สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

โปรแกรมดักจับข้อมูลและแยกประเภทของข้อมูล

PACKET SNIFFER WITH CONTENT SEPARATER

โดย

นาย ธนวัฒน์ ภู่พัฒนะกูล

นาย ปรัชญา ไชยลังกา

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2545

เลขหมู่.....
เลขทะเบียน 50285
วัน,เดือน,ปี 28 เม.ย. 2547

.b.....
.i.....

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

PACKET SNIFFER WITH CONTENT SEPARATER

BY

MR. TANAWAT POOPATTANAKUL

MR. PRATCHAYA CHAILANGKA

A THESIS SUMMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENT FOR THE DEGREE OF

BACHELOR IN DEPARTMENT OF INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2002

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปริญญานิพนธ์	โปรแกรมดักจับข้อมูลและแยกประเภทของข้อมูล
ชื่อนักศึกษา	นาย ธนวัฒน์ ภู่พัฒนะกูล รหัสประจำตัว 42010138
	นาย ปรัชญา ไชยลังกา รหัสประจำตัว 42010188
อาจารย์ที่ปรึกษา	อาจารย์ ภุชงค์ หงษ์สุวรรณ
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตรบัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสรเทศ
ปีการศึกษา	2545

บทคัดย่อ

ปริญญานิพนธ์นี้กล่าวถึงการเขียนโปรแกรมควบคุมการทำงานของโปรแกรมประเภทสนิฟเฟอร์ (sniffer) โดยแบ่งการทำงานออกเป็น 2 ส่วนด้วยกัน คือ ส่วนแรกจะเป็นโปรแกรมที่ใช้ควบคุมการทำงานของโปรแกรม สนิฟเฟอร์ ในการสั่งให้สนิฟเฟอร์ทำการดักจับข้อมูลที่ผ่านเข้ามาในระบบเครื่อข่าย ส่วนที่สองจะเป็นการแสดงผลของกลุ่มข้อมูล(packet) ที่ถูกจับมาได้ซึ่งในที่นี้ได้ทำการเลือกเอาเฉพาะกลุ่มของข้อมูลประเภท เอกสารเอสเอ็มทีพี (SMTP) และเอกสารเอชทีทีพี (HTTP) โดยสามารถแสดงผลออกมาในรูปแบบของเอกสารจริง เช่น สามารถแสดงเป็นหน้าเวปเพจสำหรับข้อมูลประเภท เอชทีทีพี และแสดงข้อมูลที่ถูกแนบมากับเอกสารเอสเอ็มทีพี ได้ นอกจากนี้ยังมีระบบตรวจสอบเอกสารว่าเอกสารใดที่มีข้อความหรือข้อมูลที่น่าสงสัย โดยจะแสดงข้อความเตือนที่เอกสารนั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Thesis Title	Packet sniffer with content separate	
Student	Mr. Tanawat Poopattanakul	ID. 42010138
	Mr. Pratchaya Chailangka	ID. 42010188
Advisor	Puchong Hongsuwan	
Graduate Level	Bachelor Degree of Information Engineering	
Department	Information Engineering	
Academic Year	2002	

ABSTRACT

In this thesis describe the programming to control sniffer program . This program has two part First,It is a program for control a sniffer to capture packet . Second, It is a program for show packet that was capture by a sniffer. In this case this program capture only SMTP's packet and HTTP's packet. And can show a packet in real format such as show a HTTP's packet in web browser or show a SMTP's packet with attract file. In addition, It has an alert function to warn when sniffer capture a suspected packet

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ไม่อาจเสร็จสมบูรณ์ได้ทุกประการถ้าปราศจากการสนับสนุนจากบุคคลหลายๆฝ่าย บุคคลที่มีส่วนสำคัญในการช่วยเหลือในการทำโครงงานนี้คือ อ.ภุชงค์ หงษ์สุวรรณ ซึ่งเป็นอาจารย์ที่ปรึกษาโดยตรง โดยให้คำปรึกษาเกี่ยวกับกับเรื่องการเขียนโปรแกรม

ขอขอบคุณ เว็ปไซต์ google.co.th และ thailinux.com สำหรับการหาข้อมูลที่จำเป็น ในการเขียนโปรแกรม

และเนื่องด้วยการได้รับการสนับสนุนจากคณาจารย์และเพื่อนนักศึกษาภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

และสุดท้ายขอขอบคุณ คุณพ่อ และคุณแม่ที่ให้กำลังใจและทุนทรัพย์เพื่อการศึกษาและการทำโครงงานนี้

นาย ธนวัฒน์ ภู่พัฒนะกูล

นาย ปรัชญา ไชยลังกา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ก
บทคัดย่อภาษาอังกฤษ	ข
กิตติกรรมประกาศ	ค
สารบัญ	ง
สารบัญรูปภาพ	ฉ
สารบัญตาราง	ซ
บทที่ 1 บทนำ	
1.1 แนวความคิดและที่มาของปัญหา	1
1.2 จุดประสงค์	2
1.3 ขอบเขตของโครงงาน	2
1.4 วิธีการดำเนินการ	2
บทที่ 2 ทฤษฎีที่เกี่ยวข้อง	
2.1 พรอมมิสคิวอัส โหมด (Promiscuous mode)	3
2.2 สถาปัตยกรรมของจดหมายอิเล็กทรอนิกส์	4
2.2.1 ซิมเปิลเมล์ ทรานส์เฟอร์ โพรโตคอล (Simple mail transfer protocol:SMTP)	4
2.2.2 ส่วนประกอบของจดหมายอิเล็กทรอนิกส์	5
2.2.3 มัลติเพอร์โพส อินเตอร์เน็ต เมล์ เอ็กซ์เทนชั่น(Multipurpose Internet Mail Extensions:MIME)	6
2.3 การพัฒนาโปรแกรมบน เอ็กซ์-วินโดว์ (x-window)	9
2.3.1 สิ่งที่จำเป็นต้องมีในการพัฒนาโปรแกรมบน เอ็กซ์-วินโดว์	9
2.3.2 จีทีเคพลัส (GTK+)	10
2.3.3 พื้นฐานโปรแกรมด้วย จีทีเคพลัส	10
2.4 การเข้าและถอดรหัส เบส64 (Base64 Encoding and Decoding)	12

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน้า

บทที่3 การออกแบบโครงงาน

3.1 กำหนดขอบเขตความสามารถของโครงงาน 15

3.2 การออกแบบส่วนติดต่อกับผู้ใช้ 15

3.3 โฟลชาร์ทของฟังก์ชั่นที่สำคัญ 18

3.3.1 ฟังก์ชั่น Make_Tree() 18

3.3.2 ฟังก์ชั่น Make_dir_list() 19

3.3.3 ฟังก์ชั่น Chk_Alert () 20

3.3.4 ฟังก์ชั่น Selecttree() 21

3.3.5 ฟังก์ชั่น SelectList() 21

3.3.6 ฟังก์ชั่น Showdialog() 22

3.3.7 ฟังก์ชั่น ShowData() 23

3.3.8 ฟังก์ชั่น Change_keyword() 24

3.3.9 ฟังก์ชั่น Delete_keyword() 25

บทที่ 4 ผลการทดลอง

4.1 เริ่มเปิดโปรแกรม 26

4.2 การแสดงผลของแพ็คเก็ต SMTP 27

4.3 การแสดงผลของแพ็คเก็ต HTTP 28

4.4 เลือกเมนู File/Start 29

4.5 เลือกเมนู File/Quit 30

4.6 เลือกเมนู Set/Alert 30

4.7 การลบและบันทึกล็อกไฟล์ 32

บทที่ 5 สรุป

5.1 สรุปการพัฒนาโครงงาน 34

5.2 ปัญหาที่เกิดขึ้นระหว่างการพัฒนาโครงงาน 34

5.3 แนวทางในการพัฒนาโครงงานต่อ 34

บรรณานุกรม 35

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

หน้า

บทที่3 การออกแบบโครงงาน

รูปที่ 3.1 widget ที่สำคัญในหน้าต่างหลัก 15

รูปที่ 3.2 widget ของหน้าต่าง SniffWindow 16

รูปที่ 3.3 widget ของหน้าต่าง AlertWindow 17

รูปที่ 3.4 ฟังก์ชั่น make_tree() 18

รูปที่ 3.5 ฟังก์ชั่น make_dir_list() 19

รูปที่ 3.6 ฟังก์ชั่น chk_alert() 20

รูปที่ 3.7 ฟังก์ชั่น selecttree() 21

รูปที่ 3.8 ฟังก์ชั่น selectlist() 21

รูปที่ 3.9 ฟังก์ชั่น showdialog() 22

รูปที่ 3.10 ฟังก์ชั่น showdata() 23

รูปที่ 3.11 ฟังก์ชั่น change_keyword() 24

รูปที่ 3.12 ฟังก์ชั่น delete_keyword() 25

บทที่ 4 ผลการทดลอง

รูปที่ 4.1 หน้าต่างหลัก 26

รูปที่ 4.2 (ก) เมนูย่อย ของ เมนูไฟล์ 26

รูปที่ 4.2 (ข) เมนูย่อย ของ เมนูเซต 26

รูปที่ 4.3 หน้าต่างแสดงรายละเอียดของแพ็คเก็ต SMTP 27

รูปที่ 4.4 (ก) แสดงรูปภาพที่แนบมากับเอกสาร SMTPรูปที่ 1 27

รูปที่ 4.4 (ข) แสดงรูปภาพที่แนบมากับเอกสาร SMTPรูปที่ 2 27

รูปที่ 4.5 หน้าต่างแสดงรายละเอียดของแพ็คเก็ต HTTP 28

รูปที่ 4.6 แสดงไฟล์ HTTP ด้วย Mozilla 28

รูปที่ 4.7 หน้าต่างSniffit Front End 29

รูปที่ 4.8 หน้าต่างSniffit Front End ขณะทำงาน 29

รูปที่ 4.9 หน้าต่าง Alert Set 30

รูปที่ 4.10 การเพิ่มคีย์เวิร์ด 30

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หน้า

รูปที่ 4.11 การแก้ไขคีย์เวิร์ด 31
รูปที่ 4.12 การลบคีย์เวิร์ด 31
รูปที่ 4.13 เมนูการลบหรือบันทึกล็อกไฟล์ 32
รูปที่ 4.14 หน้าต่างการบันทึกล็อกไฟล์ 32
รูปที่ 4.15 เลือกเมนู Delete 33
รูปที่ 4.16 ลบล็อกไฟล์ 33

