) รวมถึงจัดเก็บข้อมูลดังกล่าวลงในฐานข้อมูลที่ออกแบบไว้

1.4.9 ศึกษาการเขียน Web Application

1.4.10 ออกแบบหน้าจอ Web Application

1.4.11 เขียน Web Application พร้อมกับทำการทดลองใช้งาน

1.4.12 ทำการแก้ไขข้อบกพร่องและนำผลทดสอบที่ได้ไปใช้งาน

1.5 ประโยชน์ที่คาดว่าจะได้รับจากโครงงาน

1.5.1 สามารถจัดเก็บข้อมูลจราจรได้ตรงตามความต้องการของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.5.2 สามารถเพิ่มความสะดวกแก่ผู้ดูแลระบบในการวิเคราะห์การใช้งานคอมพิวเตอร์และเครือข่ายได้ผ่านทาง Web Browser

1.5.3 ประหยัดค่าใช้จ่ายในการสั่งซื้ออุปกรณ์ Hardware หรือ Software เพื่อใช้ในการจัดเก็บข้อมูลจราจร

1.5.4 ผู้ดูแลระบบสามารถตรวจสอบข้อมูลการใช้งาน โดยสามารถค้นหาข้อมูลจากคำค้น (Keyword Search) ได้จากชื่อ, IP Address, วันเวลาที่มีการใช้งานได้

1.5.5 ผู้ดูแลระบบสามารถทราบได้ว่า ใคร ทำอะไร ที่ไหน เมื่อไร โดยสามารถระบุตัวบุคคลที่ใช้งานเซอร์วิสต่างๆ ได้

บทที่ 2
ทฤษฎี และหลักการที่เกี่ยวข้อง

2.1 สาระสำคัญของพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550

2.1.1 คำนิยามของข้อมูลจราจรทางคอมพิวเตอร์ (ราชกิจจานุเบกษา. 2550: 4)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ได้ให้คำจำกัดความเกี่ยวกับ ข้อมูลจราจรทางคอมพิวเตอร์ไว้ว่า

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น"

2.1.2 ความสำคัญของข้อมูลจราจรทางคอมพิวเตอร์ (ราชกิจจานุเบกษา. 2550: 4)

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ปี 2550 มีสาระสำคัญว่า

"ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดี อันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว"

2.1.3 บทลงโทษของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่สอดคล้องตามพรบ. (ราชกิจจานุเบกษา. 2550: 11)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ได้กำหนดเรื่องการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ในมาตรา 26 ว่า

"ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท"

2.2 หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ตามพรบ. กำหนดนั้น แบ่งออกเป็น 4 เรื่อง คือ

2.2.1 ความครบถ้วนของข้อมูลจราจรที่จัดเก็บ

ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ ดังนี้

2.2.1.1 ข้อมูลอินเตอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย

1) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Log Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access-Control System) or RADIUS (Remote Authentication Dial-In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Services))
2) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
3) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
4) ข้อมูลหมายเลขชุดอินเตอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)
5) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)

2.2.1.2 ข้อมูลอินเตอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)

1) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log) ซึ่งได้แก่
   - ข้อมูลหมายเลขข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)
   - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-Mail Address)
   - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-Mail Address)
   - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ(Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น
2) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ(IP Address of Client Connected to Server)

3) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to Server)

4) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ในขณะนั้น (IP Address of Sending Computer)

5) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)

6) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP3 (Post Office Protocol Version 3) Log or IMAP4 (Internet Message Access Protocol Version 4) Log)

2.2.1.3 ข้อมูลอินเตอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล

2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)

3) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)

4) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)

5) ข้อมูลตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)

2.2.1.4 ข้อมูลอินเตอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ

2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ

3) ข้อมูลหมายเลขชุดอินเตอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น

4) ข้อมูลคำสั่งการใช้งานระบบ

5) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identification) เช่น ตำแหน่งของเว็บเพจ

2.2.1.5 ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP (Network News Transfer Protocol) Log)

2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)

3) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)

4) ข้อมูลชื่อเครื่องให้บริการ (Host Name)

5) ข้อมูลหมายเลขลำดับข้อความที่ถูกส่งไปแล้ว (Posted Message ID)

2.2.1.6 ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเตอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Message (IM) เป็นต้น

1) ข้อมูล Log เช่น ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client ID Server) และ

2) ข้อมูลชื่อเครื่องบนเครือข่าย

3) หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อต่ออยู่ในขณะนั้น (Host name and IP Address) เป็นต้น

2.2.2 การเก็บรักษาข้อมูลจราจรให้เป็นความลับและน่าเชื่อถือ

ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ปี 2550 ได้ระบุเกี่ยวกับหลักการเก็บรักษาข้อมูลให้มีความน่าเชื่อถือ ในข้อ 8 กล่าวว่า

"การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุ ตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

สื่อ (Media) ที่จัดเก็บข้อมูลจราจร ควรต้องเป็นสื่อที่สามารถป้องกันความปลอดภัยจากการแก้ไขข้อมูลโดยมิชอบของผู้ที่ไม่มีส่วนเกี่ยวข้องได้เป็นอย่างดี เรียกได้ว่าสามารถรักษาความถูกต้องของข้อมูลจราจรไว้ได้เพื่อให้มีน้ำหนักในชั้นศาลในการสืบสวนสอบสวนต่อไปและควรต้องมีระดับชั้นความปลอดภัยในการเข้าถึงข้อมูลจราจรดังกล่าว (Access Control) โดยระบุเป็นตัวบุคคลได้ ซึ่งควรต้องมีระบบ Authentication หรือ Identity Management เป็นต้น (ระบบ Authentication ยกตัวอย่าง เช่น การใช้ระบบ Microsoft Active Directory)

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

การเก็บlog fileไว้ในเครื่องนั้น อาจทำให้ความปลอดภัยของ log fileไม่ดีพอและไม่น่าเชื่อถือเนื่องจาก log file อาจถูกแก้ไขโดย system admin ของเครื่องนั้น หรืออาจถูกแก้ไขโดยแฮกเกอร์ ดังนั้นจึงควรจัดเก็บ log file ในแบบรวมศูนย์ (Centralized Log) และมีการตรวจสอบ Integrity โดยการทำ Data hashing เมื่อ log file มีปริมาณมากก็ควรทำ Data Archiving เพื่อทำให้มีพื้นที่ในการจัดเก็บ log fileเพิ่มขึ้น รวมทั้งผู้ที่สามารถเข้าถึงข้อมูล log file ควรเป็นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือ ผู้เชี่ยวชาญด้านความปลอดภัยข้อมูล หรือ บุคคลที่องค์กรมอบหมายให้ติดต่อกับพนักงานเจ้าหน้าที่เท่านั้น โดยที่ system admin ไม่ควรมีสิทธิเข้ามาแก้ไข log file ดังกล่าว

2.2.3 อุปกรณ์ที่ให้บริการทุกชนิดต้องมีการตั้งเวลาให้ตรงกับเวลาอ้างอิงสากล

เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

การอ้างอิงเวลาของระบบที่องค์กรใช้งานอยู่ให้ตรงกับเวลาสากล ได้แก่ การรับสัญญาณนาฬิกาจากดาวเทียม หรือ การใช้ระบบ GPS หลายคนรู้จักกันในนาม atomic clock ซึ่งเทียบได้กับ Stratum 0 สำหรับการรับสัญญาณนาฬิกาโดยการใช้ Network Time Protocol จาก NTP server ก็ถือว่าอนุโลมได้เพราะตัว NTP server มีการอ้างอิงเวลามาจาก Stratum 0 เช่นกัน

2.2.4 การระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้

การที่จะระบุผู้ใช้บริการเป็นรายบุคคลได้นั้นองค์กรจำเป็นที่จะต้องมีระบบ Authentication เพื่อให้ผู้ใช้บริการเข้ามา Log on หรือ Sign On กับระบบ โดยอาจผ่านทางระบบ proxy หรือ ระบบ cache โดยสามารถตรวจสอบผู้ใช้บริการเป็นรายบุคคลแบบหนึ่งต่อหนึ่ง ซึ่งผู้ใช้บริการควรเก็บรักษารหัสผ่านของตนไว้เป็นความลับ และไม่ควรมีการใช้ชื่อกลาง (Shared User ID)ในการเข้าใช้งานระบบทุกระบบโดยเฉพาะระบบอินเทอร์เน็ต

2.3 การตั้งเวลาให้ตรงกับเวลาอ้างอิงสากล

เป็นที่เข้าใจกันดีแล้วว่าอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่าย ต่างๆ ในระบบสารสนเทศนั้นมีความสามารถของการรักษาความเที่ยงตรง และแม่นยำของเวลาได้แตกต่างกัน ทั้งนี้ขึ้นอยู่กับปัจจัยหลายด้าน เช่น วัสดุที่ให้สร้างวงจรเวลาของอุปกรณ์คอมพิวเตอร์, อุณหภูมิ, ความชื้น, คลื่นแม่เหล็กไฟฟ้า หรือ ความสม่ำเสมอของพลังงานที่จ่ายให้กับวงจรเวลา เป็นต้น ส่งผลให้อุปกรณ์ต่างกันอาจจะให้ค่าเวลาที่แตกต่างกัน

หากอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่ายในระบบสารสนเทศมีค่าเวลาที่แตกต่างกันแล้วนั้นจะส่งผลให้เกิดปัญหากับผู้ใช้งาน รวมทั้งผู้ดูแลระบบในการปฏิบัติงานต่างๆ เช่น

- ความคาดเคลื่อนของเวลาในการการแจ้งปัญหาของระบบสารสนเทศ ระหว่างผู้ใช้งานและผู้ดูแลระบบ

- ความสับสนในการตรวจสอบ และวิเคราะห์เหตุการณ์ต่างๆ เช่น เหตุการณ์การบุกรุก เหตุการณ์ของปัญหาด้านเครือข่าย หรือระบบคอมพิวเตอร์

- ผู้พัฒนามีความสับสนในเวอร์ชันของโค้ดระหว่างการพัฒนา

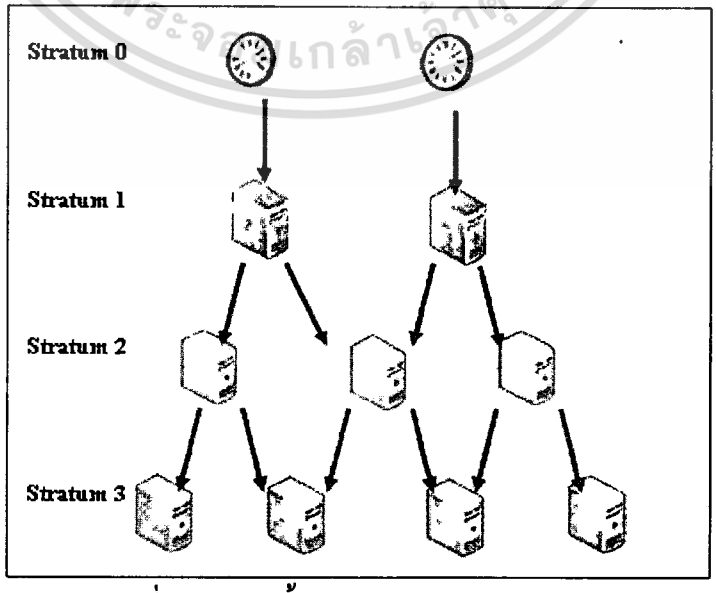
- มีการใช้งานไฟล์ข้อมูล หรือฐานข้อมูล ที่ซ้อนทับกัน

จากตัวอย่างปัญหาข้างต้นจะเห็นว่าผู้ดูแลระบบ และผู้ใช้งานระบบสารสนเทศมีความจำเป็นต้องทำให้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายของระบบสารสนเทศในองค์กรมีค่าเวลาเที่ยงตรง และแม่นยำเหมือนกัน

2.3.1 ความรู้พื้นฐานของ NTP

Network Time Protocol เป็นโพรโตคอลในระดับ Application Layer ของระบบเครือข่ายแบบ TCP/IP ที่ทำหน้าที่ในการเทียบเวลาระหว่างอุปกรณ์คอมพิวเตอร์ ซึ่งอ้างอิงจาก RFC หมายเลข RFC 778, RFC 891, RFC 956, RFC 958, และ RFC 1305 การทำงานของโพรโตคอลชนิดนี้จะต้องอาศัยเครื่องให้บริการที่เปิดพอร์ตหมายเลข 123 ชนิด UDP ในการรอรับข้อมูลร้องขอการเทียบเวลาจากเครื่องลูกข่าย

ลักษณะการแจกจ่ายเวลาของ NTP นั้นจะอยู่ในรูปแบบลำดับชั้น ที่เรียกว่า “Clock Strata” โดยแบ่งลำดับชั้นของการเทียบเวลาดังนี้



รูปที่ 2.1 ลำดับชั้นของการเทียบเวลาใน NTP

ตารางที่ 2.1 แสดงความหมายของการเทียบเวลาในระดับชั้นต่างๆ

ระดับชั้น	รายละเอียด
Stratum 0	เป็นอุปกรณ์ของแหล่งกำเนิดเวลา เช่น Atomic clocks, GPS เป็นต้น ซึ่งอุปกรณ์แต่ละชนิดมีข้อดีและข้อเสียแตกต่างกัน เช่น การประยุกต์ใช้ GPS จะมีต้นทุนที่ต่ำกว่า Atomic clock มาก แต่จะมีเสถียรภาพที่น้อยกว่า หากสภาพอากาศไม่เหมาะสม GPS จะไม่สามารถรับสัญญาดาวเทียมได้ เป็นต้น
Stratum 1	เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับ stratum 0 ได้รับค่าเวลามาจาก stratum 0 โดยตรงผ่านการเชื่อมต่อในระบบคอมพิวเตอร์ เช่น RS-232 เป็นต้น
Stratum 2	เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 1 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้อาจจะร้องขอการเทียบเวลาจาก stratum 1 ได้มากกว่า 1 แหล่งเพื่อรองรับการทำงานแบบทดแทนกันเมื่อไม่สามารถเข้าถึง stratum 1 ตัวใดตัวหนึ่งก็จะสามารถร้องขอการเทียบเวลาจาก stratum 1 ตัวอื่นได้ต่อไป นอกจากนี้เครื่องคอมพิวเตอร์ใน stratum 2 สามารถเทียบเคียงเวลาระหว่างกันแบบ peer-to-peer เพื่อรักษาเวลาให้เทียบเท่ากันในระดับเดียวกัน
Stratum 3	เป็นเครื่องคอมพิวเตอร์ที่ร้องขอการเทียบเวลาจากเครื่องคอมพิวเตอร์แม่ข่าย stratum 2 ผ่านระบบเครือข่าย TCP/IP ด้วยการใช้งาน NTP เครื่องคอมพิวเตอร์ในระดับนี้จะสามารถอ้างอิง stratum 2 ได้มากกว่า 1 แหล่ง และสามารถทำงานในรูปแบบ peer-to-peer ได้เช่นเดียวกัน

ตารางที่ 2.2 รายชื่อ NTP Server ที่มีอยู่ในประเทศไทย

สถาบัน	NTP Server	Clock Strata
สถาบันมาตรวิทยาแห่งชาติ	time1.nimt.or.th	Stratum-1
	time2.nimt.or.th	Stratum-1
	time3.nimt.or.th	Stratum-1
กระทรวงวิทยาศาสตร์และเทคโนโลยี	time.most.go.th	Stratum-2
กรมอุทกศาสตร์ กองทัพเรือ	time.navy.mi.th	Stratum-1
มหาวิทยาลัยเกษตรศาสตร์	ntp.ku.ac.th	-
มหาวิทยาลัยสงขลานครินทร์	time.psu.ac.th	Stratum-1
NECTEC	clock.thaicert.nectec.or.th	-

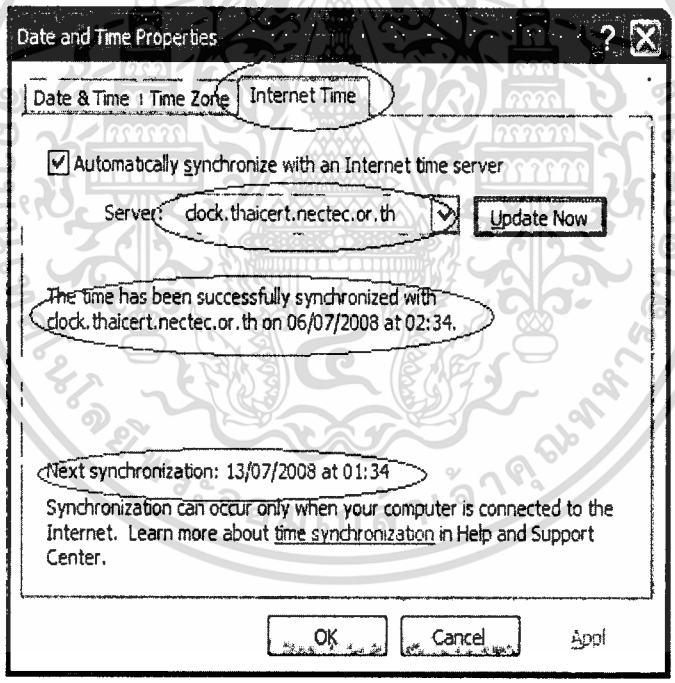
2.3.2 วิธีการปรับเทียบเวลามาตรฐาน

2.3.2.1 การปรับเทียบเวลามาตรฐานผ่าน Network Time Protocol

Network Time Protocol (NTP) เป็นโพรโตคอลที่ใช้สำหรับปรับเทียบเวลา (Time Synchronization) ของ อุปกรณ์ทางคอมพิวเตอร์ ผ่านพอร์ตหมายเลข 123 ชนิด UDP โดยมีเครื่องแม่ข่าย (NTP Server) เป็นตัวให้บริการส่งเวลามาตรฐานผ่านทางเครือข่ายอินเทอร์เน็ตไปยังเครื่องปลายทาง เพื่อปรับเทียบเวลาให้ตรงกับเวลามาตรฐาน

<u>สำหรับระบบปฏิบัติการ Windows</u>

ในระบบปฏิบัติการ Windows XP Service Pack 2 , Windows Vista และ Windows 2003 Server จะมีโปรแกรมสำหรับการเทียบเวลาที่ติดตั้งมาพร้อมกับระบบ ปฏิบัติการ ซึ่งสามารถปรับแต่งเวลาได้โดยการ Double Click พื้นที่ของวันเวลาบน Task Bar ในตำแหน่งมุมขวาล่าง จะปรากฏโปรแกรม Clock ดัง 2.1



รูปที่ 2.2 แสดงวิธีการปรับเทียบเวลา เวลากับเครื่อง Time Server ของ Nectec (clock.thaicert.nectec.or.th)

จากรูปที่ 2.2 นั้น จะเห็นว่าวิธีการปรับเทียบเวลาดังกล่าว จะมีรอบการปรับเทียบเวลาแบบอัตโนมัติ โดยจากตัวอย่าง คือ อุปกรณ์ได้มีการปรับแต่งเวลาครั้งล่าสุดในวันที่ 06/07/2008 เวลา 02.34 น. และจะปรับเวลารอบถัดไป ในวันที่ 13/07/2008 เวลา 01.34 น.

สำหรับระบบปฏิบัติการ Unix / Linux

ในระบบปฏิบัติการ Unix/Linux นั้น การปรับเทียบเวลามาตรฐานผ่าน Network Time Protocol สามารถทำได้ 2 วิธี ดังนี้

วิธีที่ 1 การเทียบเวลาด้วยการใช้คำสั่ง ntpdate

ntpdate เป็นคำสั่งระบบปฏิบัติการ Linux ที่ใช้ในการตั้งค่าเวลาผ่านโพรโตคอล ntp ซึ่งผู้ดูแลระบบ หรือ root เท่านั้นที่สามารถใช้ งานคำสั่ง ntpdate ได้โดยจะต้องเรียกใช้คำสั่ง ntpdate เองทุกครั้งเมื่อต้องการเทียบเวลา

ตัวอย่างคำสั่งที่ทำการเทียบเคียงเวลาจากเครื่อง clock.wu.ac.th

```
# ntpdate clock.wu.ac.th
 24 Apr 15:35:42 ntpdate[4317]: step time
server 202.28.68.130 offset -6.245777 sec
```

ผู้ดูแลระบบสามารถปรับแต่งให้ระบบทำการเทียบเคียงเวลาที่ถูกต้องอย่างต่อเนื่อง โดยการสร้าง cron job ที่มีรูปแบบดังตัวอย่าง

```
# crontab –e
30 * * * * ntpdatc clock.wu.ac.th
```

จากตัวอย่างการสร้าง cron job ข้างต้นนั้น หมายถึง กำหนดให้ระบบทำการเทียบเวลากับเครื่อง Time Sever : clock.wu.ac.th ทุกๆ ครึ่งชั่วโมง (เวลาปรับเปลี่ยนตามต้องการ)

วิธีที่ 2 การเทียบเวลาด้วยการใช้ Network Time Protocol Daemon (ntpd)

ntpd เป็นเดมอนที่ใช้ในการเทียบเวลากับเครื่องให้บริการตามมาตรฐานของเครือข่ายอินเทอร์เน็ตผ่านโพรโตคอล ntp โดยไฟล์ที่ใช้กำหนดค่าการทำงานของ ntpd คือ /etc/ntp.conf ซึ่ง ntpd ใช้ตรวจสอบแหล่งที่ใช้ในการเทียบค่าเวลา

ตัวอย่างวิธีการกำหนดค่าในไฟล์ /etc/ntp.conf

```
# vi /etc/ntp.conf
server clock.nectec.or.th
server clock2.nectec.or.th
```

การกำหนดชื่อเครื่องให้บริการ สามารถกำหนดได้หลายเครื่อง จากตัวอย่าง โปรแกรมจะทำหน้าที่ในการเปรียบเทียบและเลือกว่าจะเทียบเวลากับ Time server ใด ระหว่าง clock.nectec.or.th และ clock2.nectec.or.th ซึ่งหลังจากนั้นจะต้องสั่งให้โปรแกรมทำงานโดยใช้คำสั่ง ntpd ดังนี้

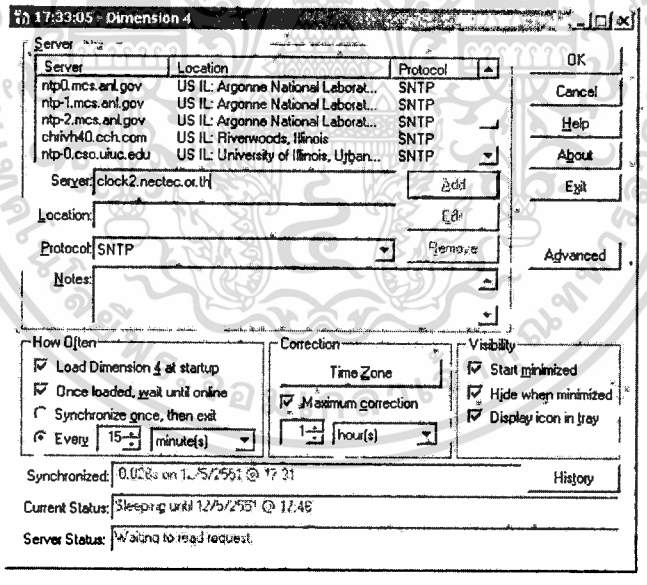
```
# ntpd
```

นอกจากนี้ ผู้ดูแลระบบยังสามารถกำหนดให้ ntpd ทำงานอัตโนมัติเมื่อมีการ start เครื่องใหม่ทุกครั้ง โดยใช้คำสั่งดังนี้

```
# chkconfig ntpd on
```

2.3.2.2 การเทียบเวลาโดยใช้โปรแกรมประยุกต์

ในระบบปฏิบัติการ Windows มีโปรแกรมประยุกต์อีกตัวหนึ่งที่รองรับการทำงานของระบบ NTP ชื่อ Dimension 4 โดยมี User Interface ให้สามารถใช้งานง่ายขึ้น (สามารถดาวโหลดโปรแกรม Dimension4 ได้จาก http://58.137.28.174/downloads/d4time50.msi)

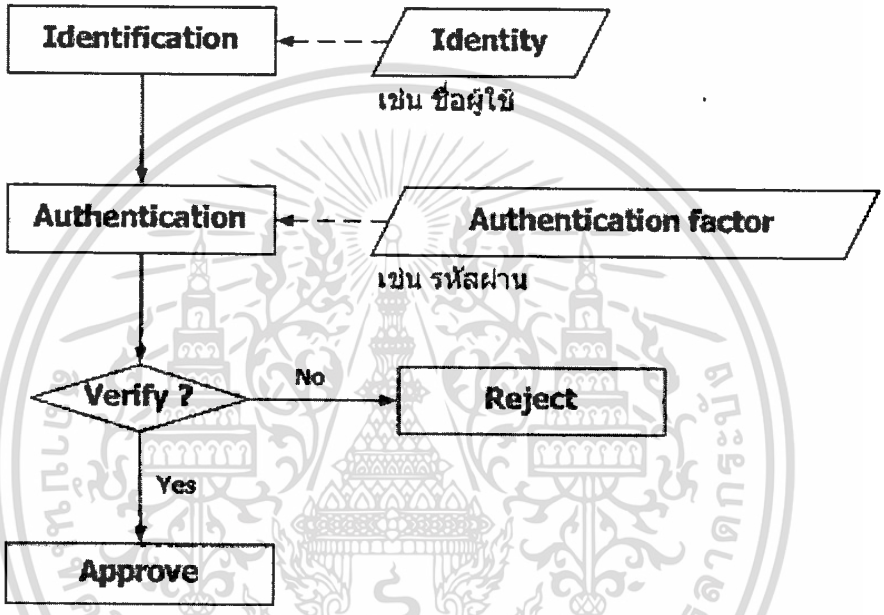


รูปที่ 2.3 แสดง User Interface ของโปรแกรม Dimension4

จากรูปที่ 2.3 จะเห็นได้ว่าในช่อง Synchronized: จะปรากฏค่า -0.026 s on 12/5/2551 @ 17:31 หมายถึง เวลาในคอมพิวเตอร์ต่างจากเวลามาตรฐานไป 0.026 วินาที ณ วันที่ 12/5/2551 เปรียบเทียบที่เวลา 11:12 น.

