โปรแกรมจัดการล็อกไฟล์

LOG FILE MANAGEMENT SOFTWARE

นายธีระศักดิ์ จิตรัก รหัส 48364760

นายปฏิภาณ สดใส รหัส 48364807

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2551

ใบรับรองโครงงานวิศวกรรม

หัวข้อโครงการ	โปรแกรมจัดการล็อกไฟล์
ผู้ดำเนินโครงงาน	นายธีระศักดิ์ จิตรัก รหัส 48364760
	นายปฏิภาณ สดใส รหัส 48364807
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์ สอนคม
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์
ปีการศึกษา	2551

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้โครงงานฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะกรรมการสอบโครงงานวิศวกรรม

.....ประธานกรรมการ

(อาจารย์ภาณุพงศ์ สอนคม)

.....กรรมการ

(ดร.สุรเดช จิตประไพกุลศาล)

.....กรรมการ

(อาจารย์จิราพร พุกสุข)

หัวข้อโครงงาน	โปรแกรมจัดการล็อกไฟล์			
ผู้ดำเนินโครงงาน	นายธีระศักดิ์	จิตรัก	รหัส	48364760
	นายปฏิภาณ	สดใส	รหัส	48364807
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์ สอนคม			
สาขาวิชา	วิศวกรรมคอมพิวเตอร์			
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์			
ปีการศึกษา	2551			

บทคัดย่อ

โครงงานนี้ได้พัฒนาโปรแกรมเพื่อทำการจัดการล็อกไฟล์ ซึ่งโปรแกรมจะทำงานโดยการรวบรวมข้อมูลจากอีเทอร์เน็ตการ์ดของเซิร์ฟเวอร์ จากนั้นนำมาคัดกรองและคำนวณเพื่อให้ได้ผลที่ต้องการ แล้วนำไปเก็บไว้ในฐานข้อมูล ซึ่งข้อมูลส่วนนี้จะเป็นล็อกไฟล์ที่เกิดจากการเข้าใช้งานเว็บไซต์ ตรงตามที่ "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐" บัญญัติไว้ทุกประการ จากนั้นนำมาวิเคราะห์และสรุปเป็นรายงานในหลากหลายรูปแบบ เช่น ไอพี ช่วงเวลาที่การใช้งาน จำนวนครั้งที่เรียกดู เป็นต้น ซึ่งสามารถนำไปวิเคราะห์เพื่อปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น

Project Title	Log File Management Sotfware	
Name	Mr. Teerasak Jitrak	ID. 48364760
	Mr. Patipan Sodsai	ID. 48364807
Project Advisor	Mr. Panupong Sornkhom	
Major	Computer Engineering.	
Department	Electrical and Computer Engineering.	
Academic Year	2008	

ABSTRACT

This project develops a program to manage log file. The software collects data packet from ethernet card in a computer working server then filtered and process to suitable result. Which is confirm to "Computer-Related Crime Act B.E. 2550" After we get the required result stored in database. Then, we can analyze and generate a report to make it easier understand. The report will display data in several ways. For example IP address, time usage, hits count, etc. Therefore, we can use the analysis result improve system security and efficiency.

กิตติกรรมประกาศ

ขอขอบคุณ อาจารย์ภาณุพงศ์ สอนคม ที่คอยให้คำปรึกษา ความช่วยเหลือตลอดจนคำแนะนำและแนวทางต่างๆ ในการทำโครงงานนี้

ขอขอบคุณอาจารย์ทุกท่าน บิดา มารดา ญาติพี่น้อง เพื่อนๆ และ SH-GROUP ทุกคน ที่คอยให้คำปรึกษาและเป็นกำลังใจที่ดีเสมอมา และสุดท้ายขอขอบคุณผู้ที่มีส่วนช่วยเหลือในการแนะนำติชมและให้กำลังใจ ให้สามารถทำโครงงานนี้จนสำเร็จลุล่วงไปด้วยดี ทุกๆ ท่านมา ณ โอกาสนี้

นายธีระศักดิ์ จิตรัก

นายปฏิภาณ สดใส

สารบัญ

หน้า

บทคัดย่อ ..... ก

ABSTRACT ..... ข

กิตติกรรมประกาศ ..... ค

สารบัญ ..... ง

สารบัญตาราง ..... ฉ

สารบัญรูปภาพ ..... ช

บทที่ 1 บทนำ 1

1.1 ที่มาและความสำคัญของโครงงาน 1

1.2 วัตถุประสงค์ของโครงงาน 1

1.3 ขอบข่ายของโครงงาน 2

1.4 ขั้นตอนของการดำเนินงาน 2

1.5 ผลที่คาดว่าจะได้รับ 2

1.6 งบประมาณของโครงการ 3

บทที่ 2 ทฤษฎีพื้นฐาน 4

2.1 ล็อกไฟล์ (Log File) 4

2.2 เว็บเซิร์ฟเวอร์ (Web Server) 7

2.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ 7

2.4 โปรโตคอลเอชทีทีพี (HTTP : Hyper Text Transfer Protocol) 10

2.5 ระบบฐานข้อมูล (Database System) 17

2.6 ทำความรู้จักกับ C# 19

สารบัญ(ต่อ)

หน้า

บทที่ 3 การออกแบบและพัฒนาระบบ 21

3.1 แนวคิดในการออกแบบ 21

3.2 ความสามารถของโปรแกรม 21

3.3 ภาพรวมของโปรแกรม 22

3.4 รายละเอียดแต่ละส่วนของโปรแกรม 23

3.5 ความต้องการของระบบ (Requirement Specification) 30

3.6 ขอบเขตของระบบ 30

3.7 การออกแบบซอฟต์แวร์ 31

บทที่ 4 ผลการทดลอง 39

4.1 การใช้งานฝั่งเซิร์ฟเวอร์ 39

4.2 การใช้งานฝั่งผู้ดูแลระบบ 40

บทที่ 5 บทสรุป 50

5.1 หน้าที่การทำงานของโปรแกรม 50

5.2 วิเคราะห์ผลการทดลอง 50

5.3 ปัญหาและแนวทางการแก้ไข 50

5.4 แนวทางการพัฒนาต่อ 51

เอกสารอ้างอิง 52

ประวัติผู้เขียนโครงงาน 53

สารบัญตาราง

ตารางที่ หน้า

2.1 แสดงคำสั่งของโปรโตคอล HTTP 17

3.1 แสดงรายละเอียดของตาราง Standard Format 26

3.2 แสดงมุมมองในการออกแบบซอฟต์แวร์ 31

3.3 แสดงรายละเอียดของตารางยูสเคสไดอะแกรมของโปรแกรม 32

สารบัญรูปภาพ

รูปที่ หน้า

2.1 แสดงตัวอย่าง W3C Extended Log Format 5

2.2 แสดงตัวอย่าง IIS log file format 6

2.3 แสดงการร้องขอข้อมูลจากเซิร์ฟเวอร์ 12

2.4 แสดงการให้บริการลูกข่ายจำนวนมาก 12

2.5 แสดงเมสเซจร้องขอ (Request Messages) 13

2.6 แสดงรูปแบบของ Request line 13

2.7 แสดงรูปแบบของ URL 14

2.8 แสดงเมสเซจตอบสนอง (Response Messages) 15

2.9 แสดงรูปแบบของ Status line 15

2.10 แสดงรูปแบบของเฮดเดอร์ 16

2.11 แสดงเฮดเดอร์ของเมสเซจร้องขอ และเมสเซจตอบสนอง 16

3.1 แสดงโครงสร้างโดยรวมของโปรแกรม 22

3.2 แสดงหน้าจอ interface ในส่วนวิเคราะห์แพ็กเก็ตของโปรแกรม 23

3.3 แสดงการเก็บรวบรวมข้อมูล 24

3.4 แสดงเก็บรวบรวมข้อมูลของโปรโตคอล HTTP 25

3.5 แสดงการทำในส่วนสรุปและรายงานผล (Report) 26

3.6 แสดงหน้าจอ interface ในส่วนสรุปและรายงานผล (Report) 28

3.7 แสดงหน้าจอ interface ในส่วนการค้นหา 29

3.8 แสดง Context Diagram ของระบบ ฝั่งเซิร์ฟเวอร์ 30

3.9 แสดง Context Diagram ของระบบ ฝั่งผู้ดูแลระบบ 31

3.10 แสดง Use Cases Diagram 32

3.12 แสดง Sequence Diagram ของโปรแกรมฝั่งผู้ดูแลระบบ 33

3.13 แสดง Component Diagram 34

สารบัญรูปภาพ(ต่อ)

รูปที่	หน้า
3.14 แสดง Activity Diagram ของโปรแกรมฝั่งเซิร์ฟเวอร์	35
3.15 แสดง Activity Diagram ของโปรแกรมฝั่งผู้ดูแลระบบ	36
3.16 แสดง Class Diagram ของ HTTP Analysis	37
3.17 แสดง Class Diagram ของ Log file report	37
4.1 แสดงการเลือกอีเทอร์เน็ตการ์ดของเซิร์ฟเวอร์	39
4.2 แสดงการทำงานของโปรแกรม HTTP Analysis	40
4.3 แสดงหน้า interface ของโปรแกรม Log File Report	41
4.4 แสดงหน้า interface ในส่วนที่ 1	41
4.5 แสดงหน้า interface ในส่วนที่ 2	41
4.6 แสดงหน้า interface ในส่วนที่ 3	42
4.7 แสดงผลการรายงานโดยสรุปประจำเดือน	42
4.8 แสดงผลการรายงานประวัติรายเดือน	43
4.9 แสดงผลการรายงานประวัติรายสัปดาห์	44
4.10 แสดงผลการรายงานผู้เข้าใช้งาน (สูงสุด 10 อันดับ)	45
4.11 แสดงผลการรายงานหน้า (Page) ที่ถูกเรียกใช้งาน (สูงสุด 10 อันดับ)	46
4.12 แสดงผลการรายงานระบบปฏิบัติการ	47
4.13 แสดงผลการรายงานบราวเซอร์	48
4.14 แสดงหน้า interface ส่วนของค้นหา	49
4.15 แสดงผลการค้นหา	49

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของโครงงาน

เนื่องจากในวันที่ ๑๘ กรกฎาคม พ.ศ. ๒๕๕๐ ที่ผ่านมา ประเทศไทยได้มี " พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐" ขึ้นมา เพื่อใช้ปราบปรามผู้ที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์ อีกทั้งปัจจุบันนี้การติดต่อสื่อสารผ่านระบบเครือข่ายได้พัฒนาไปอย่างมากเมื่อเทียบกับไม่กี่ปีที่ผ่านมา ส่งผลให้เครื่องคอมพิวเตอร์ต้องมีการติดตั้งเครื่องให้บริการเครือข่ายมากขึ้น เพื่อรองรับต่อความต้องการ อุปกรณ์ในระบบเครือข่ายเหล่านั้นสิ่งหนึ่งที่ต้องมี คือ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือเรียกว่า ล็อกไฟล์ (log file) ให้เป็นไปตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้กำหนดเอาไว้ ซึ่งสามารถนำไปใช้เป็นพยานหลักฐานที่สำคัญและเป็นประโยชน์อย่างยิ่งต่อการสืบสวนสอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษได้ อีกทั้งยังสามารถรายงานสถิติต่างๆ ที่เป็นประโยชน์มากมายที่องค์กรสามารถนำไปใช้ในการปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น ซึ่งในขนาดของระบบที่ใหญ่ขึ้นมากนั้นการจะวิเคราะห์โดยไม่มีเครื่องมือช่วยก็เป็นไปได้ยาก และตัวล็อกไฟล์เองนั้นก็เข้าใจได้ยากสำหรับผู้ที่ไม่มีความรู้ทางด้านนี้ จึงได้ทำการพัฒนาเครื่องมือที่ใช้ในการจัดการล็อกไฟล์เหล่านี้ขึ้นมา

โปรแกรมนี้จะช่วยให้การจัดการกับล็อกไฟล์นั้นทำได้ง่ายขึ้น โดยทำหน้าที่ในการรวบรวมล็อกไฟล์ของเวปเซิร์ฟเวอร์ ให้เป็นไปตามที่ พ.ร.บ.คอมพิวเตอร์ได้กำหนดเอาไว้ และยังสามารถนำมาคำนวณเพื่อสรุปเป็นรายงานที่ง่ายต่อการวิเคราะห์มากขึ้น

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อสร้างโปรแกรมที่สามารถเก็บตัวล็อกไฟล์ของเวปเซิร์ฟเวอร์ให้เป็นไปตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ บัญญัติไว้ได้

1.2.2 เพื่อเป็นเครื่องมือให้ผู้ดูแลระบบสามารถนำไปใช้ในการวิเคราะห์และปรับปรุง ระบบสารสนเทศให้มีประสิทธิภาพและความปลอดภัยเพิ่มขึ้น

1.3 ขอบข่ายของโครงงาน

1.3.1 โปรแกรมสามารถจัดเก็บล็อกไฟล์ของเวปเซิร์ฟเวอร์ได้อย่างครบถ้วนตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ บัญญัติไว้ได้ และเพียงพอต่อการนำไปใช้เป็นหลักฐานในการสืบสวนสอบสวน

1.3.2 โปรแกรมสามารถจัดเก็บล็อกไฟล์ให้อยู่ในรูปแบบที่ค้นหาได้ง่าย และสามารถนำเอาข้อมูลไปใช้ในการพัฒนาระบบสารสนเทศได้

1.3.3 โปรแกรมสามารถนำล็อกไฟล์มารายงานสถิติ (statistic report) ที่เป็นประโยชน์ต่อองค์กรในการปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น

1.3.4 จะพัฒนาโปรแกรมในรูปแบบของ window-based application เพื่อง่ายต่อการใช้งาน

1.4 ขั้นตอนของการดำเนินงาน

รายละเอียด	ปี 2551							ปี 2552		
	มิ.ย	ก.ค	ส.ค	ก.ย	ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค
1. ศึกษาเนื้อหารายละเอียดต่างๆ ที่จำเป็นต้องใช้ในโครงงาน										
2. ออกแบบโปรแกรมและส่วนประกอบ										
3. ทำการพัฒนาโปรแกรมและส่วนประกอบต่าง ๆ ตามที่ได้ออกแบบไว้										
4. ทดลองทำการใช้งานประเมินผลและแก้ไขโปรแกรม										
5. สรุปผลการทำโครงงานและจัดทำรายงาน										

1.5 ผลที่คาดว่าจะได้รับ

1.5.1 ทำให้มีความรู้ความเข้าใจเกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

1.5.2 ได้รับความรู้ความเข้าใจเกี่ยวกับการออกแบบแอพพลิเคชันด้วยโปรแกรม C#

1.5.3 ได้รับความรู้ความเข้าใจในการเขียนโปรแกรมเกี่ยวกับ Network Programming

1.5.4 สามารถนำโปรแกรมไปใช้เพื่อช่วยให้ผู้ดูแลระบบสามารถใช้ในการวิเคราะห์และปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น

1.6 งบประมาณของโครงการ

1.6.1 ค่าจัดทำรายงาน	เป็นจำนวนเงิน	500	บาท
1.6.2 ค่าถ่ายเอกสาร	เป็นจำนวนเงิน	500	บาท
	รวมเป็นเงินทั้งสิ้น	1,000	บาท

หมายเหตุ ขออนุมัติถัวเฉลี่ยทุกรายการ

บทที่ 2
ทฤษฎีพื้นฐาน

ในบทนี้จะกล่าวถึงทฤษฎีพื้นฐานหรือความรู้ต่างๆที่จะนำมาใช้ในโครงงาน โดยในที่นี้จะกล่าวถึงเรื่องต่างๆ ดังนี้

1. ล็อกไฟล์ (Log File)
2. เว็บเซิร์ฟเวอร์ (Web Server)
3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
4. โปรโตคอลเอชทีทีพี (HTTP : Hyper Text Transfer Protocol)
5. ระบบฐานข้อมูล (Database System)
6. ทำความรู้จักกับ C#

2.1 ล็อกไฟล์ (Log File)

ล็อกไฟล์ คือ ไฟล์ที่เก็บบันทึกกิจกรรมการดำเนินงานที่เกิดขึ้นหรือข้อมูลทางจราจร ซึ่งทางเทคนิค ถ้ามีปัญหาอะไรเกิดขึ้นก็จะเปิดเรียกดู ล็อกไฟล์เพื่อหาสาเหตุของปัญหาและแก้ไข นอกจากนี้ข้อมูลในล็อกไฟล์ยังสามารถนำไปวิเคราะห์เป็นสถิติหรือรายงานเพื่อปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและปลอดภัยยิ่งขึ้น อีกทั้งยังสามารถเก็บไว้เพื่อเป็นหลักฐานในการสืบสวนสอบสวนตามที่ พ.ร.บ คอมพิวเตอร์ ได้กำหนดไว้ได้ด้วย

ในอินเทอร์เน็ตจะมี เซิร์ฟเวอร์ที่ให้บริการมากมาย อย่างเช่น เว็บเซิร์ฟเวอร์ ก็จะมีการสร้างล็อกไฟล์โดยข้อมูลในล็อกไฟล์ก็จะเกี่ยวกับการร้องขอบริการที่มีเข้ามาในเซิร์ฟเวอร์ เช่น เวลาที่มีการร้องขอบริการ ใครที่ร้องขอบริการ ไฟล์ไหนที่ถูกให้บริการ เป็นต้น

2.1.1 Log File in Internet Information Services (IIS)

Internet Information Services (IIS) ได้เสนอทางเลือกสำหรับบันทึกกิจกรรมที่เกิดขึ้นใน web sites, File Transfer Protocol (FTP) sites, Network News Transfer Protocol (NNTP) service และ Simple Mail Transfer Protocol (SMTP) service และยังอนุญาตให้เลือกรูปแบบของล็อกไฟล์ที่คิดว่าเหมาะสมที่สุดกับสถานการณ์ IIS ล็อกไฟล์ประกอบด้วยข้อมูลต่างๆ เช่น ใครเข้ามาที่เว็บไซต์

เข้ามาเมื่อไร จึงทำให้เราสามารถตรวจสอบได้ว่าบริการนี้มีความต้องการมากแค่ไหน โดย IIS จะบันทึกเหตุการณ์ต่างๆ ที่เกิดขึ้นในการให้บริการ

2.1.1.1 W3C Extended Log Format

Log format นี้ถูกใช้สำหรับ Microsoft IIS ภายในประกอบด้วยบรรทัดของตัวอักษร ASCII ต่อเนื่องกัน โดยแต่ละบรรทัดนั้นจะมี directive และ entry ซึ่ง

- Entries จะประกอบขึ้นมาจากหลายๆ fields ซึ่งแต่ละ fields จะมีข้อมูลจาก HTTP TRANSANCTION ซึ่งจะแยกออกจากกันด้วยเครื่องหมายวรรคตอน และถ้า fields นั้นไม่มีการใช้งานก็ถูกแทนที่ด้วยเครื่องหมาย – ใน fields นั้นๆ

- Directives จะบันทึกข้อมูลของการบันทึก ล็อกไฟล์โดยแต่ละบรรทัดนั้นจะมีเครื่องหมาย # นำหน้าเพื่อเป็นสัญลักษณ์ในการแยกออกจาก Entries โดยลักษณะการเก็บข้อมูลของ directives ของ W3C Extended format มีรายละเอียดดังนี้

Version: <integer>.<integer>	Version ของ extended log file format ที่ใช้
Fields: [<specifier>…]	กำหนด field ที่บันทึกลงในล็อกไฟล์
Software: string	
Start-Date: <data><time>	วันเวลาที่ล็อกไฟล์ เริ่มทำงาน
End-Date: <data><time>	วันเวลาที่ล็อกไฟล์ ทำงานเสร็จ
Data: <data><time>	วันเวลาที่ entry ถูกบันทึก
Remark: <text>	ข้อคิดเห็น

Version และ Fields directives ควรจะนำหน้า entry ทั้งหมดในล็อกไฟล์ โดย Field directive จะกำหนดข้อมูลที่จะบันทึกลงใน field ของแต่ละ entry ดังรูปที่ 2.1