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

หน้า

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง

ตารางที่ 2.1 คำสั่งในการติดต่อของเมล์ไคลเอนต์กับเมล์เซิร์ฟเวอร์ 4-5

ตารางที่ 2.2 ชนิดของ content-type 7-8

ตารางที่ 2.3 ชนิดของ Content-Transfer-Encoding 8

ตารางที่ 2.4 ตารางอักษรของ base 64 13

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 แนวความคิดและที่มาของปัญหา

ระบบเครือข่ายคอมพิวเตอร์ ได้กลายเป็นสิ่งจำเป็นมากขึ้นในการสื่อสารของข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่ง เนื่องจากการสื่อสารของข้อมูลเป็นไปอย่างรวดเร็ว และมีความน่าเชื่อถือทำให้มีการใช้ระบบเครือข่ายคอมพิวเตอร์ เพิ่มมากขึ้น

เนื่องจากการเพิ่มขึ้นของอัตราการใช้ระบบเครือข่าย ทำให้ผู้บริหารระบบต้องปรับปรุงการดูแลระบบ เพื่อลดความคับคั่งให้อยู่ในระดับที่ให้ผลดีที่สุด การตรวจสอบการใช้งานระบบเครือข่ายของผู้ใช้เป็นอีกวิธีหนึ่งที่จะช่วยลดความคับคั่งของระบบได้ โดยทำการห้ามมิให้มีการใช้ระบบเครือข่ายที่ผิดวัตถุประสงค์ของระบบเครือข่ายที่ตั้งไว้

ในขณะเดียวกันการเพิ่มขึ้นของผู้ที่เข้ามาใช้ระบบ เปิดโอกาสให้ผู้ไม่หวังดีต่อระบบสามารถแฝงตัวเข้ามาได้ง่ายขึ้นเนื่องจากผู้ดูแลระบบไม่สามารถดูแลได้อย่างทั่วถึง รวมถึงการใช้งาน อย่างไม่ถูกต้องของผู้ใช้ในระบบเองด้วย

เพื่อเป็นการช่วยเหลือผู้ดูแลระบบในการตรวจสอบการใช้งานของผู้ที่ใช้ระบบเครือข่าย โปรแกรมดักจับข้อมูลจึงมักถูกนำมาใช้เสมอ เราเรียกโปรแกรมประเภทนี้ว่า “แพ็คเก็ตสนิฟเฟอร์ (Packet Sniffer)”

โปรแกรมดักจับข้อมูลสามารถดักจับข้อมูลที่ผ่านเข้ามาในระบบ แต่ไม่สามารถแสดงได้ว่าข้อมูลนั้นเป็นข้อมูลอะไรจำเป็นต้องใช้ผู้ดูแลระบบที่มีความเชียวชาญจึงจะสามารถเข้าใจข้อมูลที่ดักจับมาได้

โปรแกรมดักจับข้อมูลและแยกประเภทของข้อมูล (Packet sniffer with content separater) สามารถช่วยแยกแยะประเภทของข้อมูลแต่ละข้อมูลว่าเป็นเอกสารประเภท SMTP (Simple Mail Transfer Protocol) หรือ HTTP (Hyper Text Transfer Protocol) ได้ และสามารถแจ้งเตือนหากมีข้อมูลที่น่าสงสัยเข้ามาหรือมีการส่งเอกสารที่น่าสงสัยออกไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.2 จุดประสงค์

1. เพื่อศึกษาการใช้งานและการเขียนโปรแกรมบนระบบปฏิบัติการลินุกส์ (Linux) ด้วยภาษา ซี
2. เพื่อศึกษาการทำงานของโพรโตคอล SMTP และ HTTP และสามารถนำมาประยุกต์ใช้งานได้
3. สามารช่วยเหลือผู้ดูแลระบบในการตรวจสอบการใช้งานของผู้ใช้ในระบบได้

1.3 ขอบเขตของโครงงาน

1. ศึกษาการทำงานของโปรแกรม สนิฟอิท (Sniffit) แล้วเขียนโปรแกรม ฟรอนท์เอนด์ (front end) ควบคุมการทำงานของ สนิฟอิท ได้
2. สามารถแยกแยะชนิดของโพรโตคอลของแต่ละข้อมูล ว่าเป็น SMTP หรือ HTTP ได้
3. สามารถแสดงผลข้อมูลในรูปแบบข้องข้อมูลนั้นๆได้ เช่น สามารถแสดงเป็นหน้าเวปเพจ สำหรับข้อมูลประเภท HTTP และแสดงข้อมูลที่ถูกแนบมากับเอกสาร SMTP ได้
4. มีระบบตรวจสอบข้อมูลที่น่าสงสัยและสามารถแจ้งเตือนได้

1.4 วิธีการดำเนินการ

ในเทอมแรกเป็นการศึกษาการใช้งานของโพรโตคอลต่างๆ และลักษณะของแพ็คเก็ตที่โปรแกรมสนิฟอิทจับได้ ศึกษาการทำงานของโปรแกรมสนิฟอิท ออกแบบภาพรวมของโครงงาน และทดลองเขียนด้วยโปรแกรมตัวอย่างออกมาในรูปของเวปเพจด้วยภาษาเพิร์ล

ในเทอมที่สอง ทำการศึกษาเครื่องมือที่ช่วยในการพัฒนาโปรแกรมบน เอ็กซ์-วินโดว์ และเลือกเครื่องมือที่เหมาะสมและเข้าใจมาช่วยในการพัฒนา จากนั้นจึงทำการพัฒนาโปรแกรมด้วยภาษา ซี และเครื่องมือที่เลือกมา ตามที่ออกแบบไว้เบื้องต้น และเพื่อเติมรายละเอียดเข้าไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 พรอมมิสคิวอัส โหมด (Promiscuous mode)

การที่สนิฟเฟอร์สามารถดักอ่านข้อมูลที่อยู่บนเครือข่ายได้นั้นมีสาเหตุที่สำคัญคือ ด้วยลักษณะของโพรโตคอลอีเทอร์เน็ตที่ใช้หลักการกระจายของข้อมูลไปยังทุกโฮสต์(Host) ที่อยู่ในเครือข่ายและอาศัยโฮสต์แต่ละตัวจำแนกการสื่อสารของตนเอง นั่นหมายความว่าข้อมูลทุกแพ็คเก็ตที่ใช้สื่อสารกันนั้นได้ถูกส่งไปยังโฮสต์ทุกตัว ซึ่งจะได้รับพร้อมกันและเหมือนกัน เพียงแต่การที่จะสื่อสารกันได้อย่างถูกต้องนั้นโฮสต์แต่ละตัวจะต้องมีกระบวนการที่สามารถรู้ได้ว่าข้อมูลแพ็คเก็ตใดเป็นของตัวเอง และข้อมูลแพ็คเก็ตใดมิใช่ของตนเอง ทุกๆแพ็คเก็ตที่กระจายลงบนเครือข่ายนั้นจะมีหมายเลขระบุชัดคือ หมายเลข แม็คแอดเดรส (MAC Adsress) หรือ เรียกอีกอย่างหนึ่งว่าอีเทอร์เน็ตแอดแดรส (Ethernet Address) ซึ่งเป็นสิ่งที่บอกว่าแพ็กเก็ตมาจากฮาร์ดแวร์ใดในเครือข่าย ทำให้สามารถระบุได้ว่าแพ็กเก็ตนั้นส่งมาจากโฮสต์ใด และต้องการส่งให้โฮสต์ใด

แม็คแอดเดรสจะเป็นหมายเลขเฉพาะตามฮาร์ดแวร์ทุกชนิดที่ใช้ในการสื่อสารโดยโพรโตคอล อีเทอร์เน็ต และในทางทฤษฎีแล้วฮาร์ดแวร์ทุกชนิดจะไม่มี แม็คแอดเดรส ที่ซ้ำกัน โดยทั่วไป แม็คแอดเดรส จะถูกกำหนดตายตัวอยู่ใน รอม(Rom) ของฮาร์ดแวร์และไม่สามารถเปลี่ยนแปลงได้โดยซอฟแวร์ แต่เนื่องจาก การใช้งานของฮาร์ดแวร์นั้นต้องควบคู่ไปกับไดรเวอร์ของฮาร์ดแวร์นั้นๆ ซึ่งโดยปกติแล้วไดรเวอร์จะถูกกำหนดให้ปฏิบัติตามโพรโตคอลอย่างเข้มงวดคือ

- ให้รับข้อมูลที่มี แม็คแอดเดรส เป็นของตนเองเท่านั้น
- ให้ส่งข้อมูลโดยใช้ แม็คแอดเดรส เท่านั้น

โดยเฉพาะคุณสมบัติที่ให้รับเฉพาะข้อมูลที่มี แม็คแอดเดรส เป็นของตนเองเท่านั้น เป็นอุปสรรคอย่างยิ่งของ สนิฟเฟอร์ หากสามารถผ่านข้อห้ามนี้ไปได้ก็จะทำให้รับข้อมูลของผู้อื่นที่ถูกกระจายเข้ามาได้โดยอัตโนมัติ โหมดการทำงานนี้เรียกว่า “พรอมมิสคิวอัส โหมด”

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 สถาปัตยกรรมของจดหมายอิเล็กทรอนิกส์

2.2.1 ซิมเปิลเมล์ ทรานส์เฟอร์ โพรโตคอล (Simple mail transfer protocol:SMTP)

[1]SMTP (RFC 821) เป็นโพรโตคอล TCP/IP ที่ใช้ในการรับส่งอิเล็กทรอนิกส์เมล์ในเครือข่ายอินเตอร์เน็ต โดยปรกติแล้ว การติดต่อไปยัง MTA (Message transfer agent) ในรูปแบบของ SMTP จะติดต่อไปที่พอร์ต 25 ซึ่งเป็นพอร์ตมาตรฐานของเมล์เซิร์ฟเวอร์

การติดต่อของโพรโตคอล SMTP จะอยู่ในรูปแบบของข้อความปรกติ โดยผู้ต้องการส่งเรียกว่าไคลเอนต์ ผู้รับเรียกว่าเซิร์ฟเวอร์ เมื่อการติดต่อไปยังพอร์ตของ SMTP สำเร็จแล้ว ไคลเอนต์จะส่งคำสั่งไปยังเซิร์ฟเวอร์ และเซิร์ฟเวอร์จะตอบผลของคำสั่งกลับเป็นรหัสตัวเลข โดยมีคำสั่งดังนี้