2.4 การระบุตัวตนและการพิสูจน์ตัวตน

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐานที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง โดยแบ่งออกเป็น 2 ขั้นตอน คือขั้นตอนแรกผู้ใช้จะทำการแสดงหลักฐานในการพิสูจน์ตัวตนต่อระบบหรือเรียกว่า ขั้นตอนการระบุตัวตน ขั้นต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างหรือที่เรียกว่า ขั้นตอนการพิสูจน์ตัวตนหลังจากนี้ ระบบจะทำการตรวจสอบหลักฐาน ถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ



รูปที่ 2.4 วิธีหรือกระบวนการพิสูจน์ตัวตน [สิริพรและคณะ, 2547]

2.4.1 ส่วนประกอบของการพิสูจน์ตัวตน

ส่วนประกอบเบื้องต้นของการพิสูจน์ตัวตนสามารถแบ่งได้เป็น 3 ส่วนดังนี้

1) การพิสูจน์ตัวตน (Authentication) หมายถึง ขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบก่อนที่จะเข้าสู่ระบบได้ การพิสูจน์ตัวตนถือว่าเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

2) การกำหนดสิทธิ์ (Authorization) หมายถึง ข้อจำกัดของบุคคลที่เข้ามาในระบบว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง

3) การบันทึกการใช้งาน (Accountability) หมายถึง การบันทึกรายละเอียดของการใช้ระบบรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบสามารถตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้ทำการเปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

2.4.2 ประเภทของการพิสูจน์ตัวตน

จากส่วนประกอบข้างต้นของการพิสูจน์ตัวตนถือว่าเป็นปัจจัยสำคัญมากในการนำมาประยุกต์ใช้เพื่อการขอเข้าใช้บริการในระบบซึ่งสามารถแบ่งประเภทของการพิสูจน์ตัวตน (Authentication Types) ได้ดังนี้

1) ไม่มีการพิสูจน์ตัวตน (No Authentication) หมายถึง หลักการของการพิสูจน์ตัวตนสำหรับเงื่อนไข ของข้อมูลที่มีลักษณะเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือข้อมูลข่าวสารที่แหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

2) การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) หมายถึงรหัสผ่านที่จำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้น และเป็นวิธีการที่ใช้กันอย่างแพร่หลายแต่ยังไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอน3617 .พิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไปของผู้ใช้และวิทยาการความก้าวหน้าทำให้รหัสผ่านสามารถถูกดักจับได้ระหว่างการสื่อสารผ่านทางเครือข่าย

3) การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) หมายถึง PIN (Personal Identification Number) ที่เป็นรหัสลับส่วนบุคคลที่ ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบที่ใช้กันแพร่หลายในปัจจุบัน คือการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และ เครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

4) การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens หมายถึง Authenticator หรือ Token ซึ่งเป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านที่เปลี่ยนแปลงได้ (Dynamic Password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย แบ่งออกเป็น 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส

5) การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits) หมายถึง การนำลักษณะเฉพาะทางชีวภาพของแต่ละบุคคลมาใช้ในการพิสูจน์ตัวตน เพื่อเพิ่มความน่าเชื่อถือได้มากขึ้นเพราะลักษณะเหล่านี้ทำการลอกเลียนแบบกันไม่ได้ เช่น การใช้ลายนิ้วมือ เสียงม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน

6) การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password :OTP) หมายถึง รหัสผ่านที่จะถูกเปลี่ยนทุกๆ ครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกันวิธีนี้จะทำให้ระบบมี ความปลอดภัยมากขึ้น การทำงานของ

OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่งChallenge Stringกลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้า แฮชฟังก์ชันแล้วออกมาเป็นค่า Response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบ กับค่าที่เซิร์ฟเวอร์คำนวณเองได้ โดยเซิร์ฟเวอร์จะใช้วิธีการคำนวณเดียวกับฝั่งผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

7) การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key Cryptography) หมายถึง การเข้ารหัสข้อมูลโดยใช้ กุญแจ (Key) ในการทำงาน 2 ตัวหรือเรียกว่า การเข้ารหัสแบบคู่ รหัสกุญแจ โดยกุญแจตัวหนึ่งเรียกว่า กุญแจสาธารณะ (Public Key) ใช้ในส่วนของการเข้ารหัสข้อความและอีกตัวหนึ่งเรียกว่ากุญแจส่วนตัว (Private Key) ใช้ในส่วนของการถอดรหัสข้อความ โดยตัวกุญแจสาธารณะจะถูกเผยแพร่ให้กับผู้อื่น ส่วนกุญแจส่วนตัวจะถูกเก็บไว้กับเจ้าของ แนวคิดของการเข้ารหัสแบบกุญแจสาธารณะ ใช้หลักคณิตศาสตร์ที่เรียกว่า ฟังก์ชันทางเดียว (One – Way Function) ซึ่งมีความเกี่ยวข้องกับตัวเลขจำนวนเฉพาะ (Prime Number) คือถ้าเอาจำนวนเฉพาะสองจำนวนมาคูณกันแล้วเอาผลคูณที่ได้มาทำการหาตัวประกอบย้อนกลับ ในกรณีตัวเลขมีขนาดใหญ่มากๆ ก็จะทำให้หาตัวประกอบยากและใช้เวลาคำนวณมากขึ้นด้วย จากตรงจุดนี้จึงนำสมบัติในข้อนี้มาใช้ในการเข้ารหัสลับ คนแรกที่คิดเรื่องนี้คือ Whitfield Diffie และ Martin Hellman โดยพวกเขาได้นำเสนอใน National Computer Conference เมื่อ ปี 1976 ซึ่งได้รับการยอมรับกันโดยทั่วไป และถูกนำมาใช้เป็นหลักการพื้นฐานในการสร้างกุญแจ สำหรับการเข้าและถอดรหัสข้อมูลในปัจจุบัน [Menezes , 1996]

8) การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature) หมายถึงลายมือชื่อดิจิทัล เป็นเทคนิคที่นำมาใช้เพื่อวัตถุประสงค์เดียวกันกับการเซ็นชื่อหรือการลงลายมือชื่อแบบเดิมคือใช้ในการตรวจสอบความถูกต้องของข้อความต้นฉบับรวมถึงการยืนยันของตัวบุคคลว่าบุคคลใดได้รับหรือส่งข้อความดังกล่าวจริง ซึ่งแตกต่างจากการลงลายมือชื่อแบบเดิมๆ ที่ง่ายต่อการปลอมแปลงและไม่สามารถทำ การตรวจสอบและยืนยันข้อเท็จจริงต่างๆ ได้ประกอบด้วย 2 ขั้นตอนคือ Digital Signature Creation เป็นกระบวนการสร้างลายมือชื่อดิจิทัล Digital Signature Verification เป็นกระบวนการพิสูจน์ลายมือชื่อดิจิทัล เพื่อตรวจสอบว่าข้อความที่ได้รับถูกแก้ไขระหว่างการส่งข้อมูลหรือไม่ [Menezes , 1996]

9) การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (Zero-Knowledge Proofs) หมายถึง การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริงนั่นก็คือ ระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม -คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อ 3629 .ผู้ใช้คนนั้นๆ เข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่

ผู้ใช้คนนั้นๆ สร้างขึ้นมาถามผู้ใช้คนนั้นๆ ก่อนที่จะยอมให้เข้าใช้ระบบได้จริงการให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบนั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ วิธีการพิสูจน์ตัวตนแบบนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ หรืออาจจะเรียกได้ว่าเป็นการนำความรู้ด้าน Artificial Intelligence มาใช้ควบคู่ด้วย

2.5 เครื่องแม่ข่าย (Server)

เครื่องแม่ข่ายเป็นเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่างๆ โดยแต่ละเครือข่ายสามารถมีเครื่องแม่ข่ายได้หลายเครื่องตามความต้องการ โดยชนิดของเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องแม่ข่าย มีดังนี้

2.5.1 Web server

เป็นเครื่องคอมพิวเตอร์ที่ให้บริการบนระบบอินเตอร์เน็ตที่เก็บข้อมูลในรูปแบบของโฮมเพจ (HTML Document) โดยเครื่อง Client จะมี Browser ได้แก่ Netscape และ internet Explorer ที่จะทำการร้องขอไปยัง host ที่ต้องการ แล้ว host ก็จะทำการส่ง HTML กลับมายังเครื่อง Client เพื่อนำมาประมวลผล แล้วจึงแสดงผลออกมา

2.5.2 FTP server

FTP ย่อมาจาก File Transfer Protocol เป็นบริการรับส่งไฟล์ระหว่างเครื่องคอมพิวเตอร์ โดยที่ FTP Server เป็นคอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการถ่ายโอนแฟ้มข้อมูลโดยบริการของ FTP แบ่งออกเป็น 2 ประเภท คือ

1) Download เป็นบริการรับไฟล์ หรือ copy ไฟล์จากเครื่องคอมพิวเตอร์ที่เป็น FTP Server มายังเครื่องคอมพิวเตอร์ลูกข่าย

2) Upload เป็นบริการส่งไฟล์ หรือ copy ไฟล์จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์ที่เป็น FTP Server

2.5.3 Mail server

เป็นเครื่องคอมพิวเตอร์ที่มีหน้าที่รับและส่งอีเมล์ เปรียบเหมือนที่ทำการไปรษณีย์ในระบบธรรมดา ใครจะส่งจดหมายก็ส่งมารวมไว้ที่นี่ แล้วบุรุษไปรษณีย์จะนำจดหมายส่งต่อถึงผู้รับอีกทีหนึ่ง โดยผู้อ่านไม่ต้องรับหรือส่งจดหมายเองโดยตรง ตัวอย่าง mail server ที่เป็นที่รู้จักทั่วไป เช่น hotmail.com หรือ thaimail.com เป็นต้น

โปรโตคอลหรือมาตรฐานในการรับและส่งเมล์นั้นหลัก ๆ แล้วจะใช้กันอยู่ 3 อย่างคือ SMTP, POP, IMAP

1) SMTP (Simple Mail Transfer Protocol) ใช้เป็นโปรโตคอลมาตรฐานในการติดต่อกันระหว่าง mail server กับ mail server
2) POP (Post Office Protocol) เป็นโปรโตคอลมาตรฐานที่โปรแกรมอีเมล์ใช้ดึงข้อมูลจาก mail server ปัจจุบันพัฒนามาถึงรุ่นที่ 3 และมักเรียกว่า POP3
3) IMAP (Internet Message Access Protocol) เป็นโปรโตคอลมาตรฐานที่ใช้ในการติดต่อระหว่างโปรแกรมอีเมล์ของเครื่องผู้ใช้งานกับ mail server

2.5.4 DNS server

เป็นเครื่องคอมพิวเตอร์ที่เก็บข้อมูลชื่อเครื่องคอมพิวเตอร์ในระบบอินเตอร์เน็ตและหมายเลขไอพีของเครื่องคอมพิวเตอร์ชื่อนั้นไว้ เมื่อเครื่องคอมพิวเตอร์ลูกข่ายต้องการติดต่อกับเครื่องคอมพิวเตอร์เครื่องอื่น โดยใช้ชื่อโดเมน ก็จะต้องถามที่ DNS Server เพื่อขอหมายเลขไอพีของเครื่องคอมพิวเตอร์เครื่องนั้น เนื่องจากในการติดต่อจริง จะต้องใช้หมายเลขไอพีเท่านั้น

2.5.5 DHCP server

เป็นเครื่องคอมพิวเตอร์ที่มีหน้าที่ในการแจกจ่าย IP Address แบบอัตโนมัติแก่เครื่องลูกข่ายแบบไม่คงที่ (Dynamic) โดยเครื่องคอมพิวเตอร์ลูกข่ายจะทำการร้องขอข้อมูลที่จำเป็น ในการเข้าร่วมเครือข่ายจากแม่ข่าย ซึ่งเครื่องแม่ข่ายจะเป็นฝ่ายกำหนดหมายเลขไอพีให้กับเครื่องลูกข่าย

2.5.6 Proxy Server

เป็นเครื่องคอมพิวเตอร์ที่อยู่ตรงกลางระหว่างเครื่อง Client กับอินเทอร์เน็ต ทำหน้าที่ในการรับการร้องขอใช้บริการ (request) จากเครื่อง Client ได้แก่ โปรแกรมเว็บบราวเซอร์ หรือโปรแกรม FTP Client แล้วส่งผ่านการร้องขอนั้นไปยังเซิร์ฟเวอร์ปลายทางในเครือข่ายอินเทอร์เน็ต ดังนั้น Proxy Server จึงเปรียบเสมือนตัวแทนของเครื่อง Client ที่อยู่ภายในระบบและเป็นตัวกลางระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยมีภาระหน้าที่ที่ถูกกำหนดให้รับผิดชอบ แตกต่างกันออกไปตามความต้องการของผู้ออกแบบระบบ ตัวอย่างเช่น

- Firewall Proxy ทำหน้าที่รักษาความปลอดภัยให้แก่ระบบ
- Proxy Caching Server ทำหน้าที่ให้บริการ Web Caching Service คือ จะคอยรับคำร้องขอบริการจากเครื่อง Client และส่งผ่านไปยังเซิร์ฟเวอร์ปลายทางที่เหมาะสมข้อมูลต่าง ๆ ที่ผ่านเข้ามาจะถูกสำเนาเก็บไว้ในหน่วยความจำแคช และดิสก์ ดังนั้นเมื่อมีการ

ร้องขอข้อมูลซ้ำอีกในครั้งต่อมาจะ สามารถนำข้อมูลในแคชมาให้บริการได้รวดเร็วกว่าการติดต่อไปยังเซิร์ฟเวอร์โดยตรง ช่วยให้ลดการใช้ช่องทางสื่อสารข้อมูลลงได้

2.6 โปรโตคอลและพอร์ตที่เกี่ยวข้อง

ตารางที่ 2.3 แสดงรายละเอียดของโปรโตคอลและพอร์ตที่เกี่ยวข้อง

Protocol	Description	Port	หน้าที่ของ Protocol
SMTP	Simple Mail Transfer Protocol	25	ใช้ในการรับส่งข้อมูลระหว่างMail Server กับMail Server
POP3	Post Office Protocol	110	ใช้ในการรับส่งข้อมูลระหว่างMail Client กับMail Server
NNTP	Network News Transfer Protocol	119	ใช้ในการส่งข่าว
FTP	File Transfer Protocol	21	ใช้ในการถ่ายโอนไฟล์
HTTP	Hyper Text Transfer Protocol	80	ใช้ในการเปิดเว็บไซต์ต่างๆ

2.7 ล็อกในระบบปฏิบัติการ Windows

Event Log คือ ล็อกไฟล์ที่จัดเก็บเหตุการณ์สำคัญๆ ที่เกิดขึ้นในระบบปฏิบัติการ Windows

2.7.1 รายละเอียดที่จัดเก็บใน Event Log

1) วันและเวลาที่เกิดเหตุการณ์นั้นขึ้น

2) บันทึกเหตุการณ์ที่เกิดขึ้น พร้อมทั้งชื่อของเหตุการณ์ ซึ่งถ้าระบบแบ่งการจดบันทึกเป็นหลายหมวดหมู่ ก็จะระบุด้วยว่าเหตุการณ์ดังกล่าวอยู่ในหมวดไหน

3) รายละเอียดของเหตุการณ์ (description) ซึ่งจะบอกว่าเหตุการณ์ดังกล่าวมีรายละเอียดอะไร เกิดความผิดปกติที่ตรงตำแหน่งไหน อาจเป็นที่ตัวอุปกรณ์หรือไฟล์ข้อมูลในระบบ

4) ชนิดของเหตุการณ์ที่ผิดปกติ (type) หรือระดับความรุนแรงของเหตุการณ์ที่ผิดปกติดังกล่าว เช่น ถ้าเหตุการณ์นั้นไม่มีความรุนแรงกับระบบมากนัก แต่เข้าข่ายผิดสังเกต ก็แจ้งเตือนในระดับของ Warning หรือถ้าเหตุการณ์นั้นร้ายแรงมากจนถึงขั้นทำให้ระบบเกิดความเสียหายจนไม่สามารถปฏิบัติการได้ ก็จะแจ้งเตือนว่าเป็น Error ในการจดบันทึกการทำงานของระบบที่ดีนั้น ควรจะบันทึกไว้ทั้งที่เป็นการทำงานปกติและไม่ปกติ เพื่อให้ผู้ดูแลระบบสามารถติดตามความเปลี่ยนแปลงที่เกิดขึ้นในระบบได้ครบถ้วน

2.7.2 ประเภทของ Event Log

2.7.2.1 ล็อกแอปพลิเคชัน (Application Log)

จะเก็บรายละเอียดการทำงานของแอพพลิเคชันต่างๆ ที่รันอยู่บนโอเอส เช่น เว็บเซิร์ฟเวอร์ เมล์เซิร์ฟเวอร์ ดีเอ็นเอสเซิร์ฟเวอร์ ฯลฯ ล็อกไฟล์ประเภทนี้จะบันทึกการทำงานของแอพพลิเคชันนั้น ไม่ว่าจะเป็นการทำงานที่สำเร็จหรือไม่สำเร็จก็ตาม ซึ่งผู้ดูแลระบบจะสามารถกลับมาตรวจสอบและแก้ไขความผิดปกติได้อย่างตรงจุด

2.7.2.2 ล็อกการรักษาความปลอดภัย (Security Log)

เหตุการณ์บันทึกล็อกการรักษาความปลอดภัย เช่น ความพยายามในการล็อกอินที่ถูกต้องและไม่ถูกต้อง รวมทั้งกิจกรรมต่างๆ ที่เกี่ยวข้องกับทรัพยากรที่ใช้ เช่น การสร้าง การเปิดหรือการลบแฟ้ม ตัวอย่างเช่น เมื่อเปิดใช้การตรวจสอบการล็อกอิน เหตุการณ์ได้รับการบันทึกไว้ในล็อกการรักษาความปลอดภัยแต่ละครั้งที่ผู้ใช้ พยายามล็อกอินไปยังคอมพิวเตอร์ คุณต้องล็อกอินเป็นผู้ดูแลระบบหรือเป็นสมาชิกของกลุ่ม Administrator เพื่อเปิด ใช้ และระบุกับเหตุการณ์ต่างๆ ที่ได้รับการบันทึกไว้ในล็อกการรักษาความปลอดภัย

2.7.2.3 ล็อกระบบ (System Log)

ล็อกระบบ จะบันทึกล็อกของเหตุการณ์ต่างๆ ปัญหาที่พบระหว่างการทำงาน มีเซอร์วิสไหนทำงานได้หรือไม่ได้บ้าง ตัวอย่างเช่น หากไดรเวอร์ไม่สามารถโหลดได้ระหว่างการเริ่มต้น เหตุการณ์จะได้รับการบันทึกลงในล็อกระบบ โดยตลอดระยะเวลาที่โอเอสนั้นยังคงทำงานอยู่ ถ้ามีเหตุการณ์ใดๆ เกิดขึ้นและส่งผลกระทบกับระบบ ก็จะมีการบันทึกข้อมูลเหตุการณ์นั้นไว้เสมอ

2.8 ล็อกของเซอร์วิสต่างๆ ใน IIS (IIS Log)

เซอร์วิสต่างๆ ใน IIS ไม่ว่าจะเป็น www, FTP, SMTP, NNTP ล้วนสามารถบันทึกข้อมูลการทำงานลงในไฟล์ เพื่อเอาไว้ช่วยให้ผู้ดูแลระบบสามารถวิเคราะห์และแก้ปัญหาได้ทุกเซอร์วิส

2.8.1 รูปแบบของ IIS Log (IIS Log Format)

การบันทึกข้อมูล Log ใน IIS 6.0 มีฟอร์แมตให้เลือกใช้ 4 แบบ ดังนี้

2.8.1.1 W3C Extended Log File Format

เป็นไฟล์ที่ใช้เก็บข้อมูล Log ตามมาตรฐานขององค์กร world Wide Web Consortium และเป็นไฟล์ประเภทที่นิยมใช้กันมากที่สุด เพราะฟิลด์ข้อมูลในรายการที่บันทึกลงไฟล์ มีหลากหลายมากที่สุด อีกทั้งยังมีออปชันให้ผู้ดูแลระบบเลือกบันทึกเฉพาะฟิลด์ข้อมูลบางฟิลด์ที่สนใจได้ด้วย ตัวอย่างของรูปแบบการจัดเก็บข้อมูล แสดงดังรูปที่ 2.5

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2002-05-02 17:42:15
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query
2002-05-02 17:42:15 172.22.255.255 - 172.30.255.255 80 GET /images/picture.jpg - 20
```

รูปที่ 2.5 ตัวอย่างรายการข้อมูลในไฟล์เก็บข้อมูล Log ประเภท W3C Extended Log File Format

ตารางที่ 2.4 แสดงฟิลด์ต่างๆ ของข้อมูล Log ประเภท W3C Extended Log File Format

Field	Appears As	Description
Date	date	วันที่เกิดเหตุการณ์ โดยบันทึกในรูปแบบ yyyy-mm-dd เช่น 2004-11-19
Time	time	เวลาที่เกิดเหตุการณ์ เช่น 14:17:50
Client IP Address	c-ip	ไอพีแอดเดรสของไคลเอนต์ที่ทำงานในเหตุการณ์นี้
User Name	cs-username	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้ (Anonymous ใช้ "-")
Service Name and Instance Number	s-sitename	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้ โดยบันทึกชื่อตาม identifier เช่น W3SVC1
Server Name	s-computername	ชื่อเซิร์ฟเวอร์
Server IP Address	s-ip	ไอพีแอดเดรสของเซิร์ฟเวอร์
Server Port	s-port	หมายเลขพอร์ตที่เซิร์ฟเวอร์เปิดใช้งาน เช่น 80
Method	cs-method	เมธอดที่ไคลเอนต์ใช้ทำงานในเหตุการณ์นี้ เช่น Get , Post

ตารางที่ 2.4 (ต่อ)

Field	Appears As	Description
URI Stem	cs-uri-stem	ส่วนท้ายของ URI (ไม่รวมชื่อเว็บไซต์) ของ Object หรือไฟล์ที่โหลด เช่น /index.php
URI Query	cs-uri-query	บันทึก URI query ที่ส่งมากจากไคลเอนต์ไปยังเซิร์ฟเวอร์
HTTP Status	sc-status	รหัสสถานะของโปรโตคอล เช่น 200 หมายถึง การส่งข้อมูลจากเซิร์ฟเวอร์ไปยังไคลเอนต์สำเร็จเรียบร้อย
Win32 Status	sc-win32-status	รหัสสถานะของระบบ Windows ในเครื่องเซิร์ฟเวอร์ ถ้าสถานะปกติจะมีรหัสเป็น 0
Bytes Sent	sc-bytes	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์
Bytes Received	cs-bytes	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์
Time Taken	time-taken	ระยะเวลาที่ใช้ในการโหลด Object หรือไฟล์ (มิลลิวินาที)
Protocol Version	cs-version	เวอร์ชันของโปรโตคอลที่ใช้ เช่น HTTP/1.1
Host	cs-host	Host Header ที่เรียกจากไคลเอนต์ เช่น www.arc.com
User Agent	cs(User-Agent)	ชื่อโปรแกรม Browser ของผู้ชมที่ทำงานตามเหตุการณ์นี้
Cookie	cs(Cookie)	ไฟล์ที่โหลดนี้ มีการเรียกใช้ Cookie ที่เก็บอยู่ทางฝั่งไคลเอนต์หรือไม่ ถ้าไม่มี จะบันทึกด้วยเครื่องหมาย "-" แต่ถ้ามี ก็จะบันทึกชื่อไฟล์ Cookie ที่เรียกใช้
Referrer	cs(Referrer)	เว็บไซต์ก่อนหน้าที่จะมายังเว็บไซต์นี้

2.8.1.2 Microsoft IIS Log File Format

เป็นไฟล์ที่เก็บข้อมูล Log ตามมาตรฐานของไมโครซอฟต์ ฟิลด์ข้อมูลในรายการที่บันทึกลงไฟล์เก็บข้อมูล log แต่ละฟิลด์ จะคั่นด้วยเครื่องหมายจุลภาค (,) ซึ่งเป็นรูปแบบที่ช่วยให้สามารถแปลงไฟล์ไปเป็นไฟล์เก็บข้อมูล log ประเภทอื่นๆ ได้ง่าย

```
192.168.114.201, -, 03/20/01, 7:55:20, W3SVC2, SERVER, 172.21.13.45, 4502, 163, 3223,
```

รูปที่ 2.6 ตัวอย่างรายการข้อมูลในไฟล์เก็บข้อมูล Log ประเภท Microsoft IIS Log File Format

ตารางที่ 2.5 แสดงฟิลด์ต่างๆ ของข้อมูล Log ประเภท Microsoft IIS Log File Format

Field	**Description**
Client IP address	ไอพีแอดเดรสของไคลเอนต์ที่ทำงานในเหตุการณ์นี้
User name	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้ (Anonymous ใช้ "-")
Date	วันที่เกิดเหตุการณ์ โดยบันทึกในรูปแบบ mm/dd/yy
Time	เวลาที่เกิดเหตุการณ์ เช่น 7:55:20
Service and instance	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้ โดยบันทึกชื่อตาม identifier เช่น W3SVC2
Server name	ชื่อเซิร์ฟเวอร์
Server IP	ไอพีแอดเดรสของเซิร์ฟเวอร์
Time taken	ระยะเวลาที่ใช้ในการโหลด Object หรือไฟล์ (มิลลิวินาที)
Client bytes sent	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์
Server bytes sent	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์
Service status code	รหัสสถานะของโปรโตคอล เช่น 200 หมายถึง การส่งข้อมูลจากเซิร์ฟเวอร์ไปยังไคลเอนต์สำเร็จเรียบร้อย
Windows status code	รหัสสถานะของระบบ Windows ในเครื่องเซิร์ฟเวอร์ (สถานะปกติ คือ 0)
Request type	เมธอดที่ไคลเอนต์ใช้ทำงานในเหตุการณ์นี้ เช่น Get , Post
Target URL	ส่วนท้ายของ URL (ไม่รวมชื่อเว็บไซต์) ของ Object หรือไฟล์ที่โหลด
Parameters	พารามิเตอร์ที่ไคลเอนต์ส่งมากับเมธอด Get หรือ Post·

2.8.1.3 NCSA Common Log File Format

เป็นไฟล์ที่เก็บข้อมูล Log ตามมาตรฐานของ NCS (National Center for Super Computing Application) ซึ่งเกิดขึ้นก่อนไฟล์เก็บข้อมูล log ประเภทอื่น