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2002-05-24 20:18:01
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status sc-bytes
cs-bytes time-taken cs(User-Agent) cs(Referrer)
2002-05-24 20:18:01 172.224.24.114 - 206.73.118.24 80 GET /Default.htm - 200 7930 248 31
Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+2000+Server) http://64.224.24.114/
```

รูปที่ 2.1 แสดงตัวอย่าง W3C Extended Log Format

จากตัวอย่าง W3C Extend Log File จาก Internet ในส่วนของ Field สามารถอธิบายได้ดังนี้

date	วันเดือนปีที่ ล็อกไฟล์ถูกบันทึก
time	เวลาที่ ล็อกไฟล์ถูกบันทึก
c-ip	IP address ของไคลแอน
cs-username	user name ที่เข้าใช้เซิร์ฟเวอร์
s-ip	IP address ของเซิร์ฟเวอร์
s-port	เซิร์ฟเวอร์ port
cs-method	HTTP method ที่ใช้ในการ request
cs-uri-stem	Request Stem
cs-uri-query	Request Query string
sc-status	จำนวนไบต์ที่เซิร์ฟเวอร์ ส่งไปให้ ไคลแอน
cs-bytes	จำนวนไบต์ที่ไคลแอน ส่งไปให้ เซิร์ฟเวอร์
time-taken	เวลาที่ใช้ในการ request
cs (User-Agent)	ข้อมูลเกี่ยวกับ browser ที่ขอ request
cs (Referrer)	เว็บเพจที่ให้ลิงค์เชื่อมต่อมาที่เว็บไซต์

2.1.1.2 IIS Log File Format

รูปแบบของ IIS log file format จะเป็นแบบ fixed ASCII text-based format โดยที่ไม่สามารถปรับเปลี่ยนไปตามความต้องการของผู้ใช้ เนื่องจาก IIS log file format ถูกควบคุมโดย HTTP.sys

192.168.114.201, -, 03/20/01, 7:55:20, W3SVC2, SERVER, 172.21.13.45, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, -,

รูปที่ 2.2 แสดงตัวอย่าง IIS log file format

จากตัวอย่าง IIS log file format ในส่วนของ Field สามารถอธิบายได้ดังนี้

Client IP address: 192.168.114.201 (IP address ของไคลแอน)

User name: -

Date:	03/20/01
Time:	7 : 55 : 20
Service and instance:	W3SVC2
Server name:	SERVER
Server IP:	172.21.113.45 (IP address ของ เซิร์ฟเวอร์)
Time taken:	4502 (หน่วยเป็น milliseconds)
Client bytes sent:	163 (จำนวนไบต์ที่ส่งจาก ไคลแอนไปเซิร์ฟเวอร์)
Server bytes sent:	3223 (จำนวนไบต์ที่ส่งจาก เซิร์ฟเวอร์ไปไคลแอน)
Service status code:	200 (การร้องขอสมบูรณ์เรียบร้อย)
Windows status code:	0 (การร้องขอสมบูรณ์เรียบร้อย)
Request type:	GET
Target of operation:	/DeptLogo.gif (user ต้องการ download ไฟล์ DeptLogo.gif)
Parameters: -	

2.2 เว็บเซิร์ฟเวอร์ (Web Server)

เว็บเซิร์ฟเวอร์ คือ เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องบริการเว็บแก่ผู้ร้องขอด้วยโปรแกรมประเภทเว็บบราวเซอร์ ที่ร้องขอข้อมูลผ่านโปรโตคอลเฮชทีที เครื่องจะส่งข้อมูลให้ผู้ร้องขอในรูปของข้อความ ภาพ เสียง หรือสื่อผสม เครื่องบริการเว็บจะเปิดบริการพอร์ท 80 และ 443 ให้ผู้ร้องขอได้เชื่อมต่อผ่านโปรแกรมประเภทเว็บบราวเซอร์ เช่น โปรแกรมอินเทอร์เน็ตเอ็กโพเลอร์ หรือฟายฟร็อก แล้วแจ้งชื่อที่ร้องขอในรูปของที่อยู่เว็บ เช่น http://www.google.com เป็นต้น โปรแกรมที่นิยมนำใช้เป็นเครื่องบริการเว็บ ได้แก่ อาปาเช่ และไมโครซอฟท์ไอไอเอส

2.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายหลักที่ใช้ควบคุม จับกุมผู้ที่ใช้คอมพิวเตอร์ในการกระทำความผิด และผู้ที่กระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์ ๒๕๕๐ ที่มีผลบังคับใช้เมื่อวันที่ ๑๘ กรกฎาคม ๒๕๕๐ ที่ผ่านมาถือได้ว่าเป็นกฎหมายที่อยู่ในความสนใจของสาธารณะชนและมีผลกระทบต่อบุคคลทุกกลุ่มอย่างกว้างขวาง ซึ่ง

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ยังมีเนื้อหาครอบคลุมลักษณะและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และสารสนเทศ โดยการเก็บข้อมูลจราจรทางคอมพิวเตอร์ และหลักฐานที่จำเป็นอย่างครบถ้วนเพื่อใช้เป็นหลักฐานในการสืบสวนหาผู้กระทำความผิดได้

ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับดังกล่าวได้มีการกำหนดรายละเอียดของข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องมีหน้าที่ต้องเก็บรักษาดังต่อไปนี้

2.3.1 ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย (Network Access System)

Network Access System เป็นการเข้าถึงระบบเครือข่าย จะมี Authentication Server เป็นข้อมูลล็อกการพิสูจน์ตัวตนของเซิร์ฟเวอร์หรืออุปกรณ์พิสูจน์ตัวตน ซึ่งจะต้องเก็บข้อมูลจราจรที่สามารถระบุตัวตนของผู้ใช้ดังนี้

- ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่ายหรือ Access Log
- ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address)
- ข้อมูลที่บ่งบอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)

2.3.2 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บเซิร์ฟเวอร์ (Web Server)

Web Service จะมีเว็บเซิร์ฟเวอร์ เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Hypertext Transfer Protocol (HTTP) ซึ่งรวมถึง Hypertext Transfer Protocol Security (HTTPS) ซึ่งผู้ให้บริการจะต้องเก็บข้อมูลจราจรที่สามารถระบุตัวตนของผู้ใช้ดังนี้

- ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ (HTTP Log)
- ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น
- ข้อมูลแสดงรูปแบบคำสั่งในการเข้ามาใช้ (Type of Command)

- ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier)

2.3.2 ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (E – mail Servers)

E – mail Servers เป็นการบริการจดหมายอิเล็กทรอนิกส์ จะมี SMTP Server หรือ POP/IMAP Server เป็นข้อมูลล็อกของอีเมล์เซิร์ฟเวอร์ ที่สื่อสารกับด้วย Simple Mail Transfer Protocol (SMTP) หรือ Post Office Protocol version 3 (POP3) หรือ Internet Message Access Protocol Version 4 (IMAP4)ซึ่งผู้ให้บริการจะต้องเก็บข้อมูลจราจรที่สามารถระบุตัวตนของผู้ใช้ดังนี้

- ข้อมูล log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (SMTP Log)
- ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องที่ให้บริการ (Date and Time of Connection of Client Connected to Server)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)
- ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)
- ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address)
- ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address)
- ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator)
- หมายเลขสมาชิกของผู้ใช้งาน (User ID)
- ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ในเครื่องให้บริการ (POP3 Log/IMAP 4)

2.3.3 ข้อมูลอินเทอร์เน็ตที่เกิดจากการถ่ายโอนข้อมูลบนเครื่องให้บริการถ่ายโอนข้อมูล (FTP/ File Sharing Service)

FTP/File Sharing Service จะมี FTP Server เป็นข้อมูลล็อกจากเซิร์ฟเวอร์ที่ถ่ายโอนไฟล์ข้อมูลด้วย File Transfer Protocol (FTP) ซึ่งผู้ให้บริการจะต้องเก็บข้อมูลจราจรที่สามารถระบุตัวตนของผู้ใช้ดังนี้

- ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนถ่ายแฟ้มข้อมูล (FTP Log)

- ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องที่ให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
- หมายเลขสมาชิกของผู้ใช้งาน (User ID)
- ข้อมูลตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งมาขึ้นมาบันทึกหรือให้ดึงข้อมูลออกไป

2.3.4 ชนิดข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) จะมี News Server เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Network News Transfer Protocol (NNTP) ซึ่งผู้ให้บริการจะต้องเก็บข้อมูลจราจรที่สามารถระบุตัวตนของผู้ใช้ดังนี้

- ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP)
- ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องผู้ให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลหมายเลขพอร์ท (Port) ในการใช้งาน (Protocol Process ID)
- ข้อมูลชื่อเครื่องให้บริการ (Host Name)
- ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)

2.4 โปรโตคอลเอชทีทีพี (HTTP : Hyper Text Transfer Protocol)

HTTP เป็นโปรโตคอลแบบไคลเอ็นต์/เซิร์ฟเวอร์ในลักษณะ transactionoriented คือมีการติดต่อระหว่างโปรแกรม 2 โปรแกรม ซึ่งโดยทั่วไปได้แก่เว็บบราวเซอร์และเว็บเซิร์ฟเวอร์ เพื่อให้มีความน่าเชื่อถือ HTTP จึงใช้ประโยชน์จากโปรโตคอลทีซีพี แต่ถึงกระนั้น HTTP ก็เป็นโปรโตคอลที่ "ปราศจากสถานะ" กล่าวคือ การติดต่อในแต่ละครั้งเป็นอิสระต่อกัน โดยการเชื่อมต่อระหว่างไคลเอ็นต์และเซิร์ฟเวอร์จะถูกสร้างขึ้นมาใหม่สำหรับการติดต่อในแต่ละครั้ง และถูกตัดขาดจากกันทันทีที่การติดต่อเสร็จสิ้นสมบูรณ์ ถึงแม้ว่าข้อกำหนดของ HTTP จะไม่ได้ระบุความสัมพันธ์ในแบบหนึ่งต่อหนึ่งระหว่างการติดต่อและช่วงเวลาของการเชื่อมต่อเช่นนี้ไว้ก็ตามที

คุณสมบัติ "ปราศจากสถานะ" ดังกล่าวของโปรโตคอล HTTP นี้เหมาะสมต่อการนำมาประยุกต์ใช้เป็นอย่างยิ่ง การใช้งานเว็บบราวเซอร์นั้นโดยปกติเกี่ยวข้องกับการรับเอากลุ่มของเว็บเพจและเอกสารเข้ามา ซึ่งการดำเนินการตรงนี้เกิดขึ้นรวดเร็วมาก โดยเว็บเพจและเอกสารเหล่านี้อาจมาจากเซิร์ฟเวอร์ที่แตกต่างกันไป

คุณลักษณะที่สำคัญอีกประการหนึ่งของโปรโตคอล HTTP ก็คือ ความยืดหยุ่นในแง่ของรูปแบบที่มันสามารถจัดการได้ เมื่อไคลเอ็นต์ส่งคำร้องขอไปยังเซิร์ฟเวอร์ ไคลเอ็นต์อาจระบุรายการของรูปแบบต่างๆ ที่มันสามารถจัดการได้ไปให้เซิร์ฟเวอร์ด้วย ฝ่ายเซิร์ฟเวอร์เองก็จะตอบสนองกลับมาด้วยรูปแบบที่เหมาะสม ยกตัวอย่างเช่น บราวเซอร์ lynx ซึ่งเป็นบราวเซอร์ที่ทำงานภายใต้เทิร์มโหมดของยูนิกซ์นั้นไม่สามารถจัดการกับรูปภาพได้ เว็บเซิร์ฟเวอร์จึงไม่จำเป็นต้องส่งรูปภาพใดๆ ที่ปรากฏอยู่บนเว็บเพจไปให้ การเตรียมการเช่นนี้ป้องกันมิให้เกิดการส่งข้อมูลที่ไม่จำเป็น และยังเป็นหลักสำคัญสำหรับการเพิ่มเติมรูปแบบตามข้อกำหนดที่จะถูกสร้างขึ้นใหม่ให้เป็นมาตรฐานในอนาคตอีกด้วย

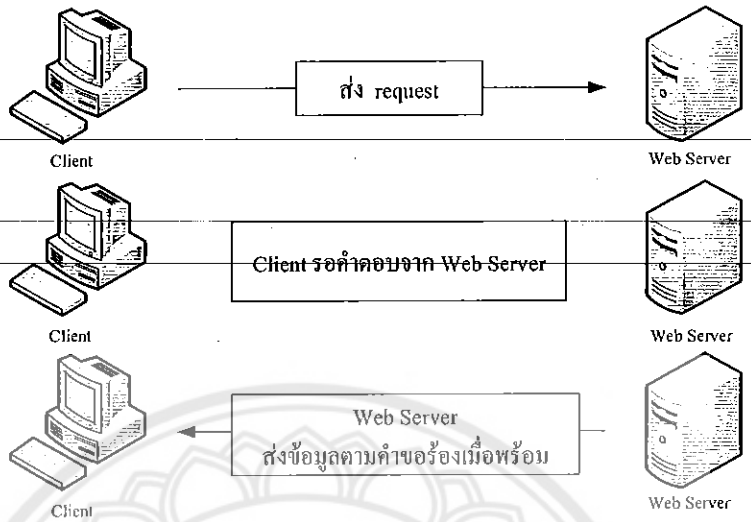
2.4.1 ภาพโดยรวมของโปรโตคอล HTTP

โปรโตคอล HTTP เป็นกลไกหรือโปรโตคอลหลักที่ใช้แลกเปลี่ยนข้อมูลกันระหว่างเซิร์ฟเวอร์และไคลเอนต์ของเวิลด์ไวด์เว็บ โดยถูกออกแบบมาให้มีความกระทัดรัด สามารถทำงานได้รวดเร็ว มีกระบวนการทำงานไม่ซับซ้อน และมีคำสั่งที่ใช้งานไม่มากนัก แต่สามารถรองรับข้อมูลได้ทุกแบบ ไม่ว่าจะเป็นข้อมูลทั่วไปที่เข้ารหัสแบบ MIME หรือข้อมูลที่เป็นกราฟิก เช่น ไฟล์ที่เป็น GIF หรือ JPEG เป็นต้น

หลักการทำงานทั่วๆ ไปของ HTTP ก็คือ จะแบ่งการทำงานออกเป็น 2 ด้านคือ ด้านเว็บเซิร์ฟเวอร์และด้านไคลเอนต์ โดยไคลเอนต์จะติดต่อเข้ามายังเซิร์ฟเวอร์โดยใช้โปรแกรมบราวเซอร์และอ้างอิงแอดเดรสของเซิร์ฟเวอร์โดยใช้รูปแบบของ URL ส่วนด้านเซิร์ฟเวอร์จะส่งข้อมูลกลับมาในรูปแบบที่เป็นภาษา HTML (Hyper Text Markup Language) โดยที่โปรโตคอล HTTP ใช้วิธีการเข้ารหัสในแบบ MIME เป็นมาตรฐานของการทำงาน

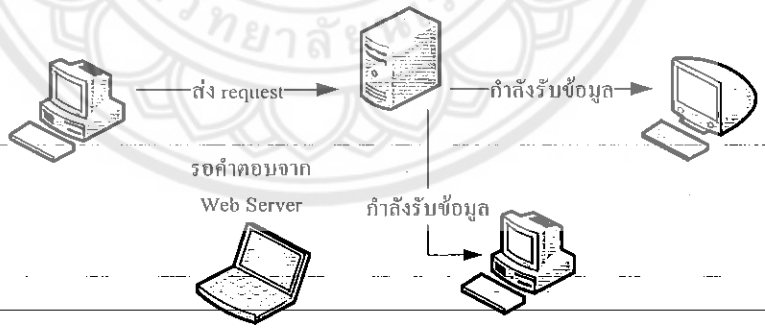
โครงสร้างข้อมูลของ HTTP จะแบ่งออกเป็น 2 ส่วนใหญ่ๆ คือ ส่วนเฮดเดอร์ หรือเรียกว่า metadata จะเป็นส่วนเก็บข้อมูลที่จำเป็นต้องใช้ภายในโปรโตคอล ส่วนที่สองเป็นส่วนเป็นข้อมูลจริงที่ต้องการรับส่ง ทั้งนี้ HTTP ถูกออกแบบมาให้สามารถรับส่งข้อมูลผ่าน Proxy หรือ Firewall ต่างๆ ได้ โดยการทำงาน HTTP จะอาศัยโปรโตคอลพื้นฐาน TCP/IP ซึ่งทั่วไปจะใช้หมายเลขพอร์ต

ที่ 80 ซึ่งรูปแบบการทำงานจะไม่มีการจองสาย โดย client จะเรียกข้อมูลจาก server โดยการส่ง request ไป แล้วจะตัดการติดต่อทันที จากนั้นจะรอจนกระทั่ง server ส่งข้อมูลมาให้ดังรูปที่ 2.3



รูปที่ 2.3 แสดงการร้องขอข้อมูลจากเซิร์ฟเวอร์

ประโยชน์ของการทำงานแบบไม่จองสายของโปรโตคอล HTTP ทำให้ Web Server สามารถให้บริการ client ได้หลายๆ คนพร้อมๆ กัน การสื่อสารของ WWW จึงมีประสิทธิภาพมากขึ้น ดังรูปที่ 2.4



รูปที่ 2.4 แสดงการให้บริการลูกข่ายจำนวนมาก

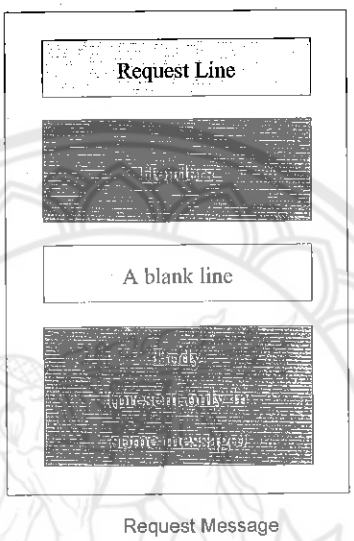
2.4.2.1 เมสเซจ (Messages)

วิธีที่อธิบายการทำงานของ HTTP ได้ดีที่สุดก็คือการอธิบายถึงแต่ละองค์ประกอบของ

เมสเซจ HTTP โดย HTTP ประกอบด้วยเมสเซจ 2 ประเภทคือ คำร้องขอจากไคลเอ็นต์ไปยังเซิร์ฟเวอร์และคำตอบสนองจากเซิร์ฟเวอร์ไปยังไคลเอ็นต์ ซึ่งโครงสร้างทั่วไปของเมสเซจทั้งสองประเภทนี้จะมีรูปแบบคล้ายคลึงกัน

เมสเซจร้องขอ (Request Messages)

เมสเซจร้องขอ นี้จะประกอบไปด้วย request line เฮดเดอร์ (header) และบอดี้ (body) ดังรูปที่ 2.5

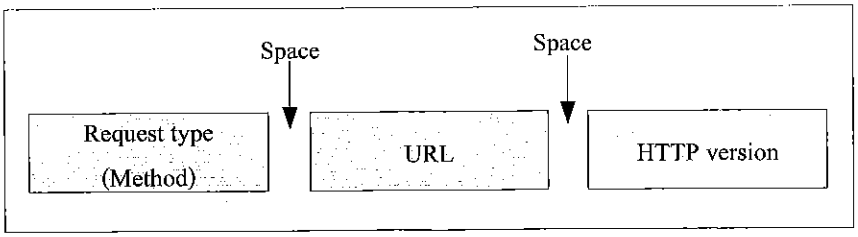


Request Message

รูปที่ 2.5 แสดงเมสเซจร้องขอ (Request Messages)

Request line

Request line จะใช้สำหรับการกำหนดชนิดของ request, URL และเวอร์ชันของ HTTP ดังรูปที่ 2.6



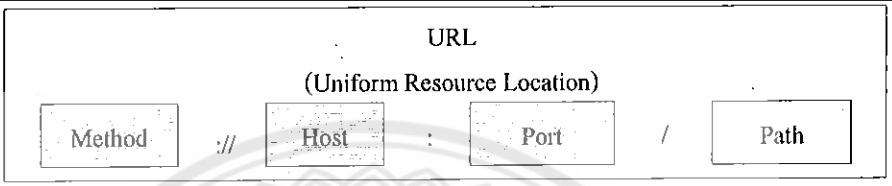
รูปที่ 2.6 แสดงรูปแบบของ Request line

- ชนิดของ request : ใน HTTP เวอร์ชั่น 1.1 จะมีชนิดของ request อยู่หลายชนิด ซึ่งจะใช้

ในการแบ่งประเภทของเมสเซจ request เป็นเมธอดต่างๆ ส่วนเมธอดที่มีการใช้งานนั้นจะ กล่าวในหัวข้อถัดไป

- URL (Uniform Resource Location) : เป็นมาตรฐานในการระบุตำแหน่งของสิ่งใดๆ ที่อยู่ในอินเทอร์เน็ตที่สามารถเข้าถึงหรือเรียกใช้งานได้ URL จะประกอบด้วย 4 ส่วนคือ เมธอด โฮลต์ พอร์ต และพาธ ดังรูปที่ 2.7

- HTTP version : เป็นส่วนที่ใช้ในการบ่งบอกถึงเวอร์ชันของ HTTP



รูปที่ 2.7 แสดงรูปแบบของ URL

รายละเอียดของ URL ในแต่ละส่วนจะเป็นดังนี้

- เมธอด (method) : เป็นโปรโตคอลที่ใช้ในการดึงหรือรับเอกสารมาจากเซิร์ฟเวอร์ ซึ่งจะมีหลายเมธอด แต่ที่ใช้กันจะเป็นเมธอด FTP และ HTTP ข้อสังเกตคือ คำว่าเมธอด ในที่นี้จะไม่เหมือนกับเมธอดที่ใช้กันในส่วนของ ชนิดของ request เนื่องจากเมธอดใน ที่นี้เป็นโปรโตคอล แต่เมธอดอีกอันหนึ่งนั้นจะเป็นฟังก์ชันการทำงาน

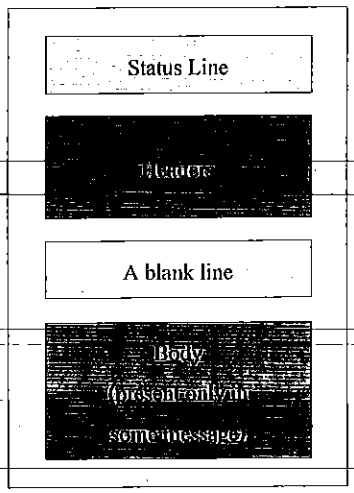
- โฮสต์ (host) : จะเป็นสถานที่ที่เก็บข้อมูลหรือเอกสารต่างๆ เอาไว้

- พอร์ต (port) : ใน URL สามารถที่จะใส่ค่าของพอร์ตที่ต้องการติดต่อไปยังเซิร์ฟเวอร์ได้ด้วย โดยการใช้เครื่องหมาย “ : ” (colon) เพื่อแยกโฮสต์กับพอร์ตออกจากกัน

- พาธ (path) : เป็นชื่อของพาธที่ใช้ในการเก็บแฟ้มข้อมูล

เมสเซจตอบสนอง (Response Messages)

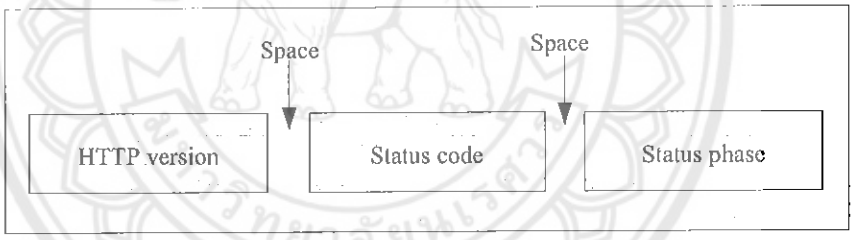