ตารางที่ 2.1 คำสั่งในการติดต่อของเมล์ไคลเอนต์กับเมล์เซิร์ฟเวอร์

SMTP command	Description
HELO	ใช้แสดงตัวของไคลเอนต์ให้เซิร์ฟเวอร์ จะตามด้วยชื่อเครื่องไคลเอนต์ในลักษณะ fully qualify domain name เช่น HELO cc2.cpe.ku.ac.th
MAIL	ใช้เริ่มต้นการส่งเมล์ มีรูปแบบคือ MAIL FROM:<reverse-path> Reverse path บอกแอดเดรสของผู้ส่งเมล์ และอาจเป็นลิสต์ของโฮสต์ที่เมล์ได้ผ่านมา โดยโฮสต์ที่ปรากฏจะเป็นโฮสต์ล่าสุดที่เมล์ผ่านมา ลิสต์นี้จะใช้เป็นประโยชน์ในการส่งข้อความเตือนกลับไปยังผู้ส่งต้นทางหากเมล์ไม่สามารถส่งไปถึงปลายทางได้
RCPT	บอกถึงแอดเดรสของผู้รับเมล์ ถ้ามีผู้รับมากกว่าหนึ่ง อาจใช้คำสั่ง RCPT หลายๆครั้งสำหรับผู้รับแต่ละคน มีรูปแบบคือ RCPT TO :<forward path > Forward path เป็นแอดเดรสของผู้รับเมล์ และอาจเป็นโฮสต์ที่เป็น Relay host เมื่อเมล์ผ่านโฮสต์ใดชื่อโฮสต์ในลิสต์ของ forward path จะถูกลบออก และไปเพิ่มใน reverse path แทน
DATA	สำหรับการส่งเนื้อหาโดนข้อมูลจะสิ้นสุดเมื่อพบบรรทัดที่มีจุด “.” เพียงตัวเดียว เมื่อเซิร์ฟเวอร์รับเมล์เพื่อส่งต่อแล้วจะมีการแทรกข้อมูลผู้ส่งเมล์,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

	ชื่อโฮสต์ที่ได้รับเมล์พร้อมทั้งเวลาลงไปยังส่วนหัวของเมล์
SEND,SOML,SAML	รูปแบบเช่นเดียวกับคำสั่งเมล์แต่ SEND จะส่งไปยัง terminal ของผู้รับแทน mailbox SOMLจะส่งไปยัง terminal หากเครื่องนั้นใช้งานอยู่ หากไม่ได้ใช้งานจะส่งไปยัง mailbox แทน SAML จะส่งไปทั้ง terminal และ mailbox ของผู้รับ
REST	ใช้ยกเลิกการส่งเมล์ ข้อมูลผู้ส่ง,ผู้รับ และ เนื้อหาจะถูกยกเลิก
VRFY	ใช้ตรวจสอบแอดเดรสของผู้รับเมล์ โดยไม่มีการส่งจริง ใช้เพื่อตรวจสอบปัญหาของการส่งเมล์
EXPN	ใช้ตรวจสอบ mailing list เซิร์ฟเวอร์จะตอบกลับมาเป็นรายชื่อของแอดเดรสใน mailing list นั้น
HELP	จะแสดงข้อความช่วยเหลือซึ่งจะเป็นคำสั่ง SMTP ที่มีอยู่
NOOP	ไม่มีผลใดๆนอกจากทำให้เซิร์ฟเวอร์ตอบกลับว่า OK (รหัส 200)
QUIT	ใช้สิ้นสุดการส่งเมล์และยกเลิกการติดต่อ
TURN	ทำให้ไคลเอนต์และเซิร์ฟเวอร์ทำหน้าที่ สลับกัน ซึ่งทำให้สามารถส่งเมล์กลับทิศทาง โดยไม่ต้องยุติการติดต่อ และสร้างการติดต่อใหม่

2.2.2 ส่วนประกอบของจดหมายอิเล็กทรอนิกส์

RFC 822 เป็นเอกสารกำหนดรูปแบบของข้อความที่ส่งในระบบอิเล็กทรอนิกส์เมล์ แบ่งออกเป็นส่วน เอนวีโลป(Envelop) ที่ระบุข้อมูลผู้รับและผู้ส่ง ส่วน เฮดเดอร์ (header) และ บอดี (body)

ENVELOPE

เป็นข้อมูลสำหรับ MTA ใช้ในการส่ง ส่วนนี้กำหนดโดนคำสั่ง SMTP 2 คำสั่ง คือ MAIL และ RCPT ตัวอย่างเช่น

MAIL FROM:<>

RECP TO:<>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

HEADER

เป็นส่วนของเฮดเดอร์ของเมล์ใช้โดย User agent

BODY

คือเนื้อหาภายในเมล์ โดย RFC 822 กำหนดให้ บอดี เป็นบรรทัดประกอบด้วย NVT ASCII (7 bits) ในทางปฏิบัติ

2.2.3 มัลติเพอร์โพส อินเตอร์เน็ต เมล์ เอ็กซ์เทนชั่น(Multipurpose Internet Mail Extensions:MIME)

MIME คือข้อกำหนดเพิ่มเติมจาก RFC822 เพื่อแก้ข้อจำกัดบางอย่างในการใช้งานอิเล็กทรอนิกส์เมล์ ได้แก่

1. SMTP ไม่สามารถส่งไฟล์ประเภทไบนารีได้โดยตรง โดยต้องแปลงให้อยู่ในรูปของเทกซ์ โดยใช้โปรแกรม เช่น Uuencode/Uudecode
2. SMTP ไม่สามารถส่งข้อมูลตัวอักษรขนาด 8 บิตได้โดยจะรองรับเฉพาะการส่งข้อมูลในรูปแบบของ 7 บิต ASCII ซึ่งทำให้ไม่สามารถส่งข้อมูลที่ไม่ใช้ภาษาอังกฤษได้
3. เซิร์ฟเวอร์ SMTPที่เป็นเกตเวย์บางชนิดอาจจะมีการเปลี่ยนแปลงข้อมูลจาก ASCII เป็น EBCDIC ซึ่งจะทำให้ข้อมูลบางอย่างเสียหายได้
4. ปัญหาที่เกิดจากความไม่สมบูรณ์ในการพัฒนาของ SMTP เซิร์ฟเวอร์ทำให้ข้อมูลที่ส่งไปในแต่ละเซิร์ฟเวอร์มีการเปลี่ยนแปลง

ข้อกำหนดของ MIME จะอยู่ใน RFC2045 ถึง RFC2049 โดยสามารถระบุได้ดังนี้

1.มีการกำหนดฟิลด์ใหม่ในส่วนของเฮดเดอร์ของ RFC2049 ใหม่ 5 ฟิลด์ ซึ่งเป็นข้อมูลที่เกี่ยวข้องกับส่านบอดีของเมล์

2.มีการกำหนดรูปแบบของเนื้อหาในเมล์ ซึ่งใช้ในการระบุการนำเสนอตามรูปแบบนั้นๆ เช่น text/plain , text/html

3.มีการกำหนด transfer encoding ซึ่งช่วยป้องกันความเสียหายจากการเปลี่ยนแปลงรูปแบบของเนื้อหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

MIME Header

MIME version มักมีค่าเป็น 1.0 เพื่อระบุว่าแมสเสจนี้เป็นไปตาม RFC2045 และ RFC2049

- Content-Type ระบุถึงข้อมูลที่อยู่ในส่วนของบอดี ซึ่ง user agent จะใช้ข้อมูลส่วนนี้ในการดำเนินงานเพื่อจัดการกับข้อมูลนั้นต่อไป
- Content-Transfer-Encoding ระบุชนิดการเปลี่ยนแปลงรูปแบบที่ใช้ในการแสดงส่วนของ บอดี ซึ่งทำให้การแสดงผลเป็นไปอย่างไม่ถูกต้อง และการเปลี่ยนแปลงรูปแบบเมื่อเมล์ถูกส่งผ่าน เมล์เกตเวย์ (mail gateway) ไม่เกิดผลกระทบ
- Content-ID ใช้ในการกำหนดแต่ละเอนติตี้ของเมล์ในกรณีที่มีเนื้อหามากกว่า 1 ส่วน(multi path)
- Content-Description รายละเอียดของออบเจคท์ในส่วนบอดี

ฟิลด์ MIME-Version , Content-Type , Content-Transfer-Encoding เป็นฟิลด์ที่ต้องมีในส่วนของเฮดเดอร์ ส่วนฟิลด์ Content-ID และ Content-description อาจจะมีหรือไม่มีก็ได้

ตารางที่ 2.2 ชนิดของ content-type

Type	Plain	Description
Text	Plain	Unformatted text อาจเป็น ASCII หรือ ISO 8859
	Enriched	เทกซ์ที่มีรูปแบบหลากหลาย
Multipart	Mixed	เนื้อหาที่แยกเป็นส่วนๆ แต่ส่งมาพร้อมกัน แสดงผลตามลำดับที่ปรากฏในเนื้อหา
	Parallel	เหมือนกับ mixed แต่ไม่กำหนดลำดับการแสดงผล
	Alternative	ข้อมูลที่มีเนื้อหาเดียวกันแต่มีหลายเวอร์ชัน
	Digest	เหมือนกับ mixed แต่ค่าของ type/subtype ของแต่ละส่วนจะเป็น message/rfc822 ถ้าไม่ได้กำหนดเป็นอย่างอื่น
Message	Rfc822	ส่วนของ บอดีอยู่ในรูปแบบที่กำหนดใน RFC822
	Partial	ใช้สำหรับการยอมให้มีการแยกส่วนของเมล์ที่มีขนาดใหญ่เกินกว่าหนดไว้ในเซิร์ฟเวอร์ แต่ในระดับผู้ใช้จะไม่รับทราบถึงการแยกส่วนนี้
	External-body	กำหนดค่าที่ชี้ไปยัง ออบเจคท์ ที่ไม่อยู่ในเมล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Image	Jpeg Gif	รูปแบบภาพแบบ JPEG รูปแบบภาพแบบ GIF
Video	Mpeg	รูปแบบภาพเคลื่อนไหวแบบMPEG
Audio	Basic	รูปแบบของเสียงเป็นการเข้าแบบ single-channel 8-bit ISDN mu-law ที่ sample rate 8kHz
Application	PostScript Octet-stream	รูปแบบของเนื้อหาเป็น Postscript รูปแบบของเนื้อหาเป็น binary 8-bit bytes