```
172.21.13.45 - Microsoft\JohnDoe [08/Apr/2001:17:39:04 -0800] "GET /scripts/iisadmin/
```

รูปที่ 2.7 ตัวอย่างรายการข้อมูลในไฟล์เก็บข้อมูล Log ประเภท NCSA Common Log File Format

ตารางที่ 2.6 แสดงฟิลด์ต่างๆ ของข้อมูล Log ประเภท NCSA Common Log File Format

Field	**Description**
Remote host address	ไอพีแอดเดรสของไคลเอนต์ที่ทำงานในเหตุการณ์นี้
Remote log name	ชื่อยูสเซอร์ที่ผ่านการตรวจสอบสิทธิจาก Authentication Server
User name	ชื่อยูสเซอร์ที่ผ่านการตรวจสอบสิทธิจากเว็บไซต์ เช่น Microsoft\JohnDoe
Date, time, and GMT offset	วันที่-เวลาที่เกิดเหตุการณ์ โดยอ้างอิงตามมาตรฐาน GMT เช่น [08/Apr/2001:17:39:04 -0800]
Request and protocol version	เมธอดที่ไคลเอนต์ใช้ทำงานในเหตุการณ์นี้ เช่น Get , Post รวมถึง URI และชนิดของโปรโตคอลที่ใช้ด้วย ตัวอย่างเช่น GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0
Service status code	รหัสสถานะของโปรโตคอล เช่น 200 หมายถึง การส่งข้อมูลจากเซิร์ฟเวอร์ไปยังไคลเอนต์สำเร็จเรียบร้อย
Bytes sent	จำนวนไบต์รวมของการรับ-ส่งระหว่างเซิร์ฟเวอร์กับไคลเอนต์

2.8.1.4 ODBC (Open Database Connectivity) Logging

การบันทึกข้อมูล Log ประเภทนี้ ไม่ใช่การบันทึกลงไฟล์เหมือนประเภทอื่น แต่เป็นการบันทึกลงในฐานข้อมูลผ่านทาง ODBC เพราะฉะนั้นจึงสามารถใช้งานได้กับระบบฐานข้อมูลชั้นนำทุกระบบ ไม่ว่าจะเป็น MS Access , MS SQL Server , Oracle ฯลฯ

ตารางที่ 2.7 แสดงฟิลด์ต่างๆ ของข้อมูล Log ประเภท ODBC Logging

Field	Data Type	Description
ClientHost	varchar(255)	ไอพีแอดเดรสของไคลเอนต์ที่ทำงานในเหตุการณ์นี้
UserName	varchar(255)	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้ (Anonymous ใช้ "-")
LogTime	datetime	วันที่-เวลาที่เกิดเหตุการณ์นี้
Service	varchar(255)	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้ โดยบันทึกชื่อตาม identifier
Machine	varchar(255)	ชื่อเซิร์ฟเวอร์
ServerIP	varchar(50)	ไอพีแอดเดรสของเซิร์ฟเวอร์
ProcessingTime	integer	ระยะเวลาที่ใช้ในการโหลด object หรือไฟล์ตามเหตุการณ์นี้
BytesRecvd	integer	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์
BytesSent	integer	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์
ServiceStatus	integer	รหัสสถานะของโปรโตคอล เช่น 200 หมายถึง การส่งข้อมูลจากเซิร์ฟเวอร์ไปยังไคลเอนต์สำเร็จเรียบร้อย
Win32Status	integer	รหัสสถานะของระบบ Windows ในเครื่องเซิร์ฟเวอร์ ถ้าสถานะปกติจะมีรหัสเป็น 0
Operation	varchar(255)	เมธอดที่ไคลเอนต์ใช้ทำงานในเหตุการณ์นี้ เช่น Get , Post
Target	varchar(255)	ส่วนท้ายของ URI (ไม่รวมชื่อเว็บไซต์) ของ Object หรือไฟล์ที่โหลด เช่น /index.php
Parameters	varchar(255)	พารามิเตอร์ที่ไคลเอนต์ส่งมากับเมธอด Get หรือ Post

2.9 การจัดเก็บข้อมูลล็อก

การจัดเก็บข้อมูลล็อกที่มีประสิทธิภาพ เพื่อให้ข้อมูลล็อกมีความน่าเชื่อถือและสามารถจัดเก็บเป็นระยะเวลานาน ควรกระทำดังนี้

2.9.1 Log rotation เป็นการจัดเก็บล็อกไฟล์โดยการหมุนข้อมูลล็อก หมายถึงการบันทึกไฟล์ข้อมูลล็อกไว้เป็นชื่ออื่น และสร้างไฟล์ล็อกใหม่เพื่อรองรับการบันทึกข้อมูลต่อไป ตัวอย่างเช่น การบันทึกไฟล์ล็อกเป็น /var/log/message เมื่อมีการหมุนข้อมูลล็อกจะบันทึกข้อมูลล็อกเป็น /var/log/message.1 และสร้างไฟล์ล็อกใหม่เป็นชื่อ /var/log/message เป็นต้น เพื่อป้องกันไม่ให้มีไฟล์ข้อมูลล็อกขนาดใหญ่เกินจนไม่สามารถใช้งานได้ โดยปกติการหมุนข้อมูลล็อกจะดำเนินการตามระยะเวลาที่เหมาะสมเช่น ทุกวัน หรือทุกสัปดาห์ หรือเมื่อมีขนาดของไฟล์ข้อมูลล็อกมีขนาดถึงที่กำหนดไว้ นอกจากนี้ยังนำข้อมูลล็อกเดิมเมื่อมีการหมุนข้อมูลล็อกไปบีบอัดข้อมูลเพื่อเพิ่มพื้นที่เก็บข้อมูล หรือทำ Log archive ได้ การหมุนข้อมูลล็อกที่เหมาะสมคือการบันทึกข้อมูลล็อกแยกเป็นรายวัน และแยกตามเซิร์ฟเวอร์หรืออุปกรณ์ในระบบเครือข่าย

2.9.2 Log archival คือการสำรองข้อมูลล็อกเพื่อให้สามารถรักษาระยะเวลาในการจัดเก็บข้อมูลล็อกตามความต้องการ โดยการบันทึกข้อมูลล็อกบนสื่อบันทึกข้อมูลภายนอก หรือการบันทึกข้อมูลบน Storage area network หรือ SAN หรือการบันทึกบนเซิร์ฟเวอร์หรือข้อมูลที่ทำหน้าที่เฉพาะในการบันทึกข้อมูลล็อกเป็นต้น ยังรวมถึงการสำรองข้อมูลล็อกบนสื่อบันทึกข้อมูลอื่น เช่น เทปสำรองข้อมูล ซีดีรอมหรือดีวีดีเป็นต้น

การจัดทำ Log archival แบ่งเป็นสองแบบ คือ

2.9.2.1 Log retention เป็นการบันทึกข้อมูลล็อกของเหตุการณ์จากระบบอย่างสม่ำเสมอ

2.9.2.2 Log preservation เป็นกระบวนการรักษาข้อมูลล็อกเพื่อให้สามารถนำไปใช้ร่วมกับการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย หรือเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบสารสนเทศ และสามารถรักษาข้อมูลล็อกได้ตามระยะเวลาที่กำหนดไว้หรือตามความต้องการจากภายนอก เช่น ความต้องการของ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น

2.9.3 Log compression คือ การบีบอัดข้อมูลล็อกเพื่อเพิ่มพื้นที่ในการจัดเก็บข้อมูลล็อก และง่ายในการสำรองข้อมูลล็อกหรือการย้ายข้อมูลล็อกไปเก็บไว้บนสื่อบันทึกข้อมูลอื่น มักดำเนินการต่อเนื่องจาก Log rotation หรือ Log archival

2.9.4 Log reduction เป็นการตัด ลบ หรือลดข้อมูลล็อกบางส่วนที่ไม่เกี่ยวข้อง เช่นการลบตัวอักษรหรืออักขระที่ไม่จำเป็นต่อเก็บบันทึกข้อมูลล็อก มักจะดำเนินการควบคู่กับกระบวนการ Log archival เพื่อลดข้อมูลล็อกที่ไม่เกี่ยวข้องก่อนจะบันทึกข้อมูลล็อกในสื่อบันทึกข้อมูล

2.9.5 Log conversion เป็นการแปลงรูปแบบการจัดเก็บข้อมูลล็อกเช่น แปลงข้อมูลล็อกจากรูปแบบของไฟล์ TEXT เป็นรูปแบบข้อมูลล็อกแบบ XML เป็นต้น เป็นวิธีการแปลงรูปแบบการเก็บข้อมูลล็อกจากรูปแบบหนึ่งไปเป็นอีกรูปแบบหนึ่ง ส่วนหนึ่งแล้วการทำ Log conversion มักทำกระบวนการ Event filtering และ Event aggregation จนถึง Log normalization

2.9.6 Log normalization เป็นการปรับรูปแบบของข้อมูลล็อกให้อยู่ในรูปแบบเดียวกัน เช่น การปรับรูปแบบของวันที่ที่แตกต่างกัน เช่น หรือความแตกต่างของชื่อตำแหน่งของข้อมูลล็อก เช่น

- ข้อมูลล็อกวันที่จากเว็บเซิร์ฟเวอร์เป็นรูปแบบ 12 ชั่วโมงหรือเขียนเป็น 2:34:56 P.M. IDT ในขณะที่ข้อมูลล็อกวันที่ของเว็บเซิร์ฟเวอร์อีกเซิร์ฟเวอร์จัดเก็บในรูปแบบ 24 ชั่วโมง เช่น 14:34 GMT+7 เป็นต้น
- ในระบบหนึ่งเรียกข้อมูลล็อกวันที่ว่า Timestamp ในขณะที่อีกระบบหนึ่งเรียกว่า Event Time เป็นต้น
- บางระบบเก็บข้อมูลล็อกของ Timezone เป็น GMT+7 ในขณะที่อีกระบบหนึ่งเก็บข้อมูลล็อกเป็น Zone-21 เป็นต้น ดังนั้นกระบวนการ Log normalization ต้องทราบว่าความหมายของ Zone-21 หมายถึง GMT+7 เป็นต้น

กระบวนการ Log normalization มีความสำคัญมากยิ่งเฉพาะกับการใช้ล็อกเซิร์ฟเวอร์แบบศูนย์กลางเพื่อเก็บข้อมูลล็อก และสามารถวิเคราะห์ข้อมูลล็อก ซึ่งต้องมีความสามารถในการรับข้อมูลล็อกหลายรูปแบบและต้องทำ Log normalization ในการแปลงข้อมูลล็อกให้อยู่ในรูปแบบที่สามารถจัดเก็บ สืบค้น และวิเคราะห์ได้โดยผู้ที่มีความรู้ความเชี่ยวชาญต่อไป

2.9.7 Log file integrity checking เป็นกระบวนการตรวจสอบความถูกต้องของล็อกไฟล์ โดยการทำ **Data Hashing** กับล็อกไฟล์ที่ไม่มีการเขียนข้อมูลแล้ว ตัวอย่างดำเนินการทำ Log rotation เป็นวันดังนั้นสามารถนำข้อมูล ล็อกไฟล์ของเดือนก่อนหน้ามาเข้ากระบวนการนี้ได้ หรือการทำ Log compression กับล็อกไฟล์ที่ผ่านกระบวนการ Log archival แล้ว เช่น ข้อมูลล็อกของสัปดาห์ที่แล้วนำมาบีบอัดและคำนวณด้วยวิธีการนี้เป็นต้น ซึ่งจะได้เป็นข้อมูลเป็น Message Digest เช่นการคำนวณด้วยอัลกอริทึม MD5 ขนาด 128 บิต หรือใช้อัลกอริทึม SHA-1 ขนาด 128 บิตเป็นต้น ผลลัพธ์ที่ได้หรือที่เรียกว่า Message Digest จะมีความยาวขนาด 128 บิตเพื่อใช้เป็นตัวแทนของล็อกไฟล์ ข้อมูล Message Digest ควรจะต้องเก็บไว้ในสื่อบันทึกข้อมูลที่ปลอดภัยเช่น สื่อบันทึกข้อมูลแบบเขียนได้อย่างเดียวเป็นต้น

2.10 การวิเคราะห์ข้อมูลล็อก

การวิเคราะห์ข้อมูลล็อก ประกอบด้วยเรื่องต่างๆ ดังนี้

2.10.1 Event correlation เป็นกระบวนการสร้างความสัมพันธ์ของข้อมูลล็อกตัวอย่างเช่นการสร้างกฎความสัมพันธ์หรือ Rule-based correlation ระหว่างข้อมูลล็อก เช่นการสร้างความสัมพันธ์ของข้อมูลล็อกจาก วันเวลา จากไอพีแอดเดรส จากชนิดของเหตุการณ์จากข้อมูลล็อกเป็นต้น กระบวนการ Event correlation สามารถนำระเบียบวิธีการประมวลผลข้อมูลระดับสูงมาใช้ร่วมได้ เช่นการใช้วิธีการทางสถิติมาหาแนวโน้มของเหตุการณ์ที่เกี่ยวข้องกัน หรือการใช้ความน่าจะเป็นมาคำนวณเพื่อวิเคราะห์หาความสัมพันธ์ของเหตุการณ์เป็นต้น จนถึงการนำเทคนิคของ Data Mining มาใช้เพิ่มเติมเพื่อจัดแบ่งกลุ่มข้อมูลและความสัมพันธ์ของข้อมูลล็อกหรือเหตุการณ์ที่เกิดขึ้นได้อย่างแม่นยำมากขึ้น

2.10.2 Log viewing เป็นระบบการแสดงข้อมูลล็อก มีความสามารถของ Event filtering เช่น สามารถการจัดเรียงข้อมูลล็อกตามวันที่ การแยกข้อมูลล็อกตามเซิร์ฟเวอร์หรืออุปกรณ์

2.10.3 Log reporting เป็นการแสดงผลลัพท์จากการวิเคราะห์ข้อมูลล็อก ระบุความสัมพันธ์ที่เกี่ยวข้อง หรือข้อมูลสรุปการวิเคราะห์ข้อมูลล็อกหรือเหตุการณ์ที่เกี่ยวข้อง แสดงความต่อเนื่องของเหตุการณ์ที่เกิดขึ้นและคัดกรองรวมถึงแสดงเป็นกราฟหรือแผนภูมิเพื่อให้ง่ายต่อการแสดงผลเป็นต้น

2.11 วิธีการเก็บรวบรวมข้อมูลล็อก (Log Collection)

การเก็บรวบรวมข้อมูลล็อก ที่นิยมใช้ในปัจจุบัน มี 3 วิธี ดังตารางที่ 2.8

ตารางที่ 2.8 เปรียบเทียบข้อดีและข้อเสียของการส่งข้อมูลแต่ละวิธี

	วิธีการส่งข้อมูลโดยใช้ FTP	วิธีการส่งข้อมูลโดยใช้ SFTP	วิธีการส่งข้อมูลโดยใช้ syslog
Server	ติดตั้งโปรแกรม FTP Server จาก IIS บน Windows Server 2003	ติดตั้งโปรแกรม SFTP Server เช่น OpenSSH , WinSSHD (Bitvise)	ติดตั้งโปรแกรม Kiwi syslog
Client	ใช้ Dos Command	ติดตั้งโปรแกรม SFTP Client ได้แก่ OpenSSH , SSHSecureShellClient , WinSCP เป็นต้น	ติดตั้งโปรแกรม Snare

ตารางที่ 2.8 (ต่อ)

	วิธีการส่งข้อมูลโดยใช้ FTP	วิธีการส่งข้อมูลโดยใช้ SFTP	วิธีการส่งข้อมูลโดยใช้ syslog
ข้อดี	มีการจัดส่ง Log ในรูปแบบของไฟล์ ดังนั้น หากเครื่อง Centralized Log Server ไม่สามารถให้บริการได้ แต่ข้อมูล Log ยังถูกจัดเก็บอยู่ที่เครื่อง Client	1. sftp คือ การ ftp ด้วย Secure Shell (SSH) โดยโดยมีการเข้ารหัสทั้ง user, password และข้อมูลระหว่างทางที่ส่งเพื่อความปลอดภัย 2. มีการจัดส่ง Log ในรูปแบบของไฟล์ ดังนั้น หากเครื่อง Centralized Log Server ไม่สามารถให้บริการได้ แต่ข้อมูล Log ยังถูกจัดเก็บอยู่ที่เครื่อง Client	สามารถจัดส่งข้อมูล Log ได้แบบ RealTime
ข้อเสีย	1. การส่งไฟล์ด้วย ftp นั้น จะไม่มีการเข้ารหัส username และ password ซึ่งเสี่ยงต่อการถูกดักเอาข้อมูลไปใช้ได้ 2. ข้อมูล Log ไม่ได้ถูกจัดส่งไปยังเครื่อง Centralized Log Server แบบ RealTime	ข้อมูล Log ไม่ได้ถูกจัดส่งไปยังเครื่อง Centralized Log Server แบบ RealTime	หากเครื่อง Centralized Log Server ไม่สามารถให้บริการได้ จะทำให้ไม่สามารถจัดเก็บข้อมูล Log ในช่วงเวลาดังกล่าวได้

2.12 ตัวอย่างข้อมูลจราจรประเภทต่างๆ

2.12.1 ข้อมูลจราจรของการใช้บริการโอนแฟ้มข้อมูล (FTP Log)

```
192.168.2.1, thanawas, 24/1/2552, 19:27:36, MSFTPSVC1, INSERVER1, 192.168.2.2, 47, 0,
1656, 226, 0, [1]sent, /multi_sendfile/secedit.txt, -,
```

รูปที่ 2.8 ข้อมูล FTP Log ในรูปแบบของ Microsoft IIS Log File Format

ตารางที่ 2.9 ตัวอย่างรายละเอียดข้อมูล FTP Log ในรูปแบบของ Microsoft IIS Log File Format

Field	Log Deail
Client IP address	192.168.2.1
User name	thanawas
Date	24/1/2552
Time	0.810833333
Service and instance	MSFTPSVC1
Server name	INSERVER1
Server IP	192.168.2.2
Time taken	47
Client bytes sent	0
Server bytes sent	1656
Service status code	226
Windows status code	0
Request type	[1]sent
Target URL	/multi_sendfile/secedit.txt
Parameters	-

2009-02-11 13:10:26 192.168.10.101 thanawas MSFTPSVC1 INSERVER1 192.168.2.3 21
[9]created /sqmdata00.sqm - 226 0 0 268 32 FTP - - - -

รูปที่ 2.9 ข้อมูล FTP Log ในรูปแบบของ W3C Extended Log File Format

ตารางที่ 2.10 ตัวอย่างรายละเอียดข้อมูล FTP Log ในรูปแบบของ W3C Extended Log File Format

Field	Appears As	Log Detail
Date	date	2/11/2009
Time	time	0.548912037
Client IP Address	c-ip	192.168.10.101
User Name	cs-username	thanawas

ตารางที่ 2.10 (ต่อ)

Field	Appears As	Log Detail
Service Name and Instance Number	s-sitename	MSFTPSVC1
Server Name	s-computername	INSERVER1
Server IP Address	s-ip	192.168.2.3
Server Port	s-port	21
Method	cs-method	[9]created
URI Stem	cs-uri-stem	/sqmdata00.sqm
URI Query	cs-uri-query	-
HTTP Status	sc-status	226
Win32 Status	sc-win32-status	0
Bytes Sent	sc-bytes	0
Bytes Received	cs-bytes	268
Time Taken	time-taken	32
Protocol Version	cs-version	FTP
Host	cs-host	-
User Agent	cs(User-Agent)	-
Cookie	cs(Cookie)	-
Referrer	cs(Referrer)	-

2.12.2 ข้อมูลอินเตอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย (Proxy Log)

192.168.10.104 project.com\thanawas Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322) Y 2009-05-03 12:42:36 w3proxy ISA -
runonce.msn.com 207.46.61.20 80 140 493 162 http
GET http://runonce.msn.com/images/tighter-security.png Inet 304
permit HTTP/HTTPS deny executables Req ID: 08ccf7e9 Internal External
0xd80 Allowed

รูปที่ 2.10 ข้อมูล Proxy Log ที่สร้างจากโปรแกรม ISA Server 2004

ตารางที่ 2.11 ตัวอย่างรายละเอียดข้อมูล Proxy Log ที่สร้างจากโปรแกรม ISA Server 2004

Field	**Log Detail**
c-ip	192.168.10.104
cs-username	project.com\thanawas
c-agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)
sc-authenticated	Y
Date	39936
Time	0.529583333
s-svcname	w3proxy
s-computername	ISA
cs-referred	-
r-host	runonce.msn.com
r-ip	207.46.61.20
r-port	80
time-taken	140
cs-bytes	493
sc-bytes	162
cs-protocol	http
s-operation	GET
cs-uri	http://runonce.msn.com/images/tighter-security.png
s-object-source	Inet
sc-status	304
Rule	permit HTTP/HTTPS deny executables
FilterInfo	Req ID: 08ccf7e9
cs-Network	Internal
sc-Network	External
error-info	0xd80
Action	Allowed

2.12.3 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ (Web Log)

2009-05-05 15:38:40 192.168.2.1 - W3SVC1 WEBSERVER 192.168.2.6 80 GET /diary/top.htm - 304 0 165 490 0 HTTP/1.1 192.168.2.6 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1; +.NET+ CLR+1.1.4322) ASPSESSIONIDASDCCQRT=AJCDAJLBFDCFMEKEAMKGAEJK http://192.168.2.6/diary/main.htm

รูปที่ 2.11 ข้อมูล Web Log ในรูปแบบของ W3C Extended Log File Format

ตารางที่ 2.12 ตัวอย่างรายละเอียดข้อมูล Web Log ในรูปแบบของ W3C Extended Log File Format

Field	Appears As	Log Detail
Date	date	5/5/2009
Time	time	0.651851852
Client IP Address	c-ip	192.168.2.1
User Name	cs-username	-
Service Name and Instance Number	s-sitename	W3SVC1
Server Name	s-computername	WEBSERVER
Server IP Address	s-ip	192.168.2.6
Server Port	s-port	80
URI Stem	cs-uri-stem	/diary/top.htm
URI Query	cs-uri-query	-
HTTP Status	sc-status	304
Win32 Status	sc-win32-status	0
Bytes Sent	sc-bytes	165
Bytes Received	cs-bytes	490
Time Taken	time-taken	0
Protocol Version	cs-version	HTTP/1.1
Host	cs-host	192.168.2.6
User Agent	cs(User-Agent)	Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)

ตารางที่ 2.12 (ต่อ)

Field	Appears As	Log Detail
Cookie	cs(Cookie)	ASPSESSIONIDASDCCQRT=AJCDAJLBF DCFMEKEAMKGAEJK
Referrer	cs(Referrer)	http://192.168.2.6/diary/main.htm

2.12.4 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการอีเมล์ (Mail Log)

```
20090501170645765 - 7    - Connection opened from 192.168.10.104
20090501170645765 - 13   - ************Starting SMTP session************
20090501170645765 - 13   - Server: 220 mail Majodio ESMTP Version 1.2.49.0 Service Ready
20090501170645765 - 13   - Client: HELO client
20090501170645765 - 13   - Server: 250 Hello  Welcome to the Majodio ESMTP Server
20090501170645765 - 13   - Client: MAIL FROM: <thanawas@project.com>
20090501170645765 - 13   - Server: 250 ok
20090501170645781 - 13   - Client: RCPT TO: <nawakit@project.com>
20090501170645781 - 13   - Server: 250 ok its for <nawakit@project.com>
20090501170645781 - 13   - Client: RCPT TO: <exuser1@external.com>
20090501170645781 - 13   - Server: 250 ok its for <exuser1@external.com>
20090501170645781 - 13   - Client: DATA
20090501170645781 - 13   - Server: 354 ok, send it; end with <CRLF>.<CRLF>
20090501170645781 - 13   - Client: Message-ID: <001601c9ca48$56681e90$680aa8c0@project.com>
20090501170645781 - 13   - Client: From: "thanawas" <thanawas@project.com>
20090501170645781 - 13   - Client: To: <nawakit@project.com>,
20090501170645781 - 13   - Client:        <exuser1@external.com>
20090501170645781 - 13   - Client: Subject: test send mail
20090501170645781 - 13   - Client: Date: Fri, 1 May 2009 17:33:58 +0700
20090501170645781 - 13   - Client: MIME-Version: 1.0
20090501170645781 - 13   - Client: Content-Type: multipart/alternative;
20090501170645781 - 13   - Client:        boundary="----=_NextPart_000_0013_01C9CA83.02713570"
20090501170645781 - 13   - Client: X-Priority: 3
20090501170645781 - 13   - Client: X-MSMail-Priority: Normal
20090501170645781 - 13   - Client: X-Mailer: Microsoft Outlook Express 6.00.2900.3138
```

```
20090501170645781 - 13   - Client: X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
20090501170645781 - 13   - Client: This is a multi-part message in MIME format.
20090501170645781 - 13   - Client: ------=_NextPart_000_0013_01C9CA83.02713570
20090501170645781 - 13   - Client: Content-Type: text/plain;
20090501170645781 - 13   - Client:        charset="windows-874"
20090501170645781 - 13   - Client: Content-Transfer-Encoding: quoted-printable
20090501170645781 - 13   - Client: aaaaaaaaaa
20090501170645781 - 13   - Client: ------=_NextPart_000_0013_01C9CA83.02713570
20090501170645781 - 13   - Client: Content-Type: text/html;
20090501170645781 - 13   - Client:        charset="windows-874"
20090501170645781 - 13   - Client: Content-Transfer-Encoding: quoted-printable
20090501170645781 - 13   - Client: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 //EN">
20090501170645781 - 13   - Client: <HTML><HEAD>
20090501170645781 - 13   - Client: <META http-equiv=3DContent-Type content=3D"text/html; =
20090501170645781 - 13   - Client: charset=3Dwindows-874">
20090501170645781 - 13   - Client: <META content=3D"MSHTML 6.00.6000.20710">
20090501170645781 - 13   - Client: <STYLE></STYLE>
20090501170645781 - 13   - Client: </HEAD>
20090501170645781 - 13   - Client: <BODY bgColor=3D#ffffff>
20090501170645781 - 13   - Client: <DIV><FONT face=3DArial=20
20090501170645781 - 13   - Client: size=3D2>aaaaaaaaaa</FONT></DIV></BODY></HTML>
20090501170645781 - 13   - Client: ------=_NextPart_000_0013_01C9CA83.02713570--
20090501170645796 - 13   - Saving Queued Message
20090501170645812 - 13   - Queued Message Saved
20090501170645827 - 13   - Saving Queued Message
20090501170645827 - 13   - Queued Message Saved
20090501170645827 - 13   - Server: 250 Message Queued
20090501170645827 - 13   - Client: QUIT
20090501170645827 - 13   - Server: 250 Goodbye
20090501170645827 - 13   - ************Ending SMTP session************
```

รูปที่ 2.12 ข้อมูล SMTP Log ในที่สร้างโดยโปรแกรม Majodio Mail

```
20090501174221703 - 11  - Connection opened from 192.168.10.104
20090501174221703 - 13  - ************Starting POP3 session************
20090501174221703 - 13  - Server: +OK Majodio POP3 mail
20090501174221703 - 13  - Client: USER thanawas@project.com
20090501174221703 - 13  - Server: +OK Welcome thanawas, password required
20090501174221703 - 13  - Client: PASS R@inny_fon
20090501174221703 - 13  - Server: +OK Mailbox locked and ready
20090501174221703 - 13  - Client: STAT
20090501174221703 - 13  - Server: +OK 1 2322
20090501174221703 - 13  - Client: LIST
20090501174221703 - 13  - Server: +OK 1 messages (2322 octets)
20090501174221703 - 13  - Server: 1 2322
20090501174221703 - 13  - Server: .
20090501174221703 - 13  - Client: RETR 1
20090501174221703 - 13  - Server: +OK 2322 octets
20090501174221703 - 13  - Server: Received: from client [192.168.10.104] by Majodio ESMTP Version
1.2.49.0 id 20090501174213750; Fri, 01 May 2009 17:42:13 0700
20090501174221703 - 13  - Server: Message-ID: <002701c9ca49$8358fb80$680aa8c0@project.com>
20090501174221703 - 13  - Server: From: "nawakit" <nawakit@project.com>
20090501174221703 - 13  - Server: To: <thanawas@project.com>,
20090501174221703 - 13  - Server:       <exuser1@external.com>
20090501174221703 - 13  - Server: Subject: test send mail
20090501174221703 - 13  - Server: Date: Fri, 1 May 2009 17:42:23 +0700
20090501174221703 - 13  - Server: MIME-Version: 1.0
20090501174221703 - 13  - Server: Content-Type: multipart/alternative;
20090501174221703 - 13  - Server:       boundary="----=_NextPart_000_0024_01C9CA84.2F7C2A10"
20090501174221703 - 13  - Server: X-Priority: 3
20090501174221703 - 13  - Server: X-MSMail-Priority: Normal
20090501174221703 - 13  - Server: X-Mailer: Microsoft Outlook Express 6.00.2900.3138
20090501174221703 - 13  - Server: X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
20090501174221703 - 13  - Server: This is a multi-part message in MIME format.
20090501174221703 - 13  - Server: ------=_NextPart_000_0024_01C9CA84.2F7C2A10
```

20090501174221703 - 13 - Server: Content-Type: text/plain;

20090501174221703 - 13 - Server: charset="windows-874"

20090501174221703 - 13 - Server: Content-Transfer-Encoding: quoted-printable

20090501174221703 - 13 - Server: ----- Original Message -----=20

20090501174221703 - 13 - Server: From: thanawas=20

20090501174221703 - 13 - Server: To: nawakit@project.com ; exuser1@external.com=20

20090501174221703 - 13 - Server: Sent: Friday, May 01, 2009 5:33 PM

20090501174221703 - 13 - Server: Subject: test

=CA=E8=A7=A2=E9=D2=C1=E0=A4=C3=D7=CD=A2=E8=D2=C2 99

20090501174221703 - 13 - Server: aaaaaaaaaa

20090501174221703 - 13 - Server: ------=_NextPart_000_0024_01C9CA84.2F7C2A10

20090501174221703 - 13 - Server: Content-Type: text/html;

20090501174221703 - 13 - Server: charset="windows-874"

20090501174221703 - 13 - Server: Content-Transfer-Encoding: quoted-printable

20090501174221703 - 13 - Server: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

20090501174221703 - 13 - Server: <HTML><HEAD>

20090501174221703 - 13 - Server: <META http-equiv=3DContent-Type content=3D"text/html; =

20090501174221703 - 13 - Server: charset=3Dwindows-874">

20090501174221703 - 13 - Server: <META content=3D"MSHTML 6.00.6000.20710" name=3DGENERATOR>

20090501174221703 - 13 - Server: <STYLE></STYLE>

20090501174221703 - 13 - Server: </HEAD>

20090501174221703 - 13 - Server: <BODY bgColor=3D#ffffff>

20090501174221703 - 13 - Server: <DIV><FONT face=3DArial size=3D2></FONT> </DIV>

20090501174221703 - 13 - Server: <DIV style=3D"FONT: 10pt arial">----- Original Message -----=20

20090501174221703 - 13 - Server: <DIV style=3D"BACKGROUND: #e4e4e4; font-color: black"><B>From:</B> <A=20

20090501174221703 - 13 - Server: title=3Dthanawas@project.com =

20090501174221703 - 13 - Server: href=3D"mailto:thanawas@project.com">thanawas</A>=20

20090501174221703 - 13 - Server: </DIV>

20090501174221703 - 13 - Server: <DIV><B>To:</B> <A title=3Dnawakit@project.com=20

```
20090501174221703 - 13   - Server: href=3D"mailto:nawakit@project.com">nawakit@project.com</A>
; <A=20
20090501174221703 - 13   - Server: title=3Dexuser1@external.com=20
20090501174221703 - 13   - Server:
href=3D"mailto:exuser1@external.com">exuser1@external.com</A> </DIV>
20090501174221703 - 13   - Server: <DIV><B>Sent:</B> Friday, May 01, 200. . .
20090501174221703 - 13   - Server: .
20090501174221703 - 13   - Client: DELE 1
20090501174221703 - 13   - Server: +OK message deleted
20090501174221703 - 13   - Client: QUIT
20090501174221703 - 13   - Server: +OK Majodio POP3 signing off
20090501174221703 - 13   - ************Ending POP3 session************
```

รูปที่ 2.13 ข้อมูล POP3 Log ในที่สร้างโดยโปรแกรม Majodio Mail

2.12.5 ข้อมูลบนเครื่องแจกจ่ายหมายเลขไอพีแอดเดรส (DHCP Log)

โดยปกติแล้ว ข้อมูลการแจกจ่ายหมายเลขไอพีแอดเดรสจะเก็บอยู่ที่ "C:\WINDOWS\System32\dhcp\log" โดยรูปแบบของชื่อไฟล์คือ "DhcpSrvLog-XXX.log" (XXX คือ ชื่อย่อของวัน) ดังนั้นการเก็บข้อมูลของ DHCP Server จะมีไฟล์อยู่ 7 ไฟล์ คือ

DhcpSrvLog-Sun.log DhcpSrvLog-Mon.log
DhcpSrvLog-Tue.log DhcpSrvLog-Wed.log
DhcpSrvLog-Thu.log DhcpSrvLog-Fri.log
DhcpSrvLog-Sat.log

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address
10,05/11/09,15:43:34,Assign,192.168.10.16,client.project.com,000C29C0F9A4,
30,05/11/09,15:47:23,DNS Update Request,5.10.168.192,client2.project.com,,
11,05/11/09,15:47:23,Renew,192.168.10.5,client2.project.com,000C29330FB3,
30,05/11/09,15:48:38,DNS Update Request,16.10.168.192,client.project.com,,
```

รูปที่ 2.14 ข้อมูล DHCP Log

ตารางที่ 2.13 ตัวอย่างรายละเอียดข้อมูล DHCP Log

Field	Log Detail	Description
ID	10	10 = A new IP address was leased to a client. 11 = A lease was renewed by a client. 17 = A lease was expired. 30 = DNS update request to the named DNS server
Date	05/11/09	-
Time	15:43:34	-
Description	Assign	ID=10 , Description = Assign ID=11 , Description = Renew ID=17 , Description = Expired ID=30 , Description = DNS Update Request
IP Address	192.168.10.16	-
Host Name	client.project.com	-
MAC Address	000C29C0F9A4	-

บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 ระบบงานปัจจุบัน

ในระบบงานปัจจุบันนั้น เครื่องคอมพิวเตอร์แม่ข่ายมีหน้าที่ในการให้บริการที่หลากหลายรูปแบบ เช่น บริการรับ-ส่งอีเมล์ (Mail Server) , บริการถ่ายโอนไฟล์ข้อมูล (FTP Server) , บริการการเชื่อมต่ออินเทอร์เน็ต (Proxy Server) , บริการการเข้าถึงเวปไซต์ (Web Server) เป็นต้น โดยเมื่อมีการเข้าใช้บริการดังกล่าวแล้ว เครื่องคอมพิวเตอร์แม่ข่ายจะทำการบันทึกข้อมูลล็อกการใช้งานไว้ที่เครื่องนั้นๆ โดยไม่ได้มีการส่งข้อมูลล็อกดังกล่าวไม่จัดเก็บไว้ที่เครื่องส่วนกลาง โดยการจัดเก็บข้อมูลล็อกนั้น จะจัดเก็บในรูปแบบของล็อกไฟล์หรือฐานข้อมูลตามที่ตั้งค่าไว้ ซึ่งเป็นหน้าที่ของผู้ดูแลระบบ (Administrator) ในการพิจารณารูปแบบและลักษณะของการจัดเก็บข้อมูล รวมถึงมีหน้าที่ในการตรวจสอบล็อกไฟล์ต่างๆ ที่เกิดขึ้นในระบบ อาทิเช่น บันทึกการเข้าใช้งานของผู้ใช้งานระบบ , ล็อกการรับส่งอีเมล์ เป็นต้น เพื่อทำการวิเคราะห์และหาความสัมพันธ์ของข้อมูลการใช้บริการเครื่องคอมพิวเตอร์แม่ข่าย และประโยชน์ในการตรวจสอบความผิดปกติต่าง ๆ ที่เกิดขึ้นกับระบบ โดยเฉพาะการพยายามบุกรุกเครือข่าย ซึ่งเป็นงานที่ยากลำบากของผู้ดูแลระบบ และเสียเวลาเป็นอย่างมากในการวิเคราะห์ข้อมูลล็อก เนื่องจากผู้ดูแลระบบแต่ละคน มีหน้าที่ดูแลเครื่องเซิร์ฟเวอร์หลายเครื่อง ส่งผลให้การบริหารจัดการเครือข่ายไม่มีประสิทธิภาพเพียงพอ