เมสเซจตอบสนองจะประกอบไปด้วย Status line เฮดเดอร์ (header) และบอดี้ (body) ดังรูปที่ 2.8



รูปที่ 2.8 แสดงเมสเซจตอบสนอง (Response Messages)

Status line

Status line จะใช้ในการกำหนดสถานะของเมสเซจตอบสนอง ซึ่งจะประกอบไปด้วยเวอร์ชันของ HTTP, status code และ status phase ดังรูปที่ 2.9



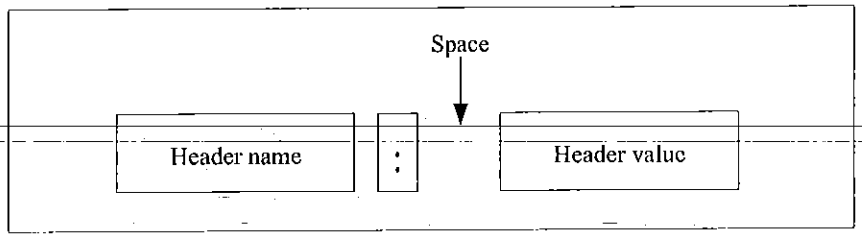
รูปที่ 2.9 แสดงรูปแบบของ Status line

- HTTP version : เป็นส่วนที่ใช้ในการบ่งบอกถึงเวอร์ชันของ HTTP
- Status code : ฟิลด์นี้จะคล้ายกันกับของ FTP และ SMTP ซึ่งจะเป็นตัวเลขที่มีอยู่ 3 หลัก
- Status phase : ฟิลด์นี้จะใช้ในการอธิบาย status code ในรูปของเท็กซ์

เฮดเดอร์ (Header)

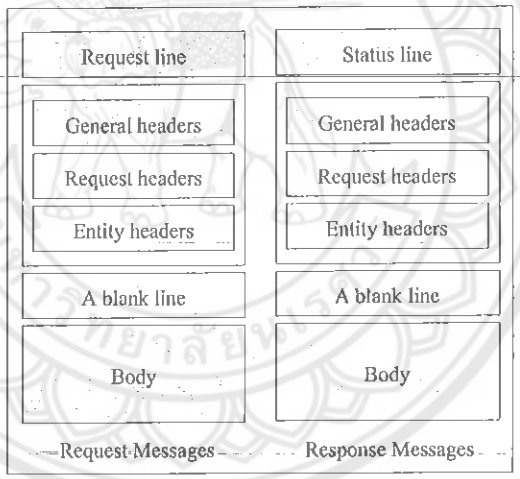
เฮดเดอร์จะใช้ในการแลกเปลี่ยนข้อมูลเพิ่มเติมระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ เช่น ไคลเอ็นต์สามารถร้องขอให้เซิร์ฟเวอร์ส่งเอกสารในรูปแบบที่ไคลเอ็นต์ต้องการได้ หรือเซิร์ฟเวอร์สามารถส่งข้อมูลเพิ่มเติมบางอย่างที่เกี่ยวข้องกับเอกสารนั้นๆ เป็นต้น

เฮดเดอร์สามารถมีบรรทัดเดียวหรือหลายบรรทัดก็ได้ ซึ่งแต่ละบรรทัดจะประกอบไปด้วยชื่อเฮดเดอร์และค่าของเฮดเดอร์ โดยจะใช้เครื่องหมาย " : " (colon) คั่นกลาง ดังรูปที่ 2.10



รูปที่ 2.10 แสดงรูปแบบของเฮดเดอร์

ในแต่ละบรรทัดของเฮดเดอร์จะสามารถแบ่งออกได้ 4 ประเภทคือ general, request, response และ entity ดังรูปที่ 2.11 จะแสดงให้เห็นถึงเฮดเดอร์ในเมสเซจร้องขอ (Request Messages) และเมสเซจตอบสนอง (Response Messages)



รูปที่ 2.11 แสดงเฮดเดอร์ของเมสเซจร้องขอ และเมสเซจตอบสนอง

2.4.2.2 คำสั่งของโปรโตคอล (HTTP)

โปรโตคอล HTTP มีคำสั่งต่างๆ ไม่มากนัก เพื่อให้สามารถใช้งานได้อย่างสะดวกและรวดเร็ว โดยมีคำสั่งที่ใช้งานแพร่หลายอยู่เพียง 3 คำสั่ง คือ GET, HEAD และ POST ส่วนคำสั่งอื่นๆ มีใช้งานเหมือนกัน แต่ไม่เป็นที่นิยมมากนัก รายละเอียดคำสั่งของ HTTP มีดังตารางที่ 2.1

ตารางที่ 2.1 แสดงคำสั่งของโปรโตคอล HTTP

คำสั่ง(Method)	รายละเอียด
GET	เป็นเมธอดที่จะต้องใช้เมื่อไคลเอ็นต์ต้องการดึงข้อมูลหรือเอกสารจากเซิร์ฟเวอร์
HEAD	เป็นเมธอดที่จะใช้เมื่อไคลเอ็นต์ต้องการข้อมูลบางอย่างที่เกี่ยวข้องกับเอกสาร แต่ไม่ใช้ตัวเอกสารนั้นๆ
POST	เป็นเมธอดที่จะใช้เมื่อไคลเอ็นต์ต้องการส่งข้อมูลบางอย่างให้กับเซิร์ฟเวอร์
PUT	เป็นเมธอดที่จะใช้เมื่อไคลเอ็นต์สร้างเอกสารใหม่ หรือแทนเอกสารเก่าในที่เก็บอยู่ในเซิร์ฟเวอร์
PATCH	จะคล้ายกับ PUT
COPY	เป็นเมธอดที่ใช้ในการก๊อปปี้แฟ้มข้อมูลไปยังที่อื่นๆ
MOVE	เป็นเมธอดที่ใช้ในการย้ายแฟ้มข้อมูลไปยังที่อื่นๆ
DELETE	เป็นเมธอดที่ใช้ในการลบเอกสารออกจากเซิร์ฟเวอร์
LINK	เป็นเมธอดที่ใช้สำหรับการสร้างการเชื่อมโยงเอกสารจากเอกสารหนึ่งไปยังอีกเอกสารหนึ่ง
UNLINK	เป็นเมธอดที่ใช้ในการยกเลิกการเชื่อมโยงเอกสารที่ถูกสร้างโดยเมธอด LINK
OPTION	เป็นเมธอดที่ถูกใช้โดยไคลเอ็นต์ เมื่อต้องการสอบถามเซิร์ฟเวอร์เกี่ยวข้องกับออบชันเพิ่มเติมต่างๆ

2.5 ระบบฐานข้อมูล (Database System)

ฐานข้อมูล คือ กลุ่มของข้อมูลที่มีความสัมพันธ์เกี่ยวข้องเป็นเรื่องเดียวกัน เช่น กลุ่มข้อมูลเกี่ยวกับพนักงานบริษัท ประกอบด้วย รหัสพนักงาน ชื่อ นามสกุล เบอร์โทรศัพท์ และกลุ่มข้อมูลดังกล่าวถูกจัดเก็บอยู่รวมกันหลายๆ กลุ่มซึ่งอาจจะเก็บอยู่ในรูปแฟ้มเอกสาร

กล่าวโดยสรุปแล้ว ฐานข้อมูลมีลักษณะดังต่อไปนี้

- เป็นเรื่องเกี่ยวกับการจัดเก็บข้อมูล
- ข้อมูลที่จัดเก็บมีความสัมพันธ์เกี่ยวข้องเป็นเรื่องเดียวกัน
- สามารถแสดงออกมาอยู่ในรูปแบบของตารางได้

ส่วนประกอบของตารางข้อมูลในฐานข้อมูล

โดยทั่วไปแล้วตารางข้อมูลที่ใช้งานกันจะประกอบด้วยแถว และคอลัมน์ ต่างๆ แต่ถ้ามองกันในรูปแบบของฐานข้อมูลแล้ว จะเรียกรายละเอียดแต่ละแถวว่า เรคอร์ด และเรียกรายละเอียดในแนวคอลัมน์ว่า ฟิลด์ ในฐานข้อมูล 1 ระบบ อาจประกอบด้วยตารางข้อมูลมากกว่า 1 ตาราง ฐานข้อมูล และถ้ามีตารางตั้งแต่ 1 คู่ขึ้นไปที่มีความสัมพันธ์กันด้วยฟิลด์ใดฟิลด์หนึ่งเรียกฐานข้อมูลประเภทนี้ว่า

"ฐานข้อมูลเชิงสัมพันธ์" หรือ Relational Database

ประโยชน์ของระบบฐานข้อมูล

ฐานข้อมูลช่วยสร้างระบบการจัดเก็บข้อมูลขององค์กรให้เป็นระเบียบ แยกข้อมูลตามประเภททำให้ข้อมูลประเภทเดียวกันจัดเก็บอยู่ด้วยกันสามารถค้นหาแก้ไข และเรียกใช้งานได้ง่าย ไม่ว่าจะนำมาพิมพ์รายงาน นำมาคำนวณหรือนำมาวิเคราะห์ซึ่งทั้งนี้ขึ้นอยู่กับการใช้ประโยชน์ขององค์กร

จากประโยชน์ของระบบฐานข้อมูล อาจกล่าวได้ว่าระบบฐานข้อมูลมีข้อดีมากกว่าการเก็บข้อมูลในระบบแฟ้มข้อมูล ดังนี้

1. สามารถลดจำนวนข้อมูลที่ซ้ำซ้อนของข้อมูลได้
2. สามารถหลีกเลี่ยงความขัดแย้งของข้อมูลได้
3. สามารถกำหนดความเป็นมาตรฐานเดียวกันได้
4. สามารถใช้ข้อมูลร่วมกันในเวลาเดียวกันได้
5. สามารถกำหนดระบบรักษาความปลอดภัยให้กับข้อมูลได้
6. สามารถรักษาความถูกต้องและความน่าเชื่อถือของข้อมูลได้
7. มีความเป็นอิสระของข้อมูล

โครงสร้างของฐานข้อมูล

โครงสร้างของฐานข้อมูลประกอบด้วย

1. Character คือ ตัวอักขระแต่ละตัว / ตัวเลข / เครื่องหมาย

2. Field คือ เขตข้อมูล / ชุดข้อมูลที่ใช้แทนความหมายของสื่อโครงสร้าง เช่น ชื่อของบุคคล ชื่อของวัสดุสิ่งของ

3. Record คือ ระเบียน หรือรายการข้อมูล เช่น ระเบียนของพนักงานแต่ละคน หรือข้อมูลสิ่งของ

4. Table / File คือ ตาราง หรือแฟ้มข้อมูลประกอบขึ้นด้วยระเบียนต่างๆ เช่น ตารางข้อมูลของบุคคล ตารางข้อมูลของวัสดุสิ่งของ

5. Database คือฐานข้อมูลประกอบด้วยตาราง และแฟ้มข้อมูลต่างๆ ที่เกี่ยวข้องหรือมีความสัมพันธ์กัน

ระบบฐานข้อมูลมีองค์ประกอบ 5 ประเภท คือ

1. ฮาร์ดแวร์ (Hardware) ประกอบด้วย อุปกรณ์บันทึกข้อมูลเช่น จานแม่เหล็ก I/O device Device controller I/O channels หน่วยประมวลผล และหน่วยความจำหลัก

2. โปรแกรม (Program หรือ Software) ซึ่งมีหน้าที่ควบคุมดูแลการสร้างฐานข้อมูล การเรียกใช้ข้อมูล และ การจัดทำรายงาน เรียกว่า โปรแกรมระบบจัดการฐานข้อมูล (Database Management System: DBMS)

3. ข้อมูล (Data) คือ สิ่งที่เราจะเก็บไว้ในฐานข้อมูล เช่น ชื่อ นามสกุล ที่อยู่ เป็นต้น

4. บุคลากร (People ware) ได้แก่ ผู้ใช้งาน (User) พนักงานปฏิบัติการ (Operator) นักวิเคราะห์และออกแบบระบบ (System Analyst) ผู้เขียนโปรแรมประยุกต์ใช้งาน (Programmer) และผู้บริหารฐานข้อมูล (Database Administrator : DBA)

5. ขั้นตอนการปฏิบัติงาน (Procedure) เป็นขั้นตอนและวิธีการต่าง ๆ ในการปฏิบัติงานเพื่อการทำงานที่ถูกต้องและเป็นไปตามขั้นตอนที่ได้กำหนดไว้ จึงควรทำเอกสารที่ระบุขั้นตอนการทำงานของหน้าที่ต่าง ๆ ในระบบฐานข้อมูล ทั้งขั้นตอนปกติ และขั้นตอนในสภาวะที่ระบบเกิดปัญหา (Failure)

2.6 ทำความรู้จักกับ C#

ภาษา C# เป็นภาษาที่ถูกสร้างขึ้นมาเพื่อทำงานบน .NET Platform สร้างและมีการทำงานโดยใช้หลักการแบบ Object Oriented ได้อย่างสมบูรณ์ (ซึ่งเมื่อเปรียบเทียบกับ C++ ที่ยังทำงานในลักษณะของ Object Oriented Programming (OOP) ได้แค่บางส่วน) ซึ่งไลบรารี่ของ C# ถูกสร้างขึ้นเพื่อที่ให้ทำงานได้ครอบคลุมตั้งแต่การสร้างรูปแบบการติดต่อแบบ GUI ไปจนถึงการแอ็คเซสฐานข้อมูลผ่านอินเทอร์เน็ตหรือแม้แต่การทำงานร่วมกับ XML เพื่อทำให้การแลกเปลี่ยนข้อมูลระหว่าง