MIME Transfer Encoding

ค่าที่กำหนดในฟิลด์ Content-Transfer-Encoding สามารถเป็นได้ 7 ค่า

ตารางที่ 2.3 ชนิดของ Content-Transfer-Encoding

7 bit	ข้อมูลทั้งหมดอยู่ในรูป 7 bit ASCII และมีขนาดความยาวบรรทัดจำกัดตามการส่งข้อมูลของ SMTP
8 bit	ข้อมูลทั้งหมดอยู่ในรูป 8 bit ASCII และมีขนาดความยาวบรรทัดจำกัดตามการส่งข้อมูลของ SMTP
Binary	ข้อมูลทั้งหมดอยู่ในรูป 8 bit ASCII แต่มีขนาดความยาวบรรทัดไม่จำกัด
Quoted-printable	ข้อมูลถูกเข้ารหัสในรูปแบบของ ASCII
Base64	ข้อมูลถูกเข้ารหัสโดยการแม็พจาก 6 bit เป็น 8bit
x-token	สำหรับการเข้ารหัสที่ไม่เป็นมาตรฐาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 การพัฒนาโปรแกรมบน เอ็กซ์-วินโดว์ (x-window)

2.3.1 สิ่งที่จำเป็นต้องมีในการพัฒนาโปรแกรมบน เอ็กซ์-วินโดว์

1. XFree86 เป็น เอ็กซ์-วิน โดว์ ที่แจกจ่ายฟรี โดยมากจะติดมากับยูนิกส์ทุกตัว
2. ระบบปฏิบัติการยูนิกส์
3. ซี คอมไพล์เลอร์ มาพร้อม ยูนิกส์
4. วิน โดว์เมเนเจอร์ (Window Manager)
5. วิน โดว์ ทูลคิต (Windows Toolkit) เป็นส่วนติดต่อกับ เอ็กซ์-วิน โดว์ เหมือนกับ Microsoft Windows API แต่ บน ยูนิกส์ เรียก วิน โดว์ ทูลคิต
6. ความรู้เรื่อง อีเวนท์ไดร์เวน(Event-Driven) ซึ่งเป็นเรื่องของการตอบสนองกับข้อความหรือสัญญาณ

วิน โดว์ ทูลคิต

ธรรมดาในการเขียนโปรแกรมติดต่อกับระบบปฏิบัติการนั้นเราจะต้องมีสิ่งที่เรียกว่าไลบาร์รี่ ในการเชื่อมต่อ ส่วน ไลบาร์รี่ ของ เอ็กซ์-วิน โดว์ นั้นก็คือ XLib ซึ่งเขียนเยอะมากกว่าจะได้งานสักงานหนึ่ง หลาย ๆ คนจึงได้สร้างคลาส ไลบาร์รี่ ขึ้นมาใหม่ ซึ่งที่ใช้ กันอยู่มีหลายชนิด เช่น Xview ,QT ,GTK ,G.N.O.M.E. และอีกหลายๆชนิด

อีเวนท์ไดร์เวน

หลักการของ อีเวนท์ไดร์เวน คือ เป็นการดักทางผู้ใช้ล่วงหน้าว่า ถ้าทำอย่างนี้แล้วโปรแกรมของเราจะทำอะไร เช่น เขียนโปรแกรมขึ้นมาหนึ่งโปรแกรม ให้แสดงปุ่ม 2 ปุ่ม คือ ปุ่ม hello กับ exit แล้วเราออกแบบเอาไว้แล้วว่า ถ้ากดที่ hello จะสวัสดีทักทายทันที และถ้ากดที่ปุ่ม Exit ก็ให้ออกจากโปรแกรม... จากการที่เราออกแบบโปรแกรมไว้อย่างนี้แสดงว่าเราได้ดักเหตุการณ์เอาไว้ 2 กรณี คือ

1.ถ้ากดที่ปุ่มhello

2.ถ้ากดที่ปุ่มexit

ถ้ากดปุ่มใดก็ตอบสนองอย่างหนึ่ง ถ้าไม่กดอะไรเลยก็ไม่ทำอะไร การเขียนโปรแกรมแบบนี้เราเรียกว่า อีเวนท์ไดร์เวน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.2 จีทีเคพลัส (GTK+)

[3]จีทีเคพลัส เป็นอุปกรณ์ที่ช่วยในการสร้างส่วนเชื่อมต่อกับผู้ใช้ (user interfaces) แบบกราฟฟิก โดยขึ้นอยู่กับ ไลบารี่3ไลบารี่ที่ถูกพัฒนาโดย ทีมงานจีทีเค ได้แก่

- Glib เป็นไลบารี่แกนกลางระดับล่าง ซึ่งสร้างพื้นฐานของ จีทีเคพลัส และ GNOME ประกอบด้วยโครงสร้างข้อมูลของภาษาซี , threads, dynamic loading และ object system
- Pango เป็นไลบารี่เกี่ยวกับการจัดวางและการแสดง เกี่ยวกับตัวอักษร
- ATK เป็นไลบารี่เกี่ยวกับกลุ่มของส่วนเชื่อมต่อสำหรับการเข้าถึงโดยง่าย

2.3.3 พื้นฐานโปรแกรมด้วย จีทีเคพลัส

ภาษา C ที่เราเขียนกันนั้น ตามหนังสือต่าง ๆ จะเห็นว่าทำงานแบบ ลำดับ(sequence) คือ ทำทีละคำสั่ง ต่อ ๆ กันไปจนจบโปรแกรม แต่ว่า อีเวนท์ไดร์เวน นั้นใช้หลักของการมีกระบวนการหลายกระบวนการทำงานพร้อม ๆ กัน หรือทำงานเฉพาะงานที่ตัวเองกระทำเมื่อถึงเวลาอันเหมาะสม... เช่น คุณต้องการที่จะสำรองข้อมูลจากฐานข้อมูลที่คุณได้สร้างเอาไว้ และคุณต้องการทำการตรวจสอบข้อมูลไปด้วยพร้อม ๆ กัน จากตรงนี้จะเห็นว่ามีด้วยกัน 2 กระบวนการ คือ หนึ่งจะต้องสำรอง ข้อมูล และสองจะต้องทำการตรวจสอบความถูกต้องของข้อมูล ถ้าเราเขียนโปรแกรมโดยวิธีทั่ว ๆ ไป เราจะต้องสั่ง สำรอง ข้อมูลก่อน แล้วค่อยไปจัดการตรวจสอบความถูกต้องของข้อมูล เป็นขั้นตอนต่อไป

ด้วยเหตุนี้ จึงมีการเพิ่มระบบที่เรียกว่า คอลล์แบ็ค(callback) ลงไปในระบบปฏิบัติการที่ทำงานแบบ มัลติทาสค์กิง (multitasking) และรองรับงานแบบ มัลติโปรแกรมมิ่ง(multiprogramming) หลักการทำงานของมันก็คือว่า มันจะ load process ต่าง ๆ ไปก่อน แล้วเมื่อจะใช้งานมันก็ค่อยเรียกมันมาใช้ ถ้าไม่ได้ใช้ก็ปล่อยเอาไว้เฉยๆ จากตรงนี้เอง ในการออกแบบโปรแกรมเชิง อีเวนท์ไดร์เวน คุณจะต้องมาออกแบบ (กำหนด) ในเรื่องต่อไปนี้อย่างน้อย 3 เรื่อง คือ

1. การสร้างวัตถุ
2. กำหนดความสัมพันธ์ของเหตุการณ์ต่าง ๆ กับวัตถุที่เราสร้างขึ้น
3. เข้าสู่ แมสเสจลูป (message loop) เพื่อให้ทำงานจนกว่าจะออกตามเงื่อนไขที่เรากำหนดในข้อ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนแรก ก็จะเป็นการสั่งสร้างวัตถุต่าง ๆ ที่เราจะให้มีอยู่ในโปรแกรมของเรา

ส่วนที่สอง นั้นก็เป็นการกำหนดว่า เราจะดักเหตุการณ์อะไรบ้าง และเหตุการณ์นั้นจะเกิดขึ้นกับวัตถุอะไรได้บ้าง

ส่วนสุดท้ายก็คือส่วนของ อีเวนท์ลูป(EventLoop) ที่ทำหน้าที่ตรวจสอบเหตุการณ์ที่เกิดขึ้นจริงบนโปรแกรมของเรา แล้วมันก็จะเรียก คอลล์แบ็ค ที่เกี่ยวข้องกับเหตุการณ์นั้นขึ้นมาทำงาน การที่มันรู้ได้ว่าเกิดเหตุการณ์อะไรกับส่วนไหนนั้น เป็นเพราะในความเป็นจริงแล้วตัวผู้ใช้นั้นไม่ได้ติดต่อกับโปรแกรมของเรา แต่เขากำลังติดต่อกับส่วน อินพุท ของระบบปฏิบัติการแล้ว ระบบปฏิบัติการจะทำการเก็บและเรียบเรียงลำดับเหตุการณ์ต่าง ๆ ลง แมสเสจคิว (messagequeue) แล้วโปรแกรมของเราก็มีหน้าที่ไปตรวจสอบที่ แมสเสจคิว อันนี้ว่ามีเหตุการณ์ของเราไหม ถ้ามีมันก็จะทำตามเหตุการณ์ที่เกิดขึ้น ถ้าไม่มันก็ไม่ทำอะไร

<u>การสร้างคอลล์แบ็ค</u>

รูปแบบของคอลล์แบ็ค

```
void  callback_func (GtkObject  *object, GdkEvent *event,
        gpointer  callback_data)
```

GtkObject *object เป็นค่าพอยท์เตอร์ที่ชี้ไปยังวัตถุที่เรียกคอลล์แบ็คตัวนี้ขึ้นมาใช้งาน

GdkEvent *event เป็นค่าพอยท์เตอร์ที่ชี้ไปยัง อีเวนท์ จริง ๆ ที่เราทำการซ้อนทับมันมา

gpointer callback_data เป็นข้อมูลที่ส่งมาพร้อมกับการเรียกคอลล์แบ็ค

<u>การดักสัญญาณ</u>

รูปแบบคำสั่ง

```
gint  gtk_signal_connect (GtkObject     *object,
                          gchar         *name,
                          GtkSignalFunc   func,
                          gpointer        func_data)
```

GtkObject *object เป็นค่าพอยท์เตอร์ของวัตถุที่เราจะดักเหตุการณ์ ที่จะเกิดกับมัน

gchar *name เป็นชื่อของเหตุการณ์ที่เราจะดัก

GtkSingnalFunc func เป็นชื่อของ คอลล์แบ็คฟังก์ชั่นที่จะต้องทำงานเมื่อเกิดเหตุการณ์ตามข้อที่ 2 กับวัตถุในข้อที่ 1

gpointer func_data เป็นค่าของข้อมูลที่จะส่งให้กับ คอลล์แบ็คฟังก์ชั่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตัวอย่างเช่น gtk_signal_connect (GTK_OBJECT(button), "clicked",

GTK_SIGNAL_FUNC(hello), NULL);