3.2 ปัญหาจากระบบงานปัจจุบัน

เนื่องจากระบบงานปัจจุบัน การจัดเก็บข้อมูลล็อกจะจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ที่ให้บริการ โดยไม่ได้มีการส่งข้อมูลล็อกไปเก็บไว้ที่เครื่องคอมพิวเตอร์ศูนย์กลางสำหรับจัดเก็บล็อก (Centralized Log Server) ทำให้เกิดปัญหาในการบริการจัดการขึ้น ดังต่อไปนี้

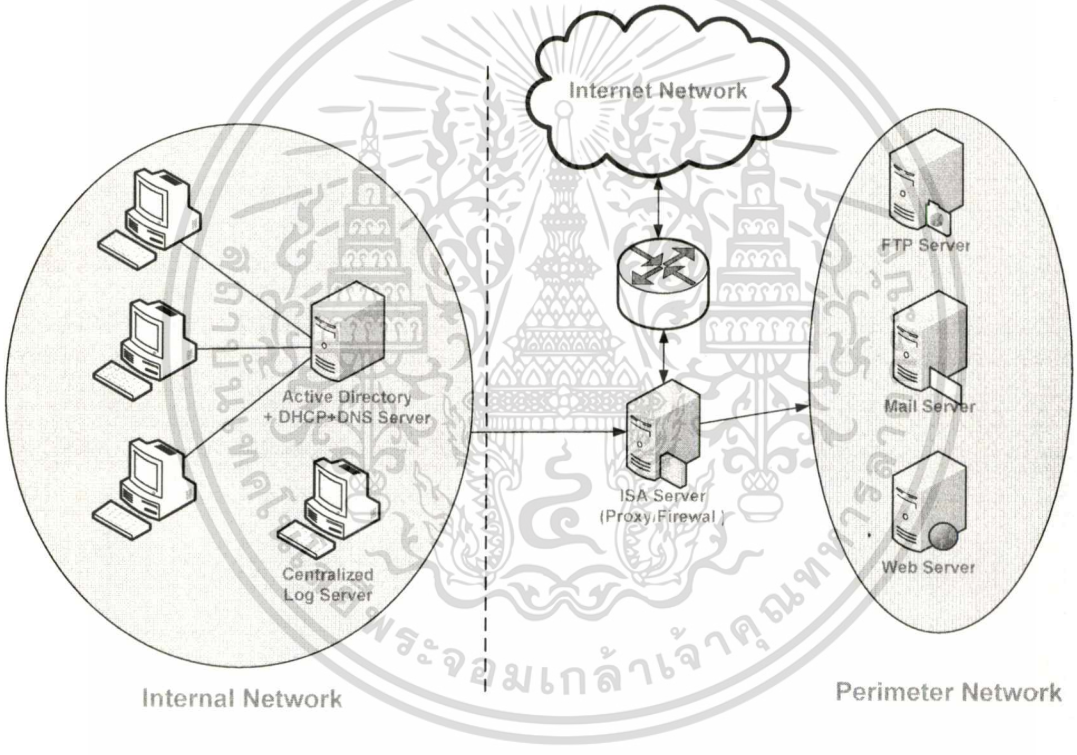
3.2.1 ข้อมูลล็อกที่จัดเก็บไม่มีความน่าเชื่อถือ เนื่องจากข้อมูลล็อกไฟล์มีการจัดเก็บอยู่ที่เครื่องที่ให้บริการนั้นๆ ซึ่งเสี่ยงต่อการที่ผู้ดูแลระบบสามารถทำการเปลี่ยนแปลง แก้ไขหรือลบข้อมูลล็อกเพื่อทำการลบหลักฐานที่กรณีที่มีการกระทำความผิด

3.2.2 การค้นหาข้อมูลล็อกไฟล์แบบเดิม มีความล่าช้าและไม่สะดวกต่อการทำงาน เนื่องจากมีการจัดเก็บข้อมูลในรูปแบบของล็อกไฟล์ ทำให้การสืบค้นข้อมูลทำได้ยาก โดยในการสืบค้นข้อมูลล็อกแบบเดิมนั้น จะต้องใช้เครื่องมือชื่อ “Logparser” ซึ่งยากต่อการใช้งาน เนื่องจากต้องสั่งงานผ่าน command Line

3.2.3 การวิเคราะห์ข้อมูลล็อกเป็นไปอย่างไม่มีประสิทธิภาพเพียงพอ โดยผู้ดูแลระบบไม่สามารถทำการวิเคราะห์ความสัมพันธ์ของข้อมูลล็อกที่เกิดขึ้นจากเครื่องแม่ข่ายหลาย ๆ เครื่องได้ เนื่องจากข้อมูลล็อกมีการจัดเก็บอย่างกระจัดกระจาย

3.3 การวิเคราะห์และออกแบบระบบใหม่

3.3.1 การออกแบบสถาปัตยกรรมของระบบเครือข่าย (Network Architecture)



รูปที่ 3.1 แสดงสถาปัตยกรรมของระบบ

จากรูปที่ 3.1 แสดงการจำลองโครงสร้างระบบเครือข่ายที่ใช้ในการทดลอง โดยในการทดลองนี้ ระบบแบ่งเครือข่ายออกเป็น 3 ส่วน คือ

(1) Internal Network (Trust Zone) เป็นโซนของเครือข่ายภายในที่มีเฉพาะโฮสต์ที่ไว้ใจได้ (Trusted Host) เป็นเครือข่ายที่มีการใช้งานภายในองค์กร และไม่อนุญาตให้เครือข่ายภายนอกเข้ามาได้ ซึ่งได้ทำการติดตั้งเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Client ภายใน

องค์กร รวมถึงเครื่อง Active Directory Server (AD Server) และเครื่อง Centralized Log Server

(2) Perimeter Network เป็นเน็ตเวิร์กที่เพิ่มเข้ามาเพื่อความปลอดภัย อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน โดยภายใน Perimeter Network จะติดตั้งเครื่องให้บริการต่างๆ ไว้ ได้แก่ FTP Server , Web Server , Mail Server

(3) External Network (No Trust Zone) เป็นโซนของเครือข่ายนอกใดๆ ที่อยู่บนอินเทอร์เน็ต เป็นโฮสต์ที่ไม่น่าไว้ใจ (Untrusted Host) เนื่องจากไม่สามารถวางใจในการเชื่อมต่อของโฮสต์และควบคุมผู้ใช้ได้

จากรูปที่ 3.1 จะเห็นได้ว่า ระบบสามารถจัดเก็บข้อมูลจราจรให้รองรับกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้ดังนี้

3.3.1.1 ระบบการระบุตัวตน (Identification) และ ระบบพิสูจน์ตัวตน (Authentication)

1) มีการติดตั้ง Active Directory Server หรือ Domain Controller ภายในองค์กรทำให้ระบบสามารถระบุตัวตนบุคคลที่ใช้บริการต่างๆ ได้ โดยเครื่องไคล์เอนต์ทุกเครื่องในระบบเครือข่ายจะทำการ join domain กับเครื่อง Active Directory Server (AD Server) ดังนั้นเมื่อผู้ใช้งานทำการล็อกออนเข้าใช้งานเครื่องไคล์เอนต์ จะได้ทำการ Authenticate กับเครื่อง Active Directory Server ก่อนเสมอ โดยจะเก็บข้อมูลล็อกการเข้าใช้งานไว้ที่ Event Log ในส่วนของ Security Log

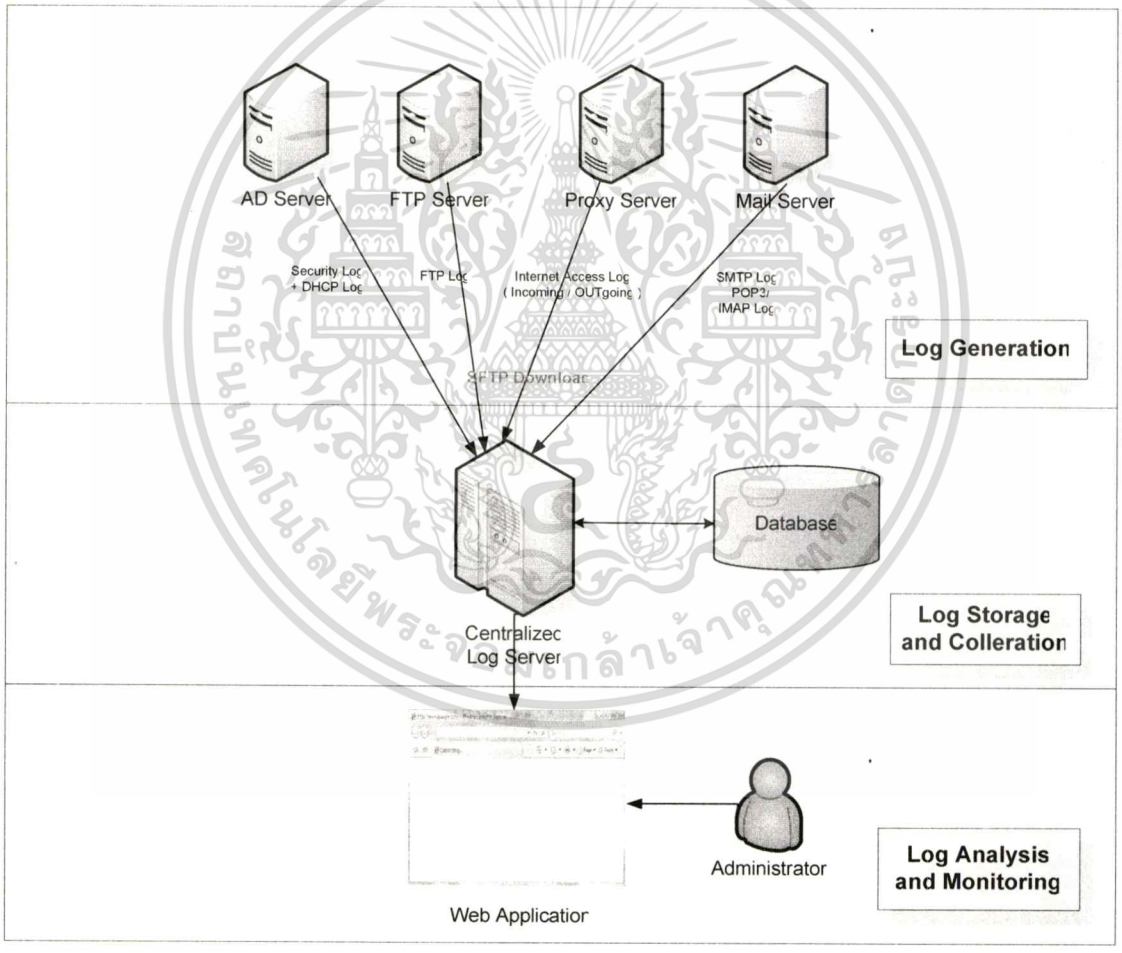
นอกจากนี้เครื่อง Active Directory Server นี้ ยังมีหน้าที่แจกจ่ายหมายเลขไอพีแอดเดรสให้กับเครื่องไคล์เอนต์เมื่อเครื่องไคล์เอนต์มีการร้องขอด้วย โดยจะทำการจัดเก็บข้อมูล DHCP Log ไว้เพื่อนำเข้าสู่ฐานข้อมูลต่อไป

2) มีการติดตั้ง Proxy Server ทำให้ทุกครั้งเมื่อผู้ใช้งานภายในองค์กร ต้องการใช้งานอินเทอร์เน็ตหรือบริการถ่ายโอนข้อมูลออกนอกองค์กรนั้น จะต้องมีการ Authenticate กับเครื่อง Proxy Server ก่อนเสมอ หรือเมื่อมีบุคคลภายในต้องการเข้าใช้งานบริการภายเครือข่ายเรา เช่น ต้องการใช้งานเวปไซต์ที่เครื่องเซิร์ฟเวอร์ภายในองค์กรเรา ก็จะมีการจัดเก็บล็อกการใช้งานไว้ที่เครื่อง Proxy Server เรียกว่า Proxy Log ทำให้เราสามารถสืบหาการใช้งานย้อนหลังได้

3.3.1.2 การจัดเก็บข้อมูลการใช้บริการเครื่องเซิร์ฟเวอร์ภายในองค์กร

ภายในเครือข่ายมีเครื่องที่ให้บริการ ได้แก่ AD Server , FTP Server , Mail Server , Web Server โดยเครื่องให้บริการทุกเครื่องจะต้องทำการ Enable Log สำหรับการเข้าใช้งานไว้ รวมถึงกำหนด Path สำหรับจัดเก็บข้อมูลการเข้าใช้บริการของผู้ใช้งานไว้ โดยกำหนดให้เครื่องให้บริการทำการจัดเก็บรายละเอียดข้อมูลจราจรทุกฟิลด์ เพื่อให้รองรับตามที่ พรบ. ได้กำนดไว้

3.3.2 การออกแบบโครงสร้างของระบบจัดเก็บข้อมูลจราจร



รูปที่ 3.2 แสดงโครงสร้างของระบบจัดเก็บข้อมูลจราจร

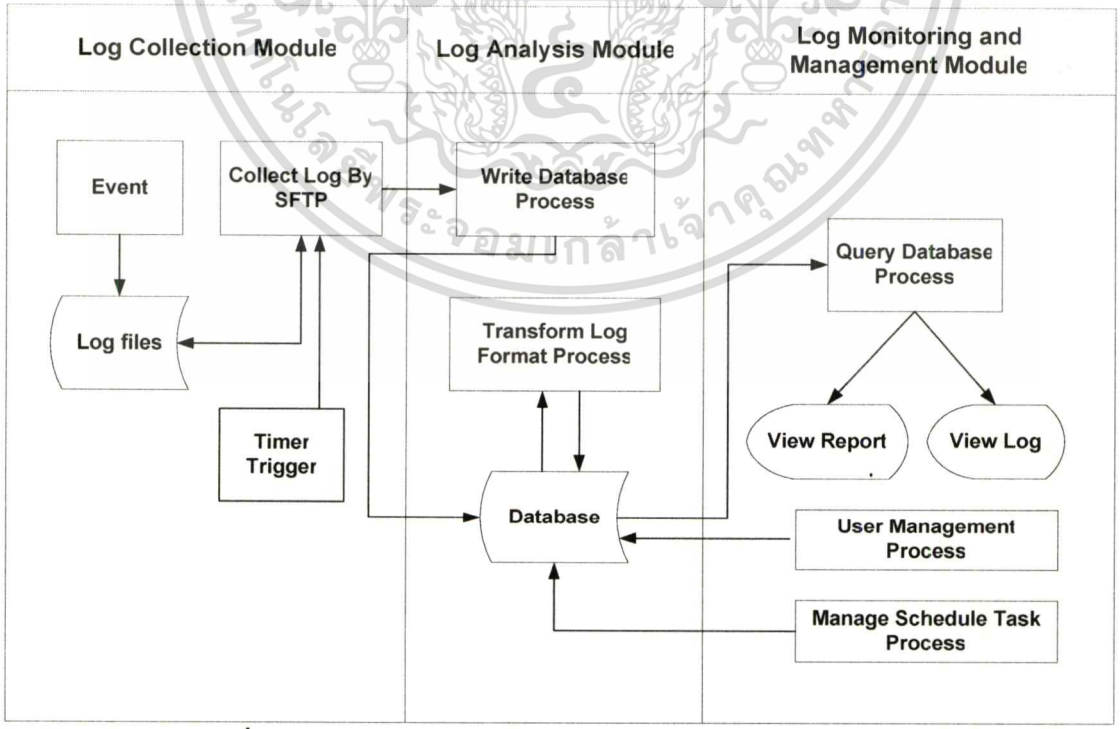
<u>ส่วนประกอบของระบบเก็บข้อมูลล็อก</u> แบ่งออกเป็น 3 ส่วนหลัก คือ

1. Log Generation เป็นแหล่งกำเนิดข้อมูลล็อก หรือสร้างข้อมูลล็อก เป็นเซิร์ฟเวอร์หรืออุปกรณ์บนระบบเครือข่ายที่มีข้อมูลล็อกจากระบบปฏิบัติการและแอพพลิเคชัน ซึ่งจากการทดลองในโครงงานนี้ได้ใช้ล็อกที่เกิดจากการใช้บริการเซิร์ฟเวอร์ต่างๆ ดังต่อไปนี้ คือ FTP Server , Proxy Server (incoming/outgoing), Mail Server , AD Server (DHCP Log + Security Log)

2. Log Storage and Correlation เป็นล็อกเซิร์ฟเวอร์สำหรับรับข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อกหรือ Log Generation เพื่อจัดเก็บตามรูปแบบที่กำหนดไว้ รวมทั้งการแปลงข้อมูลล็อกให้อยู่ในรูปแบบที่สามารถจัดเก็บได้ ซึ่งอาจรวมถึงการแปลงข้อมูล ล็อกให้มีรูปแบบที่พร้อมจะนำไปวิเคราะห์ต่อได้ ไม่ว่าจะมีรูปแบบของข้อมูลล็อกแตกต่างกัน

3. Log Analysis and Monitoring เป็นหน้าต่างสำหรับผู้ดูแลระบบหรือผู้ที่มีหน้าที่รับผิดชอบในการวิเคราะห์ข้อมูลล็อกและติดตามตรวจสอบความถูกต้องของข้อมูลล็อกระบบจัดเก็บข้อมูลล็อกบางระบบสนับสนุนการสร้างรายงานการวิเคราะห์ข้อมูลล็อก ทั้งนี้เพื่อให้สามารถวิเคราะห์ข้อมูลได้อย่างรวดเร็วและสวดวกยิ่งขึ้น

3.3.3 ขั้นตอนการทำงานของระบบจัดเก็บข้อมูลจราจร

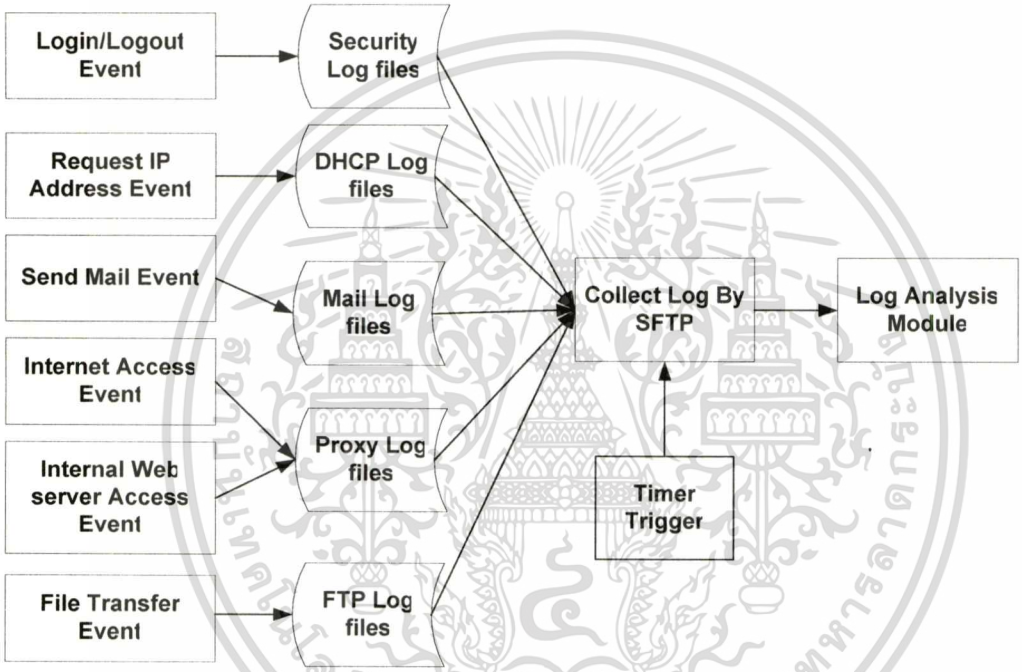


รูปที่ 3.3 แสดงกระบวนการทำงานของระบบจัดเก็บข้อมูลจราจร

ระบบจัดเก็บข้อมูลจราจร มีขั้นตอนการทำงานแบ่งออกได้เป็น 3 ส่วนคือ

3.3.3.1 Log Collection Module

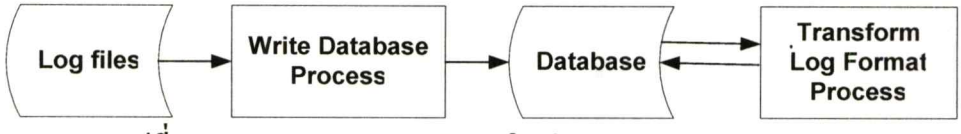
เป็น Module ที่ทำหน้าที่ในการดึงข้อมูลจราจรจากเครื่องเซิร์ฟเวอร์ต่างๆ บนระบบเครือข่าย ผ่านช่องทาง SFTP ตามรอบเวลาที่กำหนดไว้ ไปเก็บไว้ที่เครื่องเซิร์ฟเวอร์สำหรับเก็บข้อมูลจราจรส่วนกลาง (Centralized Log Server) เพื่อให้สามารถเก็บบนระบบฐานข้อมูลได้



รูปที่ 3.4 แสดงกระบวนการทำงานในส่วน Log Collection Module

3.3.3.2 Log Analysis Module

เป็น Module ที่ทำหน้าที่ในการจัดเก็บข้อมูลจากล็อกไฟล์ลงสู่ระบบฐานข้อมูล และแปลงข้อมูลจราจรแต่ละประเภทที่มีการจัดเก็บข้อมูลอยู่ในรูปแบบแตกต่างกันให้เป็นรูปแบบเดียวกัน โดยมีกระบวนการทำงานแบ่งออกเป็น 2 ขั้นตอน ดังนี้



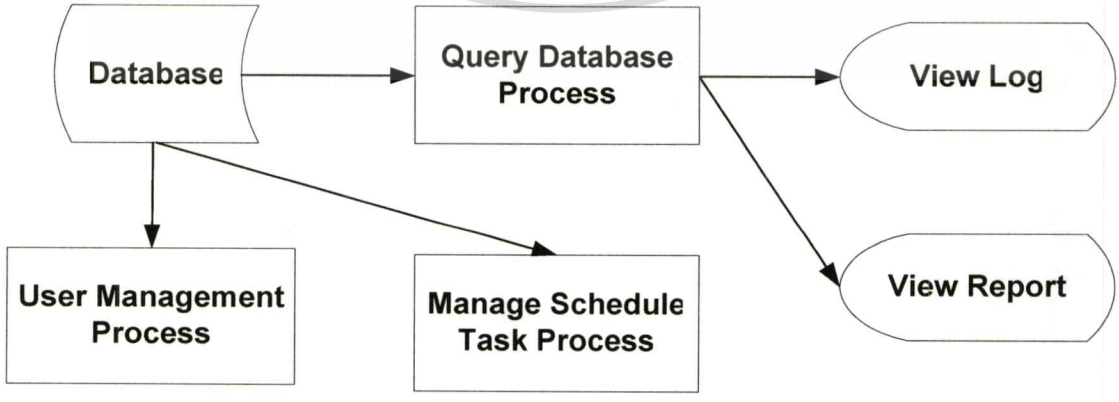
รูปที่ 3.5 แสดงกระบวนการทำงานในส่วน Log Analysis Module

1) Write Database Process เป็นกระบวนการที่ทำหน้าที่ในการอ่านข้อมูลจราจรจากล็อกไฟล์ของเครื่องเซิร์ฟเวอร์ต่างๆ อันได้แก่ FTP Log , SMTP Log , POP3 Log , Proxy Log เป็นต้น มาทำการจัดเก็บลงฐานข้อมูล SQL Server 2005 เพื่อให้ง่ายต่อการสืบค้น และวิเคราะห์ข้อมูลจราจรได้ โดยข้อมูลที่ได้จัดเก็บลงในฐานข้อมูลนั้นจะถูกนำไปแปลงรูปแบบข้อมูลในขั้นตอนยังขั้นตอน Transform Log Format Process ต่อไป

2) Transform Log Format Process เป็นกระบวนการแปลงรูปแบบของข้อมูลจราจรจากล็อกไฟล์ที่ได้บันทึกลงสู่ฐานข้อมูลแล้ว ซึ่งอยู่ในรูปแบบที่แตกต่างกัน ให้อยู่ในรูปแบบเดียวกัน (Common Log Format) เพื่อให้ระบบมีความสามารถในการรับข้อมูลจราจรหลากหลายรูปแบบ เช่น ข้อมูลจราจรวันที่จากเว็บเซิร์ฟเวอร์เป็นรูปแบบ 12 ชั่วโมงหรือเขียนเป็น 2:34:56 P.M. IDT ในขณะที่ข้อมูลจราจรวันที่ของเว็บเซิร์ฟเวอร์อีกเซิร์ฟเวอร์จัดเก็บในรูปแบบ 24 ชั่วโมง เช่น 14:34 GMT+7 เป็นต้น

3.3.3.3 Log Monitoring and Management Module

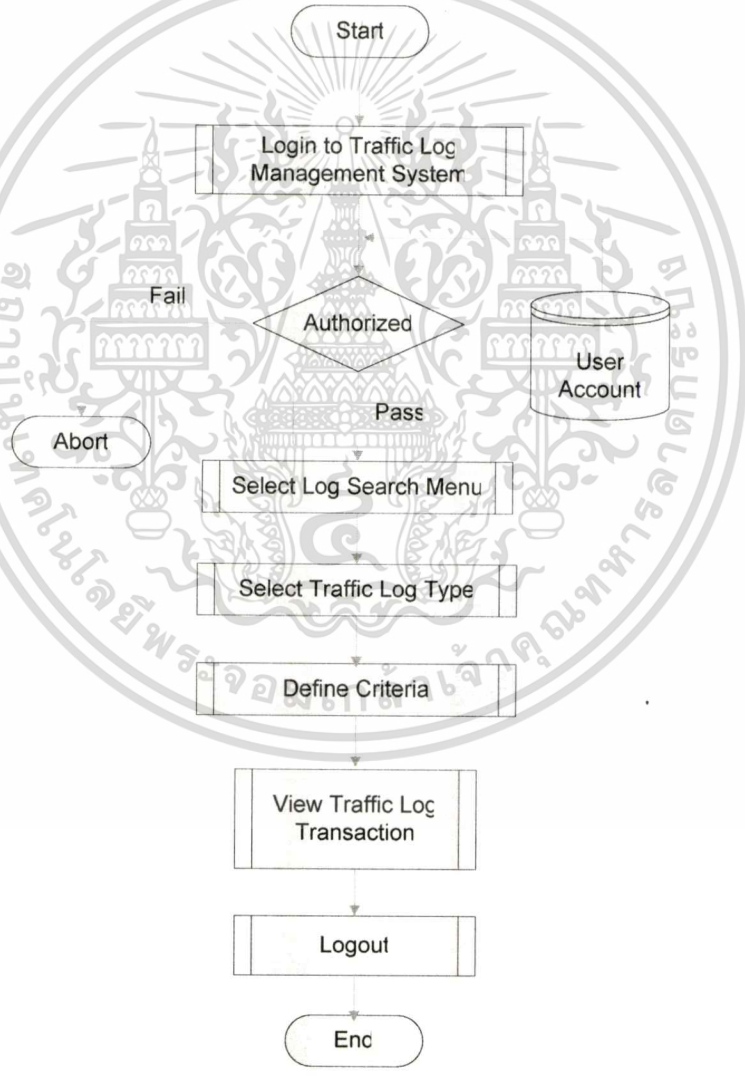
เป็น Module ที่ทำหน้าที่ช่วยในการแสดงผลข้อมูลจราจร เพื่อให้ผู้ดูแลระบบหรือผู้ที่มีหน้าที่รับผิดชอบในการวิเคราะห์ข้อมูลจราจร สามารถสืบค้นและวิเคราะห์หาความสัมพันธ์ของข้อมูลจราจรที่มีการจัดเก็บลงในฐานข้อมูล ได้ผ่านทาง Web Application รวมถึงสนับสนุนการสร้างรายงานการวิเคราะห์ข้อมูลจราจร ทั้งนี้เพื่อให้ผู้ดูแลระบบสามารถทำการวิเคราะห์ข้อมูลได้อย่างรวดเร็วและทันเวลา โดยประกอบด้วยการทำงาน 2 ลักษณะ ดังนี้