แอพพลิเคชั่นทำได้อย่างสมบูรณ์ไม่ว่าข้อมูลนั้นจะอยู่บนแพลทฟอร์มใดก็ตาม

เมื่อเปรียบเทียบกับ C++ แล้วการสร้างแอพพลิเคชั่นจะทำได้ง่ายกว่ามาก เนื่องจาก C# ถูกออกแบบมาเพื่อการสร้างแอพพลิเคชั่นให้ทำงานบนอินเทอร์เน็ต (Network) โดยตรง (.NET Framework) นอกจากนี้ C# เป็น Object Oriented Programming (OOP) อย่างสมบูรณ์ ไม่ว่าจะเป็น

- Encapsulation การรวมกลุ่มฟังก์ชั่นการทำงานของออบเจ็กต์ต่างๆ (Object Blueprint, Class) เพื่อทำให้โค้ดถูกเขียนขึ้นมาอย่างเป็นระเบียบ

- Polymorphism (Inheritance, Interfacing และ Overloading) การนำโค้ดที่เขียนขึ้นมาแล้วนั้น ยังสามารถนำไปใช้ในงานอื่นได้อีก

ซึ่งการเขียนโปรแกรม Visual Basic ทำได้ง่ายกว่าแต่ประสิทธิภาพของโปรแกรมมีข้อด้อยกว่าโปรแกรมที่เขียนขึ้นมาจาก C++ ในบางกรณีอย่างเช่น โปรแกรมที่ต้องติดต่อกับฮาร์ดแวร์ จะเลือกใช้ C++ แต่ถ้าต้องการความง่ายในการเขียนโปรแกรม แต่ถ้าไม่คำนึงถึงประสิทธิภาพการทำงานมากนัก จะเลือกใช้ Visual Basic

ซึ่ง C# ได้ทำการรวมเอาเอกลักษณะการเขียนโปรแกรมจากภาษาทั้งสองเข้ามาไว้ด้วยกัน

บทที่ 3

การออกแบบและพัฒนาระบบ

ในการออกแบบและพัฒนานั้นจะใช้ทฤษฎีที่ศึกษาในบทที่ 2 มาใช้ในการออกแบบระบบและพัฒนาระบบ—ซึ่งจะเริ่มต้นจากการกำหนดแนวคิดในการออกแบบ—กำหนดรายละเอียดความสามารถของโปรแกรมให้ชัดเจน จากนั้นก็เป็นการออกแบบภาพรวมของโปรแกรม

3.1 แนวคิดในการออกแบบ

- โปรแกรมสามารถจัดเก็บล็อกไฟล์ได้อย่างครบถ้วนตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของเว็บเซิร์ฟเวอร์กำหนดไว้ได้

- เป็นโปรแกรมที่เข้าใจการใช้งานได้ง่าย ไม่จำเป็นต้องมีความรู้พื้นฐานทางคอมพิวเตอร์มาก่อน ก็สามารถใช้งานได้ดี

- จะพัฒนาโปรแกรมในรูปแบบของ window based application เพื่อง่ายต่อการใช้งาน

- จะแบ่งโปรแกรมออกเป็น 2 ส่วน คือโปรแกรมที่ทำงานฝั่งเซิร์ฟเวอร์จะทำการวิเคราะห์แพ็กเก็ตพร้อมทั้งจัดเก็บลงฐานข้อมูลและฝั่งผู้ใช้หรือผู้ดูแลระบบจะทำหน้าที่ในการเรียกดูรายงานต่างๆ

3.2 ความสามารถของโปรแกรม

- โปรแกรมสามารถจัดเก็บล็อกไฟล์ได้อย่างครบถ้วนตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของเว็บเซิร์ฟเวอร์กำหนดไว้ได้

-การสั่งงานโปรแกรมส่วนใหญ่ผ่าน GUI ที่สามารถเข้าใจได้ง่าย

- วิเคราะห์ข้อมูลจาก ล็อกไฟล์โดยแสดงตามเงื่อนไขต่าง ๆ ได้ตามรายการดังนี้

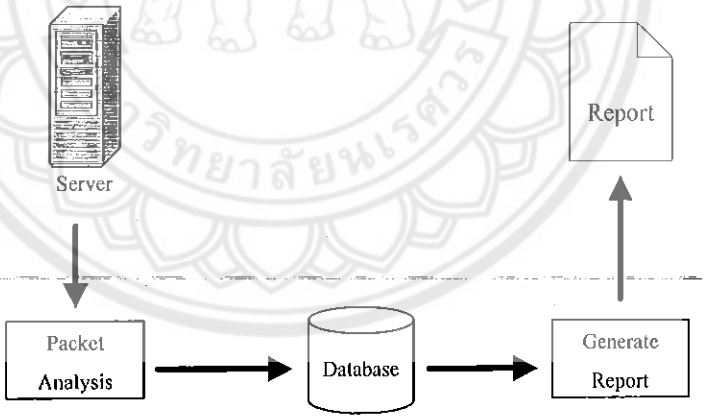
  - รายงานจำนวนคนที่เข้าใช้
  - รายงานจำนวนคนเข้าใช้ที่ไม่ซ้ำ
  - รายงานการเข้าใช้ตาม host
  - รายงานการเข้าใช้ตามจำนวนวัน

- รายงานเพจด้วย เวลาที่เข้าใช้ล่าสุด
- รายงานระบบปฏิบัติการที่เข้าใช้
- รายงานบราวเซอร์ที่เข้าใช้
- สรุปรายงานการเข้าใช้เป็นรายวัน
- สรุปรายงานการเข้าใช้เป็นรายสัปดาห์
- สรุปรายงานการเข้าใช้เป็นรายเดือน

- สามารถค้นหาตามเงื่อนไขที่ต้องการได้
- สามารถบันทึกข้อมูลของรายงานที่ได้ในลักษณะของรายงานเพื่อใช้ในการใช้งานอื่นได้
- สามารถแสดงข้อมูลที่วิเคราะห์นั้นด้วยสื่อที่สามารถเข้าใจและเปรียบเทียบได้ง่าย เช่นในลักษณะของกราฟ เป็นต้น

3.3 ภาพรวมของโปรแกรม

โปรแกรมจะประกอบไปด้วยสามส่วนหลักคือ packet analysis, database และ repor ดังรูปที่ 3.1



รูปที่ 3.1 แสดงโครงสร้างโดยรวมของโปรแกรม

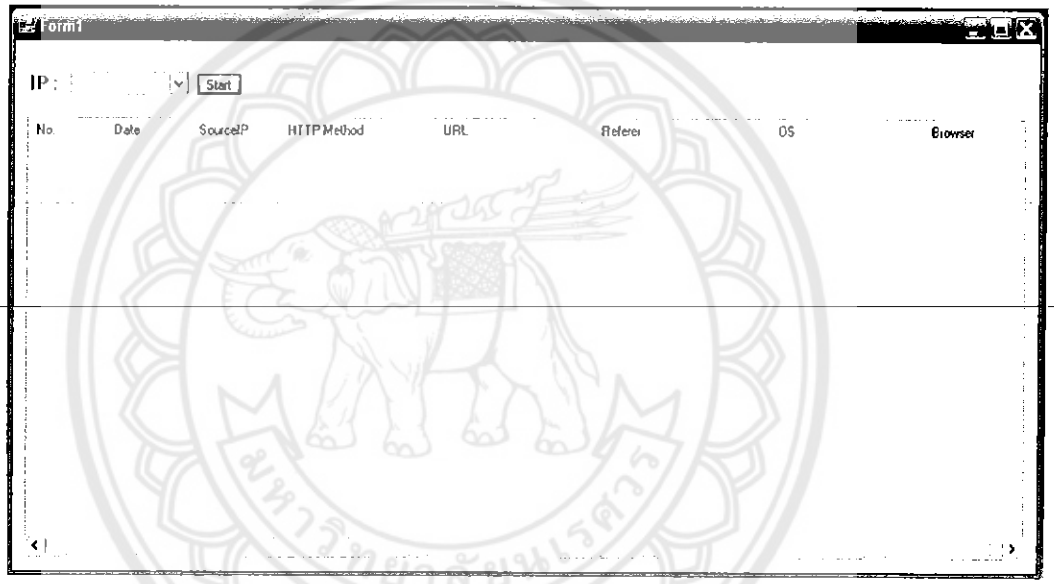
จะทำงานโดย packet analysis นั้นจะทำหน้าที่ในการดักจับแพ็กเก็ตมาจากอีเทอร์เน็ตการ์ด จากนั้นทำการถอดเฮดเดอร์ต่างๆ เพื่อเอาเฉพาะข้อมูลที่ต้องการ แล้วนำข้อมูลที่ได้ไปเก็บไว้ใน database เพื่อทำการแยกประเภทของข้อมูลแต่ละประเภท จากนั้นจึงจะเป็นส่วนของ report จะทำการนำข้อมูลจาก database มาสรุปเป็นสถิติ แสดงผลตามเงื่อนไขต่างๆ ตามที่ต้องการได้ ซึ่งส่วน

ต่างๆ ทั้งหมดจะถูกควบคุมด้วยโปรแกรมซึ่งพัฒนาบน Microsoft Visual Studio 2008 เป็นภาษา C# ผ่าน User Interface โดยการทำงานทั้งหมด

3.4 รายละเอียดแต่ละส่วนของโปรแกรม

3.4.1 โปรแกรมในส่วนวิเคราะห์แพ็กเก็ต (packer analysis)

ในส่วนนี้จะหมายถึง ส่วนที่จะการรวบรวมข้อมูลจากอีเทอร์เน็ตการ์ด และส่วนที่ทำการวิเคราะห์ข้อมูลที่ได้มา ซึ่งจะถูกพัฒนาขึ้นด้วยภาษา C# ซึ่งผู้ใช้งานจะควบคุมการทำงานผ่านทาง User Interface ดังรูปที่ 3.2



รูปที่ 3.2 แสดงหน้าจอ interface ในส่วนวิเคราะห์แพ็กเก็ตของโปรแกรม

หน้าจอของโปรแกรมจะประกอบไปด้วย 2 ส่วนหลักคือ panel และ view ซึ่งมีรายละเอียดดังนี้

1. panel จะประกอบไปด้วย 2 ส่วนคือ

1.1 ช่องสำหรับเลือกอีเทอร์เน็ตการ์ดที่ต้องการ

1.2 start เป็นคำสั่งที่สั่งให้โปรแกรมเริ่มทำงาน

2. view เป็นหน้าจอที่แสดงข้อมูลต่างๆ ที่ได้ผ่านการวิเคราะห์แล้ว

3.4.1.1 เก็บรวบรวมข้อมูล

หลังจากโปรแกรมทำการเก็บรวบรวมแพ็กเก็ตที่ถูกดักจับมาทั้งหมด ก็จะได้ตัวแปรที่เก็บส่วนของเฮดเดอร์และข้อมูลของแต่ละแพ็กเก็ตไว้ จากนั้นก็จะทำการแตกส่วนของแพ็กเก็ตดาต้า

ออกมา ซึ่งสามารถแตกส่วนต่างๆ ของแพ็กเก็ตดาต้าได้ตามลำดับของ OSI Layer ดังนี้

- ส่วนที่ 1 ส่วนของ Ethernet Header จะประกอบด้วยข้อมูลในส่วน เฮดเดอร์ที่สำคัญของเลเยอร์สองหรือ ชั้นอีเทอร์เน็ต

- ส่วนที่ 2 ส่วนของ IP Header จะประกอบด้วยข้อมูลในส่วน เฮดเดอร์ที่สำคัญของเลเยอร์สามหรือ ชั้นเน็ตเวิร์คซึ่งข้อมูลที่สำคัญๆ ได้แก่ หมายเลขไอพีต้นทางหรือปลายทาง ชนิดของโปรโตคอล และความยาวรวมของเฮดเดอร์

- ส่วนที่ 3 ส่วนของ TCP Header จะประกอบด้วยข้อมูลในส่วน เฮดเดอร์ที่สำคัญของเลเยอร์สี่หรือชั้นทรานสปอร์ต ซึ่งข้อมูลที่สำคัญๆ ได้แก่ พอร์ตต้นทางหรือปลายทาง

ส่วนที่ 4 ส่วนของ payload

ซึ่งทั้ง 4 ส่วนสามารถแสดงได้ดังรูปที่ 3.3

รูปที่ 3.3 แสดงการเก็บรวบรวมข้อมูล

หลังจากที่ได้ค่าของพอร์ตต้นทางหรือปลายทางแล้ว เราก็สามารถแยกข้อมูลตามโปรโตคอลที่ต้องการได้

3.4.1.2 วิเคราะห์ข้อมูล

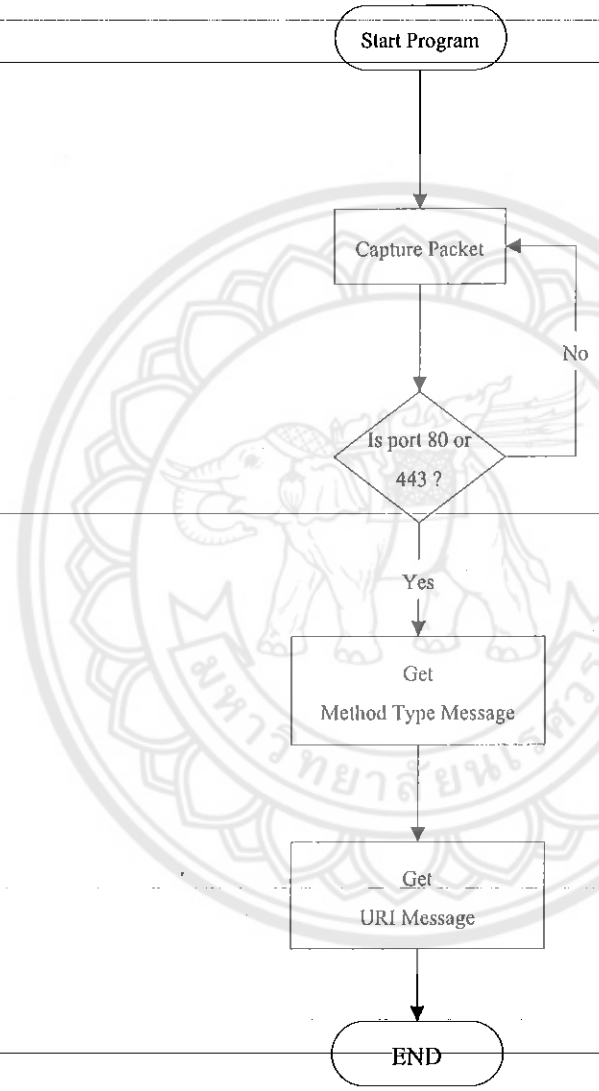
โปรแกรมจะทำการจำแนกแพ็กเก็ตที่ดักจับได้ออกเป็นหมวดหมู่ โดยจะใช้ในส่วนของพอร์ตของปลายทางในเฮดเดอร์ของทีซีพีเลเยอร์ ซึ่งจะสนใจเฉพาะแพ็กเก็ตที่มีพอร์ตปลายทางเป็นพอร์ต 80 หรือ 443 ซึ่งเป็นโปรโตคอล HTTP และ HTTPS

3.4.1.3.1 เก็บรวบรวมข้อมูลของโปรโตคอล HTTP, HTTPS

ในการเรียกใช้งานหรือเข้าสู่เว็บไซต์ใดๆนั้น ในการเรียกหน้าเว็บขึ้นมาจะทำการร้องขอโดยใช้เมสเซจร้องขอไปยังเซิร์ฟเวอร์ตัวอย่างเช่น

GET /generate_204 HTTP/1.1

ในที่นี้หมายถึงผู้ใช้ทำการเรียกใช้เว็บในหน้า generate_204 ขึ้นมา โดยใช้ method “GET” เป็นต้น ดังนั้นการทำงานจะทำการตรวจสอบว่ามีผู้ใช้งานเรียกใช้ในหน้าไหนบ้างและรูปแบบคำสั่งในการเข้ามาใช้งาน method อะไร จากนั้นก็ทำการเก็บ Uniform Resource Identifier (URI) ซึ่งเป็นข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูลในหน้าเว็บไซต์ พร้อมทั้งรูปแบบคำสั่งในการเข้ามาใช้งานมาเก็บไว้ ซึ่งแผนผังการทำงานได้แสดงในรูปที่ 3.4



รูปที่ 3.4 แสดงเก็บรวบรวมข้อมูลของโปรโตคอล HTTP

กระบวนการทำงานจะเริ่มจากการตรวจสอบว่ามีพอร์ตปลายทางเป็น 80 หรือ 443 หรือไม่ ถ้ามีก็ทำการเก็บค่าของรูปแบบคำสั่งในการเข้ามาใช้งาน method พร้อมทั้งค่าที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูลในหน้าเว็บไซต์