ทั้งหมดนี้หมายความว่าเรากำลังดักเหตุการณ์ที่ชื่อว่า "clicked" กับวัตถุที่ชี้โดยตัวแปร button เมื่อเกิดเหตุการณ์ "clicked" ขึ้นมากับวัตถุที่ button ชี้ก็จะเรียกคอลล์แบ็คฟังก์ชั่นที่ชื่อ hello ขึ้นมาทำงานแล้วก็ไม่มีค่าอะไรส่งไปให้คอลล์แบ็คฟังก์ชั่น

2.4 การเข้าและถอดรหัส เบส64 (Base64 Encoding and Decoding)

[2]Base64 Content-Transfer-Encoding ถูกออกแบบมาเพื่อเป็นตัวแทนของลำดับที่ไม่แน่นอนกลุ่มฐานแปดในรูปแบบที่มนุษย์ไม่สามารถอ่านได้ มีการเข้าหรัสและการถอดรหัสที่ง่ายแต่ข้อมูลที่ถูกเข้ารหัสจะมีขนาดเพียง 33 เปอร์เซ็นต์ ของข้อมูลเริ่มต้น

ใช้ 65 ตัวอักษรจาก ยูเอส-แอสกี(US-ASCII) ทำให้สามารถใช้ 6 บิต ในการแสดงแทน ตัวอักษรได้ (ตัวอักษรพิเศษ ตัวที่ 65 "=" ใช้เพื่อแสดงว่าเป็นกระบวนการพิเศษ)
กระบวนการเข้ารหัสแสดงให้เห็นโดย กลุ่มข้อมูลเข้า 24 บิต ไปเป็นตัวอักษรที่ถูกเข้ารหัส4ตัวอักษร โดยเริ่มจากซ้ายไปขวา โดย 24 บิตอินพุต มาจากกลุ่มของอินพุต 8 บิต 3 กลุ่ม ซึ่ง 24 บิต นี้จะถูกแบ่งเป็น 4กลุ่ม กลุ่มละ 6 บิต โดยแต่ละกลุ่มจะถูกแปลงไปเป็นตัวอักษร1ตัวจาก ตัวอักษรของเบส64 เมื่อมีการเข้ารหัสกระแสบิตโดย เบส64 กระแสบิตจะถูกสมมติฐานลำดับโดยวิธี " บิตแรกมีความสำคัญสูงสุด (most-significant-bit first)" คือบิตแรกของกระแสบิตเป็นบิตที่มีลำดับสูงสุดในไบต์แรก และบิตที่ 8 มีความสำคัญน้อยสุดในไบต์แรก และเช่นเดียวกันในไบต์ต่อๆไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 2.4 ตารางอักษรของ base 64

The Base64 Alphabet

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	P	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w	(pad)	=
15	P	32	g	49	x		
16	Q	33	h	50	y		

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กระแสของเอาท์พุตจะต้องไม่เกิน 76 ตัวอักษรต่อบรรทัด และตัวอักษรปิดบรรทัดหรือตัวอักษรอื่นๆที่ไม่ได้อยู่ในตารางจะไม่ถูกนำมาคิดในการถอดรหัส หากข้อมูลอินพุตมีน้อยกว่า24บิต บิตศูนย์จะถูกเติมเข้าไปทางด้านขวาและส่วนท้ายของข้อมูลเอาท์พุตจะถูกรองไว้ด้วยตัวอักษร “=”

สรุปได้ว่าหากอินพุตเป็นตัวเลขฐานแปด

1. หากอินพุตมี 24 บิต เอาท์พุตจะมี4ตัวอักษรโดยไม่มีตัวอักษร “=” รองท้าย
2. หากอินพุตมี 8 บิต เอาท์พุตจะมี2ตัวอักษรที่เข้ารหัสและ “=” อีก2 ตัว
3. หากอินพุตมี 16 บิต เอาท์พุตจะมี 3 ตัวอักษรที่เข้ารหัสและ “=” อีก 1 ตัว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่3
การออกแบบโครงงาน

3.1 กำหนดขอบเขตความสามารถของโครงงาน

ขอบเขตของงานที่ทำคือ

1. สามารถแสดงรายการของไฟล์ที่ดักจับมาได้

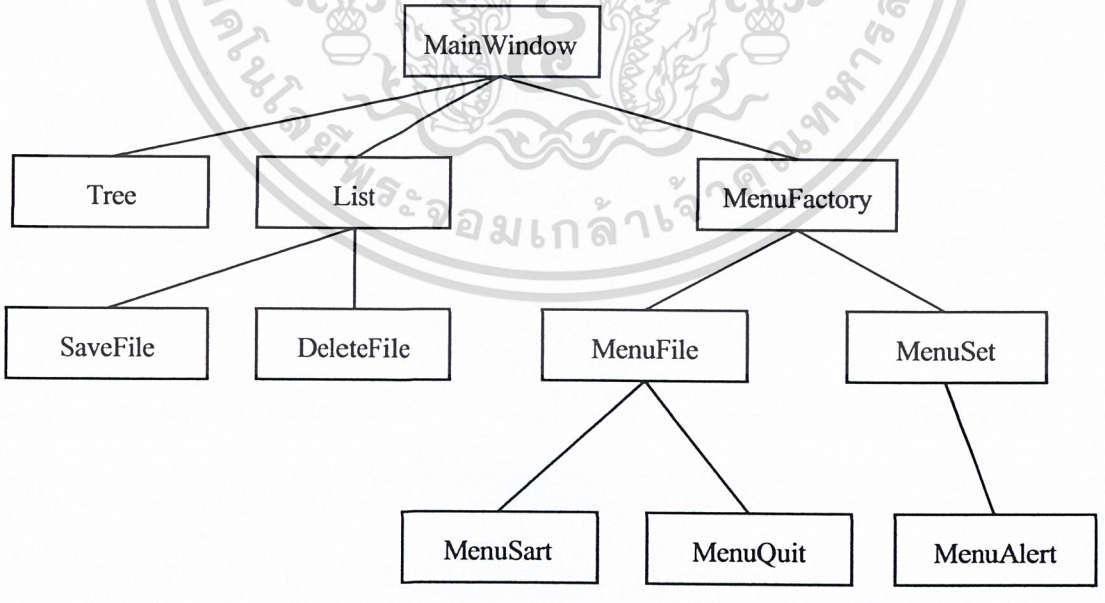
2.สามารถแสดงผลไฟล์ออกมาในรูปแบบที่เหมาะสมได้ เช่น แพ็คเก็ตของ SMTP สามารถแสดงรายละเอียดของเมล์และไฟล์ที่แนบมาได้

3.มีระบบตรวจสอบแพ็คเก็ตที่น่าสงสัยและแจ้งเตือนได้

4.สามารถควบคุมหรือสั่งการโปรแกรม สนิฟอิท เพื่อให้โปรแกรมสนิฟอิททำการจับแพ็คเก็ตได้

3.2 การออกแบบส่วนติดต่อกับผู้ใช้

ในการเขียนโปรแกรมแบบ อีเวนท์ไดรเวนจะต้องสร้างวัตถุ(widget)ขึ้นมาเพื่อรองรับสัญญาณเพื่อที่จะปฏิบัติงานตามสัญญาณนั้นๆ จึงได้ทำการออกแบบวัตถุต่างๆไว้ดังนี้



รูปที่ 3.1 widget ที่สำคัญในหน้าต่างหลัก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

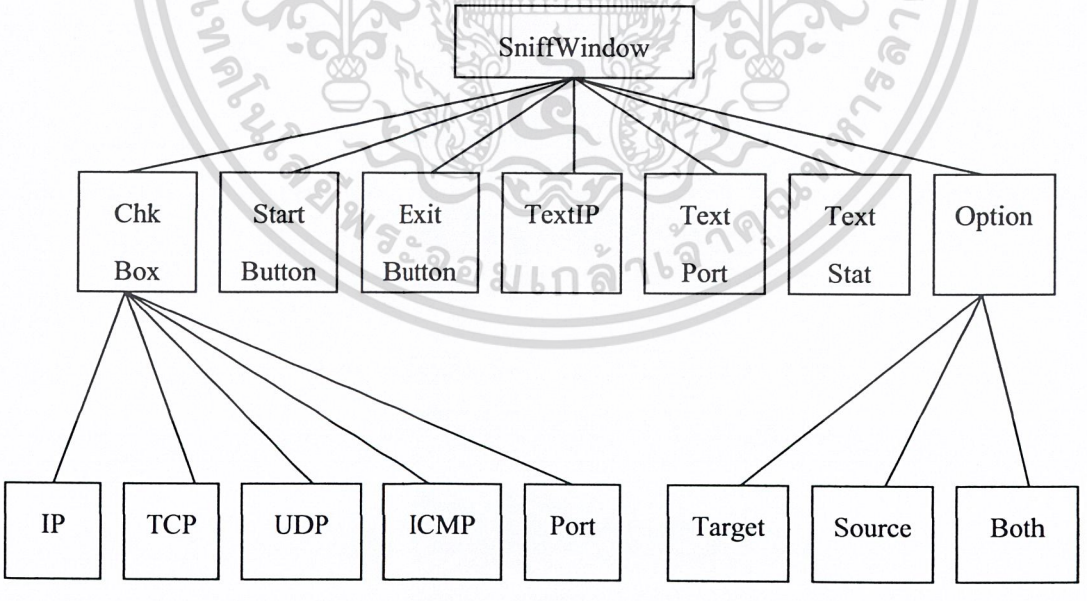
จากรูปที่ 3.1 วัตถุ MainWindow จะเป็นตัวบรรจุวัตถุต่างๆและกำหนดค่าต่างๆให้กับวัตถุ คือ ทำการสร้างรายการของ Tree ด้วยฟังก์ชั่น *Make_Tree()* และ สร้างรายการของ List ด้วยฟังก์ชั่น *Make_dir_list()* โดยจะมีสัญญาณที่รอรับคือ "Destroy" ซึ่งจะทำการเรียกฟังก์ชั่น *gtk_main_quit()* ทำให้เกิดการปิดโปรแกรม

วัตถุ Tree จะบรรจุรายการของไดเรคเทอร์รี่ซึ่งจะมี 2 ไดเรคเทอร์รี่ คือ SMTP และ HTML เมื่อมีสัญญาณ " Select-Child" จะทำการเรียกฟังก์ชั่น *SelectTree()*

วัตถุ List จะบรรจุรายการของไฟล์ในไดเรคเทอร์รี่นั้น เมื่อมีสัญญาณ " Select-Row" จะทำการเรียกฟังก์ชั่น *SelectList()*