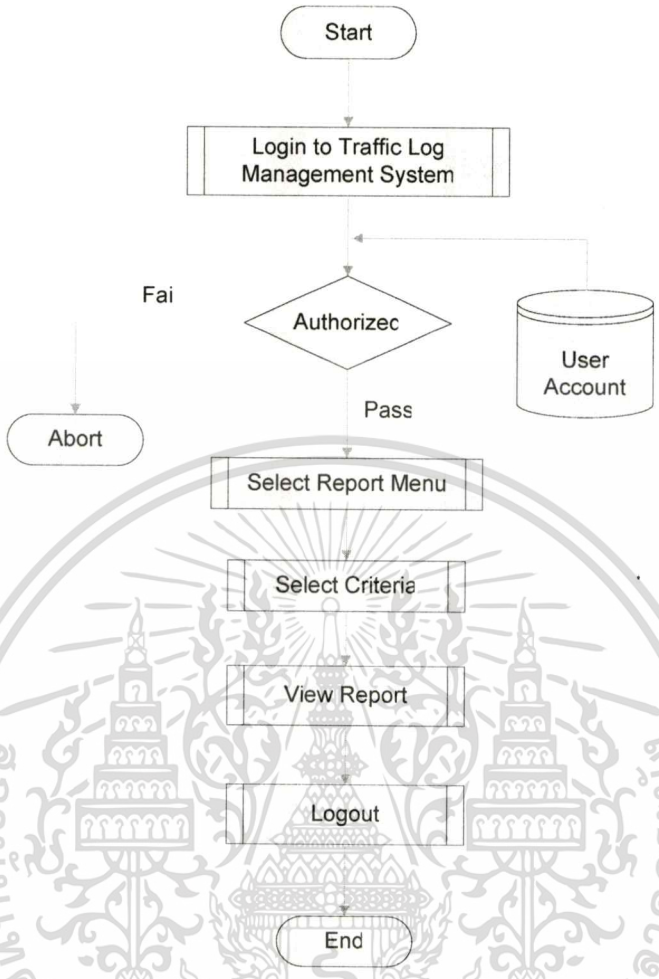
รูปที่ 3.6 แสดงกระบวนการทำงานในส่วน Log Monitoring and Management Module

1) Query Database Process

เป็นกระบวนการที่ทำหน้าที่ในการค้นหาข้อมูลจราจรจากระบบฐานข้อมูล เพื่อแสดงผลข้อมูลจราจรตามที่ผู้ใช้งานได้ระบุเงื่อนไขไว้ เช่น แสดงผลข้อมูลจราจรที่เกิดขึ้นในระหว่างวันและเวลาที่กำหนด , แสดงผลข้อมูลจราจรเฉพาะผู้ใช้งานที่มี username = somchai เป็นต้น นอกจากนี้ยังสามารถสรุปผลปริมาณข้อมูลจราจรแต่ละประเภทให้แก่ผู้ดูแลระบบสามารถทำการวิเคราะห์การใช้งานได้



รูปที่ 3.7 แสดงกระบวนการทำงานการค้นหาข้อมูลจราจรตามเงื่อนไขที่ระบุ

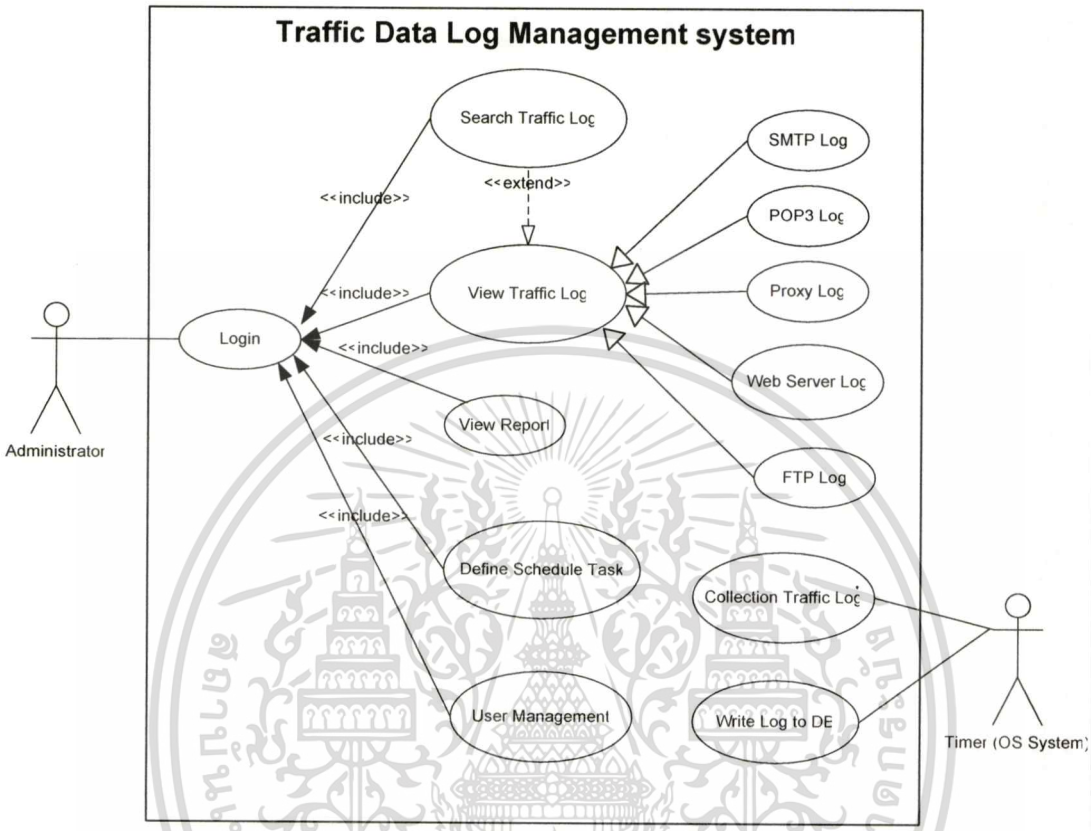


รูปที่ 3.8 แสดงกระบวนการทำงานแสดงรายงานสรุป

2) User Management Process

เป็นกระบวนการที่ทำหน้าที่ในการบริหารจัดการบัญชีรายชื่อผู้ใช้งานระบบจัดเก็บข้อมูลจราจร ซึ่งได้จัดเก็บไว้ในฐานข้อมูล โดยสามารถเพิ่ม ลบ และแก้ไขรายชื่อผู้ใช้งานได้ ผ่านทาง Web Application

3.3.4 การวิเคราะห์และออกแบบยูสเคสไดอะแกรม



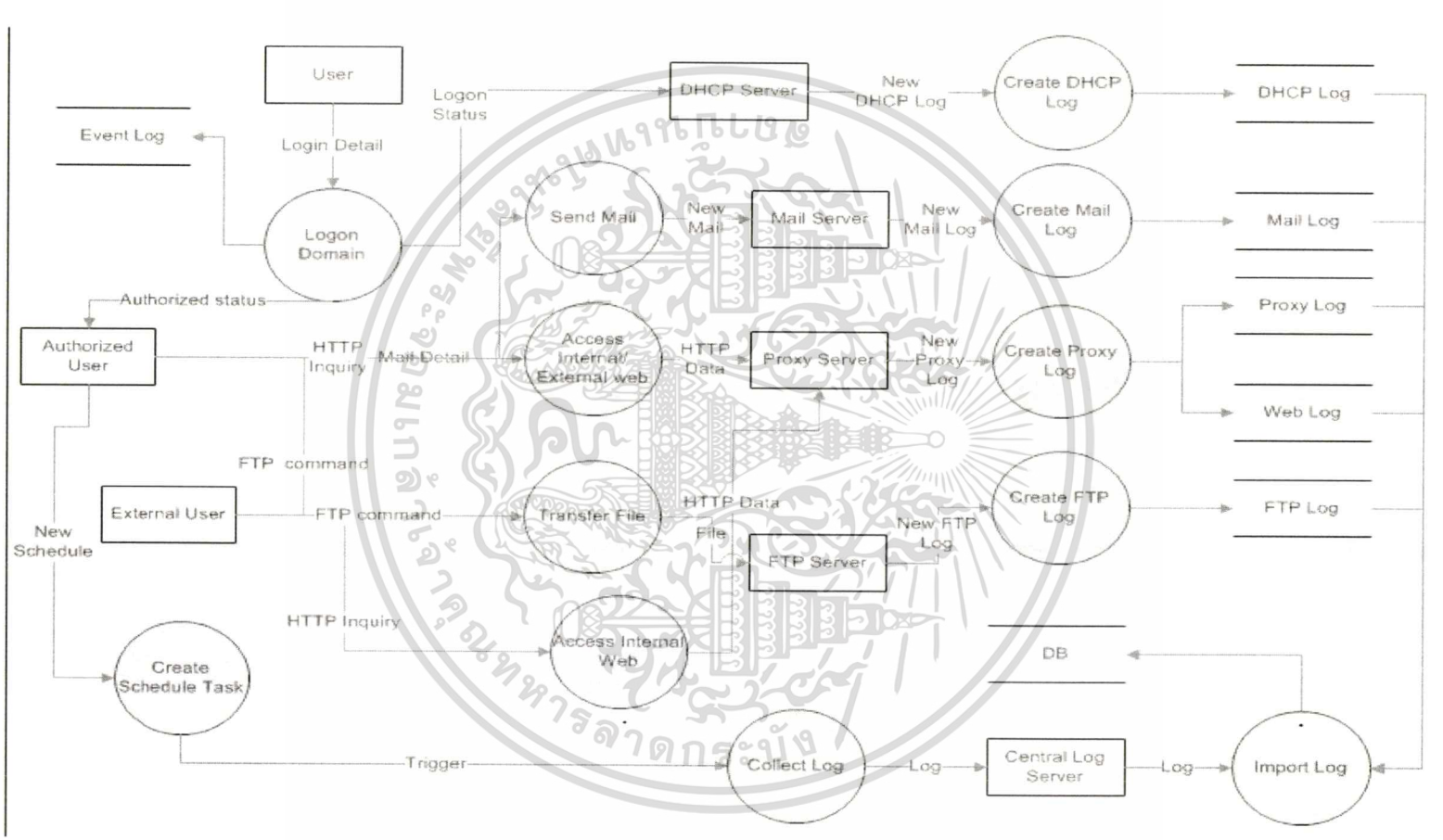
รูปที่ 3.9 ยูสเคสไดอะแกรมของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ระบบจัดเก็บข้อมูลจราจรยูสเคสที่เกี่ยวข้องกับระบบประกอบด้วย

- Actor : Administrator คือ ผู้ดูแลระบบ Traffic Log Management System โดยทำหน้าที่ในการบริหารจัดการและวิเคราะห์ข้อมูลล็อกทั้งหมด รวมถึงบริหารจัดการ user ที่จะเข้าใช้งานระบบ
- Actor : Timer (Os System) หมายถึง เวลาที่กำหนดไว้
- Usecase : Login ทำหน้าที่ในการกำหนดให้ผู้ใช้ต้องทำการ login ก่อนเข้าสู่ระบบ Traffic Log Management System
- Usecase : Search Traffic Log ทำหน้าที่ในการค้นหาข้อมูลจราจรในแต่ละประเภท ตามที่ผู้ใช้งานได้ระบุเงื่อนไขไว้
- Usecase : View Report ทำหน้าที่ในการแสดงสรุปรายงานของข้อมูลจราจรตามเงื่อนไข

- Usecase : View Traffic Log ทำหน้าที่ในการแสดงรายการข้อมูลจราจรในแต่ละประเภท ซึ่งได้แก่ SMTP Log , POP3 Log , Proxy Log , Web Server Log , FTP Log
- Usecase : User Management ทำหน้าที่ในการจัดการสิทธิผู้ใช้งานในการเข้าสู่ระบบ Traffic Log Management System
- Usecase : Define Schedule Task ทำหน้าที่ในการกำหนดตารางเวลาการดึง Log จากเครื่องเซิร์ฟเวอร์ต่างๆ
- Usecase : Collection Traffic Log ทำหน้าที่ในดึง Log จากเครื่องเซิร์ฟเวอร์ต่างๆ เมื่อถึงเวลาที่กำหนด
- Usecase : Write Log to DB ทำหน้าที่ในนำข้อมูลล็อกไฟล์ที่ดึงมาจากเครื่องเซิร์ฟเวอร์ต่างๆ เมื่อถึงเวลาที่กำหนด แล้วจัดเก็บลงสู่ฐานข้อมูล

3.3.5 การวิเคราะห์และออกแบบแผนภาพการไหลของข้อมูล



รูปที่ 3.10 แสดงแผนภาพการไหลของข้อมูล

3.3.6 การออกแบบฐานข้อมูล (Database Design)

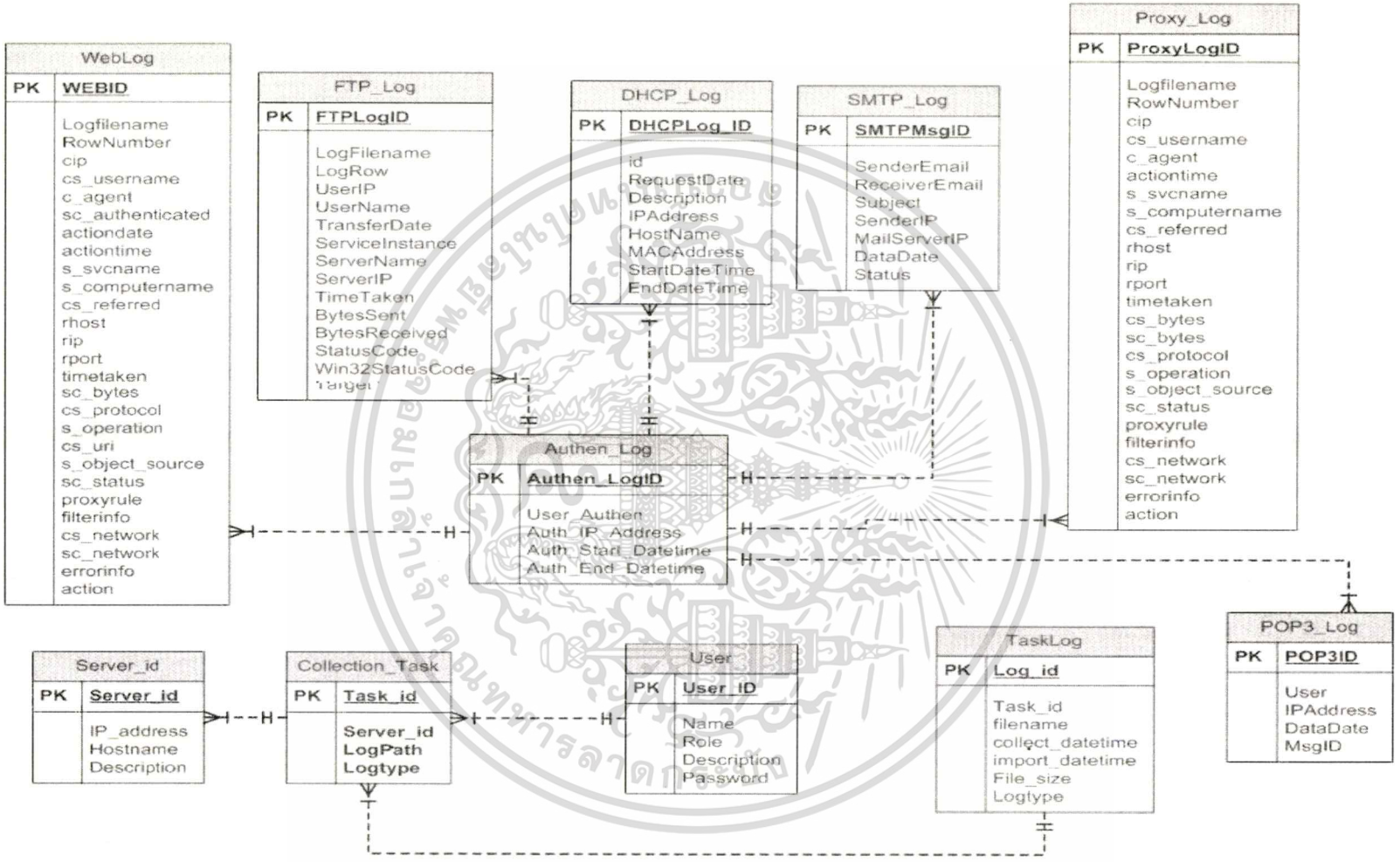
จากการศึกษาความต้องการของระบบทำให้สามารถระบุความต้องการของระบบออกมาเป็นแผนภาพแบบจำลองความสัมพันธ์ระหว่างเอนทิตีซึ่งแสดงความสัมพันธ์ระหว่างเอนทิตีและแสดงข้อมูลของเอนทิตีดังพจนานุกรมข้อมูล

3.3.6.1 แบบจำลองความสัมพันธ์ระหว่างเอนทิตี

จากการวิเคราะห์ระบบและออกแบบฐานข้อมูล โดยใช้แบบจำลองความสัมพันธ์ระหว่างเอนทิตีเพื่อแสดงความสัมพันธ์ระหว่างเอนทิตี ดังแสดงในรูปที่ 3.11

รายละเอียดของเอนทิตี ดังนี้

1. User คือ ข้อมูลของผู้ที่มีสิทธิ์เข้าใช้งานระบบ
2. ProxyLog คือ ข้อมูลล็อกการใช้บริการอินเทอร์เน็ตออกนอกระบบเครือข่าย
3. WebLog คือ ข้อมูลล็อกการเข้าเยี่ยมชมเว็บไซต์ต่างๆ
4. POP3 คือ ข้อมูลล็อกการดึง E-mail ออกจาก mailbox
5. SMTP คือ ข้อมูลล็อกการรับส่ง E-mail
6. DHCPLog คือ ข้อมูลล็อกการแจกจ่ายหมายเลขไอพีแอดเดรสให้กับเครื่องที่ร้องขอ
7. FTP_Log คือ ข้อมูลล็อกของการถ่ายโอนไฟล์ข้อมูล
8. Authen_Log คือ ข้อมูลล็อกการล็อกอินเข้าใช้งานเครื่องคอมพิวเตอร์แต่ละเครื่องที่มีการ join domain กับระบบ Domain Controller
9. Server_info คือ ข้อมูลของเครื่องเซิร์ฟเวอร์ที่ให้บริการภายในองค์กร
10. Collection_Task เก็บรายละเอียดเกี่ยวกับข้อมูลรอบการดึงข้อมูลล็อกไฟล์จากเครื่องเซิร์ฟเวอร์ที่ให้บริการภายในองค์กร
11. TaskLog เก็บรายละเอียดเกี่ยวกับรายละเอียดที่ได้ทำการดึงล็อกไฟล์จากเครื่องเซิร์ฟเวอร์ต่างๆ



รูปที่ 3.11 แสดง ER diagram ของระบบ Computer Traffic Data Management System

3.3.6.2 พจนานุกรมข้อมูล

รายละเอียดของแต่ละเอนทิตีของระบบ สามารถอธิบายได้ด้วยพจนานุกรมข้อมูลดังนี้

ตารางที่ 3.1 พจนานุกรมข้อมูลตาราง User

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
User_ID	VARCHAR(20)	ชื่อที่ใช้ในการ Login	PK
Name	VARCHAR(20)	ชื่อ นามสกุล ของผู้ใช้งาน	
Role	VARCHAR(30)	บทบาทของผู้ใช้งาน (Admin/User)	
Description	VARCHAR(50)	รายละเอียดเพิ่มเติมของผู้ใช้งาน	
Password	VARCHAR(20)	รหัสผ่าน	

ตารางที่ 3.2 พจนานุกรมข้อมูลตาราง ProxyLog

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
ProxyLogID	int	หมายเลขประจำ PROXY	PK
Logfilename	Varchar (255)	ชื่อของไฟล์ PROXY ที่นำข้อมูลเข้าฐานข้อมูล	
RowNumber	int	หมายเลขแถวของไฟล์ FTP	
cip	Varchar(20)	ไอพีแอดเดรสของไคลเอนต์	
cs_username	Varchar (20)	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้	
c_agent	Varchar (255)	-	
sc_authenticated	Varchar (255)	-	
actiondate	datetime	วันที่เกิดเหตุการณ์	
actiontime	datetime	เวลาที่เกิดเหตุการณ์	
s_svcname	Varchar (255)	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้	
s_computername	Varchar (255)	ชื่อเซิร์ฟเวอร์	
cs_referred	Varchar (255)	-	
rhost	Varchar (255)	-	
rip	Varchar(20)	ไอพีแอดเดรสของเซิร์ฟเวอร์	
rport	Varchar(5)	หมายเลขพอร์ตปลายทาง	

ตารางที่ 3.2 (ต่อ)

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
timetaken	int	ระยะเวลาที่ใช้ในการโหลด Object หรือไฟล์ (มิลลิวินาที)	
cs_bytes	int	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์	
sc_bytes	int	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์	
cs_protocol	int	หมายเลขโปรโตคอล	
s_operation	varchar(255)	-	
cs_uri	varchar(255)	ตำแหน่งของเว็บเพจ	
s_object_source	varchar(255)	-	
sc_status	varchar(255)	รหัสสถานะของโปรโตคอล	
proxyrule	Int	กฎของ Fiewwall	
filterinfo	Varchar (255)	-	
cs_network	varchar(255)	Network ต้นทาง	
sc_network	varchar(255)	Network ปลางทาง	
errorinfo	varchar(255)	รายละเอียดแสดงข้อผิดหลาด	
action	varchar(255)	-	

ตารางที่ 3.3 พจนานุกรมข้อมูลตาราง WebLog

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
WEBID	Int	หมายเลขประจำ WEB	PK
Logfilename	Varchar (255)	ชื่อของไฟล์ที่นำข้อมูลเข้าฐานข้อมูล	
RowNumber	int	หมายเลขแถวของไฟล์ FTP	
cip	Varchar(20)	ไอพีแอดเดรสของไคลเอนต์	
cs_username	Varchar (20)	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้	
c_agent	Varchar (255)	-	
sc_authenticated	Varchar (255)	-	
actiondate	Datetime	วันที่เกิดเหตุการณ์	
actiontime	Datetime	เวลาที่เกิดเหตุการณ์	

ตารางที่ 3.3 (ต่อ)

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
s_svcname	Varchar (255)	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้ โดยบันทึกชื่อตาม identifier	
s_computername	Varchar (255)	ชื่อเซิร์ฟเวอร์	
cs_referred	Varchar (255)	-	
rhost	Varchar (255)	-	
rip	Varchar(20)	ไอพีแอดเดรสของเซิร์ฟเวอร์	
rport	Varchar(5)	หมายเลขพอร์ตปลายทาง	
timetaken	Int	ระยะเวลาที่ใช้ในการโหลด Object หรือไฟล์ (มิลลิวินาที)	
cs_bytes	Int	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์	
sc_bytes	Int	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์	
cs_protocol	Int	หมายเลขโปรโตคอล	
s_operation	varchar(255)	-	
cs_uri	varchar(255)	ตำแหน่งของเว็บเพจ	
s_object_source	varchar(255)	-	
sc_status	varchar(255)	รหัสสถานะของโปรโตคอล	
proxyrule	Int	กฎของ Fiewwall	
filterinfo	Varchar (255)	-	
cs_network	varchar(255)	Network ต้นทาง	
sc_network	varchar(255)	Network ปลางทาง	
errorinfo	varchar(255)	รายละเอียดแสดงข้อผิดหลาด	
action	varchar(255)	-	

ตารางที่ 3.4 พจนานุกรมข้อมูลตาราง POP3

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
POP3ID	Int	หมายเลขประจำ POP3	PK
User	VARCHAR(50)	ชื่อยูสเซอร์ที่ดึง E-mail ออกจาก mailbox	
IPAddress	VARCHAR(50)	หมายเลขไอพีแอดเดรสของที่ดึง E-mail	
DataDate	VARCHAR(50)	วันเวลาที่มีการดึง E-mail ออกจาก mailbox	
MsgID	VARCHAR(50)	หมายเลขรหัสของ E-mail	

ตารางที่ 3.5 พจนานุกรมข้อมูลตาราง SMTP

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
SMTPMsgID	VARCHAR(50)	หมายเลขประจำ E-mail	PK
SenderEmail	VARCHAR(50)	E-mail ของผู้ส่ง	
ReceiverEmail	VARCHAR(50)	E-mail ของผู้รับ	
Subject	VARCHAR(50)	ชื่อหัวข้อ E-mail	
SenderIP	VARCHAR(50)	IP Address ของเครื่องที่ทำการส่ง e-mail	
MailServerIP	VARCHAR(50)	IP Address ของเครื่อง Mail Server	
DataDate	DATETIME	วันเวลาที่ทำรายการส่ง e-mail	
Status	Int	ข้อมูลที่บอกถึงสถานะในการตรวจสอบ	

ตารางที่ 3.6 พจนานุกรมข้อมูลตาราง DHCPLog

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
DHCPLog_ID	Int	หมายเลขประจำ DHCP	PK
id	CHAR	รหัสของเหตุการณ์ DHCP	
IPAddress	VARCHAR(20)	หมายเลขไอพีแอดเดรสของที่ DHCP ได้แจกจ่ายให้	
HostName	VARCHAR(255)	ชื่อเครื่องที่มีการร้องขอหมายเลขไอพีแอดเดรส	
MacAddress	VARCHAR(255)	หมายเลขเครื่องที่มีการร้องขอหมายเลขไอพีแอดเดรส	
StartDateTime	Datetime	วันเวลาเริ่มต้นที่มีการใช้หมายเลขไอพีแอดเดรส	
EndDateTime	Datetime	วันเวลาสิ้นสุดที่มีการใช้หมายเลขไอพีแอดเดรส	

ตารางที่ 3.7 พจนานุกรมข้อมูลตาราง FTP_Log

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
FTPLogID	Int	หมายเลขประจำ FTP	PK
LogFilename	CHAR	ชื่อของไฟล์ FTP ที่นำข้อมูลเข้าฐานข้อมูล	
LogRow	VARCHAR(20)	หมายเลขแถวของไฟล์ FTP	
UserIP	VARCHAR(255)	ไอพีแอดเดรสของไคลเอนต์	
UserName	VARCHAR(255)	ชื่อยูสเซอร์ที่ทำงานในเหตุการณ์นี้	
TransferDate	Datetime	วันที่เกิดเหตุการณ์	
ServiceInstance	Datetime	ชื่อเซอร์วิสที่เกิดเหตุการณ์นี้	
ServerName	varchar(255)	ชื่อเซิร์ฟเวอร์	
ServerIP	varchar(255)	ไอพีแอดเดรสของเซิร์ฟเวอร์	
TimeTaken	Int	ระยะเวลาที่ใช้ในการโหลด Object หรือไฟล์ (มิลลิวินาที)	
BytesSent	Int	จำนวนไบต์ที่เซิร์ฟเวอร์ส่งไปให้ไคลเอนต์	
BytesReceived	Int	จำนวนไบต์ที่เซิร์ฟเวอร์ได้รับจากไคลเอนต์	
StatusCode	Int	รหัสสถานะของโปรโตคอล	
Win32StatusCode	Int	รหัสสถานะของระบบ Windows ในเครื่องเซิร์ฟเวอร์	
Method	varchar(255)	เมธอดที่ไคลเอนต์ใช้ทำงานในเหตุการณ์นี้ เช่น Get , Post	
Target	varchar(255)	ส่วนท้ายของ URL (ไม่รวมชื่อเว็บไซต์) ของ Object หรือไฟล์ที่โหลด	

ตารางที่ 3.8 พจนานุกรมข้อมูลตาราง Authen_Log

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
Authen_LogID	int	หมายเลขประจำ AuthenLog	PK
User_Authen	CHAR(8)	ชื่อที่ใช้ในการ Login เข้าใช้งานเครื่องคอมพิวเตอร์แบบ Join Domain	
Auth_IP_Address	VARCHAR(17)	IP Address ของเครื่องคอมพิวเตอร์ที่ทำการ Login เข้าใช้งาน	
Auth_Start_Datetime	DATETIME	วันเวลาที่ทำการ Login เข้าใช้งาน	
Auth_End_Datetime	DATETIME	วันเวลาที่ทำการ Logout การเข้าใช้งาน	

ตารางที่ 3.9 พจนานุกรมข้อมูลตาราง Server_info

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
Server_id	Int	รหัสของเครื่องเซิร์ฟเวอร์	PK
IP_address	VARCHAR(17)	หมายเลข IP Address ของเครื่องเซิร์ฟเวอร์	
Hostname	VARCHAR(20)	ชื่อเครื่องเซิร์ฟเวอร์	
Description	VARCHAR(50)	รายละเอียดเพิ่มเติมของเครื่องเซิร์ฟเวอร์	

ตารางที่ 3.10 พจนานุกรมข้อมูลตาราง Collection_Task

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
Task_id	Int	รหัสของงาน	PK
Server_id	Int	รหัสของเครื่องเซิร์ฟเวอร์	FK
LogPath	VARCHAR(50)	ชื่อพาธที่เก็บข้อมูลล็อกที่เครื่องเซิร์ฟเวอร์	
Logtype	VARCHAR(20)	ชนิดของข้อมูลล็อก	

ตารางที่ 3.11 พจนานุกรมข้อมูลตาราง TaskLog

ชื่อแอตทริบิวต์	ประเภท	ความหมาย	คีย์
Log_id	Int	รหัสของข้อมูลล็อกที่มีการดึงมา	PK
Task_id	Int	รหัสของงาน	FK
Filename	VARCHAR(50)	รหัสของเครื่องเซิร์ฟเวอร์	
collect_datetime	datetime	วันเวลาที่มีการดึงข้อมูลล็อก	
import_datetime	datetime	วันเวลาที่มีการนำข้อมูลล็อกเข้าสู่ฐานข้อมูล	
File_size	float	ขนาดของล็อกไฟล์	
Logtype	VARCHAR(20)	ชนิดของข้อมูลล็อก	

บทที่ 4
การพัฒนาระบบ

จากการวิเคราะห์และออกแบบระบบ จึงทำให้ได้ทำการพัฒนาระบบงานในฟังก์ชันต่างๆ ตามที่ได้วิเคราะห์และออกแบบไว้ โดยวิธีการและขั้นตอนในการพัฒนาระบบมีดังต่อไปนี้