3.4.2 ฐานข้อมูล (Database)

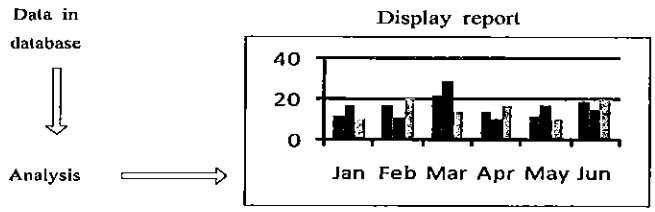
หลังจากที่ทำการเก็บรวบรวมข้อมูล วิเคราะห์ข้อมูลแล้วได้ข้อมูลตามที่ต้องการแล้ว ในส่วนนี้จะทำการออกแบบในส่วนของระบบฐานข้อมูลเพื่อเก็บรายละเอียดต่างๆโดยใช้ SQL Express 2005 เป็นตัวจัดการข้อมูล เพื่อที่จะดึงข้อมูลไปวิเคราะห์ได้สะดวก โดยรายละเอียดของ Standard Format จะแสดงดังตารางที่ 3.1

ตารางที่ 3.1 แสดงรายละเอียดของตาราง Standard Format

ชื่อฟิลด์	รายละเอียด
No	Primary key ของตาราง Standard Format
Data and Time	ข้อมูลแสดงวันเดือนปีและเวลาที่ Server ได้รับ request
SourceIP	ข้อมูลแสดง IP Address ของผู้เข้ามาใช้บริการ
Request Method	ข้อมูลแสดงรูปแบบคำสั่งในการเข้ามาใช้บริการ
URI	ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดู
Reference	ข้อมูลแสดงเว็บเพจที่ให้ลิงค์เชื่อมต่อมาที่เว็บไซต์
OS	ข้อมูลแสดงระบบปฏิบัติการของผู้ใช้บริการ
Browser	ข้อมูลแสดงบราวเซอร์ของผู้ใช้บริการ

3.4.3 สรุปและรายงานผล (Report)

ในส่วนนี้จะมีตัว Generate Report ที่ทำหน้าที่ในการดึงข้อมูลที่เก็บในระบบฐานข้อมูลมาผ่านการ query ด้วยคำสั่ง SQL ในรูปแบบต่างๆเพื่อให้ได้ข้อมูลที่ต้องการ อีกทั้งยังใช้ crystal report ของ Microsoft Visual Studio 2008 ในการสร้างกราฟ หลายรูปแบบ ที่เหมาะสมกับลักษณะของข้อมูลที่จะนำเสนอ เช่น สรุปเป็นรายวัน รายสัปดาห์ ของผู้เข้ามาใช้งาน แล้วสร้างออกมาเป็นรูปกราฟ ดังรูปที่ 3.5



รูปที่ 3.5 แสดงการทำในส่วนสรุปและรายงานผล (Report)

จากรูปที่ 3.5 ในส่วนของการ Analysis ทำหน้าที่ดึงข้อมูลจากฐานข้อมูลนำมาวิเคราะห์และสร้างเป็นรายงาน โดยต่อไปนี้จะเป็นการแสดงภาพโดยรวมของโปรแกรมที่สร้างขึ้นว่าจะสร้างรายงานอะไรบ้างดังต่อไปนี้

1. รายงานตามประเภทของผู้เข้าใช้

   แสดง - ผู้เข้าเยี่ยมชม โดยแสดงเป็น ip (10 อันดับที่มากที่สุด)

   - จำนวนเพจที่เรียกดู

   - จำนวนครั้งในการเข้าเยี่ยมชม

   - เข้าเยี่ยมชมครั้งสุดท้ายเมื่อไร

2. รายงานตามลักษณะการเยี่ยมชม

   แสดง - browser ที่ใช้งาน

   - OS ที่ใช้งาน

   - จำนวนการเข้าเยี่ยมชม

   - เปอร์เซนต์ของจำนวนการเข้าเยี่ยมชม

3. รายงานที่วิเคราะห์จากผลลัพธ์การเข้าเยี่ยมชมเว็บไซต์

   แสดง - จำนวนเพจที่เรียกดู

   - จำนวนการเข้าเยี่ยมชม

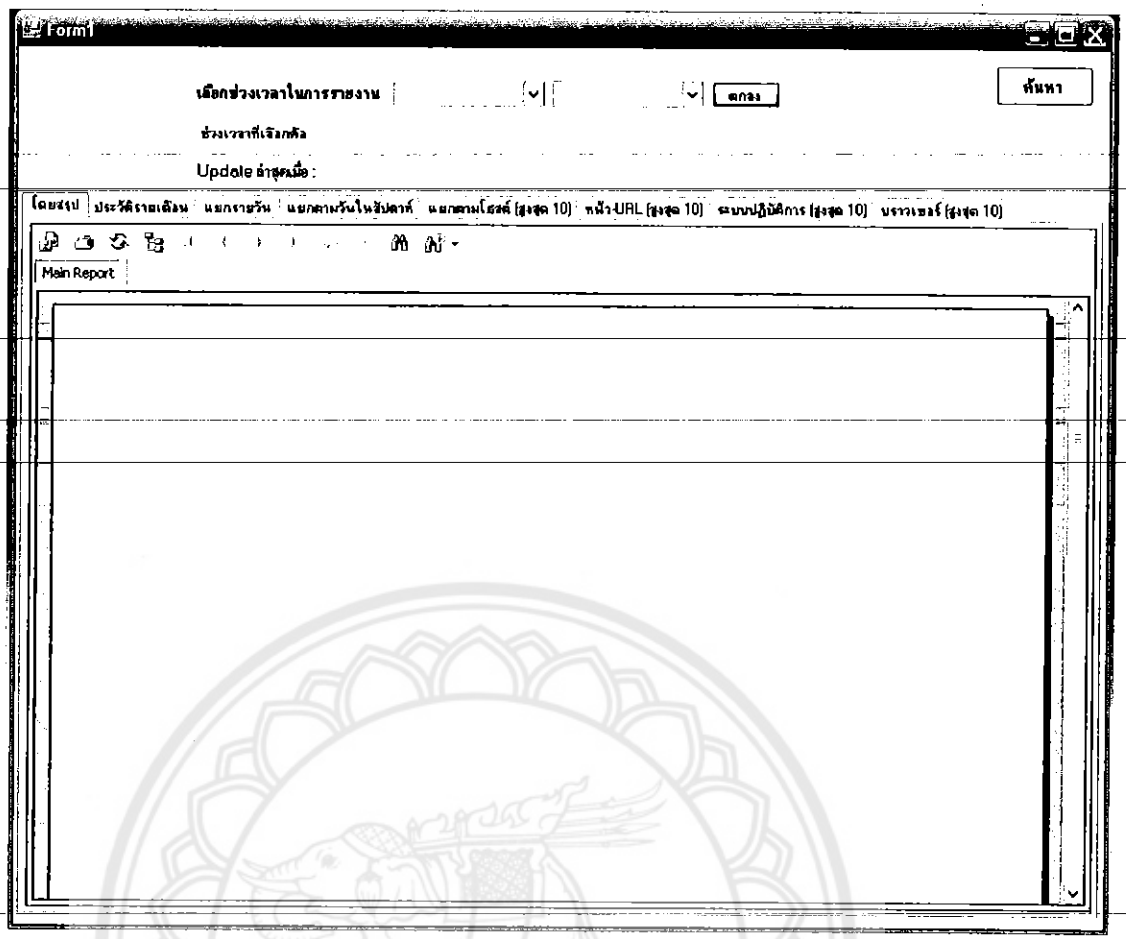
4. รายงานสรุปประจำวัน ประจำสัปดาห์และประจำเดือนในการเข้าเยี่ยมชม

   แสดง - จำนวนผู้เข้าเยี่ยมชม

   - จำนวนเพจที่เรียกดู

   - จำนวนการเข้าเยี่ยมชม

ซึ่งจะถูกพัฒนาขึ้นด้วยภาษา C# ซึ่งผู้ใช้งานจะควบคุมการทำงานผ่านทาง User Interface ดังรูปที่ 3.6



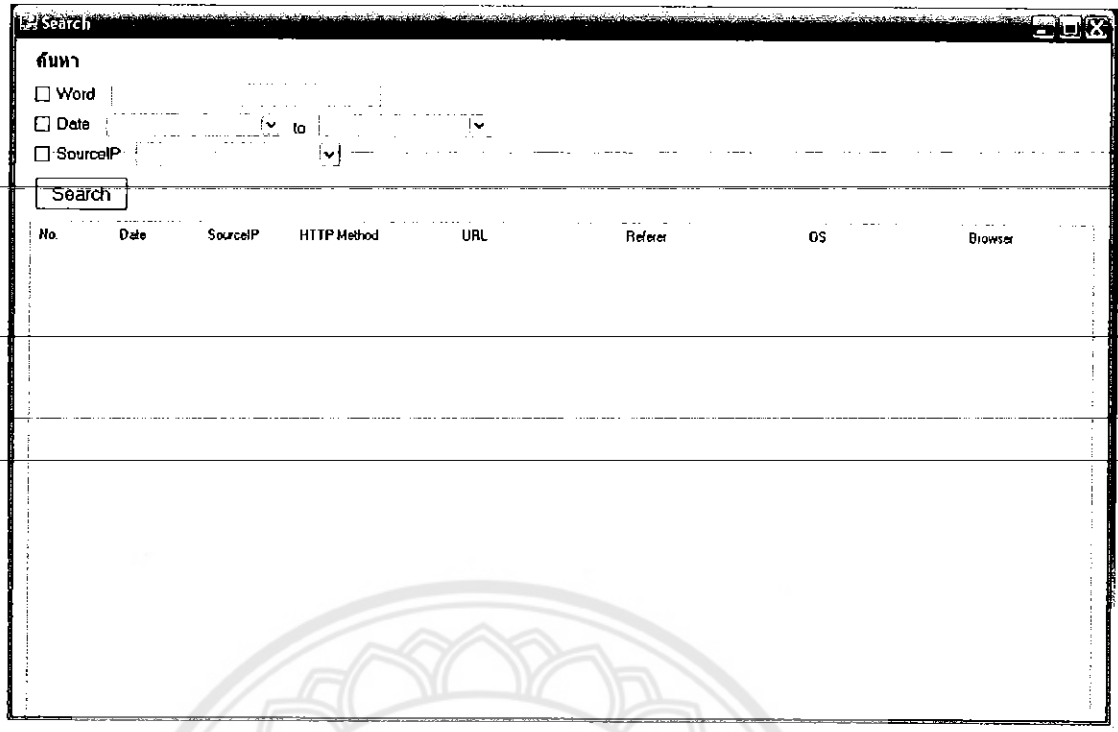
รูปที่ 3.6 แสดงหน้าจอ interface ในส่วนสรุปและรายงานผล (Report)

หน้าจอของโปรแกรมจะประกอบไปด้วย 4 ส่วนหลักคือ panel, tab, toolbar และ reportviewer ซึ่งมีรายละเอียดดังนี้

1. panel จะประกอบด้วย 2 ส่วน คือ

1.1 ช่องสำหรับเลือกช่วงเวลาในการรายงาน ซึ่งจะเลือกเป็นเดือน และปี พ.ศ. พร้อมทั้งแสดงช่วงเวลาที่เลือก และข้อมูลที่อัพเดตครั้งล่าสุดในฐานข้อมูล

1.2 ค้นหาเป็นคำสั่งที่ใช้ในการค้นหาข้อมูลที่ต้องการค้นหา ผ่านทาง User Interface ซึ่งจะประกอบด้วย 2 ส่วนคือ panel และ viewer ดังรูปที่ 3.7



รูปที่ 3.7 แสดงหน้าจอ interface ในส่วนการค้นหา

รายละเอียดในหน้าจอ interface ในส่วนการค้นหา สามารถอธิบายได้ดังนี้

1.2.1 panel เป็นส่วนที่เลือกเงื่อนไขในการค้นหาข้อมูลซึ่งจะ ประกอบด้วย 4 ส่วนคือ

- word เป็นคำสั่งในการค้นหาคำที่ต้องการค้นหา
- date เป็นคำสั่งในการเลือกช่วงเวลาที่ทำการค้นหา
- source ip เป็นคำสั่งในการเลือกไอพีแอดเดรสที่ต้องการค้นหา
- search เป็นคำสั่งในการเริ่มค้นหาข้อมูล

1.2.2 viewer เป็นส่วนที่แสดงผลการค้นหา

2. tab เป็นส่วนที่สรุปผลและแสดงผลตามเงื่อนไขที่กำหนด

3. toolbar มี tool button 5 ปุ่มดังนี้

- Export Report เป็นคำสั่งในการเซฟไฟล์
- Print Report เป็นคำสั่งในการปริ้นรายงาน
- Refrese เป็นคำสั่งในการรีเฟรสข้อมูล
- Find Text เป็นคำสั่งในการค้นหาคำที่ต้องการในรายงาน
- Zoom เป็นคำสั่งในการขยายหรือย่อรายงาน

4. reportviewer เป็นส่วนที่แสดงผลรายงาน

เนื่องจากเพื่อความสะดวกที่ผู้อื่นจะทำการศึกษาซอฟต์แวร์ที่พัฒนาขึ้นมา ในบทนี้ได้อธิบายสิ่งต่างๆ ที่จำเป็นในการพัฒนาดังนี้

1. ความต้องการของระบบ (Requirement Specification)
2. ขอบเขตของระบบ
3. การออกแบบซอฟต์แวร์ โดยใช้ UML Diagram เป็นหลัก

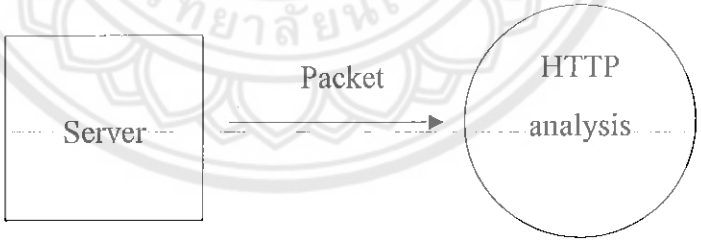
3.5 ความต้องการของระบบ (Requirement Specification)

โปรแกรมจัดการล็อคไฟล์ มีความต้องการต่างๆของระบบดังนี้

- โปรแกรมสามารถจัดเก็บล็อกไฟล์ได้อย่างครบถ้วนตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของเว็บเซิร์ฟเวอร์กำหนดไว้ได้
- โปรแกรมสามารถนำข้อมูลที่ทำการจัดเก็บไปสร้างเป็นรายงานในรูปแบบต่างๆตามความเหมาะสมได้

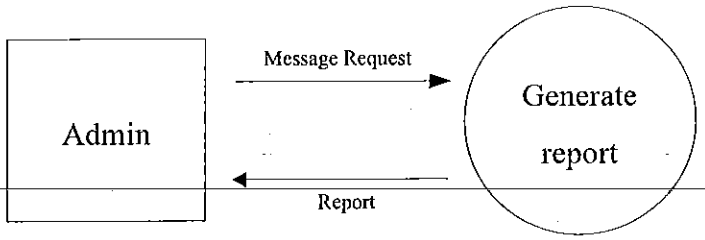
3.6 ขอบเขตของระบบ

การทำงานของระบบจะแบ่งออกเป็น 2 ส่วนด้วยกันคือ ส่วนแรกจะทำงานในฝั่งของเซิร์ฟเวอร์ ซึ่งสามารถแสดงเป็น Context Diagram ของระบบดังรูปที่ 3.8



รูปที่ 3.8 แสดง Context Diagram ของระบบ ฝั่งเซิร์ฟเวอร์

สำหรับการทำงานคือ เซิร์ฟเวอร์ทำการส่งแพ็ตเก็ตเข้าสู่ระบบ โปรแกรมทางฝั่งเซิร์ฟเวอร์ก็จะทำการรวบรวมข้อมูลและวิเคราะห์เพื่อเอาเฉพาะข้อมูลที่ต้องการเพื่อทำการจัดเก็บลงฐานข้อมูล สำหรับส่วนที่ 2 จะทำงานอยู่ฝั่งผู้ดูแลระบบซึ่งสามารถแสดงเป็น Context Diagram ของระบบดังรูปที่ 3.9



รูปที่ 3.9 แสดง Context Diagram ของระบบ ฝั่งผู้ดูแลระบบ

สำหรับการทำงานคือ ผู้ดูแลระบบทำการส่งคำร้องขอ ไปสู่ระบบ ระบบจะทำการสร้างรายงาน แล้วก็ส่งรายงานตามที่ร้องขอเข้ามาให้กับผู้ดูแลระบบ

3.7 การออกแบบซอฟต์แวร์

สำหรับการออกแบบซอฟต์แวร์จะคำนึงถึง 4 มุมมองซึ่งแสดงได้ดังตารางที่ 3.2

ตารางที่ 3.2 แสดงมุมมองในการออกแบบซอฟต์แวร์

	Dynamic	Static
External	Use cases and Sequence diagrams	Component diagrams
Internal	Activity diagrams	Class diagrams

โดยในแต่ละมุมมองมีความหมายดังต่อไปนี้

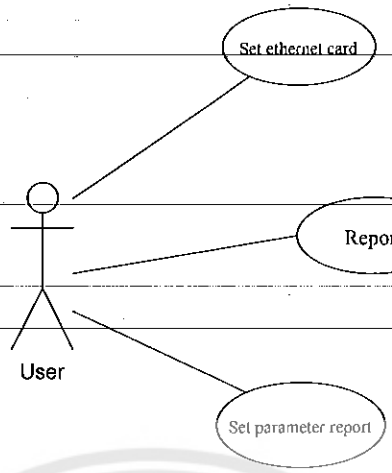
External-Dynamic จะแสดงการติดต่อกับภายนอก เช่น บริการต่างๆ ข้อความ

External-Static จะแสดงโครงสร้างและส่วนประกอบต่างๆ อย่างคร่าวๆ

Internal-Dynamic จะแสดงพฤติกรรมของระบบและสถานะต่างๆ ของระบบ

Internal-Static จะแสดงโครงสร้างภายในของระบบ

3.7.1 ยูสเคส ไดอะแกรม (Use Cases Diagram)



รูปที่ 3.10 แสดง Use Cases Diagram

รายละเอียดของยูสเคสไดอะแกรมสามารถแสดงได้ดังตารางที่ 3.3

ตารางที่ 3.3 แสดงรายละเอียดของตารางยูสเคสไดอะแกรมของโปรแกรม

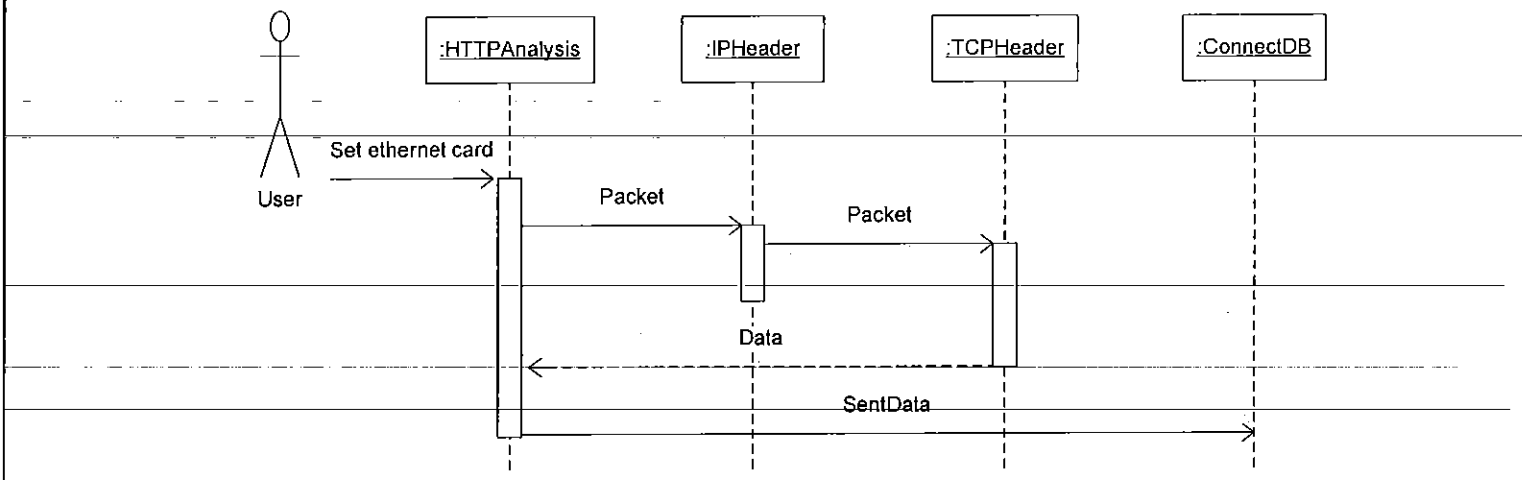
ยูสเคส	คำอธิบาย
Set ethernet card	เลือกอีเทอร์เน็ตการ์ดของเซิร์ฟเวอร์
Report	ดูรายงานที่ทำการคำนวณเรียบร้อยแล้ว
Set parameter report	กำหนดค่าเริ่มต้นของรายงาน เช่น ช่วงเวลาที่รายงาน เป็นต้น

3.7.2 ซีเควน ไดอะแกรม (Sequence Diagram)

ลำดับการทำงานของโปรแกรมจะแบ่งออกเป็น 2 ส่วน ดังนี้