วัตถุ MenuFactory คือเมนูบาร์ ซึ่งจะบรรจุวัตถุอีก 2 อย่างคือ MenuFile และ MenuSet โดยที่ MenuFile บรรจุวัตถุอีก 2 อย่างคือ MenuStart และ MenuQuit ขณะที่ MenuSet บรรจุวัตถุ MenuAlert โดยที่หากมีสัญญาณ " clicked" ที่เมนูใดก็จะทำการเรียกฟังก์ชั่นขึ้นมา โดย MenuStart จะเรียกฟังก์ชั่น *Sniff()* MenuQuit เรียกฟังก์ชั่น *file_quit_cmd_callback()* และ MenuAlert เรียกฟังก์ชั่น *get_alert_text()*

เมื่อมีการเรียกฟังก์ชั่น *Sniff()* ฟังก์ชั่น *Sniff()* จะทำการสร้างหน้าต่างขึ้นมาใหม่ดังนี้

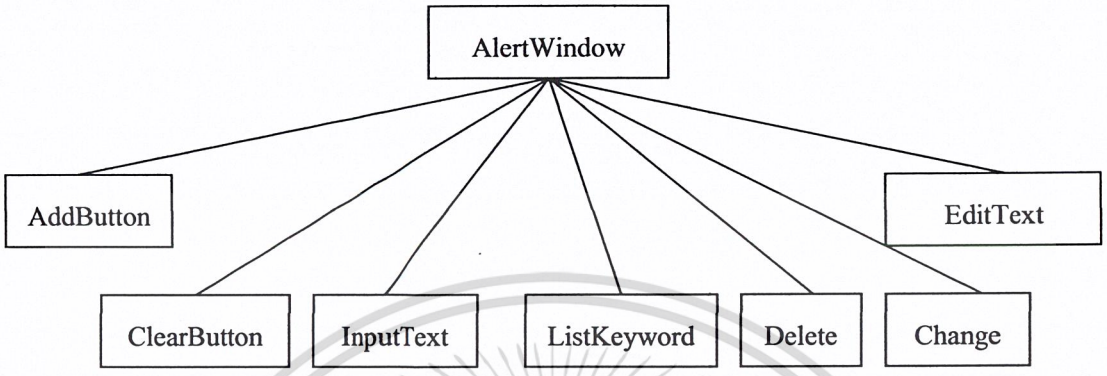


รูปที่3.2 widget ของหน้าต่าง SniffWindow

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

เมื่อมีการเรียกฟังก์ชั่น *get_alert_text()* ฟังก์ชั่น *get_alert_text()* จะทำการสร้างหน้าต่างขึ้นมาใหม่ดังนี้



รูปที่ 3.3 widget ของหน้าต่าง AlertWindow

เมื่อมีสัญญาณ "Clicked" ที่วัตถุ AlertWindow วัตถุ AlertWindow จะเรียกฟังก์ชั่น *destroy_window()*

เมื่อมีสัญญาณ "Clicked" ที่วัตถุ AddButton วัตถุ AddButton จะเรียกฟังก์ชั่น *show_dialog()*

เมื่อมีสัญญาณ "Clicked" ที่วัตถุ ClearButton วัตถุ ClearButton จะเรียกฟังก์ชั่น *clear_text()*

เมื่อมีสัญญาณ "Select_Row" ที่วัตถุ Listkeyword วัตถุ Listkeyword จะเรียกฟังก์ชั่น *put_to_edittext()*

เมื่อมีสัญญาณ "Clicked" ที่วัตถุ DeleteButton วัตถุ DeleteButton จะเรียกฟังก์ชั่น *delete_key()*

เมื่อมีสัญญาณ "Clicked" ที่วัตถุ ChangeButton วัตถุ ChangeButton จะเรียกฟังก์ชั่น *change_key()*

เมื่อวัตถุ List ได้รับสัญญาณ " Select-Row" จะทำการเรียกฟังก์ชั่น *SelectList()* ซึ่งจะสร้างหน้าต่างใหม่ขึ้นมา ชื่อว่า ShowWindow โดยจะมีการแสดง 2 แบบ คือ

1.หากแพ็คเก็ตนั้นเป็นแพ็คเก็ต SMTP จะแสดงรายละเอียดของแพ็คเก็ตนั้น และถ้ามีเอกสารแนบประเภทมาด้วยก็จะแสดงขึ้นมาในอีกหน้าต่างหนึ่ง

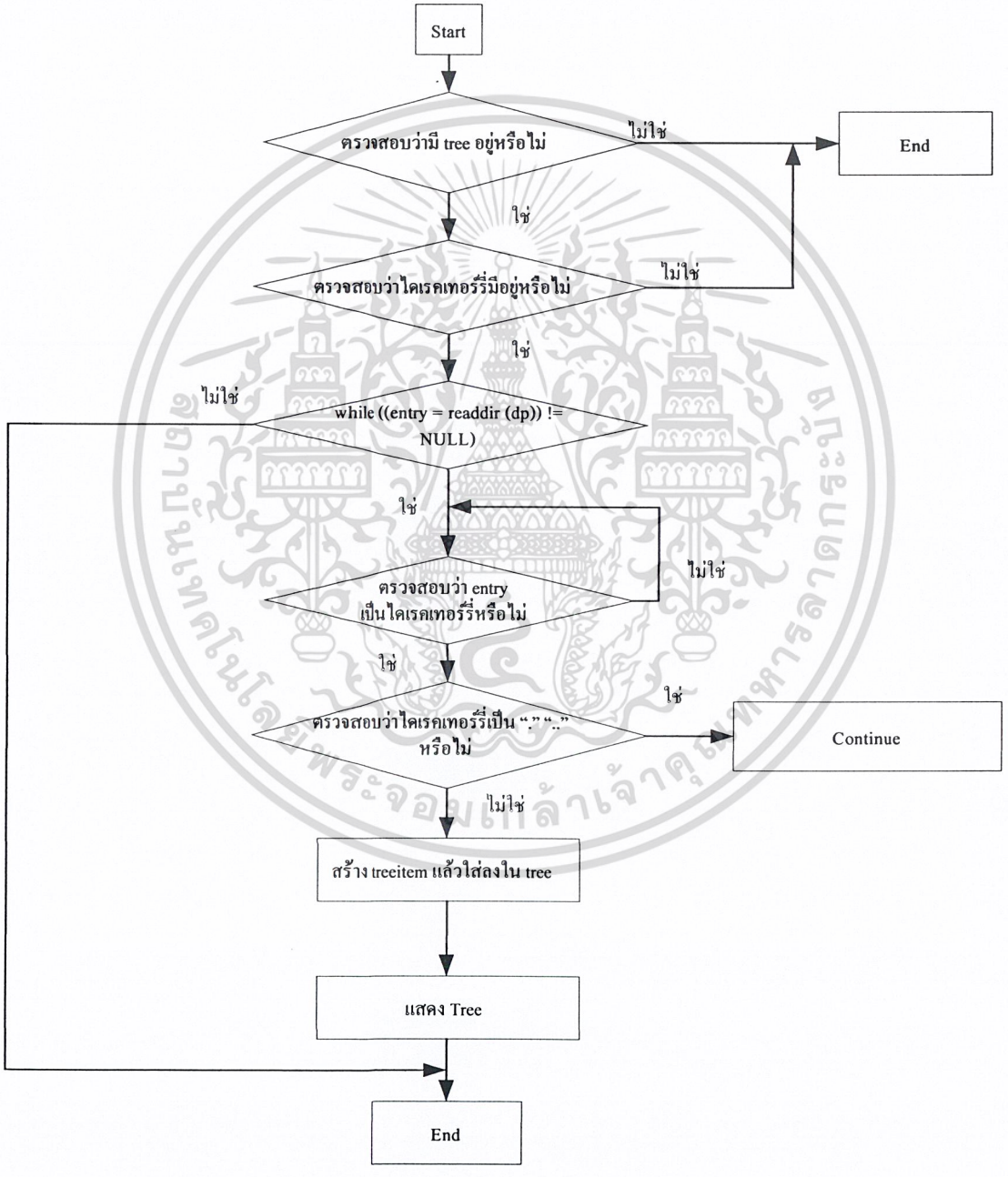
2.หากแพ็คเก็ตนั้นเป็นแพ็คเก็ต HTTP จะแสดงรายละเอียดของแพ็คเก็ตนั้น และจะทำการเรียก mozilla เพื่อแสดงหน้าเวปเพจ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
50285

3.3 โฟลชาร์ทของฟังก์ชั่นที่สำคัญ

3.3.1 ฟังก์ชั่น make_tree()