4.1 เครื่องมือที่ใช้ในการพัฒนาระบบ

โปรแกรมที่ใช้ในการพัฒนาระบบ แบ่งออกเป็น 2 กลุ่ม ดังนี้

4.1.1 โปรแกรมที่ใช้พัฒนา Computer Traffic Data Management System

4.1.1.1 Microsoft Visual Studio 2005

Microsoft Visual Studio 2005 เป็น Integrated Development Environment เป็นเครื่องมือที่ช่วยพัฒนาโปรแกรมคอมพิวเตอร์ เว็บไซต์ เว็บแอปพลิเคชัน และ เว็บเซอร์วิส ระบบที่รองรับการทำงานนั้นมีไมโครซอฟท์ วินโดวส์ พ็อคเกตพีซี และ เว็บเบราว์เซอร์ ในปัจจุบันสามารถรองรับภาษาในโปรแกรมเดียวกัน เช่น VB.NET C++ C# J# เป็นต้น

4.1.1.2 Microsoft .NET Framework

Microsoft .NET Framework เป็นแพลตฟอร์มเพื่อใช้สำหรับ การพัฒนา Application .Net Framework ถูกออกแบบมาเพื่อให้สามารถ ถูกใช้จากภาษาใดๆ ก็ได้ รวมถึง C# ด้วย รวมถึงภาษา C++, Visual Basic, JScript, Delphi และอื่นๆ เพื่อให้สิ่งเหล่านี้เป็นไปได้ จึงเกิดภาษาเหล่านี้ขึ้นมาในรูปของ Version เฉพาะ สำหรับ .Net อีกด้วย ได้แก่ภาษา Managed C++, Visual Basic.Net, Jscript .Net,Borland C#, Delphi8 เป็นต้น

4.1.1.3 Microsoft SQL Server 2005

Microsoft SQL Server 2005 เป็นแพลตฟอร์มดาต้าเบสครบวงจร ซึ่งมีระบบบริหารข้อมูลระดับเอนเตอร์ไพรซ์ พร้อมกับมีเครื่องมือระบบธุรกิจอัจฉริยะ (business intelligence -BI) ในตัว กลไกดาต้าเบสของ SQL Server 2005 ช่วยให้จัดเก็บข้อมูลรีเลชันแนลและข้อมูลที่มีโครงสร้างได้อย่างปลอดภัยมากขึ้นและมีเสถียรภาพมากขึ้น

Microsoft SQL Server 2005 สามารถทำงานร่วมกับ Microsoft Visual Studio, Microsoft Office System และชุดเครื่องมือพัฒนารุ่นใหม่ๆ อาทิเช่น Business Intelligence Development Studio เป็นต้น

4.1.2 โปรแกรมที่ใช้ในการพัฒนาส่วน Collection Log Module

4.1.2.1 Log Parser 2.2

Microsoft Log Parser เป็นโปรแกรมแบบ command line ที่ช่วยอำนวยความสะดวกในการเรียกดูข้อมูลล็อกไฟล์ของระบบปฏิบัติการ Windows โดยคำสั่งต่างๆ ที่ใช้สำหรับเรียกดูข้อมูลในล็อกไฟล์ของ Log Parser นั้น จะมีลักษณะเหมือนกับภาษา SQL (Structured Query Language) ซึ่งทำให้สามารถเรียกดูข้อมูลจากล็อกไฟล์ได้อย่างรวดเร็วและมีประสิทธิภาพ ถึงแม้ล็อกไฟล์จะมีขนาดใหญ่ก็ตาม

4.1.2.2 Editplus

โปรแกรม TextEditor ที่รันบนระบบปฏิบัติการ Windows 32-Bits ครับ และโปรแกรมนี้เป็นโปรแกรมที่มีประสิทธิภาพเหนือกว่าโปรแกรม NotePad ที่ให้มากับโปรแกรม Windows โดยสามารถใช้ในการแก้ไขเอกสารและ coding Script ต่างๆ ได้แก่ Text ,HTML, ASP,ASP.NET, JavaScript , VBScript , Perl , Java ,PHP, C/C++ ฯลฯ

4.1.2.3 Internet Security and Acceleration Server 2004 (ISA)

เป็นโปรแกรมที่ได้รวมเอา 2 บทบาทที่สำคัญเข้าไว้ด้วยกัน คือ Cache server หรือ Proxy Server ซึ่งทำหน้าที่เพิ่มความเร็วให้แก่อินเทอร์เน็ต โดยเก็บข้อมูลที่ใช้บ่อยๆ ไว้ชั่วคราว และ Firewall ที่เป็นกำแพงระบบจากผู้บุกรุก ช่วยปกป้องเครือข่ายขององค์กรจากผู้บุกรุกภายนอก

4.1.2.4 Internet Information Services

โปรแกรมสำหรับการจำลองเครื่องของเราให้กลายเป็นเครื่องเซิร์ฟเวอร์ ในรูปแบบต่างๆ ของ Internet เช่น Web Server , FTP Server , SMTP Server ฯลฯ เพื่อให้สามารถ Run โปรแกรมผ่านเครื่องของเราได้

4.1.2.5 Majodio Mail

โปรแกรมสำหรับการจำลองเครื่องของเราให้กลายเป็นเครื่อง Mail Server ช่วยเพิ่มความสะดวกต่อผู้ดูแลระบบในการเพิ่มลบผู้ใช้งานหรือโดเมนอื่นๆ เนื่องจากอยู่ในรูปแบบของ Graphic User Interface นอกจากนี้ยังสามารถบันทึกข้อมูลจราจรเกี่ยวกับ SMTP Log และ POP3 Log ได้

4.1.2.6 WinSCP3

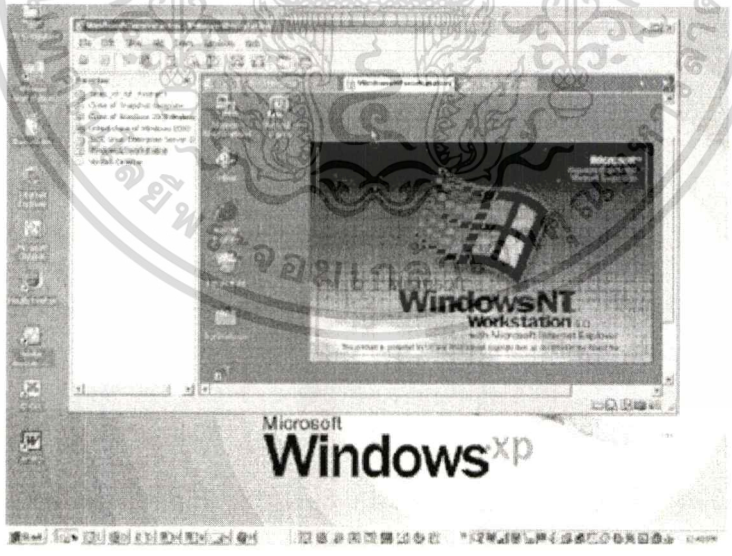
โปรแกรมสำหรับการใช้งานเป็น SFTP Client โปรแกรมสำหรับถ่ายโอนไฟล์ข้อมูลผ่าน Secure Shell (Port 22) จากเครื่องผู้ใช้งานไปยังเครื่อง SFTP Server และจากเครื่องSFTP Server ลงมายังเครื่องผู้ใช้งาน ผู้ใช้งานสามารถเข้าไปสร้าง ลบ หรือ แก้ไขไฟล์ข้อมูลที่ฝั่ง SFTP Server ได้

4.1.2.7 OpenSSH

โปรแกรมสำหรับการใช้งานเป็น SFTP Server ที่มีการจัดการเรื่องการเข้ารหัสให้กับการติดต่อเชื่อมโยงกันระหว่างผู้ดูแลระบบที่เครื่อง Workstation กับเครื่อง Server ที่อยู่ห่างไกล ที่สามารถไว้วางใจในการติดต่อกันได้ทุกเรื่องเช่น ข้อมูลตั้งแต่เริ่ม login รวมไปถึงการติดต่อกันด้วยคำสั่งต่าง ๆ ที่ใช้งานในระหว่างการติดต่อกันอยู่และมีบริการความปลอดภัยเรื่องการคัดลอกด้วยการใช้ Secure copy (scp) และ Secure Ftp (sftp)

4.1.2.8 Vmware Workstation ACE Edition

โปรแกรม VMWare เป็นโปรแกรมที่ถูกคิดค้นขึ้นมาเพื่อสร้างคอมพิวเตอร์เสมือน (Virtual Machine) ขึ้นบนระบบปฏิบัติการเดิมที่มีอยู่ ตัวอย่างเช่นในรูปที่ 4.1 เป็นรูปที่แสดงถึงเครื่องคอมพิวเตอร์ที่ลงระบบปฏิบัติการ Windows XP อยู่เดิม แล้วทำการลงระบบปฏิบัติการ Windows NT ผ่านโปรแกรม VMWare อีกทีหนึ่ง ซึ่งเมื่อลงแล้ว ทั้งสองระบบสามารถทำงานพร้อมกันได้โดยแยกจากกันค่อนข้างเด็ดขาด (เสมือนเป็นคนละเครื่อง) โดยคอมพิวเตอร์เสมือนที่สร้างขึ้นมานั้น จะมีสภาพแวดล้อมเหมือนกับคอมพิวเตอร์จริงๆ เครื่องหนึ่ง ซึ่งจะประกอบด้วย พื้นที่ดิสก์ที่ใช้ร่วมกับพื้นที่ดิสก์ของเครื่องนั้นๆ การ์ดแสดงผล การ์ดเน็ตเวิร์ก พื้นที่หน่วยความจำซึ่งจะแบ่งการทำงานมาจากหน่วยความจำของเครื่องนั้นๆ เช่นกัน



รูปที่ 4.1 แสดงการใช้ระบบปฏิบัติการ Windows NT บน Windows XP

4.2 การพัฒนาเซิร์ฟเวอร์ในการทำงานของระบบ Computer Traffic Data Management System

เนื่องจากในการพัฒนาระบบ Computer Traffic Data Management System เพื่อช่วยในการจัดเก็บและช่วยในการสืบค้นข้อมูลจราจรตามที่พรบ. กำหนดนั้น จำเป็นจะต้องมีข้อมูลจราจรประเภทต่างๆ เพื่อใช้ในการทดลอง ดังนั้นจึงต้องมีการสร้างเครื่องเซิร์ฟเวอร์ต่างๆ เพื่อทำการสร้างข้อมูลจราจรและส่งมายังเครื่องคอมพิวเตอร์สำหรับจัดเก็บข้อมูลจราจรส่วนกลาง โดยเซิร์ฟเวอร์ต่างๆ ที่ได้พัฒนามีการกำหนดสภาวะแวดล้อมและการติดตั้งโปรแกรมในการทำงานของระบบดังต่อไปนี้

ตารางที่ 4.1 สภาวะแวดล้อมของติดตั้งเครื่องเซิร์ฟเวอร์ต่าง ๆ

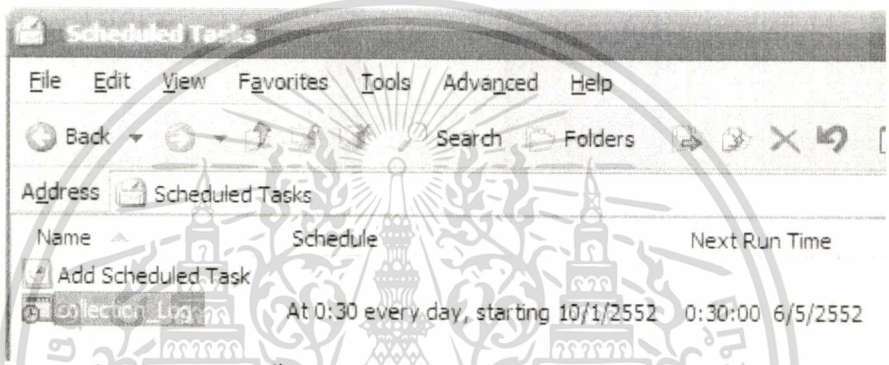
Server	IP Address	ระบบปฏิบัติการ	โปรแกรมที่ติดตั้ง
Active Directory (AD)	192.168.10.2	Window Server 2003	- Microsoft *Active Directory* - DHCP บน Window Server 2003
ISA Server	192.168.10.1 192.168.1.2 192.168.2.1	Window Server 2003	- Internet Security and Acceleration Server 2004 (ISA) + Service Pack 1 – 3 - OpenSSH
FTP Server	192.168.2.3 192.168.2.4	Window Server 2003	- Internet Information Services - OpenSSH
Mail Server	192.168.2.5	Window Server 2003	- Majodio Mail - OpenSSH
Web Server	192.168.2.6	Window XP Service Pack 2	Internet Information Services
Centralized Log Server	192.168.10.3	Window XP Service Pack 2	- Microsoft Visual Studio 2005 - Microsoft .NET Framework - Microsoft SQL Server 2005 - โปรแกรม Log Parser 2.2 - WinSCP

4.3 ฟังก์ชันการทำงานของระบบ Computer Traffic Data Management System

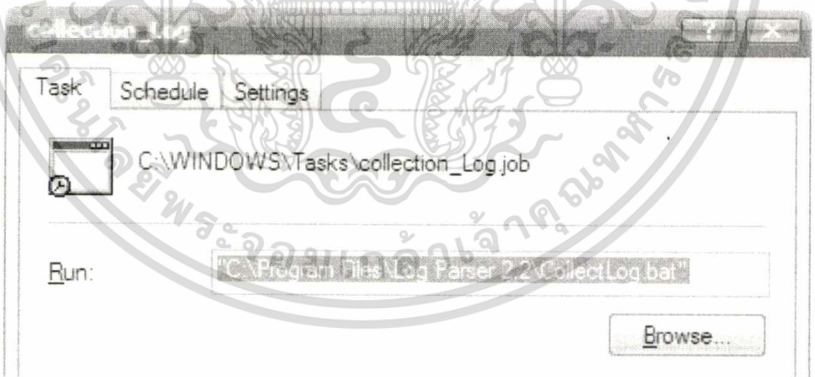
การทำงานของระบบ Computer Traffic Data Management System แบ่งออกเป็น 2 ส่วน คือ

4.3.1 ฟังก์ชันการเก็บรวบรวมข้อมูลจราจร

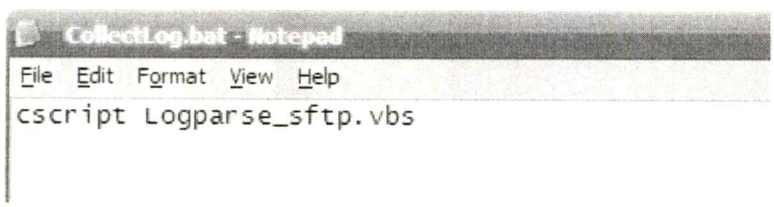
ในระบบจะตั้ง Scheduled Task (Colection_Log.job) ที่เครื่อง Centralized Log Server ให้ระบบทำการ Run Batch file (CollectLog.bat) ณ เวลา 0.30 น. ของทุกวัน เพื่อเก็บรวบรวมข้อมูลจราจรจากเครื่องให้บริการต่างๆ ตามที่ได้กำหนดไว้ในฐานข้อมูล ตาราง Collection Task



รูปที่ 4.2 แสดงการตั้งเวลาการทำงานของการเก็บรวบรวมข้อมูลจราจร



รูปที่ 4.3 แสดงที่อยู่ของ Batch file สำหรับ Schedule Task ที่ตั้งไว้



รูปที่ 4.4 แสดงคำสั่งภายในไฟล์ CollectLog.bat ที่ใช้ประมวลผล VBScript

การทำงานของการโอนถ่ายข้อมูลนั้น เครื่องให้บริการนั้นๆ จะต้องทำการเปิดบริการ SFTP นั่นคือ ต้องจำลองเครื่องเป็น SFTP Serverไว้ด้วย โดยการติดตั้งโปรแกรม OpenSSH และเครื่อง Centralize Log Server จะต้องทำการเปิดบริการ SFTP เช่นกัน นั่นคือต้องจำลองเครื่องเป็น SFTP Client โดยการติดตั้งโปรแกรม WinSCP

```
'build input file for ftp command
sFTPScript = sFTPScript & "option batch on" & vbCRLF
sFTPScript = sFTPScript & "option confirm off"& vbCrLf
sFTPScript = sFTPScript & "option transfer binary" & vbCrLf
sFTPScript = sFTPScript & "open sftp://" & sUsername & ":" & sPassword & "@" & sSite & vbCrLf
sFTPScript = sFTPScript & "dir " &   vbCrLf
sFTPScript = sFTPScript & "cd " & sRemotePath & vbCrLf
sFTPScript = sFTPScript & "dir " &   vbCrLf
sFTPScript = sFTPScript & "get " & sRemoteFile & vbCRLF
sFTPScript = sFTPScript & "close" & vbCrLf
sFTPScript = sFTPScript & "exit" & vbCrLf


sFTPTemp = oFTPScriptShell.ExpandEnvironmentStrings("%TEMP%")
sFTPTempFile = sFTPTemp & "\" & oFTPScriptFSO.GetTempName

sFTPResults = sFTPTemp & "\" & oFTPScriptFSO.GetTempName

'Write the input file for the ftp command
'to a temporary file.
Set oFTPScript = oFTPScriptFSO.CreateTextFile(sFTPTempFile, True)
oFTPScript.WriteLine(sFTPScript)
oFTPScript.Close
Set oFTPScript = Nothing

sCmd2 = """C:\Program Files\WinSCP\WinSCP.com"" /script=" & sFTPTempFile

sout2 =  oFTPScriptShell.run (sCmd2, 3, true)
Wscript.Echo sout2
```

รูปที่ 4.5 แสดง VBScript ที่ใช้ในการถ่ายโอนข้อมูลจราจรผ่าน SFTP

เมื่อระบบทำการเก็บรวบรวมข้อมูลจราจรจากเครื่องให้บริการต่างๆ มาไว้ที่เครื่อง Centralized Log Server แล้ว ระบบก็จะทำการนำข้อมูลจราจรดังกล่าวจัดเก็บลงในระบบฐานข้อมูล โดยใช้โปรแกรม Log Parser เพื่อใช้ในการสืบค้นข้อมูลโดยเวบแอพพลิเคชั่นต่อไป

```
'***************************** import ProxyLog to DB ********************
sub importProxyLogToDB (pathname)

    logTable = "proxylog"

    Set WshShell = Wscript.CreateObject("Wscript.Shell")
    str1 = "C:\Program Files\Log Parser 2.2\LogParser.exe"
    str2 = """select * INTO "& logTable &" from " & Pathname
    str3 = """ -i:iisw3c -o:SQL -server:Logserver -database:logDB "&_
           "-driver:""SQL Server"" -createTable: Off -e:0"
    str4 = str1 & " " & str2 & str3

    Wscript.Echo(str4)

    Set oExec = WshShell.exec(str4)
    WScript.Echo(oExec.StdOut.ReadAll)

End sub
```

รูปที่ 4.6 แสดง VBScript ที่ใช้ในจัดเก็บข้อมูล Proxy Log ลงในระบบฐานข้อมูล

4.3.2 ฟังก์ชันในส่วนของเวบเบสแอพพลิเคชั่น

เพื่อช่วยให้ผู้ใช้งานสามารถทำการสืบค้นข้อมูลจราจรทางคอมพิวเตอร์ตามความต้องการนั้น ระบบจึงได้พัฒนาฟังก์ชันในส่วนของเวบเบสแอพพลิเคชั่น ดังต่อไปนี้

4.3.2.1 ฟังก์ชันการแปลงรูปแบบข้อมูลในฐานข้อมูล

เป็นฟังก์ชันในการแปลงรูปแบบของข้อมูลจราจรจากระบบฐานข้อมูลที่ได้จัดเก็บโดยใช้โปรแกรม Logparser ให้อยู่ในรูปแบบเดียวกันและสามารถนำมาใช้สืบค้นข้อมูลจราจรได้ โดยข้อมูลที่ต้องทำการแปลงรูปแบบ มีดังต่อไปนี้

- เนื้อหาของข้อมูลจราจรที่จัดเก็บในแต่ละรูปแบบมีความแตกต่างกัน ดังนั้นจึงต้องทำการแปลงรูปแบบของข้อมูล และจัดเก็บข้อมูลจราจรประเภทเดียวกันไว้ในตารางเดียวกันเพื่อง่ายต่อการสืบค้นข้อมูล

  ตัวอย่างเช่น FTP Log รูปแบบ IIS และ FTP Log รูปแบบ W3C ต้องมีการรวมเป็นข้อมูลสำหรับ FTP Log เป็นต้น

- ข้อมูลวันเวลาที่ใช้บริการ เนื่องจากเมื่อโปรแกรม LogParser นำข้อมูลเข้าสู่ฐานข้อมูลนั้น การจัดเก็บวันและเวลาจะเก็บแยกกัน แต่ในระบบฐานข้อมูล SQL Server 2005 นั้นจะกำหนด DataType เป็น Datetime ทำให้ต้องมีการแปลงรูปแบบของข้อมูลจราจรให้วันและเวลามาเก็บอยู่ใน Field เดียวกัน

- เวลาที่ของข้อมูลจราจรจาก ISA Server นั้น จะจัดเก็บในรูปแบบของ UTC ทำให้เวลาที่บันทึกลงล็อกไฟล์นั้น ไม่ตรงกับเวลาที่ใช้งานจริง

2009-05-03	12:42:36	w3proxy	ISA	- runonce.msn.com
2009-05-03	12:42:36	w3proxy	ISA	- runonce.msn.com
2009-05-03	12:43:54	w3proxy	ISA	- 192.168.1.4
2009-05-03	12:43:56	w3proxy	ISA	- 192.168.1.4
2009-05-03	12:43:58	w3proxy	ISA	- 192.168.1.4
2009-05-03	12:44:02	w3proxy	ISA	- 192.168.1.4
2009-05-03	12:44:04	w3proxy	ISA	- 192.168.1.4
2009-05-03	12:44:04	w3proxy	ISA	- 192.168.1.4

รูปที่ 4.7 ตัวอย่างข้อมูลวันและเวลาของ Proxy Log ที่สร้างโดยโปรแกรม ISA Server 2004

cip	cs_username	c_agent	sc_authenticated	actiondate
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:42:36
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:42:36
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:43:54
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:43:56
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:43:58
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:44:02
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:44:04
192.168.10.104	thanawas	Mozilla/4.0 (com...	Y	3/5/2552 7:44:04

รูปที่ 4.8 ตัวอย่างข้อมูลวันและเวลาจาก Proxy Log ลงสู่ฐานข้อมูล

จากรูปที่ 4.7 และ รูปที่ 4.8 จะเห็นว่าต้องมีการแปลงรูปแบบข้อมูลของ Proxy Log 2 ส่วน ด้วยกัน คือ

1) การจัดเก็บวันและเวลาจะเก็บแยกกัน แต่ในระบบฐานข้อมูล SQL Server 2005 นั้น จะกำหนด DataType เป็น Datetime จึงต้องรวม Date และ Time ให้อยู่ในฟิลด์เดียวกัน
2) เวลาของข้อมูลจราจรที่บันทึกจาก ISA Server นั้น จะเร็วกว่าเวลาปัจจุบันอยู่ 5 ชั่วโมง ดังนั้น เมื่อนำเข้าสู่ฐานข้อมูลจึงต้องทำการแปลงเวลาให้ตรงกับเวลาที่ใช้บริการจริง

- เนื้อหาของข้อมูลจราจรการรับส่งจดหมายอิเล็กทรอนิกส์ในแต่ละครั้ง อยู่ในรูปแบบที่ยากต่อการเข้าใจ อีกทั้งยังมีข้อมูล SMTP Log และ POP3 Log ปะปนกันอยู่ ดังรูปที่ 4.9 ทำให้ต้องมีการอ่านข้อมูลจากฐานข้อมูลแล้วเก็บข้อมูล Log ทั้ง 2 ประเภทนี้แยกตารางกัน

```
20090501170315656 - 11   - Connection opened from 192.168.10.104
20090501170315656 - 3    - ************Starting POP3 session************
20090501170315656 - 3    - Server: +OK Majodio POP3 mail
20090501170315656 - 3    - Client: USER thanawas@project.com
20090501170315656 - 3    - Server: +OK Welcome thanawas, password required
20090501170315656 - 3    - Client: PASS R@inny_fon
20090501170315656 - 3    - Server: +OK Mailbox locked and ready
20090501170315656 - 3    - Client: STAT
20090501170315656 - 3    - Server: +OK 0 0
20090501170315656 - 3    - Client: QUIT
20090501170315656 - 3    - Server: +OK Majodio POP3 signing off
20090501170315656 - 3    - ************Ending POP3 session************
20090501170645765 - 7    - Connection opened from 192.168.10.104
20090501170645765 - 13   - ************Starting SMTP session************
20090501170645765 - 13   - Server: 220 mail Majodio ESMTP Version 1.2.49.0 Service Ready
20090501170645765 - 13   - Client: HELO client
20090501170645765 - 13   - Server: 250 Hello  Welcome to the Majodio ESMTP Server
20090501170645765 - 13   - Client: MAIL FROM: <thanawas@project.com>
20090501170645765 - 13   - Server: 250 ok
20090501170645781 - 13   - Client: RCPT TO: <nawakit@project.com>
```

รูปที่ 4.9 ตัวอย่างข้อมูล Mail Log ที่มี SMTP Log และ POP3 Log รวมกัน

โดยระบบจัดการข้อมูลจราจรจะทำการแปลงข้อมูลให้แยกออกมาเป็น 2 ตาราง ได้แก่ ตาราง POP3_Log และ ตาราง SMTP_Log

POP3ID	MsgID	User	IPAddress	DataDate
1067	<000701c9c83e...	exuser1@exter...	192.168.1.103	1/5/2552 15:22:53
1068		exuser2@exter...	192.168.1.103	1/5/2552 15:22:53
1069		nawakit@projec...	192.168.10.104	1/5/2552 17:03:15
1070		thanawas@proj...	192.168.10.104	1/5/2552 17:03:15
1071	<001601c9ca48...	nawakit@projec...	192.168.10.104	1/5/2552 17:07:30
1072		thanawas@proj...	192.168.10.104	1/5/2552 17:07:30
1073		nawakit@projec...	192.168.10.104	1/5/2552 17:07:40

รูปที่ 4.10 แสดงข้อมูล POP3 Log ที่จัดเก็บลงฐานข้อมูล

4.3.2.2 ฟังก์ชัน Set Collection Task

เป็นฟังก์ชันการทำงานสำหรับผู้ดูแลระบบ ทำหน้าที่ในการกำหนดการนำข้อมูลล็อกไฟล์เข้าสู่ฐานข้อมูลของระบบ โดยการระบุ IP Address , ชื่อโฟลเดอร์ และประเภทของล็อกไฟล์ เช่น FTP , Proxy , Mail เป็นต้น จากนั้นระบบจะทำการนำข้อมูลจากเครื่องเซิร์ฟเวอร์นั้นๆ เข้าสู่ฐานข้อมูลในเวลา 00.30 น. ของทุกวัน

4.3.2.3 ฟังก์ชัน Task History

ทำหน้าที่ในการแสดงข้อมูลล็อกไฟล์ ที่มีการนำข้อมูลเข้าสู่ฐานข้อมูลเป็นที่เรียบร้อย เพื่อใช้ในการตรวจสอบย้อนหลังได้ว่าข้อมูลล็อกได้เก็บบันทึกลงสู่ฐานข้อมูลตามเวลา 00.30 น. ของทุกวันครบถ้วนหรือไม่

4.3.2.4 ฟังก์ชัน Search Traffic Log

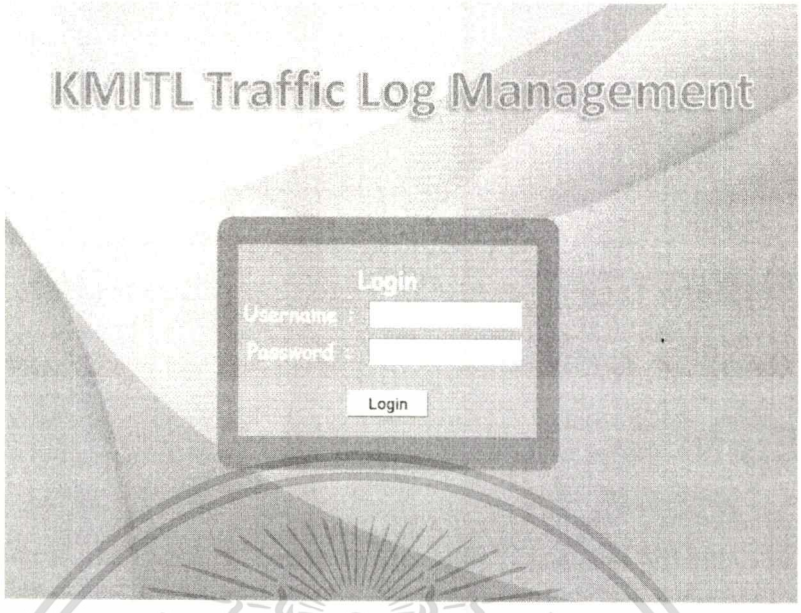
ทำหน้าที่ในการค้นหาข้อมูลจราจรแต่ละประเภทตามเงื่อนไขที่กำหนด เพื่อช่วยให้ผู้ดูแลระบบง่ายต่อการสืบค้นข้อมูล โดยประเภทของข้อมูลจราจรที่สามารถค้นหาได้มี 5 ประเภท คือ

- ข้อมูลจราจรจากการเข้าใช้งานอินเทอร์เน็ต (Proxy Log)
- ข้อมูลจราจรการถ่ายโอนไฟล์ข้อมูล (FTP Log)
- ข้อมูลจราจรการรับส่งจดหมายอิเล็อกทรอนิกส์ (SMTP Log)
- ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ (POP3 Log)
- ข้อมูลจราจรการเยี่ยมชมเว็บไซต์ (Web Log)