3.7.2.1 โปรแกรมฝั่งเซิร์ฟเวอร์

สำหรับลำดับการทำงานของโปรแกรมฝั่งเซิร์ฟเวอร์สามารถแสดงได้ดังรูปที่ 3.11



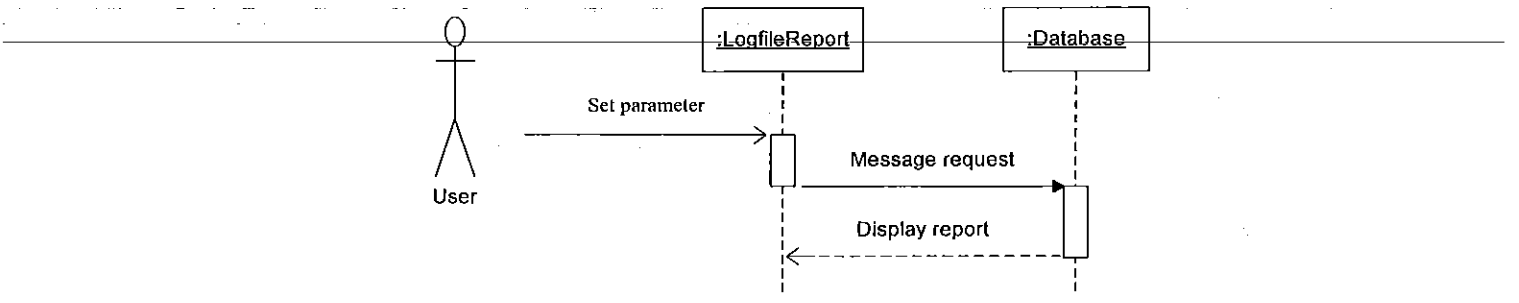
รูปที่ 3.11 แสดง Sequence Diagram ของโปรแกรมฝั่งเซิร์ฟเวอร์

จากรูปที่ 3.11 สามารถอธิบายลำดับการทำงานได้ดังนี้

เริ่มจากการที่ผู้ใช้ทำการเรียกโปรแกรมขึ้นมา จากนั้นจึงทำการเลือกอีเทอร์เน็ตการ์ดตามที่ต้องการ เมื่อได้อีเทอร์เน็ตการ์ดตามที่ต้องการแล้ว ผู้ใช้จึงสั่งให้โปรแกรมเริ่มทำงาน โปรแกรมก็จะส่งทำการส่ง packet ให้กับ IPHeader เพื่อทำการถอด IPHeader ออกมา จากนั้นก็จะทำการส่งต่อไปยัง TCPHeader เพื่อทำการถอดในส่วนของ TCPHeader ออกมา จากนั้นก็จะส่งข้อมูลไปให้กับ HTTPAnalysis เพื่อทำการวิเคราะห์และกรองเอาเฉพาะข้อมูลที่ต้อง แล้วก็จะทำการเก็บข้อมูลนั้นเข้าสู่ฐานข้อมูล

3.7.2.2 โปรแกรมฝั่งผู้ดูแลระบบ

สำหรับลำดับการทำงานของโปรแกรมฝั่งผู้ดูแลระบบสามารถแสดงได้ดังรูปที่ 3.12



รูปที่ 3.12 แสดง Sequence Diagram ของโปรแกรมฝั่งผู้ดูแลระบบ

จากรูปที่ 3.12 สามารถอธิบายลำดับการทำงานได้ดังนี้

เริ่มจากผู้ใช้ทำการเรียกโปรแกรมขึ้นมา จากนั้นทำการกำหนดค่าช่วงเวลาในการรายงาน เมื่อได้ช่วงเวลาที่ต้องการแล้ว ผู้ใช้ก็ทำการสั่งให้โปรแกรมเริ่มทำงาน จากนั้นโปรแกรมก็ทำการส่งค่าที่ผู้ใช้ทำการกำหนดไปยังระบบฐานข้อมูล จากนั้นระบบฐานข้อมูลก็ทำการสร้างรายงานแล้วส่งให้กับโปรแกรม LogFileReport

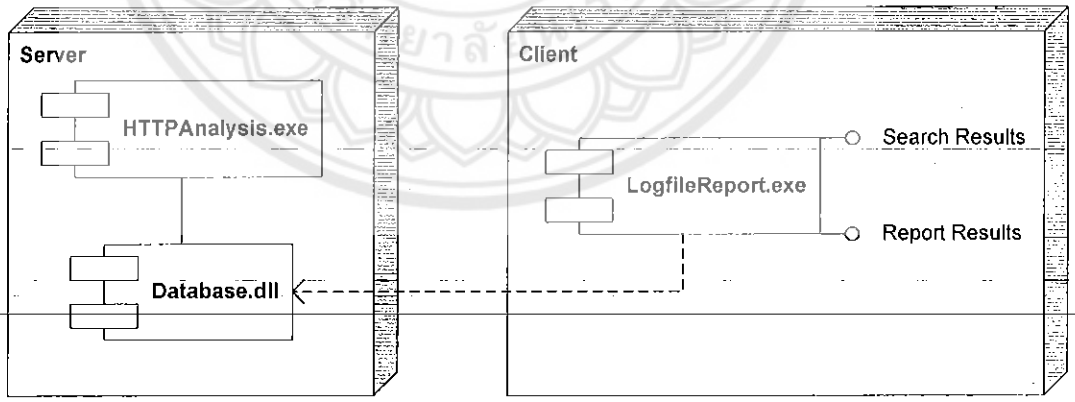
3.7.3 คอมโพเนนท์ ไดอะแกรม (Component Diagram)

สำหรับคอมโพเนนต์ ของโปรแกรมจะประกอบด้วยกันอยู่ 2 โหนดดังนี้

- โหนดของเซิร์ฟเวอร์ จะประกอบด้วยคอมโพเนนต์ของ HTTP Analysis.exeและคอมโพเนนต์ของ Database.dll ซึ่งความสัมพันธ์กันคือ คอมโพเนนต์ของ HTTP Analysis.exe จะทำการรวบรวมข้อมูลและวิเคราะห์ข้อมูลจากอีเทอร์เน็ตการ์ด แล้วนำข้อมูลไปเก็บไว้ในคอมโพเนนต์ของ Database.dll

- โหนดของไคลเอ็นต์ จะประกอบด้วยคอมโพเนนต์ของ Log File Report.exe และ interface ในส่วนของการแสดงรายงานและการค้นหา

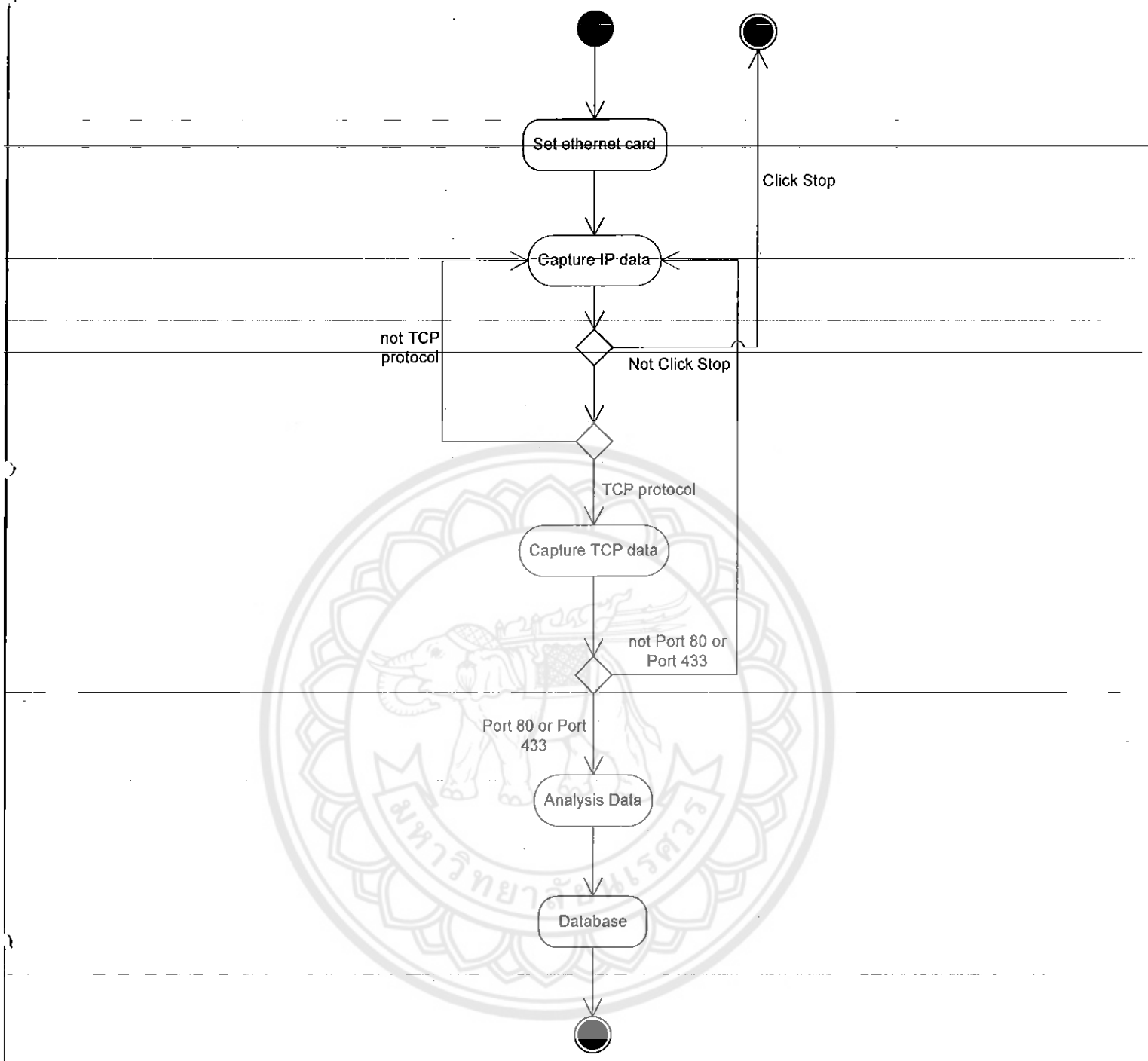
สำหรับความสัมพันธ์ระหว่างโหนดของเซิร์ฟเวอร์กับโหนดของไคลเอนต์ คือโหนดของไคลเอ็นต์ทำการสร้างรายงาน โดยการดึงข้อมูลจากคอมโพเนนต์ของ database.dll ในโหนดของเซิร์ฟเวอร์ ซึ่งสามารถแสดงได้ดังรูปที่ 3.13



รูปที่ 3.13 แสดง Component Diagram

3.7.4 แอคทีวิตี ไดอะแกรม (Activity Diagram)

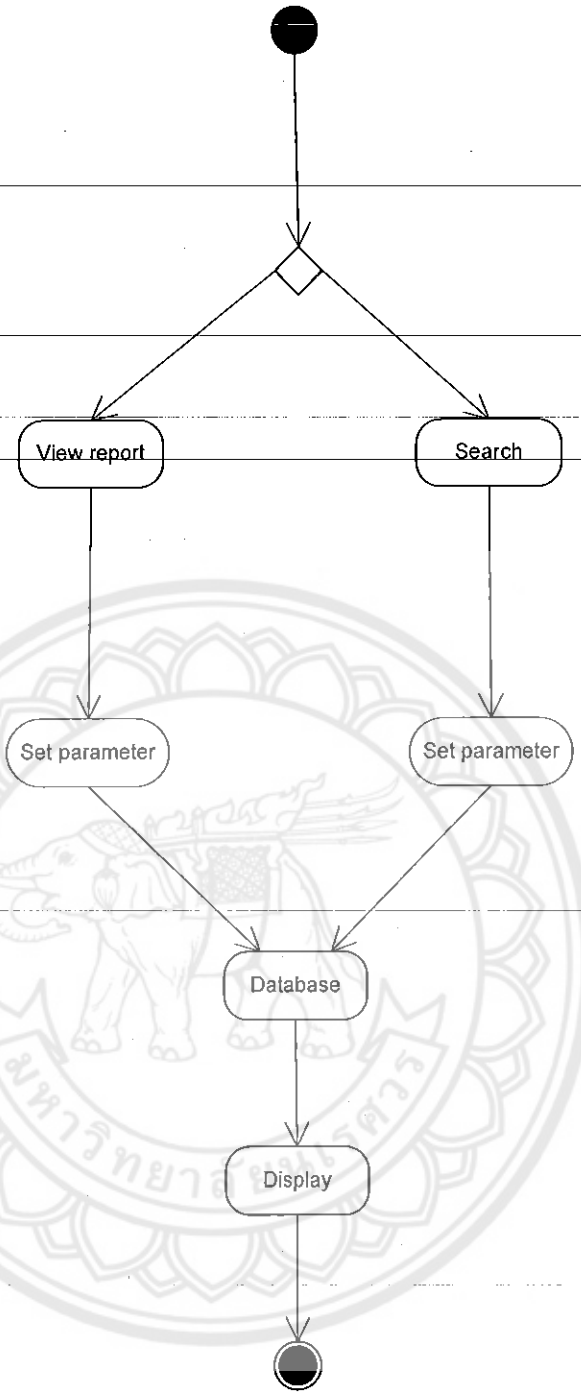
สำหรับกิจกรรมต่างๆ ในโปรแกรมแบ่งออกเป็น 2 ส่วนดังนี้



รูปที่ 3.14 แสดง Activity Diagram ของโปรแกรมฝั่งเซิร์ฟเวอร์

จากรูปที่ 3.14 สามารถอธิบายรายละเอียดการทำงานตาม Activity Diagram อธิบายได้ดังนี้

ผู้ใช้ทำการเลือกอีเทอร์เน็ตการ์ด จากนั้นก็ทำการวิเคราะห์ข้อมูล เพื่อคัดกรองเอาเฉพาะข้อมูลที่ต้องการคือข้อมูลที่มีการร้องขอมายังพอร์ต 80 หรือ 443 เมื่อได้เขียนมูลที่ต้องการแล้วก็จะส่งไปเก็บไว้ที่ฐานข้อมูล



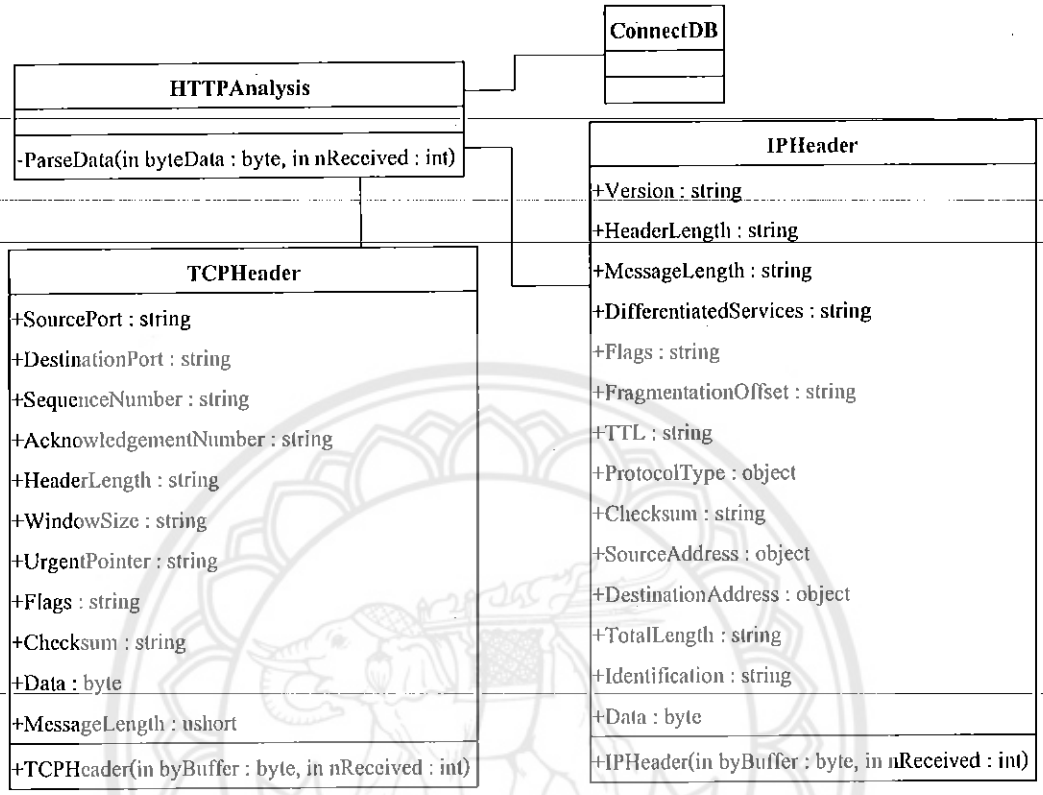
รูปที่ 3.15 แสดง Activity Diagram ของโปรแกรมฝั่งผู้ดูแลระบบ

จากรูปที่ 3.15 สามารถอธิบายรายละเอียดการทำงานตาม Activity Diagram อธิบายได้ดังนี้

ผู้ใช้ทำการเลือกว่าจะทำการเรียกดูรายงานหรือจะทำการค้นหาข้อมูล จากนั้นก็ทำการกำหนดค่าที่ต้องการแล้ว ฐานข้อมูลก็จะทำการสร้างผลออกมาแสดง

3.7.5 คลาส ไดอะแกรม (Class Diagram)

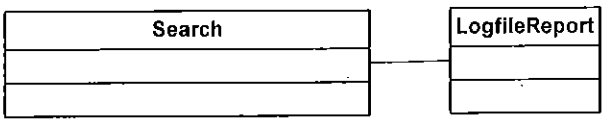
คลาสไดอะแกรมนั้นจะแบ่งออกเป็น 2 ส่วนดังนี้



รูปที่ 3.16 แสดง Class Diagram ของ HTTP Analysis

รายละเอียดของ Class diagram ของ HTTP Analysis อธิบายได้ดังนี้

1. HTTPAnalysis ทำหน้าที่ดักจับแพ็คเก็ต กรองข้อมูล และส่งข้อมูลลงดาต้าเบส
2. IPHeader ทำหน้าที่กรองข้อมูลในส่วนของ IPHeader
3. ConnectDB ทำหน้าที่ติดต่อดาต้าเบส
4. TCPHeader ทำหน้าที่กรองข้อมูลในส่วนของ TCPHeader



รูปที่ 3.17 แสดง Class Diagram ของ Log file report

รายละเอียดของ Class diagram ของ Log file report อธิบายได้ดังนี้

1. LogfileReport	ทำหน้าที่แสดงreport ตามที่ต้องการ
2. Search	ทำหน้าที่ค้นหาข้อมูล

บทที่ 4

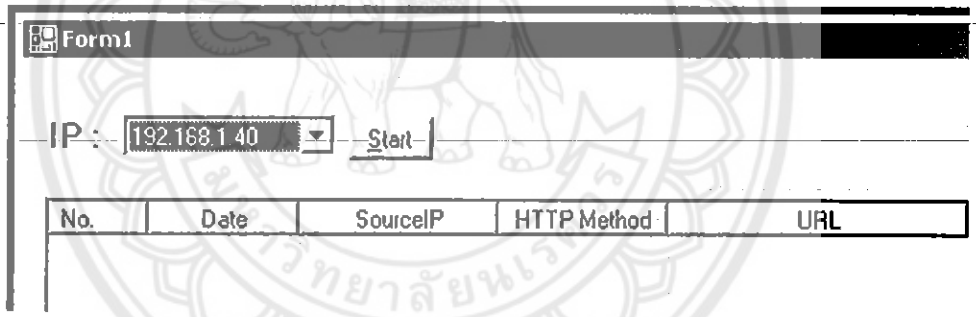
ผลการทดลอง

ในบทนี้จะกล่าวถึงรายละเอียดต่าง ๆ ของโปรแกรม การติดตั้งและใช้งาน การทำงานของโปรแกรม ซึ่งจะแบบการทำงานออกเป็น 2 ส่วนดังนี้

- ฝั่งเซิร์ฟเวอร์จะทำงานโดยทำการรวบรวมข้อมูล วิเคราะห์ข้อมูล และจัดเก็บข้อมูลลงฐานข้อมูล
- ฝั่งผู้ใช้หรือผู้ดูแลระบบจะทำงานโดยทำดึงข้อมูลจากฐานข้อมูลมาสร้างรายงาย

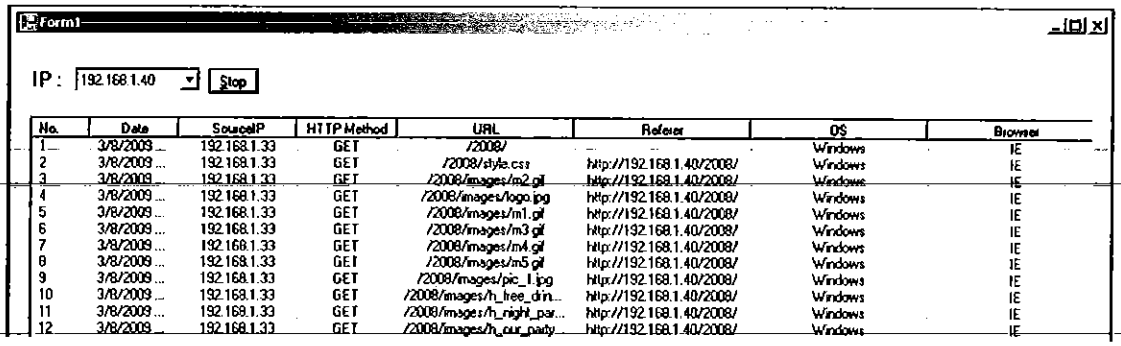
4.1 การใช้งานฝั่งเซิร์ฟเวอร์

โปรแกรมที่ได้พัฒนามานี้คือ HTTP Analysis ทำเป็นโปรแกรมที่ทำงานอยู่ฝั่งเซิร์ฟเวอร์ ซึ่งเมื่อผู้ใช้ทำการเรียกโปรแกรมขึ้นมาจะต้องการทำเลือกอีเทอร์เน็ตการ์ดที่ต้องการ ดังรูปที่ 4.1



รูปที่ 4.1 แสดงการเลือกอีเทอร์เน็ตการ์ดของเซิร์ฟเวอร์

เมื่อผู้ใช้ทำการเลือกอีเทอร์เน็ตการ์ดของเซิร์ฟเวอร์ที่ต้องการแล้ว ก็ทำการกด Start เพื่อให้โปรแกรมเริ่มทำงาน จากนั้นโปรแกรมจะทำการรวบรวมข้อมูลจากอีเทอร์เน็ตการ์ด แล้วทำการวิเคราะห์ข้อมูลเพื่อกรองเอาเฉพาะข้อมูลที่ต้องการ ดังรูปที่ 4.2



รูปที่ 4.2 แสดงการทำงานของโปรแกรม HTTP Analysis

หลังจากที่โปรแกรมได้ทำการคัดกรองข้อมูลที่ต้องการแล้ว จากนั้นก็ทำการจัดเก็บข้อมูลลงสู่ฐานข้อมูลที่ได้ทำการเตรียมไว้ ซึ่งข้อมูลที่ทำการจัดเก็บในส่วนนี้จะเป็นการระบุล็อกที่เกิดขึ้นให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของผู้ให้บริการเว็บเซิร์ฟเวอร์ ซึ่งประกอบด้วย

- ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ คือข้อมูลทั้งหมดที่ทำการจัดเก็บ

- ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ คือข้อมูลในส่วนของ Date

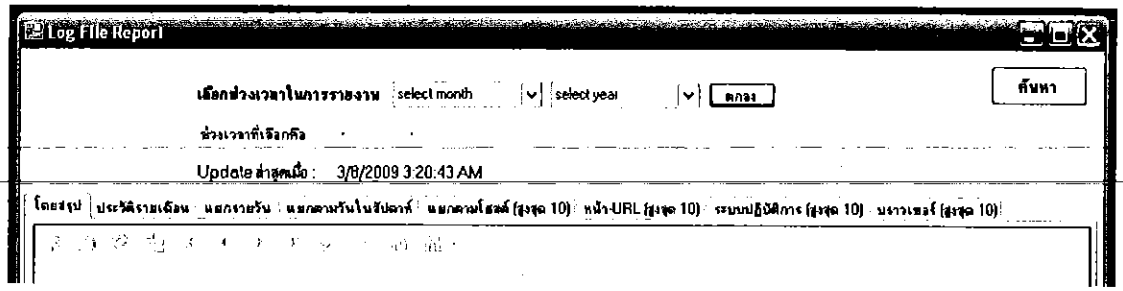
- ข้อมูลหมายเลขอินเตอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น คือข้อมูลในส่วนของ SourceIP

- ข้อมูลคำสั่งการใช้งานระบบ คือข้อมูลในส่วนของ HTTP Method

- ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพ็จ คือข้อมูลในส่วนของ URL

4.2 การใช้งานฝั่งผู้ดูแลระบบ

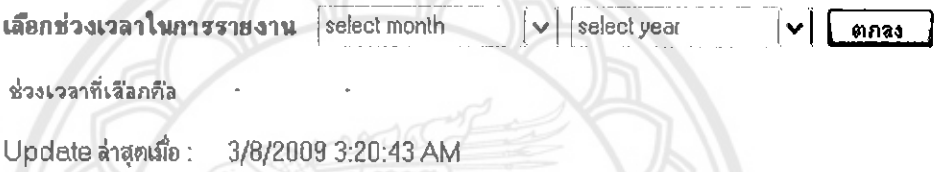
โปรแกรมที่ได้พัฒนามานี้คือ Log File Report เป็นโปรแกรมที่ทำงานอยู่ฝั่งผู้ดูแลระบบ ซึ่งเมื่อผู้ใช้ทำการเรียกโปรแกรมขึ้นมาจะมีหน้า interface ดังรูปที่ 4.3



รูปที่ 4.3 แสดงหน้า interface ของโปรแกรม Log File Report

ในหน้า interface ของโปรแกรม Log File Report จะแบ่งออกเป็น 3 ส่วนดังนี้

1. ส่วนที่ 1 ดังรูปที่ 4.4



รูปที่ 4.4 แสดงหน้า interface ในส่วนที่ 1

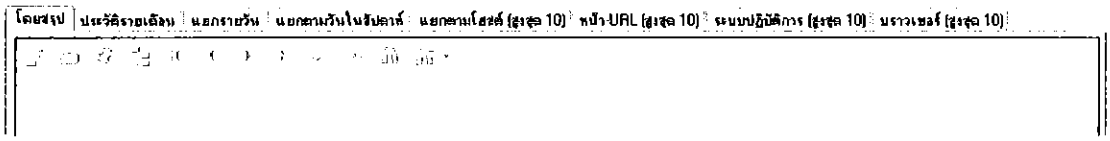
สำหรับส่วนที่ 1 นี้ จะเป็นส่วนที่ทำการกำหนดช่วงระยะเวลาที่ทำการวิเคราะห์และแสดงผลออกมา โดยเลือกเดือนและปี

2. ส่วนที่ 2 ดังรูปที่ 4.5

รูปที่ 4.5 แสดงหน้า interface ในส่วนที่ 2

สำหรับส่วนที่ 2 นี้ จะเป็นส่วนที่ทำหน้าในการค้นหาข้อมูลต่างๆ ตามที่ต้องการ

3. ส่วนที่ 3 ดังรูปที่ 4.6

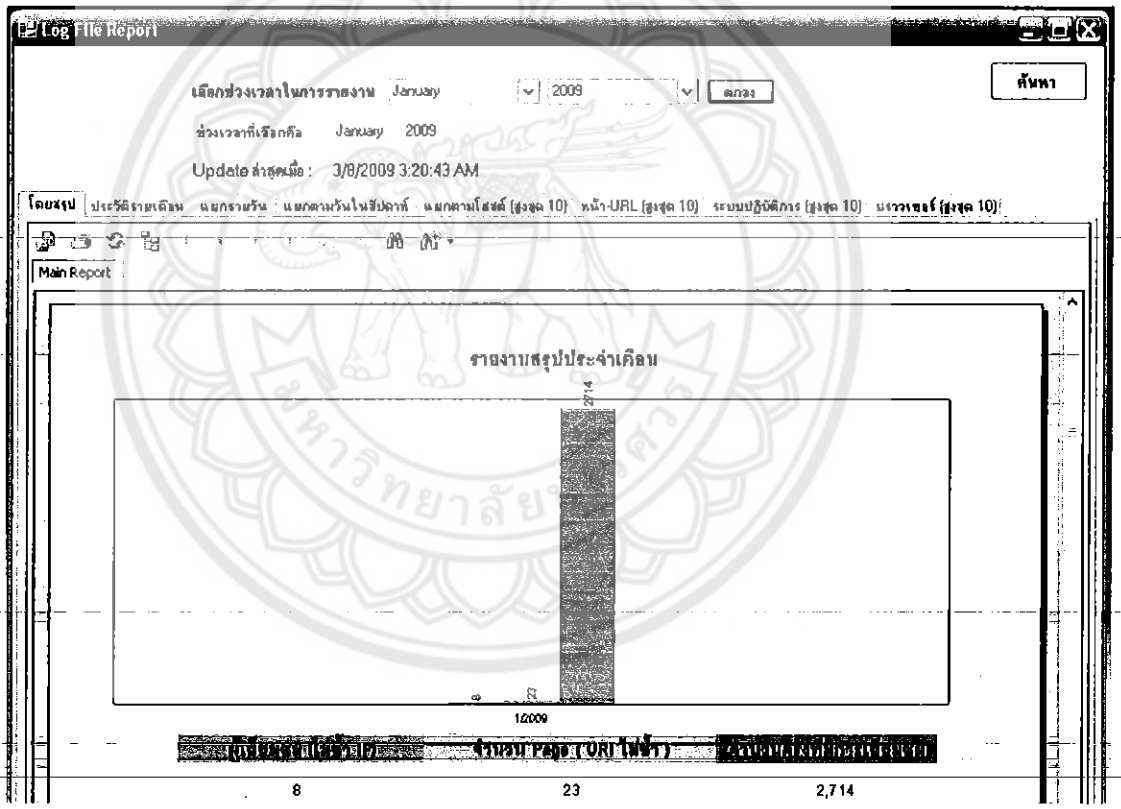


รูปที่ 4.6 แสดงหน้า interface ในส่วนที่ 3