ฟังก์ชั่น make_tree() ใช้ในการสร้างรายการของไดเรคเทอร์รี่ลงบนwidget Tree

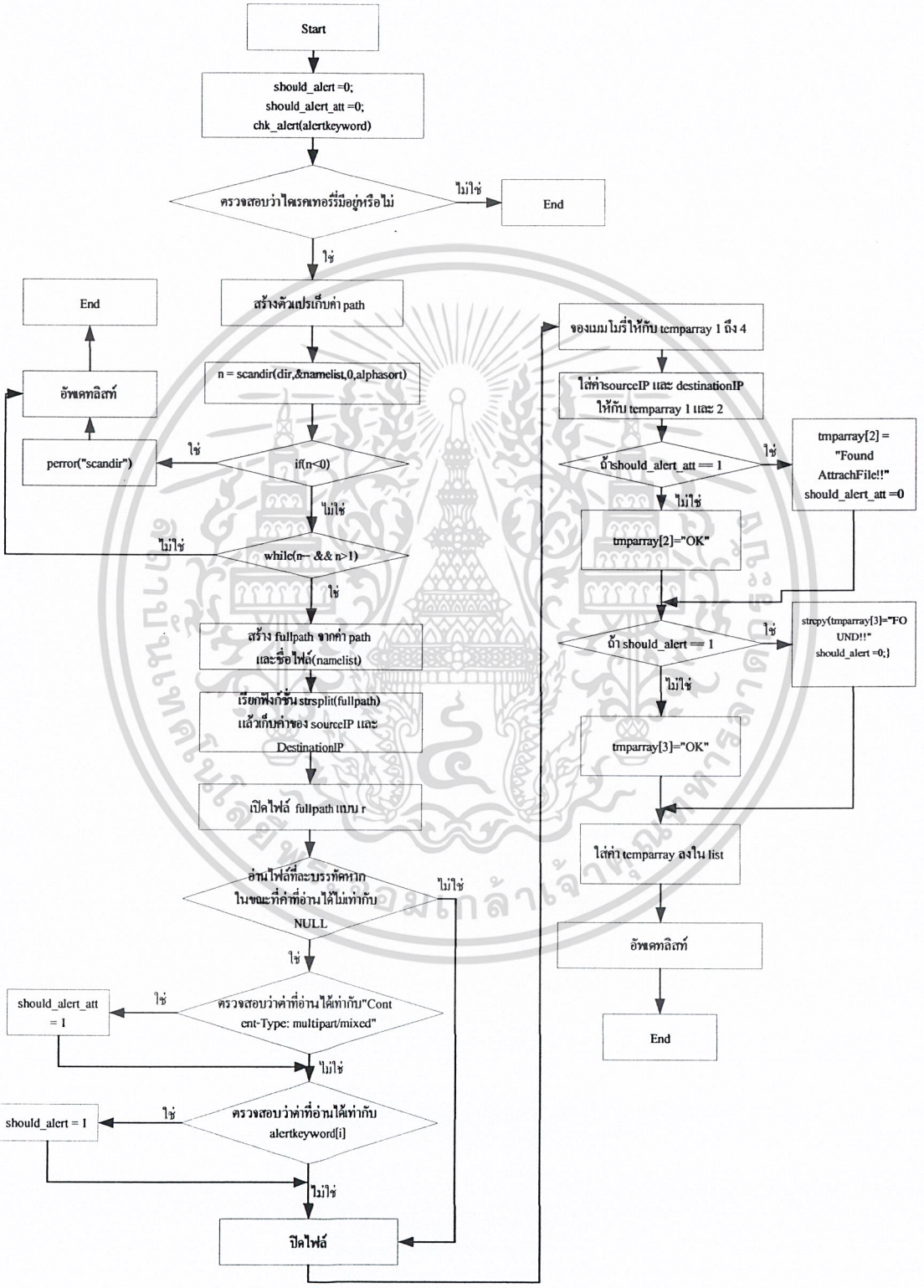


รูปที่ 3.4 ฟังก์ชั่น make_tree()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.2 ฟังก์ชั่น Make_dir_list()

ฟังก์ชั่น Make_dir_list() ใช้ในการสร้างรายการของล็อกไฟล์ ลงบนwidget List

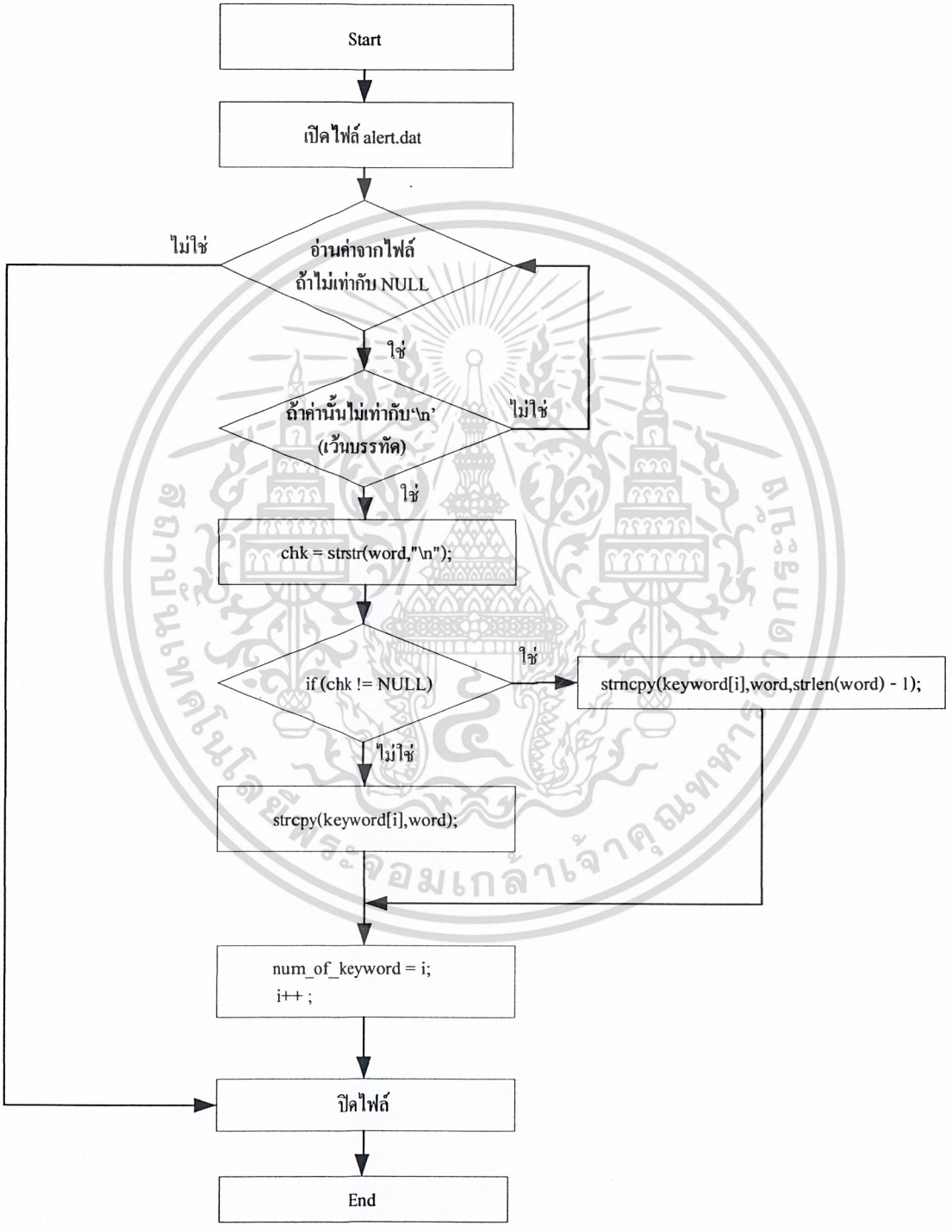


รูปที่ 3.5 ฟังก์ชั่น make_dir_list()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.3 ฟังก์ชั่น Chk_Alert ()

ฟังก์ชั่น Chk_Alert() ใช้สร้างอาเรย์ของคีย์เวิร์ดจากไฟล์

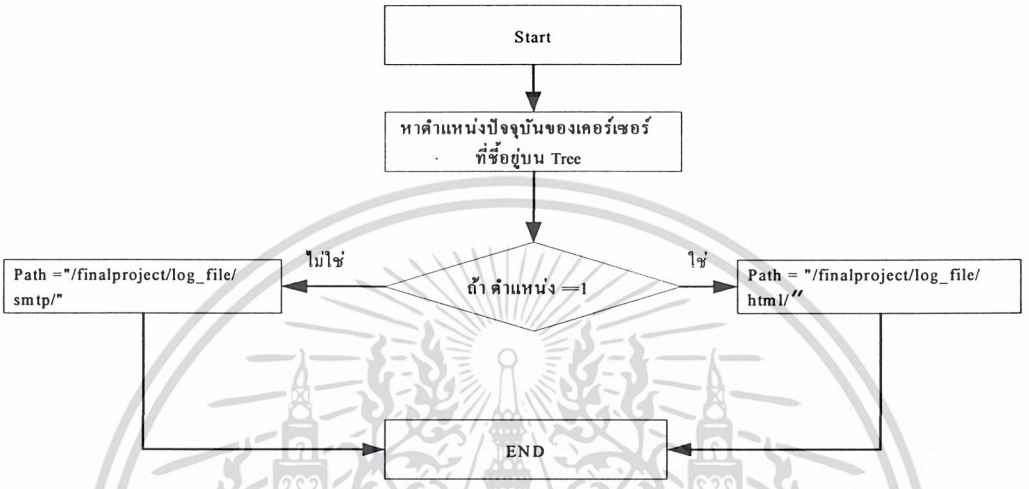


รูปที่ 3.6 ฟังก์ชั่น chk_alert()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.4 ฟังก์ชั่น Selecttree()

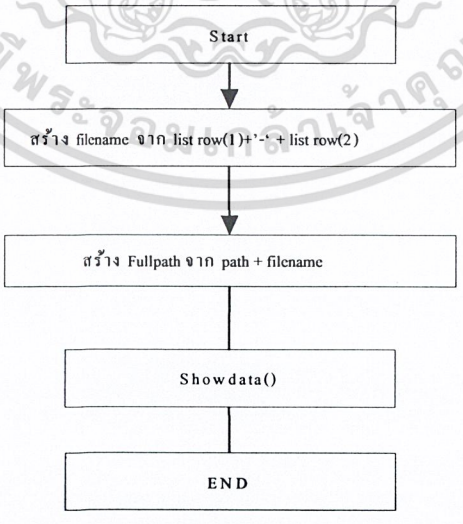
เมื่อมีสัญญาณ Select_row มาที่ widget Tree ฟังก์ชั่น Selecttree() จะทำการตรวจสอบว่าไดเรคเทอร์รี่ของล็อกไฟล์ที่เลือกเป็นไดเรคเทอร์รี่ใดแล้วจึงกำหนดค่าให้ตัวแปร Path



รูปที่ 3.7 ฟังก์ชั่น selecttree()

3.3.5 ฟังก์ชั่น SelectList()

เมื่อมีสัญญาณ Select_row มาที่ widget List ฟังก์ชั่น SelectList() จะสร้างตัวแปล Fullpath แล้วส่งไปให้ ฟังก์ชั่น Showdata()