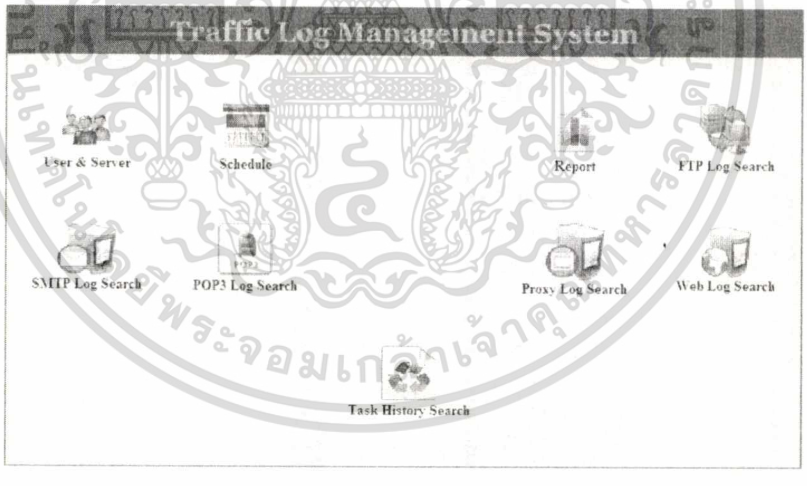
4.3.2.5 ฟังก์ชัน Report Summary

ทำหน้าที่ออกรายงานสรุปผลปริมาณการใช้บริการต่างๆ เพื่อช่วยให้ผู้ดูแลระบบสามารถนำไปวิเคราะห์ข้อมูลการใช้งานต่อไปได้ โดยจะต้องทำการกำหนดวันเริ่มต้นและวันสิ้นสุดของล็อกไฟล์ที่ต้องการ และเลือกว่าต้องการจะแสดงข้อมูลตามผู้ใช้งาน หรือ IP Address ที่มีการใช้งาน

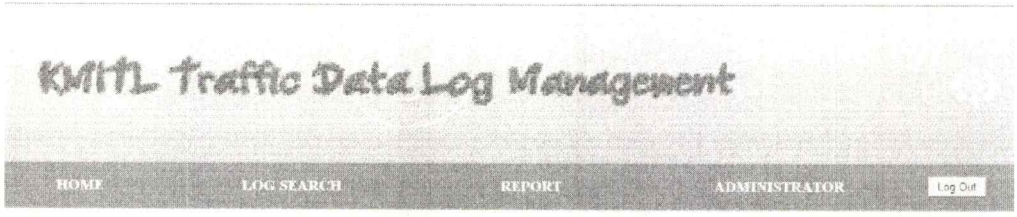
4.4. การใช้งานระบบ Computer Traffic Data Management System



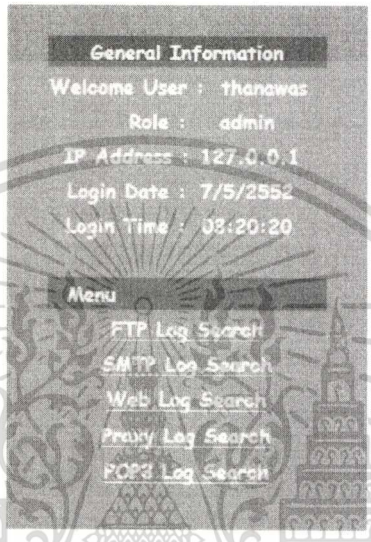
รูปที่ 4.11 แสดงหน้าจอล็อกอินของระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์



รูปที่ 4.12 แสดงหน้าจอหลักของระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์



รูปที่ 4.13 แสดงเมนูหลักของระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์



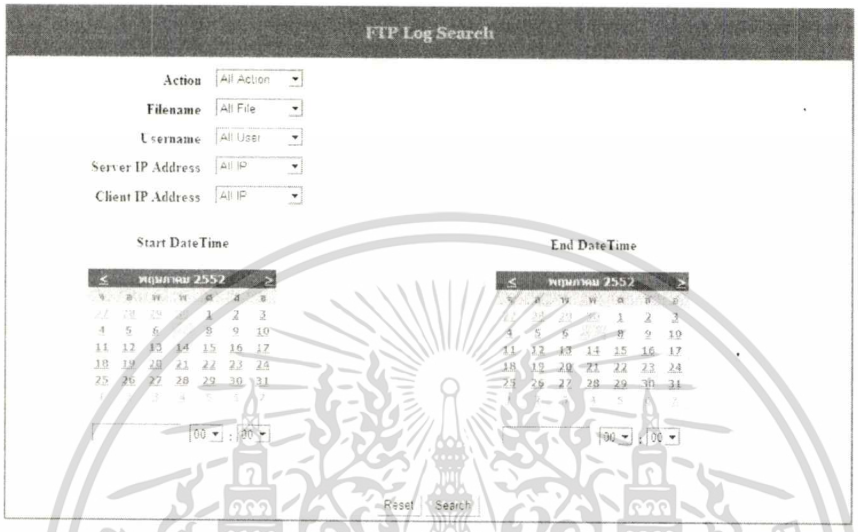
รูปที่ 4.14 ส่วนแสดงข้อมูลผู้เข้าใช้งานระบบและเมนูสำหรับค้นหาข้อมูลจราจรต่างๆ

รูปที่ 4.15 แสดงเมนูสำหรับผู้ดูแลระบบ

จากรูปที่ 4.13 แสดงเมนูหลักของระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์ แบ่งออกเป็น

1) **Home** เป็นเมนูสำหรับไปยังหน้าจอหลักของระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์ ตามรูปที่ 4.12

2) **Log Search** เป็นเมนูสำหรับการสืบหาข้อมูลจราจรประเภทต่างๆ ได้แก่ FTP Log Search ตามรูปที่ 4.14



รูปที่ 4.16 แสดงหน้าจอสำหรับสืบค้นข้อมูล FTP Log

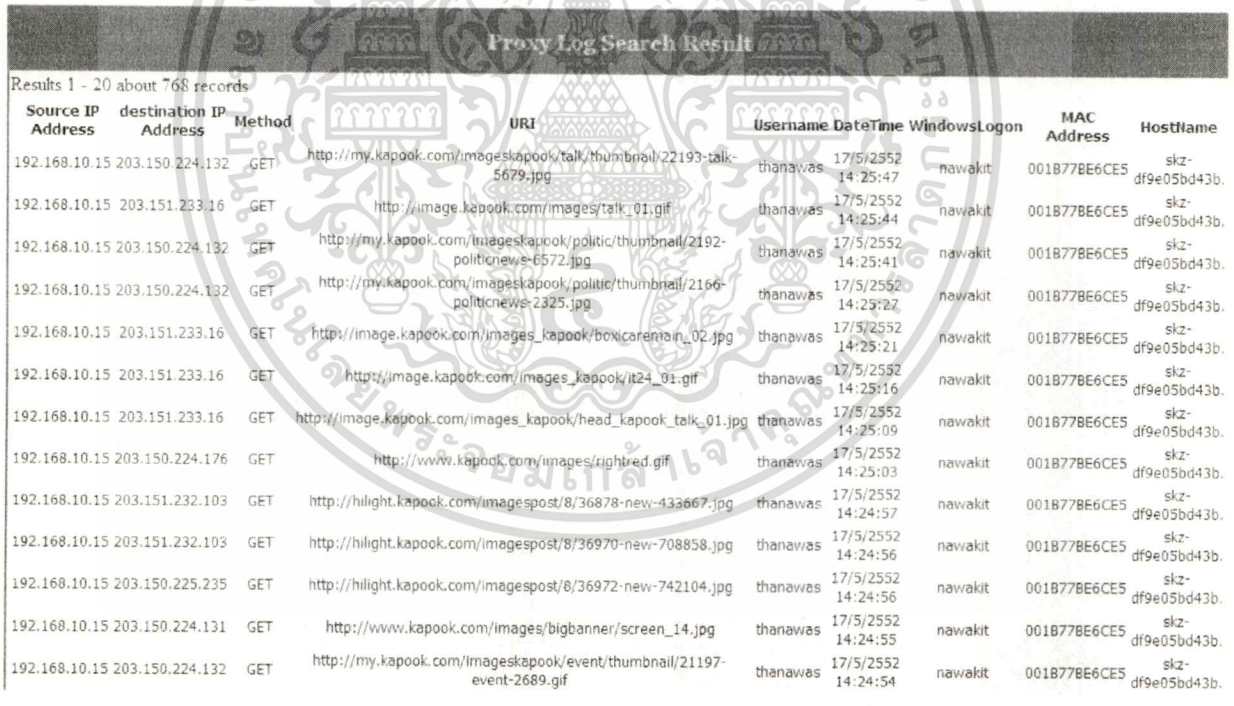
FTP Log Search Result

Results 1 - 20 about 50 records

UserIP	UserName	TransferDate	ServerName	ServerIP	BytesSent	BytesReceived	Method	Target	WindowsLogon	MAC Address	HostName
192.168.10.15	thanawas	17/5/2552 16:53:20	INSERVER1	192.168.2.3	2390	0	Download	/in090211.log	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	thanawas	17/5/2552 16:53:17	INSERVER1	192.168.2.3	0	0	[4] created	/3.txt	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	thanawas	17/5/2552 16:53:12	INSERVER1	192.168.2.3	128	0	Download	/in090509.log	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:56:38	INSERVER1	192.168.2.4	27	0	[8] created	/multi_sendfile/Copy (2) of ftpsite1.txt	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:56:25	INSERVER1	192.168.2.4	244	0	[8] created	/multi_sendfile/sqmnoopt11.sqm	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:56:08	INSERVER1	192.168.2.4	0	0	[8] created	111.txt	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:56:02	INSERVER1	192.168.2.4	0	268	Download	/multi_sendfile/sqmdata00.sqm	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:55:50	INSERVER1	192.168.2.4	0	0	[8] created	/multi_sendfile/2.txt	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:55:46	INSERVER1	192.168.2.4	0	0	[8] created	/multi_sendfile/test-multisend.txt	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	nawakit	17/5/2552 23:55:41	INSERVER1	192.168.2.4	0	1016	Download	/multi_sendfile/111.txt	thanawas	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	thanawas	17/5/2552 23:55:19	INSERVER1	192.168.2.4	745	0	[6] created	/test/in090506.log	thanawas	001B77BE6CE5	skz-df9e05bd43b.

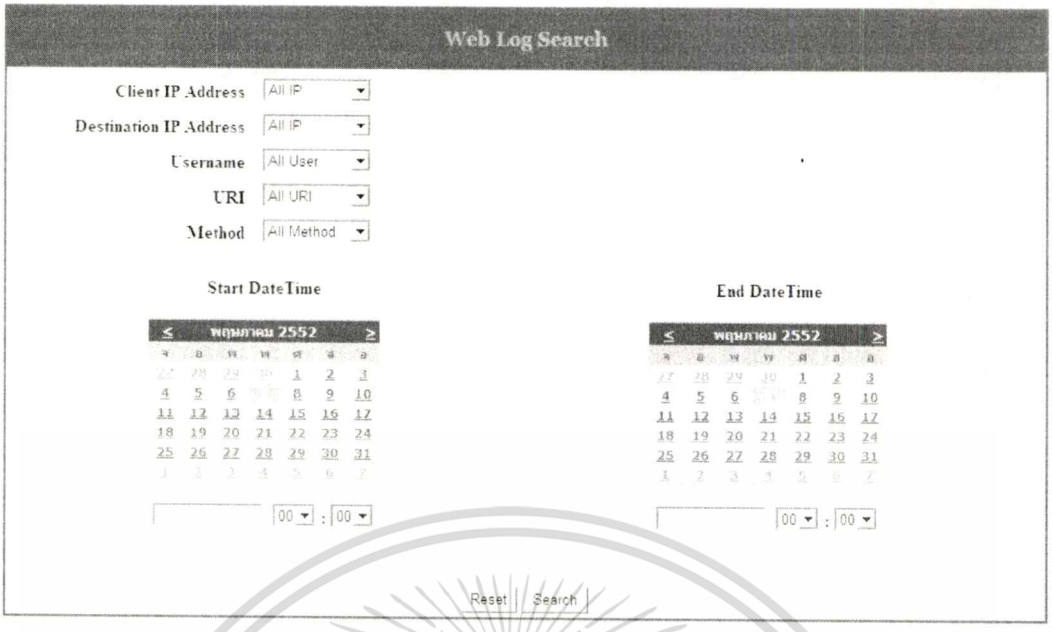
รูปที่ 4.17 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล FTP Log

รูปที่ 4.18 แสดงหน้าจอสำหรับสืบค้นข้อมูล Proxy Log



Source IP Address	destination IP Address	Method	URI	Username	DateTime	WindowsLogon	MAC Address	HostName
192.168.10.15	203.150.224.132	GET	http://my.kapook.com/imageskapook/talk/thumbnail/22193-talk-5679.jpg	thanawas	17/5/2552 14:25:47	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.233.16	GET	http://image.kapook.com/images/talk_01.gif	thanawas	17/5/2552 14:25:44	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.224.132	GET	http://my.kapook.com/imageskapook/politic/thumbnail/2192-politicnews-6572.jpg	thanawas	17/5/2552 14:25:41	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.224.132	GET	http://my.kapook.com/imageskapook/politic/thumbnail/2166-politicnews-2325.jpg	thanawas	17/5/2552 14:25:27	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.233.16	GET	http://image.kapook.com/images_kapook/boxicaremain_02.jpg	thanawas	17/5/2552 14:25:21	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.233.16	GET	http://image.kapook.com/images_kapook/it24_01.gif	thanawas	17/5/2552 14:25:16	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.233.16	GET	http://image.kapook.com/images_kapook/head_kapook_talk_01.jpg	thanawas	17/5/2552 14:25:09	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.224.176	GET	http://www.kapook.com/images/rightred.gif	thanawas	17/5/2552 14:25:03	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.232.103	GET	http://hilight.kapook.com/imagespost/8/36878-new-433667.jpg	thanawas	17/5/2552 14:24:57	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.151.232.103	GET	http://hilight.kapook.com/imagespost/8/36970-new-708858.jpg	thanawas	17/5/2552 14:24:56	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.225.235	GET	http://hilight.kapook.com/imagespost/8/36972-new-742104.jpg	thanawas	17/5/2552 14:24:56	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.224.131	GET	http://www.kapook.com/images/bigbanner/screen_14.jpg	thanawas	17/5/2552 14:24:55	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	203.150.224.132	GET	http://my.kapook.com/imageskapook/event/thumbnail/21197-event-2689.gif	thanawas	17/5/2552 14:24:54	nawakit	001B77BE6CE5	skz-df9e05bd43b.

รูปที่ 4.19 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล Proxy Log



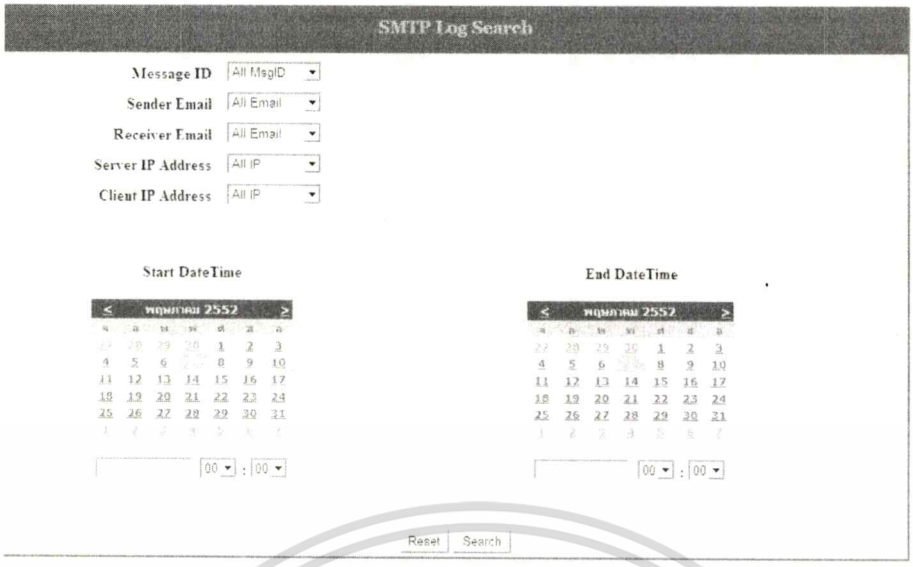
รูปที่ 4.20 แสดงหน้าจอสำหรับสืบค้นข้อมูล Web Log

Web Log Search Result

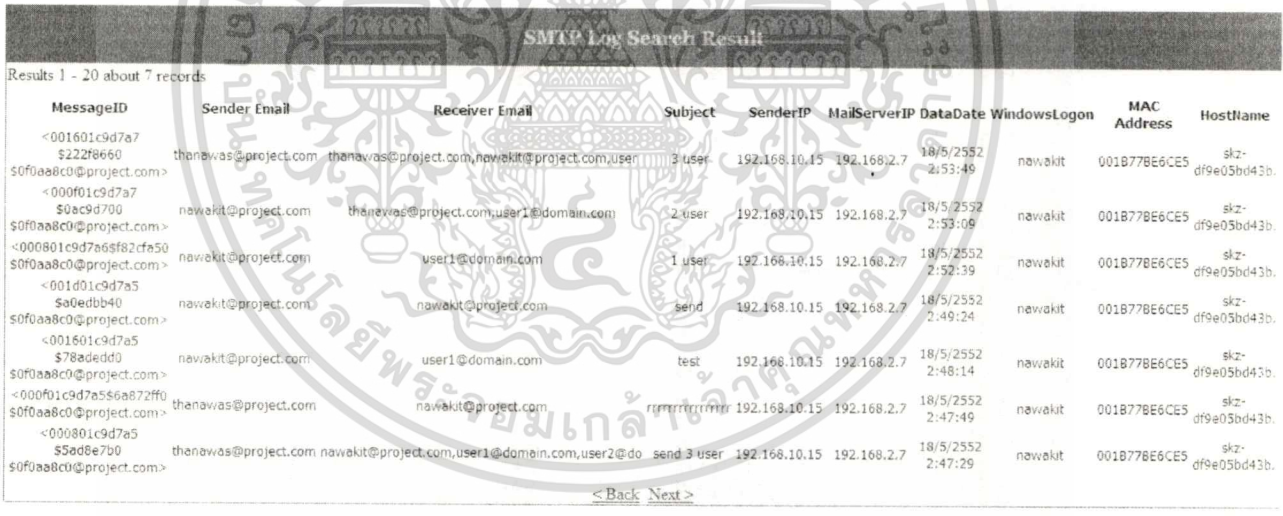
Results 1 - 20 about 560 records

Source IP Address	destination IP Address	Method	URI	Username	DateTime	WindowsLogon	MAC Address	HostName
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/diary/Pets-1/Pets-1/images/spacer.gif	nawakit	17/5/2552 14:51:51	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/diary/images/TT.gif	nawakit	17/5/2552 14:51:50	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/diary/	nawakit	17/5/2552 14:51:50	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/diary	nawakit	17/5/2552 14:51:50	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/21672-guide-3629.gif	thanawas	17/5/2552 14:29:56	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/msn_display06.gif	thanawas	17/5/2552 14:29:55	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/new.gif	thanawas	17/5/2552 14:29:55	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/images/dara_07.gif	thanawas	17/5/2552 14:29:54	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/21752-talk-1417.jpg	thanawas	17/5/2552 14:29:53	nawakit	001B77BE6CE5	skz-df9e05bd43b.
192.168.10.15	192.168.2.6	GET	http://192.168.2.6/kapook/186-kapookpr-4895.jpg	thanawas	17/5/2552 14:29:53	nawakit	001B77BE6CE5	skz-df9e05bd43b.

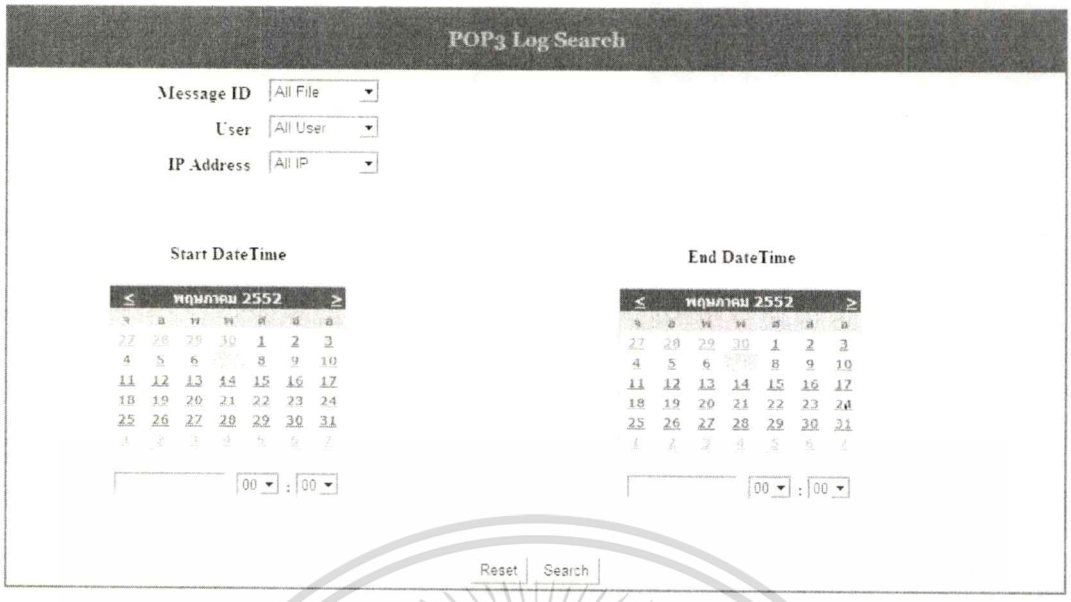
รูปที่ 4.21 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล Web Log



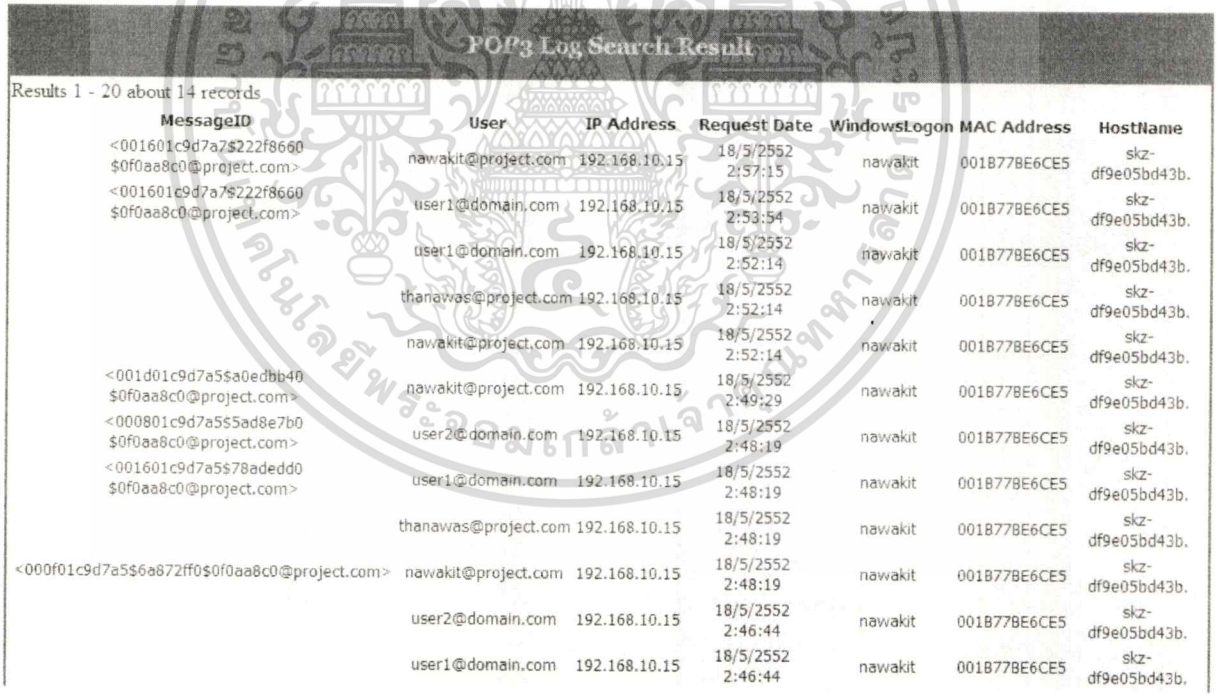
รูปที่ 4.22 แสดงหน้าจอสำหรับสืบค้นข้อมูล SMTP Log



รูปที่ 4.23 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล SMTP Log



รูปที่ 4.24 แสดงหน้าจอสำหรับสืบค้นข้อมูล POP3 Log



MessageID	User	IP Address	Request Date	WindowsLogon	MAC Address	HostName
<001601c9d7a7$222f8660 $0f0aa8c0@project.com>	nawakit@project.com	192.168.10.15	18/5/2552 2:57:15	nawakit	001B77BE6CE5	skz-df9e05bd43b.
<001601c9d7a7$222f8660 $0f0aa8c0@project.com>	user1@domain.com	192.168.10.15	18/5/2552 2:53:54	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	user1@domain.com	192.168.10.15	18/5/2552 2:52:14	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	thanawas@project.com	192.168.10.15	18/5/2552 2:52:14	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	nawakit@project.com	192.168.10.15	18/5/2552 2:52:14	nawakit	001B77BE6CE5	skz-df9e05bd43b.
<001d01c9d7a5$a0edbb40 $0f0aa8c0@project.com>	nawakit@project.com	192.168.10.15	18/5/2552 2:49:29	nawakit	001B77BE6CE5	skz-df9e05bd43b.
<000801c9d7a5$5ad8e7b0 $0f0aa8c0@project.com>	user2@domain.com	192.168.10.15	18/5/2552 2:48:19	nawakit	001B77BE6CE5	skz-df9e05bd43b.
<001601c9d7a5$78adedd0 $0f0aa8c0@project.com>	user1@domain.com	192.168.10.15	18/5/2552 2:48:19	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	thanawas@project.com	192.168.10.15	18/5/2552 2:48:19	nawakit	001B77BE6CE5	skz-df9e05bd43b.
<000f01c9d7a5$6a872ff0$0f0aa8c0@project.com>	nawakit@project.com	192.168.10.15	18/5/2552 2:48:19	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	user2@domain.com	192.168.10.15	18/5/2552 2:46:44	nawakit	001B77BE6CE5	skz-df9e05bd43b.
	user1@domain.com	192.168.10.15	18/5/2552 2:46:44	nawakit	001B77BE6CE5	skz-df9e05bd43b.