สำหรับส่วนที่ 3 นี้ จะเป็นส่วนที่แสดงรายงานออกมา โดยจะมีแทปให้เลือกว่าจะดูรายงานที่วิเคราะห์ตามเงื่อนไขต่างๆ

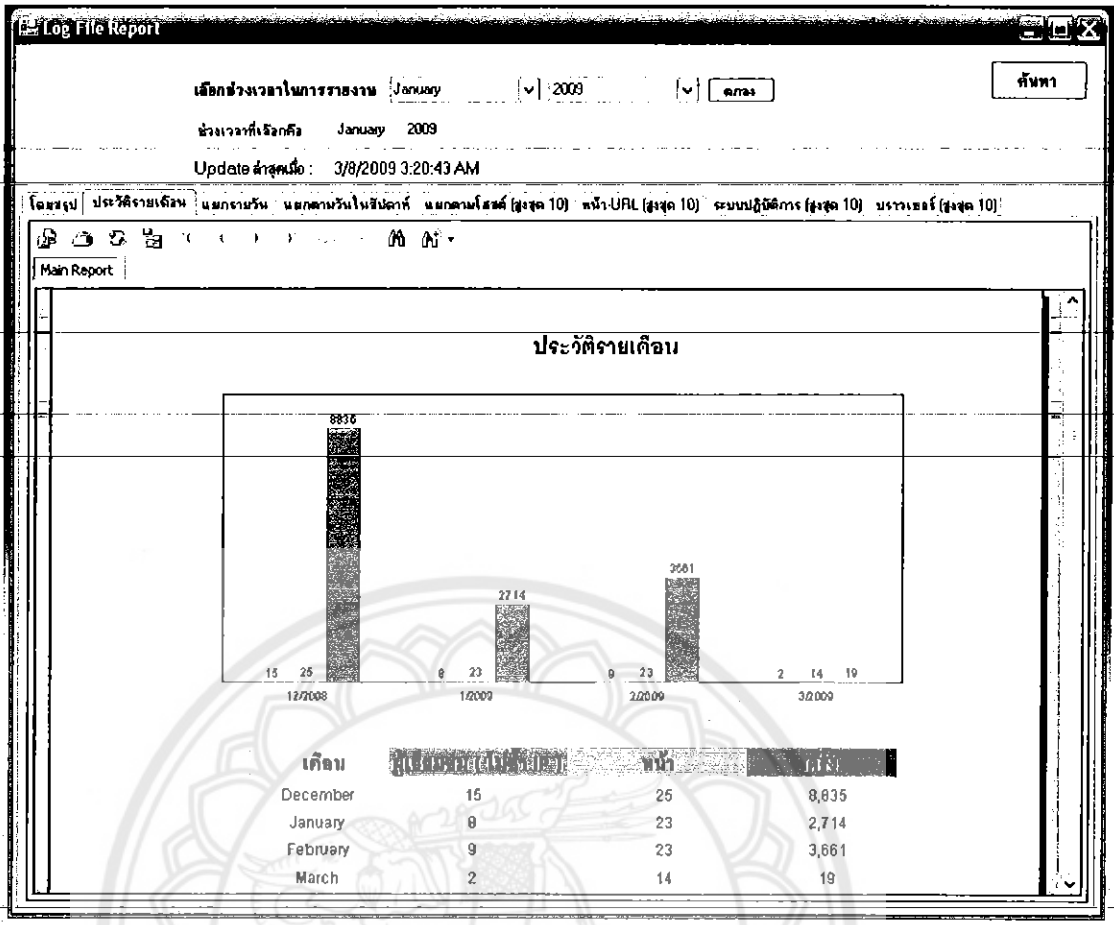
4.2.1 แสดงผลการรายงาน

หลังจากที่ผู้ใช้ทำการกำหนดช่วงระยะเวลาที่ทำการวิเคราะห์และแสดงผลออกมา โดยเลือกเดือนและปีแล้ว จะแสดงผลดังรูปที่ 4.7



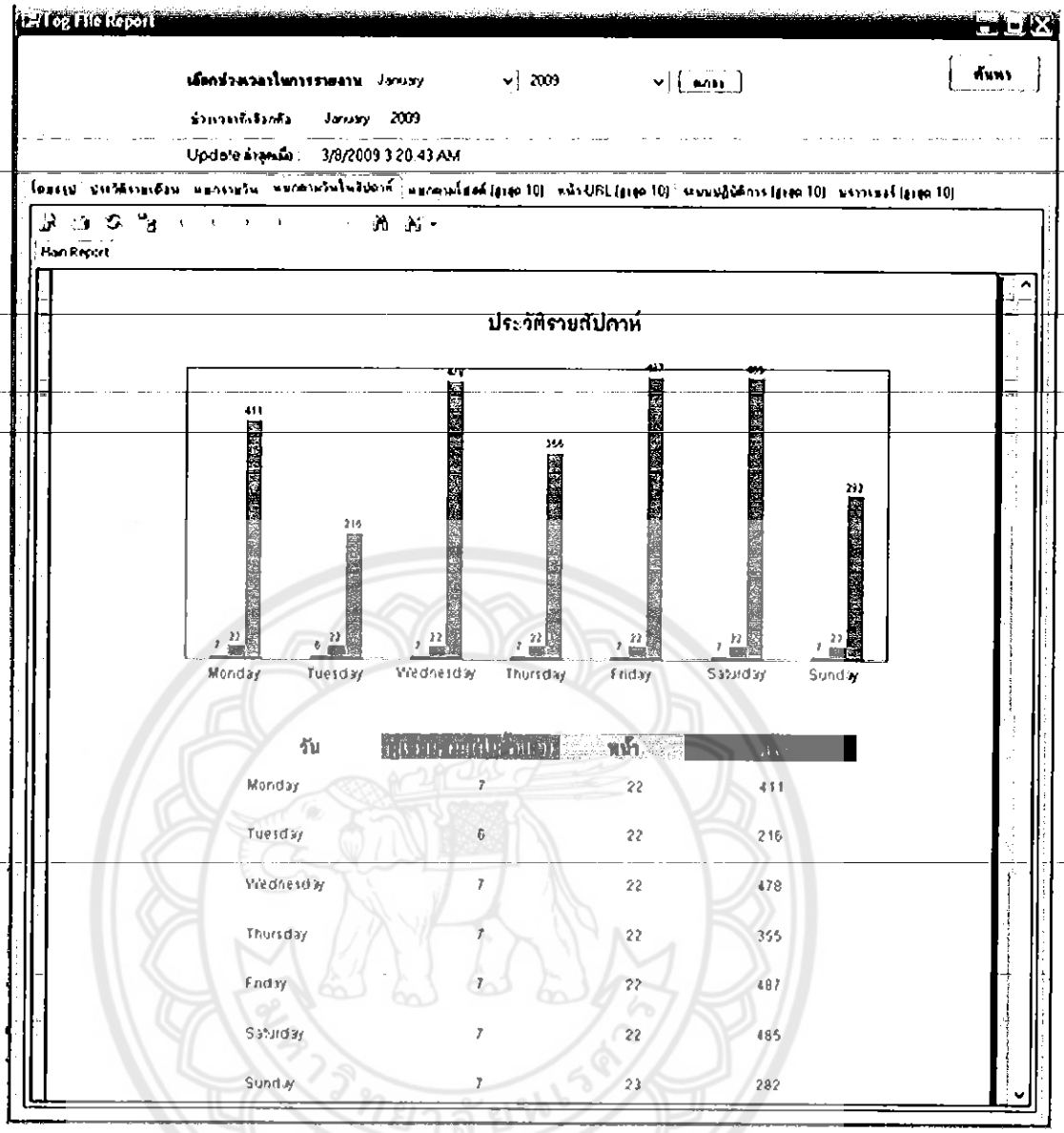
รูปที่ 4.7 แสดงผลการรายงานโดยสรุปประจำเดือน

จากรูปที่ 4.7 เป็นการแสดงโดยสรุปประจำเดือนมกราคม ปี 2009 โดยจะแสดงผู้เยี่ยมชม (ไม่ซ้ำ IP) จำนวนหน้าที่ทำการเรียกดู และจำนวนครั้งที่ทำการเข้ามา



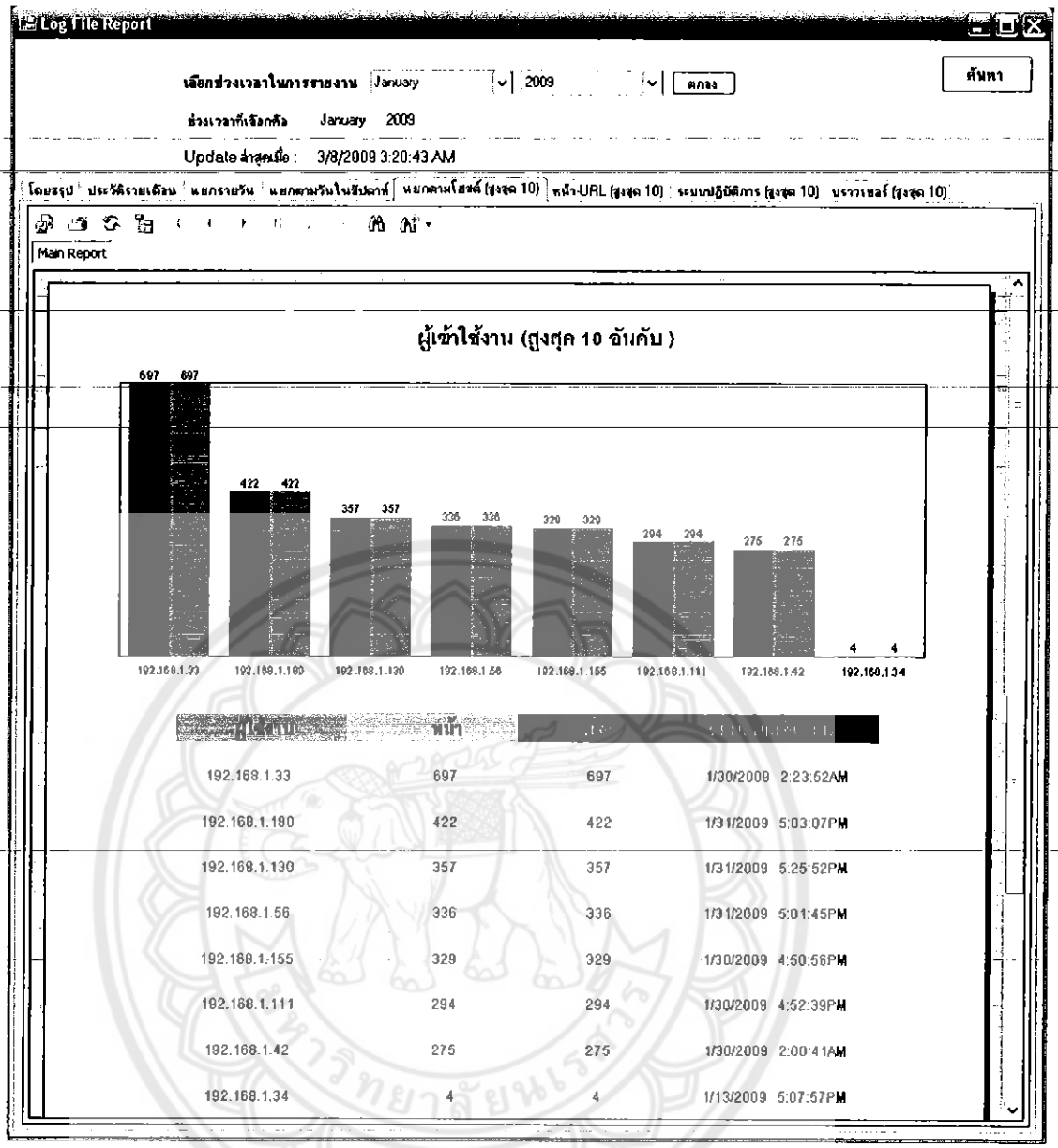
รูปที่ 4.8 แสดงผลการรายงานประวัติรายเดือน

จากรูปที่ 4.8 เป็นการแสดงที่วิเคราะห์ตามประวัติแต่ละเดือน โดยจะ**แสดงประวัติของผู้เยี่ยมชม** (ไม่ซ้ำ IP) จำนวนหน้าที่ทำการเรียกดู และจำนวนครั้งที่ทำการเข้ามา



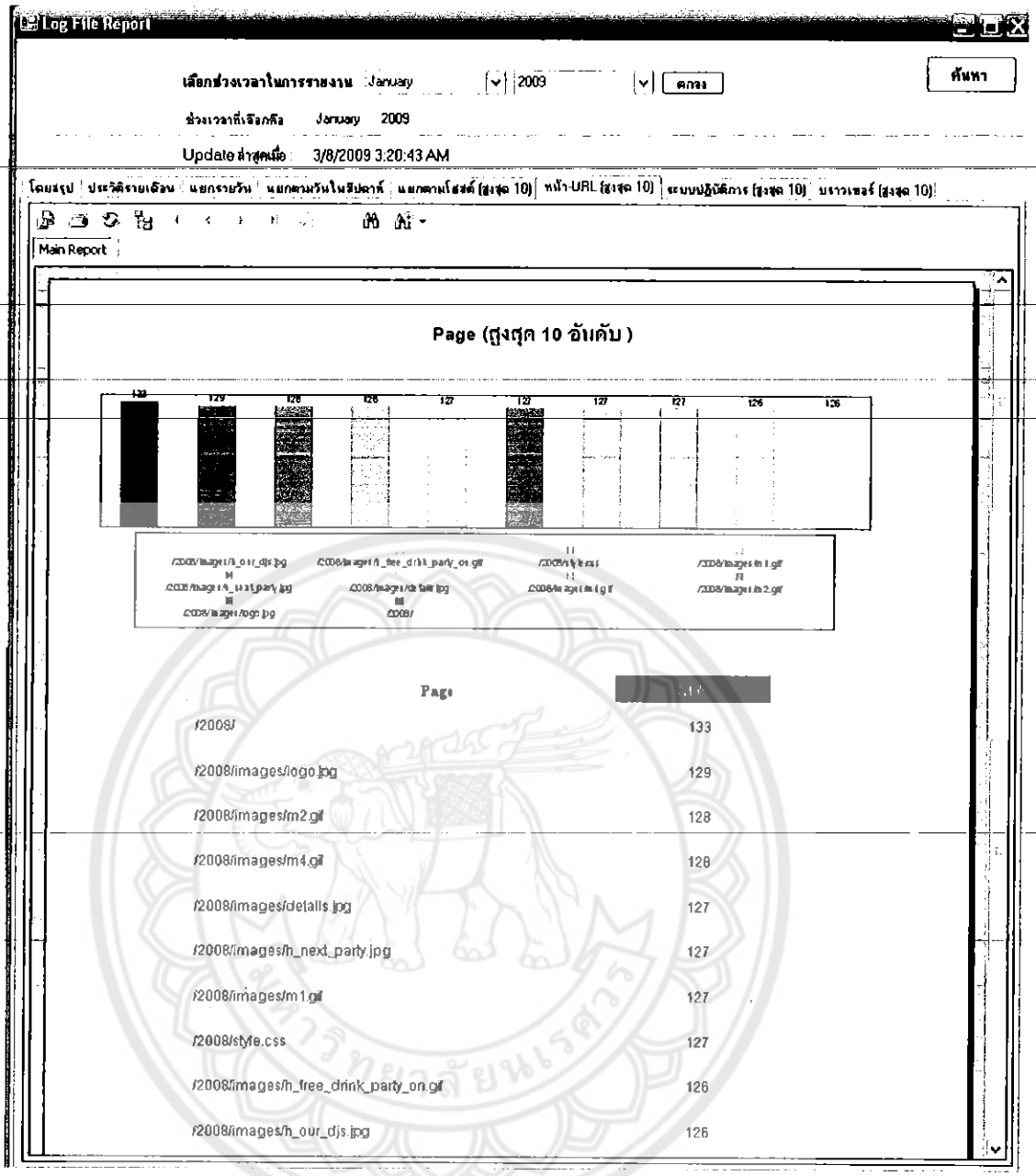
รูปที่ 4.9 แสดงผลการรายงานประวัติรายสัปดาห์

จากรูปที่ 4.9 เป็นการแสดงรายงานที่วิเคราะห์ตามประวัติรายสัปดาห์ โดยจะแสดงประวัติของผู้เยี่ยมชม (ไม่ซ้ำ IP) จำนวนหน้าที่ทำการเรียกดู และจำนวนครั้งที่ทำการเข้ามา



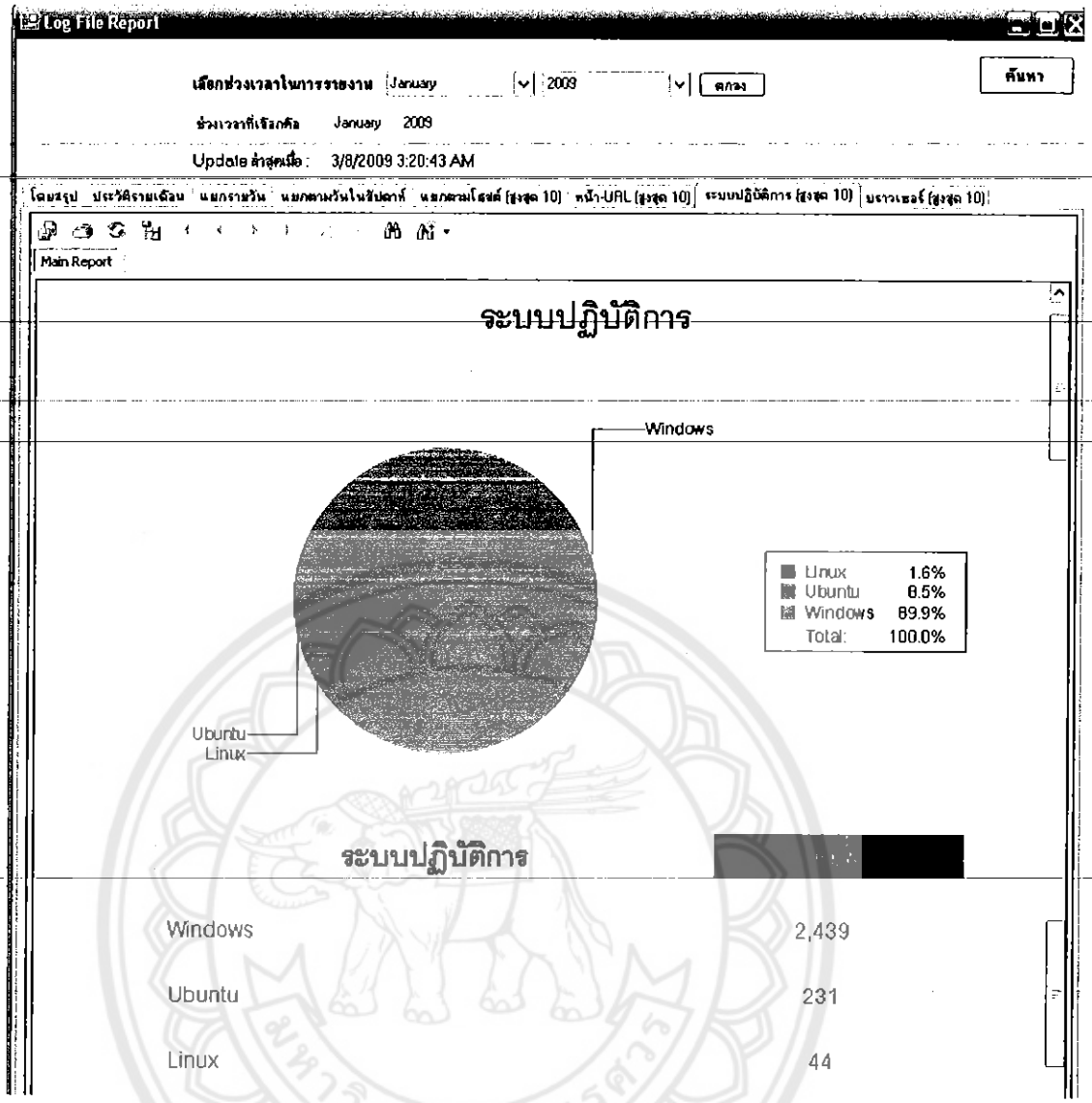
รูปที่ 4.10 แสดงผลการรายงานผู้เข้าใช้งาน (สูงสุด 10 อันดับ)

จากรูปที่ 4.10 เป็นการแสดงผลที่วิเคราะห์ตามผู้เข้าใช้งาน (สูงสุด 10 อันดับ) โดยจะแสดงไอพีของผู้เข้าใช้งาน จำนวนหน้าที่ทำการเรียกดู จำนวนครั้งที่ทำการเข้ามา และการเยี่ยมชมครั้งล่าสุด



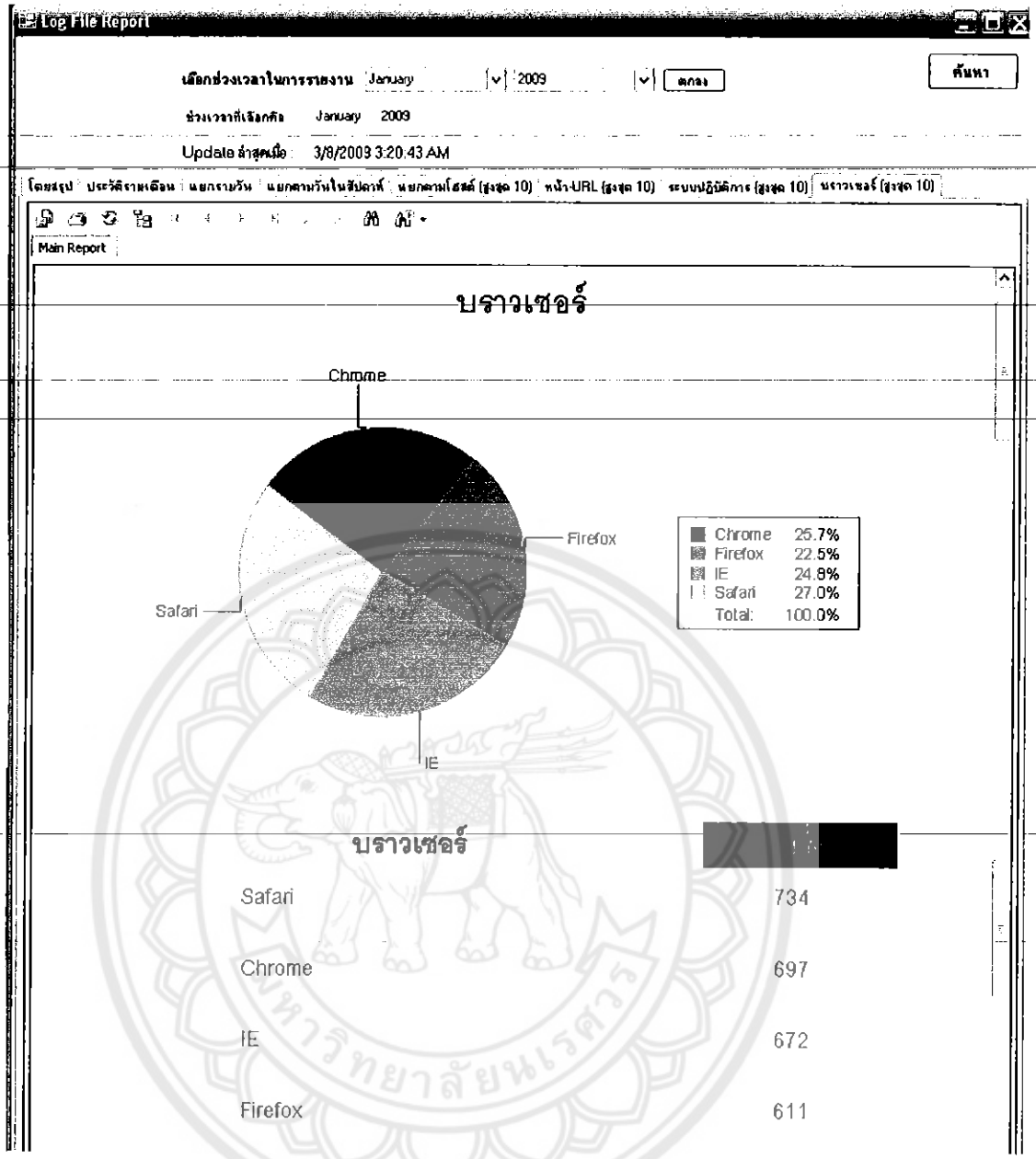
รูปที่ 4.11 แสดงผลการรายงานหน้า (Page) ที่ถูกเรียกใช้งาน (สูงสุด 10 อันดับ)

จากรูปที่ 4.11 เป็นการแสดงผลที่วิเคราะห์ตามรายงานหน้า ที่ถูกเรียกใช้งาน (สูงสุด 10 อันดับ) โดยจะแสดงหน้า และจำนวนครั้งที่ทำการเรียกดู



รูปที่ 4.12 แสดงผลการรายงานระบบปฏิบัติการ

จากรูปที่ 4.12 เป็นการแสดงผลที่วิเคราะห์ตามระบบปฏิบัติการของผู้ที่เข้ามาร้องขอใช้บริการ โดยจะแสดงชื่อของระบบปฏิบัติการ และจำนวนครั้งที่ทำการเข้ามา โดยที่จะแสดงกราฟเป็นเปอร์เซ็นต์เมื่อเทียบกับจำนวนของทั้งหมด



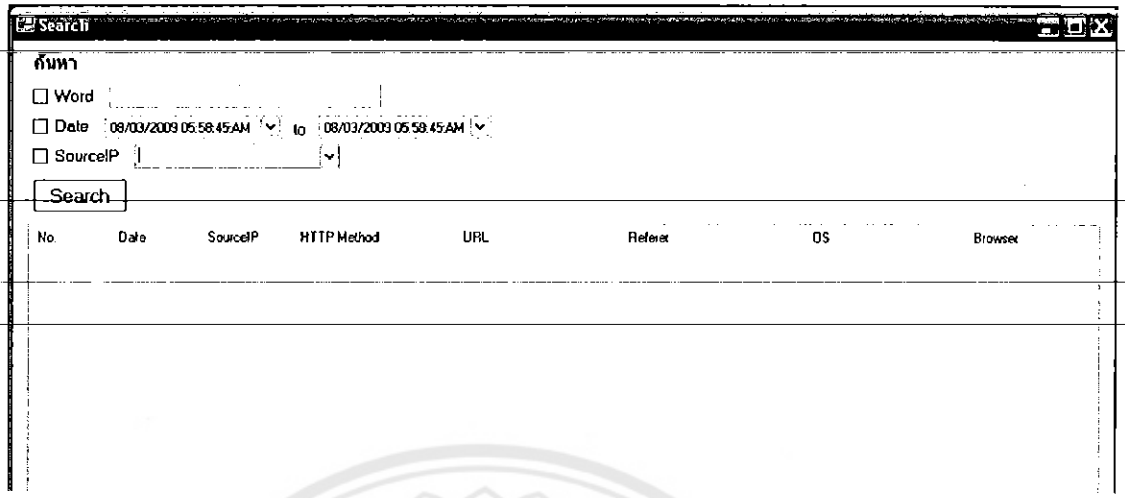
รูปที่ 4.13 แสดงผลการรายงานบราวเซอร์

จากรูปที่ 4.13 เป็นการแสดงผลที่วิเคราะห์ตามบราวเซอร์ของผู้ที่เข้ามาร้องขอใช้บริการ โดยจะแสดงชื่อของบราวเซอร์ และจำนวนครั้งที่ทำการเข้ามา โดยที่จะแสดงกราฟเป็นเปอร์เซ็นต์เมื่อเทียบกับจำนวนของทั้งหมด

4.2.1 แสดงผลการค้นหา

ในส่วนนี้จะเป็นการค้นหาข้อมูลต่างๆ ตามที่ผู้ใช้ต้องการ ซึ่งหลังจากที่ผู้ใช้ต้องการที่จะค้นหาสามารถ กดปุ่ม ค้นหา ดังรูปที่ 4.5 เพื่อจะการค้นหาจากนั้นโปรแกรมก็จะเปลี่ยนไปยังหน้า

interface ดังรูปที่ 4.14

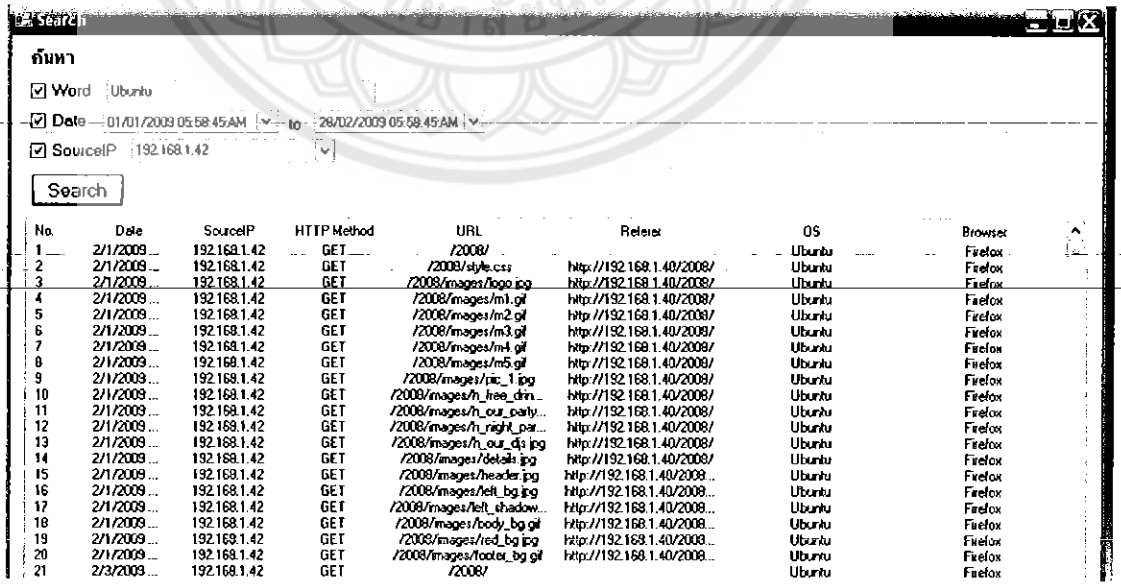


รูปที่ 4.14 แสดงหน้า interface ส่วนของค้นหา

ในส่วนของการค้นหานี้สามารถค้นหาได้ 3 รูปแบบด้วยกัน ดังนี้

- Word จะเป็นการค้นหาโดยใส่คำที่ต้องการค้นหา
- Date จะเป็นการค้นหาโดยการกำหนดเป็นช่วงที่ต้องการค้นหา
- SourceIP จะเป็นการค้นหาโดยการกำหนดเป็นไอพี

และยังสามารถทำการค้นหาโดยการกำหนดค่าทั้ง 3 แบบได้ ดังรูปที่ 4.15



รูปที่ 4.15 แสดงผลการค้นหา

บทที่ 5

บทสรุป

โครงงานนี้ได้พัฒนาโปรแกรมจัดการล็อกไฟล์ ซึ่งจะแบบโปรแกรมออกเป็น 2 ส่วนคือฝั่งเซิร์ฟเวอร์จะเป็น HTTP Analysis และฝั่งผู้ดูแลระบบจะเป็น Log File Report

5.1 หน้าที่การทำงานของโปรแกรม

สำหรับโปรแกรมที่พัฒนาในโครงงานนี้มีหน้าที่ในการทำงานต่างๆ ดังนี้

1. HTTP Analysis จะทำการรวบรวมข้อมูลจากอีเทอร์เน็ตการ์ด แล้วทำการวิเคราะห์เพื่อกรองเอาเฉพาะข้อมูลที่ต้องการ จากนั้นก็ทำการจัดเก็บลงสู่ระบบฐานข้อมูล

2. Log File Report จะทำการดึงข้อมูลจากระบบฐานข้อมูลแล้วทำการวิเคราะห์เพื่อสร้างรายงาน แล้วแสดงผลออกมา

5.2 วิเคราะห์ผลการทดลอง

จากผลการทดลองในบทที่ 5 การทำงานของโปรแกรมจัดการล็อกไฟล์ ทั้งการรวบรวมจัดเก็บข้อมูล การวิเคราะห์ข้อมูล และการแสดงผลรายงานนั้น ทำงานได้ค่อนข้างน่าพอใจ ซึ่งผลการทดลองนั้นสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของผู้ให้บริการเว็บเซิร์ฟเวอร์ และสามารถสร้างสถิติแสดงรายงานต่างๆที่สามารถนำไปพัฒนาระบบสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น นอกจากนี้ยังสามารถออกรายงานได้ ทำให้สามารถนำไปใช้งานในลักษณะต่างๆ ที่ต้องการได้

5.3 ปัญหาและแนวทางการแก้ไข

ในระหว่างการทำโครงงานนี้ได้ประสบปัญหาต่างๆ ดังนี้

1. การพัฒนาระบบไม่เป็นไปตามแผนที่วางไว้ เนื่องจากการประเมินโครงการในการพัฒนาระบบต่ำเกินไป แนวทางในการแก้ไข คือจะต้องคำนึงถึงความเสี่ยงในการพัฒนาระบบด้วย

2. ไม่สามารถวิเคราะห์คัดกรองในส่วนของระบบปฏิบัติการของเครื่อง Macintoch ได้ เนื่องจากไม่มีเครื่องให้ทำการทดสอบ

3. เนื่องจากในเครือข่ายมีปริมาณการสื่อสารเป็นจำนวนมาก อาจทำให้การดักจับแพ็กเก็ตมาความคลาดเคลื่อนได้

4. ในกรณีที่ระบบมีปริมาณ traffic มาก อาจจะทำให้มีการลบบางแพ็กเก็ตทิ้งไป ซึ่งอาจจะทำให้มีการขาดข้อมูลบางส่วนที่สำคัญไป ทำให้โปรแกรมทำงานได้ไม่สมบูรณ์

5.4 แนวทางการพัฒนาต่อ

1. พัฒนาโปรแกรมให้มีความยืดหยุ่นของโปรแกรมมากขึ้น เช่นสามารถจัดเก็บล็อกไฟล์ของไฟล์เซิร์ฟเวอร์ เมลล์เซิร์ฟเวอร์ เป็นต้น

2. พัฒนาให้โปรแกรมสามารถวิเคราะห์ การโจมตีของผู้ไม่หวังดีต่อระบบ

3. พัฒนาให้โปรแกรมสามารถวิเคราะห์โดยไม่ยึดติดกับพอร์ต

เอกสารอ้างอิง

[1] นิรุธ อำนวยศิลป์, **Visual C++ and MFC Programming,** กรุงเทพฯ : ดวงกลมสมัย 2548

[2] สุวัฒน์ ปุณณชัยยะ, ต้น ตัณฑ์สุทธิวงศ์, สุพจน์ ปุณณชัยยะ, **เปิดโลก TCP/IP และโปรโตคอลของอินเตอร์เน็ต (Second Edition)**, โปรวิชั่น, 2545

[3] สุนทริน วงศ์ศิริกุล, ชัยวัตน์ สิทธิกรโอฬารกุล, **การพัฒนาโมดุลสำหรับการเขียนโปรแกรมเชิงวัตถุด้วย UML 2.0 Unified Modeling Language,** บริษัท ซัคเซส มีเดีย จำกัด

[4] โอภาส เอี่ยมสิริวงศ์, **การวิเคราะห์และออกแบบระบบ (Systems Analysis and Design) ฉบับปรับปรุงเพิ่มเติม,** บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)

[5] **กฎหมายคอมพ์ ฉบับนักไอที รวมเรื่องที่คุณต้องรู้เกี่ยวกับกฎหมายคอมพิวเตอร์,** CS Loxinfo

[6] Behrouz A. Forouzan, **Data Communications and Networking (Fourth Edition),** McGraw-Hill Education (Asia)

[7] Richard Blum, **C# Network Programming,** John Wiley and Sons, 2002

ประวัติผู้เขียนโครงงาน

ชื่อ นายธีระศักดิ์ จิตรัก

ภูมิลำเนา 49 หมู่ 2 ต.เขาดิน อ.เดิมบางนางบวช จ.สุพรรณบุรี 72120

ประวัติการศึกษา

- จบการศึกษาระดับมัธยมศึกษาจากโรงเรียนวัดธรรมมงคล กรุงเทพฯ
- ปัจจุบันกำลังศึกษาอยู่ในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail : odfreekick@gmail.com

ชื่อ นายปฏิภาณ สดใส

ภูมิลำเนา 170 หมู่12 ถ.สกล-นาแก ต.งิ้วด่อน อ.เมือง จ.สกลนคร 47000

ประวัติการศึกษา

- จบการศึกษาระดับมัธยมศึกษาจากโรงเรียนสกลราชวิทยานุกูล
- ปัจจุบันกำลังศึกษาอยู่ในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

มหาวิทยาลัยนเรศวร

E-mail : patipan3@hotmail.com