รูปที่ 4.25 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล POP3 Log

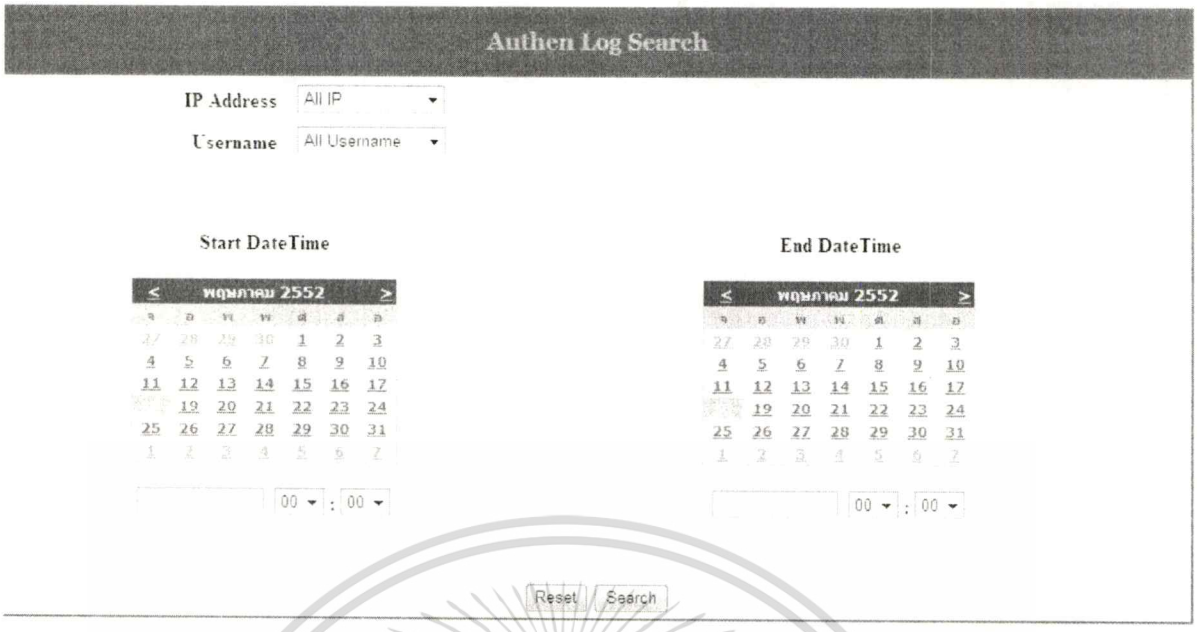
รูปที่ 4.26 แสดงหน้าจอสำหรับสืบค้นข้อมูล DHCP Log

DHCP Log Search Result

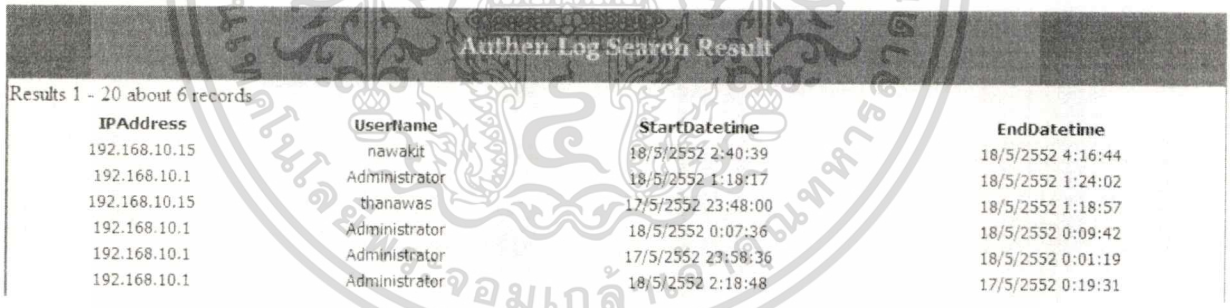
Results 1 - 20 about 20 records

IPAddress	HostName	MACAddress	StartDatetime	EndDatetime
192.168.10.15	ISA.192.168.10.1	52415320000C29796133000009000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.14	ISA.192.168.10.1	52415320000C29796133000008000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.13	ISA.192.168.10.1	52415320000C29796133000007000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.12	ISA.192.168.10.1	52415320000C29796133000006000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.11	ISA.192.168.10.1	52415320000C29796133000005000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.10	ISA.192.168.10.1	52415320000C29796133000004000000	11/5/2552 23:38:26	11/5/2552 23:58:26
192.168.10.5	client.project.com	000C29330FB3	11/5/2552 14:44:00	11/5/2552 17:17:28
192.168.10.16	client.project.com	000C29C0F9A4	10/5/2552 22:11:44	11/5/2552 23:58:39
192.168.10.15	skz-df9e05bd43b.	001B77BE6CE5	10/5/2552 18:18:45	18/5/2552 4:08:22
192.168.10.15			10/5/2552 15:48:42	10/5/2552 15:48:42
192.168.10.9	ISA.192.168.10.1	52415320000C29796133000003000000	10/5/2552 14:49:22	11/5/2552 23:58:26
192.168.10.8	ISA.192.168.10.1	52415320000C29796133000002000000	10/5/2552 14:49:22	11/5/2552 23:58:26
192.168.10.7	ISA.192.168.10.1	52415320000C29796133000001000000	10/5/2552 14:49:22	11/5/2552 23:58:26
192.168.10.6	ISA.192.168.10.1	52415320000C29796133000000000000	10/5/2552 14:49:22	11/5/2552 23:58:26
192.168.10.5	ISA.192.168.10.1	52415320000C29796133000004000000	10/5/2552 14:49:22	10/5/2552 22:56:59
192.168.10.14	ISA.192.168.10.1	52415320000C29796133000009000000	10/5/2552 14:49:22	10/5/2552 22:52:29
192.168.10.13	ISA.192.168.10.1	52415320000C29796133000008000000	10/5/2552 14:49:22	10/5/2552 22:56:29
192.168.10.12	ISA.192.168.10.1	52415320000C29796133000007000000	10/5/2552 14:49:22	10/5/2552 22:56:59
192.168.10.11	ISA.192.168.10.1	52415320000C29796133000006000000	10/5/2552 14:49:22	10/5/2552 22:56:29
192.168.10.10	ISA.192.168.10.1	52415320000C29796133000005000000	10/5/2552 14:49:22	10/5/2552 22:52:59

รูปที่ 4.27 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล DHCP Log



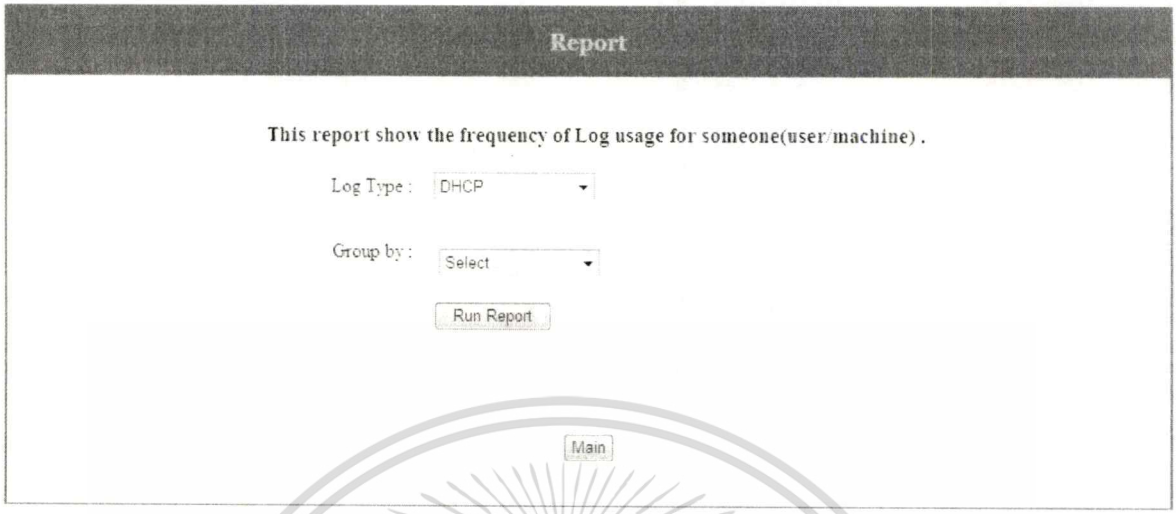
รูปที่ 4.28 แสดงหน้าจอสำหรับสืบค้นข้อมูล Authen Log



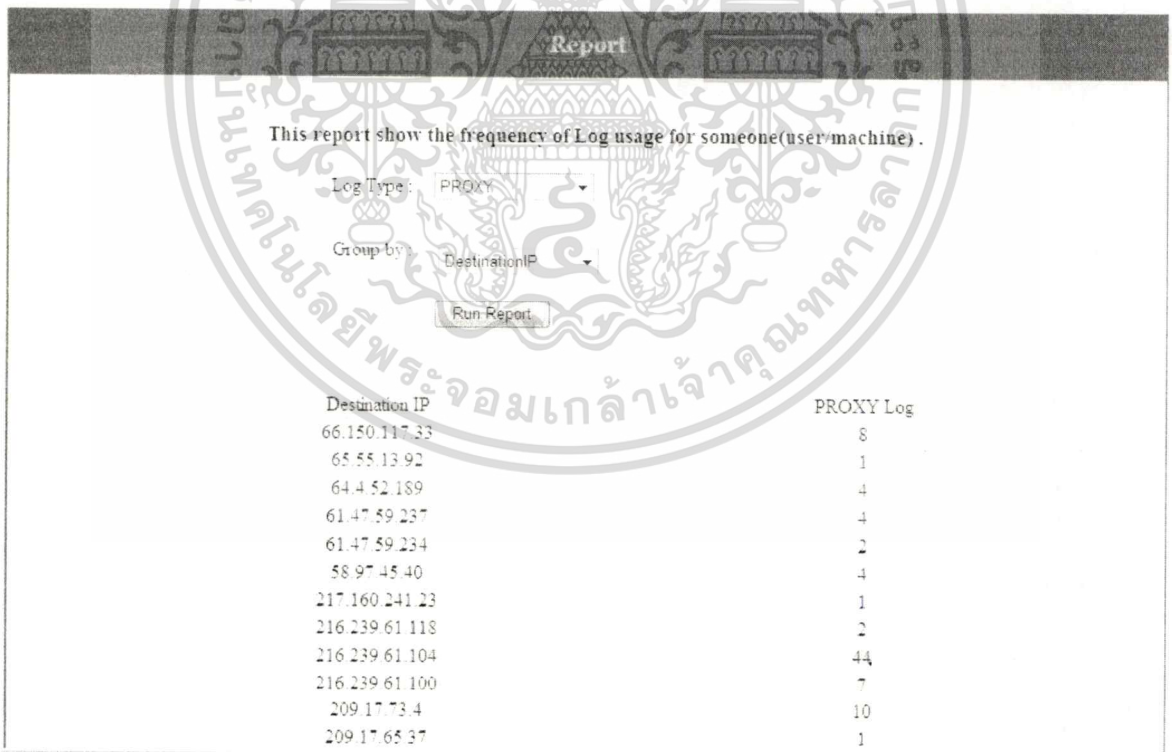
IPAddress	UserName	StartDatetime	EndDatetime
192.168.10.15	nawakit	18/5/2552 2:40:39	18/5/2552 4:16:44
192.168.10.1	Administrator	18/5/2552 1:18:17	18/5/2552 1:24:02
192.168.10.15	thanawas	17/5/2552 23:48:00	18/5/2552 1:18:57
192.168.10.1	Administrator	18/5/2552 0:07:36	18/5/2552 0:09:42
192.168.10.1	Administrator	17/5/2552 23:58:36	18/5/2552 0:01:19
192.168.10.1	Administrator	18/5/2552 2:18:48	17/5/2552 0:19:31

รูปที่ 4.29 แสดงหน้าจอผลลัพธ์ของการสืบค้นข้อมูล Authen Log

3) Report เป็นเมนูสำหรับออกรายงานสรุปผลปริมาณการใช้บริการต่างๆ

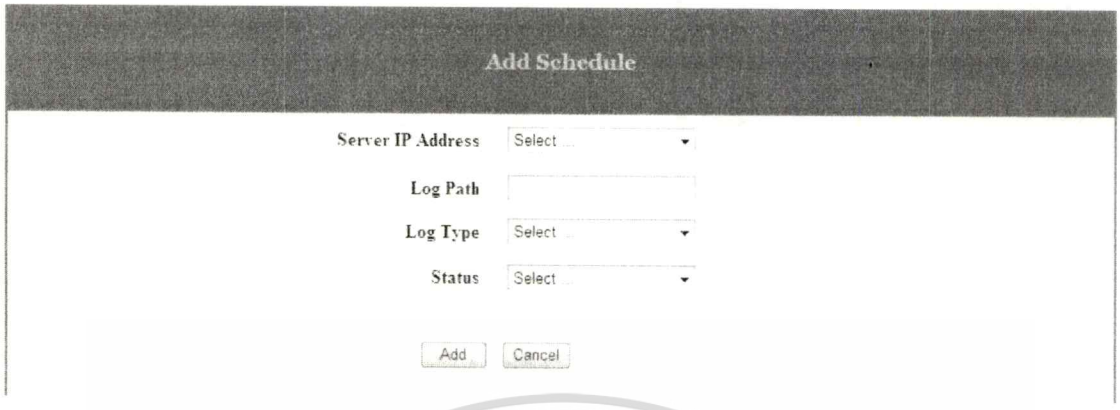


รูปที่ 4.30 แสดงหน้าจอสำหรับออกรายงานตามเงื่อนไขที่ระบุ



รูปที่ 4.31 แสดงหน้าจอผลลัพธ์ของการออกรายงานสรุป

4) Administrator เป็นเมนูสำหรับผู้ดูแลระบบ โดยสามารถทำฟังก์ชันต่างๆ ได้ ดังนี้

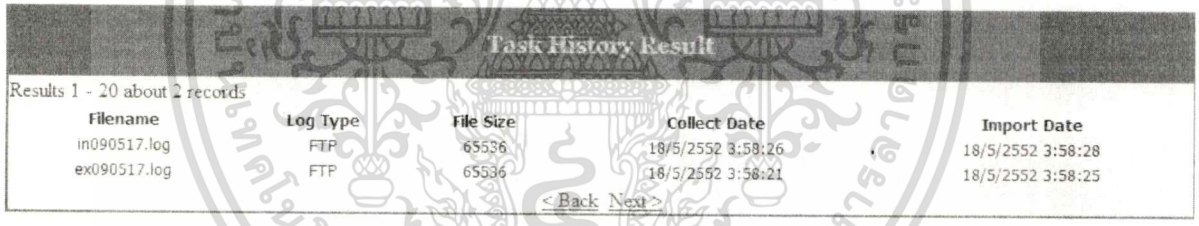


รูปที่ 4.32 แสดงหน้าจอการเพิ่มรายการข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องการจัดเก็บมาไว้ที่ส่วนกลาง(Add Schedule Task)

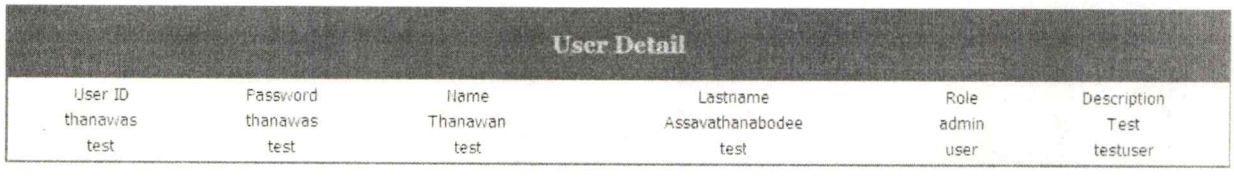
รูปที่ 4.33 แสดงหน้าจอการแสดงรายการข้อมูลจราจรทางคอมพิวเตอร์ที่จะต้องทำการจัดเก็บมาไว้ที่ส่วนกลาง(View Schedule Task)

รูปที่ 4.34 แสดงหน้าจอการแสดงการเปลี่ยนแปลงแก้ไขรายการข้อมูลจราจรทางคอมพิวเตอร์ที่กำหนดให้มีจัดเก็บมาไว้ที่ส่วนกลาง (Edit Schedule Task)

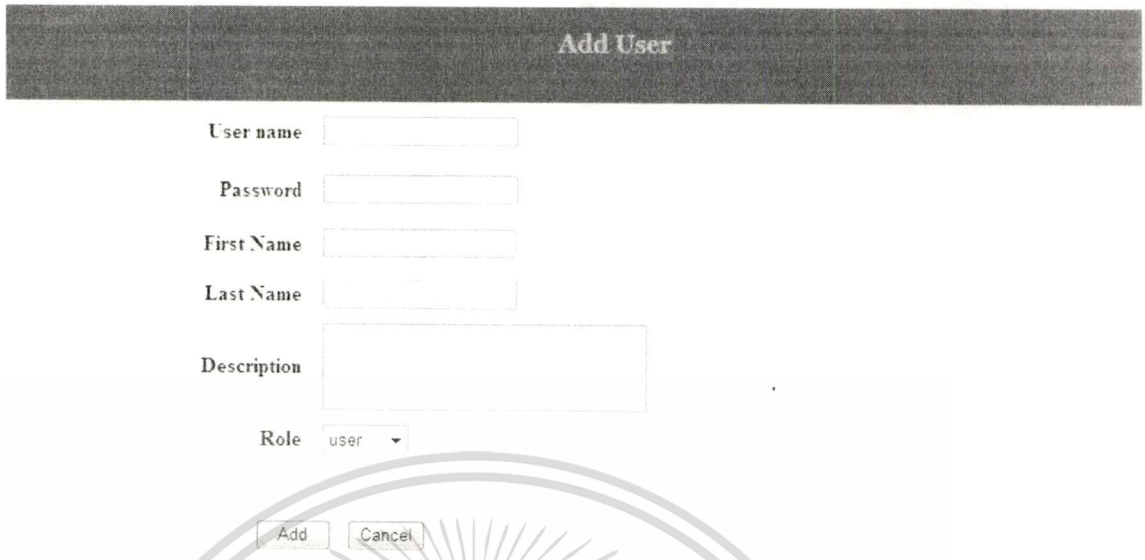
รูปที่ 4.35 แสดงหน้าจอสำหรับสืบค้นการจัดเก็บข้อมูลจราจรลงฐานข้อมูลที่สำเร็จ



รูปที่ 4.36 แสดงหน้าจอผลลัพธ์ของการสืบค้นการจัดเก็บข้อมูลจราจรลงฐานข้อมูลที่สำเร็จ

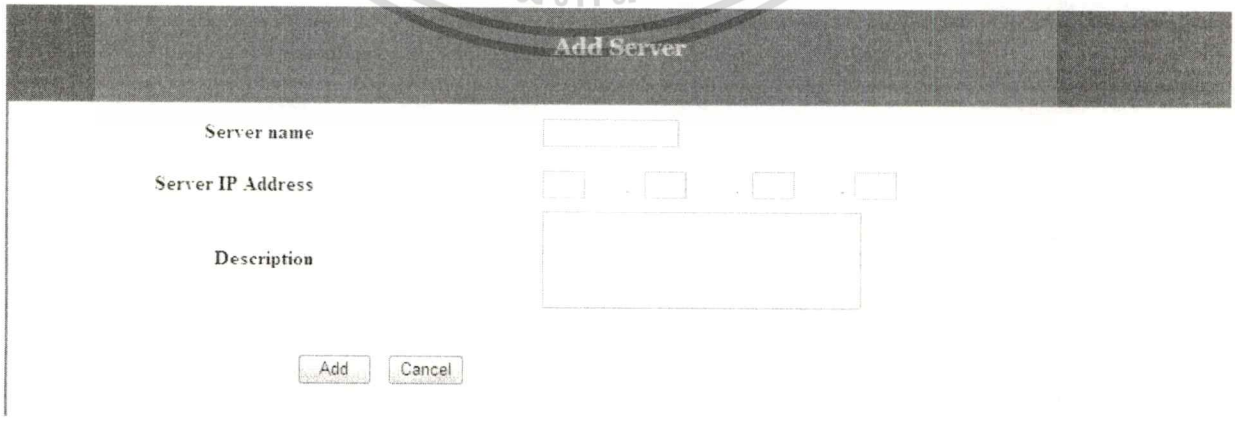


รูปที่ 4.37 แสดงหน้าจอผลลัพธ์ของการเรียกดูผู้ที่มีสิทธิ์เข้าใช้งานระบบได้ (View user)



รูปที่ 4.38 แสดงหน้าจอผลลัพธ์ของการเพิ่มรายชื่อผู้ที่มีสิทธิ์เข้าใช้งานระบบได้ (Add user)

รูปที่ 4.39 แสดงหน้าจอผลลัพธ์ของการเรียกดูข้อมูลเซิร์ฟเวอร์ที่มีอยู่ในองค์กร (View Server)



รูปที่ 4.40 แสดงหน้าจอผลลัพธ์ของการเพิ่มข้อมูลเซิร์ฟเวอร์ที่มีอยู่ในองค์กรได้ (Add Server)

บทที่ 5
สรุปผลโครงการพัฒนาระบบงานและข้อเสนอแนะ

ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data Management System) ถูกพัฒนามาในรูปแบบของเว็บเบสแอพพลิเคชั่น เพื่อช่วยให้การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์สอดคล้องตามที่พระราชบัญญัติได้กำหนดไว้ โดยระบบได้มีการเก็บรวบรวมข้อมูลจราจรจากเครื่องให้บริการต่างๆ ในระบบเครือข่ายมาไว้ที่เครื่องจัดเก็บข้อมูลจราจรแบบรวมศูนย์ รวมถึงทำการจัดเก็บข้อมูลจราจรลงฐานข้อมูล เพื่อตอบสนองต่อความต้องการของผู้ดูแลระบบ ในการสืบค้นและวิเคราะห์เหตุการณ์ที่เกิดขึ้นจากการใช้บริการต่างๆ ภายในองค์กรได้สะดวกและรวดเร็วยิ่งขึ้น

5.1 สรุปผลการพัฒนาระบบงาน

ผลจากการพัฒนาระบบงานนั้น สามารถสรุปได้ดังนี้

5.1.1 ระบบสามารถเก็บรวบรวมข้อมูลจราจรจากเครื่องให้บริการมาเก็บไว้ที่เครื่องจัดเก็บข้อมูลจราจรแบบรวมศูนย์ (Centralized Log Server) โดยใช้วิธีการ SFTP เป็นช่องทางในการเก็บรวบรวม เนื่องจากมีความปลอดภัยในการถ่ายโอนข้อมูล และใช้โปรแกรม LogParser เพื่อช่วยในการนำข้อมูลจราจรที่เก็บรวบรวมมานั้นเข้าสู่ฐานข้อมูล

5.1.2 ผู้ดูแลระบบสามารถทำการสืบค้น (Search) ข้อมูลจราจรผ่านเว็บเบสแอพพลิเคชั่นได้ 5 ประเภท ได้แก่

- ข้อมูลจราจรจากการเข้าใช้งานอินเทอร์เน็ต (Proxy Log)
- ข้อมูลจราจรการถ่ายโอนไฟล์ข้อมูล (FTP Log)
- ข้อมูลจราจรการรับส่งจดหมายอิเล็อกทรอนิกส์ (SMTP Log)
- ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ (POP3 Log)
- ข้อมูลจราจรการเยี่ยมชมเว็บไซต์ (Web Log)

5.1.3 ระบบสามารถออกรายงานสรุปผลปริมาณการใช้บริการต่างๆ ได้ เพื่อช่วยให้ผู้ดูแลระบบสามารถทำการวิเคราะห์ข้อมูลการใช้งานของผู้ใช้งานได้

5.1.4 ระบบสามารถจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรออกเป็น 2 ระดับ คือ

5.1.4.1 ระดับ Admin หมายถึง ผู้ดูแลระบบ Computer Traffic Data Management System สามารถสืบค้นข้อมูลจราจรได้ทั้งหมด รวมทั้งสามารถกำหนดสิทธิ์การใช้งานได้ กำหนดเวลาการนำข้อมูลล็อกไฟล์เข้าสู่ฐานข้อมูล

5.1.4.2 ระดับ User หมายถึง ผู้ใช้งานทั่วไป สามารถสืบค้นข้อมูลจราจรทุกประเภทได้ แต่ไม่สามารถทำการเพิ่มลบรายชื่อผู้เข้าใช้งาน Computer Traffic Data Management System และไม่สามารถกำหนดเวลาการนำข้อมูลล็อกไฟล์เข้าสู่ฐานข้อมูลได้

5.2 ประโยชน์ที่ได้รับ

จากการพัฒนาระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data Management System) สามารถสรุปประโยชน์ที่ได้รับดังนี้ คือ

5.2.1 การค้นหาข้อมูลจราจรมีความสะดวกและรวดเร็ว เนื่องจากมีการจัดเก็บข้อมูลลงในฐานข้อมูล ทำให้การสืบค้นข้อมูลทำได้ง่ายผ่านทางเว็บเบสแอพพลิเคชั่น

5.2.2 ผู้ดูแลระบบสามารถวิเคราะห์ข้อมุลล็อกได้อย่างมีประสิทธิภาพ โดยสามารถทำการวิเคราะห์ความสัมพันธ์ของข้อมูลล็อกที่เกิดขึ้นจากเครื่องแม่ข่ายหลาย ๆ เครื่องได้ เนื่องจากเก็บรวบรวมข้อมูลล็อกที่เครื่องต่างๆ มาไว้ที่ส่วนกลาง

5.2.3 สามารถจัดเก็บข้อมูลสำหรับผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ได้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดไว้

5.3 ข้อจำกัดของระบบ

จากการพัฒนาระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data Management System) สามารถสรุปข้อจำกัดของระบบได้ดังนี้

5.3.1 ระบบรองรับสำหรับผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เท่านั้น

5.3.2 ระบบรองรับข้อมูลจราจรตามรูปแบบของล็อกไฟล์ที่ใช้ในการทดลองเท่านั้น ซึ่งรูปแบบของข้อมูลจราจรขึ้นอยู่กับโปรแกรมที่ใช้ โดยในโครงงานนี้รองรับข้อมูลล็อกไฟล์แต่ละประเภทที่สร้างจากโปรแกรมดังนี้

- FTP Log รองรับข้อมูลล็อกไฟล์ประเภท IIS Log และ W3C Log

- Proxy Log รองรับข้อมูลล็อกไฟล์ประเภท W3C Log จากโปรแกรม Internet Security and Acceleration Server 2004 โดยภายใน Proxy Log นี้จะมีข้อมูลของข้อมูลจราจรการเยี่ยมชมเว็บไซต์ (Web Log) ปะปนอยู่ด้วย
- Mail Log รองรับข้อมูลล็อกไฟล์ที่สร้างจากโปรแกรม Majodio Mail ซึ่งภายในล็อกไฟล์จะประกอบด้วย SMTP Log และ POP3 Log

5.4 ข้อเสนอแนะในการพัฒนาต่อ

จากการพัฒนาระบบจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data Management System) สามารถสรุปแนวทางในการพัฒนาต่อไปได้ดังนี้

5.4.1 พัฒนาให้สามารถรองรับข้อมูลจราจรประเภทอื่นๆ ได้อีก เพื่อให้สามารถวิเคราะห์ข้อมูลได้หลายหลายประเภทมากยิ่งขึ้น

- Security Device เช่น Firewall , VPN
- Network Device เช่น Router , Switch
- Event Log ได้แก่ System Log , Security Log , Application Log

5.4.2 พัฒนาระบบให้สามารถรองรับผู้ให้บริการประเภทอื่นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วย เช่น การพัฒนาระบบสำหรับผู้ให้บริการอินเทอร์เน็ตคาเฟ่ เป็นต้น

5.4.3 พัฒนาให้สามารถรองรับข้อมูลจราจรได้จากหลายหลายแพลตฟอร์ม ได้แก่ Syslog จากระบบปฏิบัติการ Linux

5.4.4 พัฒนาระบบให้สามารถออกรายงานออกมาในรูปแบบของไฟล์ประเภทต่างๆ ได้ เช่น pdf , xls , doc โดยอาจใช้โปรแกรม Crystal Report ในการช่วยสร้างรายงาน

5.4.5 เนื่องจากในโครงงานนี้ได้ทำการกำหนดว่าให้นำข้อมูลเข้าฐานข้อมูล เวลา 00.30 น. ของทุกวัน ดังนั้นควรเพิ่มความสามารถในการกำหนดรอบวันเวลาและความถี่ในการนำข้อมูลล็อกไฟล์จากเครื่องเซิร์ฟเวอร์ต่างๆ เข้าสู่ฐานข้อมูลได้โดยผู้ดูแลระบบเอง ได้แก่

- Daily คือ กำหนดให้มีการนำข้อมูลเข้าทุกวัน
- Weekly คือ กำหนดให้มีการนำข้อมูลเข้าอาทิตย์ละ 1 ครั้ง
- Monthly คือ กำหนดให้มีการนำข้อมูลเข้าเดือนละ 1 ครั้ง

5.4.6 พัฒนาระบบให้สามารถทำการแจ้งเตือนผู้ดูแลระบบผ่าน E-mail ได้ เมื่อข้อมูลจราจรไม่ถูกนำลงฐานข้อมูลตามรอบที่กำหนด

5.4.7 เพิ่มความสามารถของระบบให้สามารถจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรออกเป็น 3 ระดับ คือ

- ระดับ Admin หมายถึง ผู้ดูแลระบบ Computer Traffic Data Management System สามารถสืบค้นข้อมูลจราจรได้ทั้งหมด รวมทั้งสามารถกำหนดสิทธิ์การใช้งานได้ กำหนดเวลาการนำข้อมูลล็อกไฟล์เข้าสู่ฐานข้อมูล
- ระดับ Auditor หมายถึง ผู้ตรวจสอบ โดยจะจำกัดสิทธิ์ให้สามารถสืบค้นข้อมูลจราจรจากทุกเครื่องให้บริการ แต่ไม่สามารถทำการเพิ่มลบรายชื่อผู้เข้าใช้งาน Computer Traffic Data Management System และไม่สามารถกำหนดเวลาการนำข้อมูลล็อกไฟล์เข้าสู่ฐานข้อมูลได้
- ระดับ User หมายถึง ผู้ใช้งานทั่วไป โดยจะจำกัดสิทธิ์ให้สามารถสืบค้นข้อมูลจราจรได้ตามสิทธิ์ที่ผู้ดูแลระบบกำหนดสิทธิ์ให้ตามกลุ่มงานเท่านั้น

บรรณานุกรม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. 2550. **พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.** [Online]. Available: http://www.etcommission.go.th/documents/laws/20070618_CC_Final.pdf

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.2550. **หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 .** [Online].Available: http://www.mict.go.th/home/Download/TrafficData.pdf

ชวลิต ทินกรสูติบุตร . 2547. **คู่มือการใช้บริการ Time Server.** [Online].Available:http://thaicert.nectec.or.th/ paper/basic/ntp_manual.php

บริษัท จีเอเบิล จำกัด. 2551. **การเตรียมความพร้อมระบบ Infrastructure เพื่อรองรับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์** [Online].Available:http://www.ku.ac.th/netday2007/paper / Prepare %20Security%20Network%20Ukrit.pdf

ปริญญา หอมอเนก.2550.**คู่มือวิธีปฏิบัติสำหรับองค์กรตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐.** [Online]. Available :http://giti.nectec.or.th/pomprom/presentation/20071128-cio16/prinya2.pdf

มรกต กุลธรรมโยธิน สมาคมผู้ให้บริการอินเทอร์เน็ตไทย.2550. **ผู้ให้บริการกับพระราชบัญญัติ** .[Online] .Available:www.webmaster.or.th/files/traffic-data-isp-20070724.ppt

เลอศักดิ์ ลิ้มวิวัฒน์กุล และคณะ. 2551. **Log implementation and auditing guideline compliance with Computer Crime Act B.E 2550 (2007).**[Online].Available: www.thaicert.org/paper/auditing/ LogImplementationandAuditingGuideline _r2.pdf

สุรางคณา วายุภาพ .2551. **ข้อควรรู้เกี่ยวกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.2550**.[Online].Available:www.oknet.in.th/autopage/file/TueJuly2008-16-16-42-20080728_CC_ Internet%20Cafe.ppt

ประวัติผู้เขียน

ชื่อผู้เขียน	นางสาวธนวรรณ อัศวธนบดี
วัน เดือน ปีเกิด	17 ตุลาคม 2526
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษาระดับปริญญาตรี	วิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์
สถานที่สำเร็จการศึกษา	มหาวิทยาลัยศิลปากร
ปีที่สำเร็จการศึกษา	2548
ตำแหน่งหน้าที่ปัจจุบัน	Senior Information Technology Auditor
ประเภทธุรกิจสถานที่ทำงาน	Telecommunication / Advance Info Service PCL.