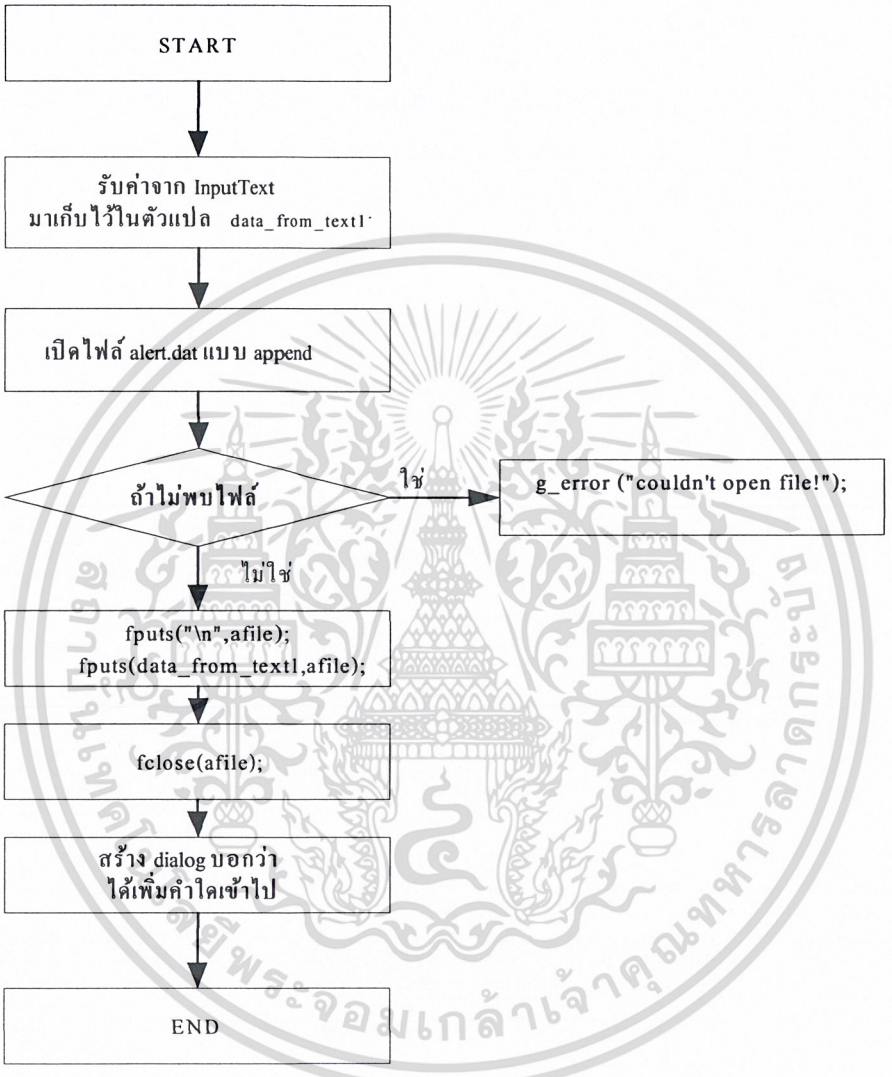


รูปที่ 3.8 ฟังก์ชั่น selectlist()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.6 ฟังก์ชั่น Showdialog()

ใช้เพิ่มคีย์เวิร์ดลงในไฟล์

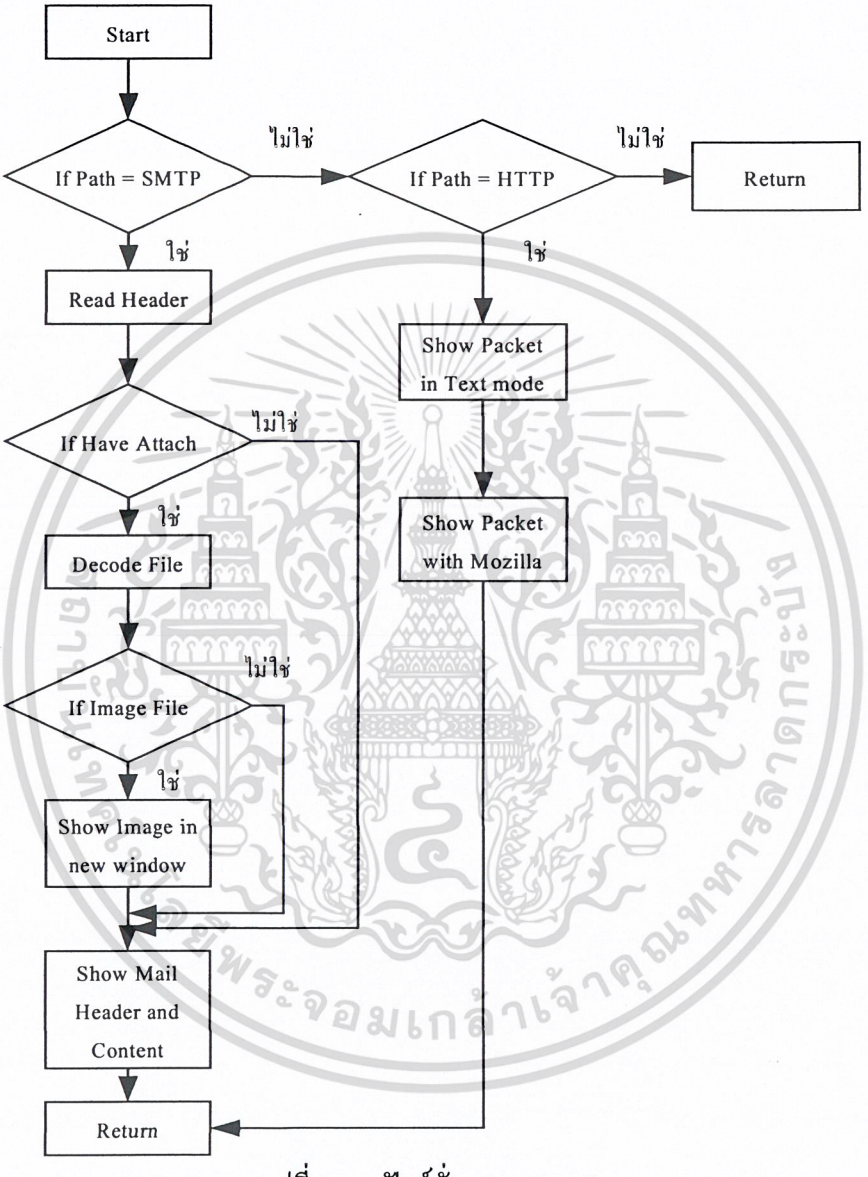


รูปที่ 3.9 ฟังก์ชั่น showdialog()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.7 ฟังก์ชั่น ShowData()

ใช้แสดงรายละเอียดของแพ็คเก็ต

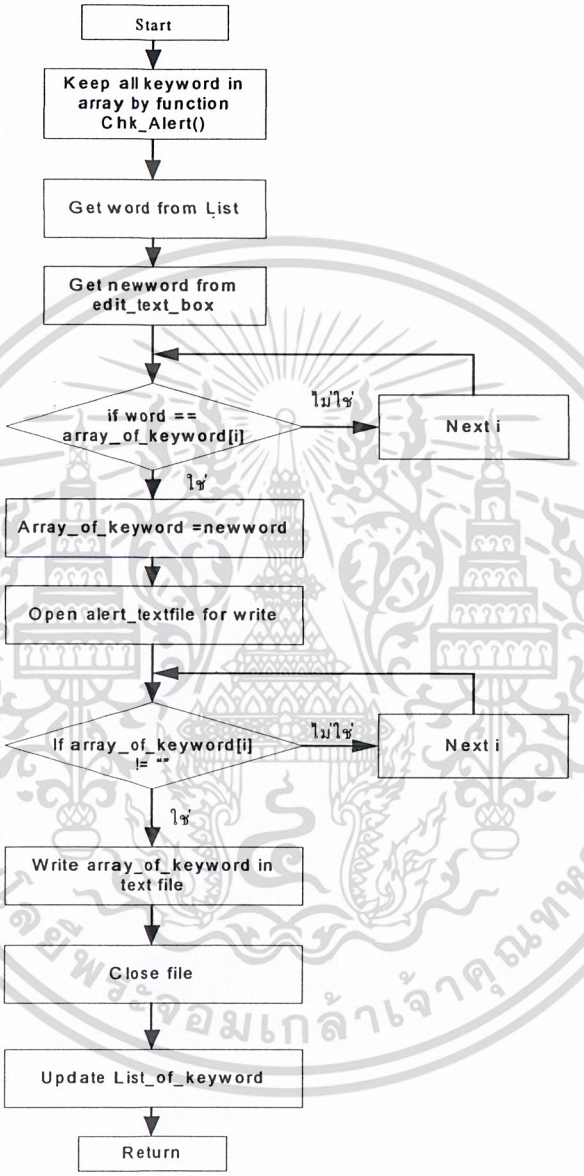


รูปที่ 3.10 ฟังก์ชั่น showdata()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.8 ฟังก์ชั่น Change_keyword()

ใช้แก้ไขคีย์เวิร์ด

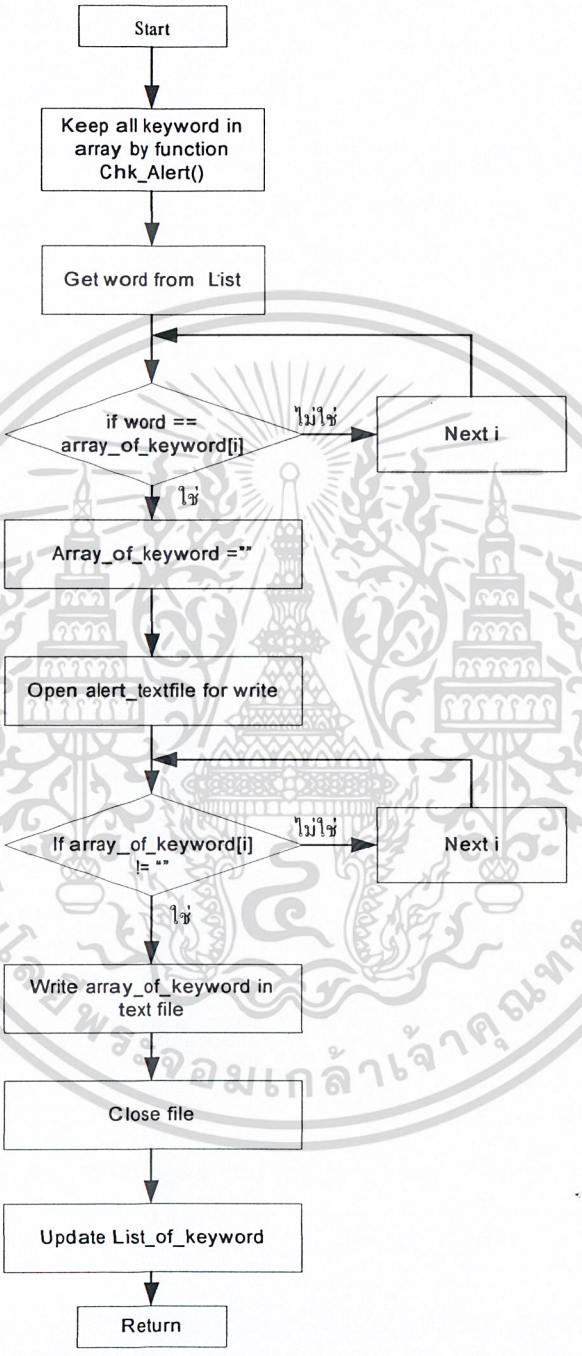


รูปที่ 3.11 ฟังก์ชั่น change_keyword()

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.8 ฟังก์ชั่น Delete_keyword()

ใช้ลบคีย์เวิร์ด



รูปที่ 3.12 ฟังก์ชั่น delete_keyword()

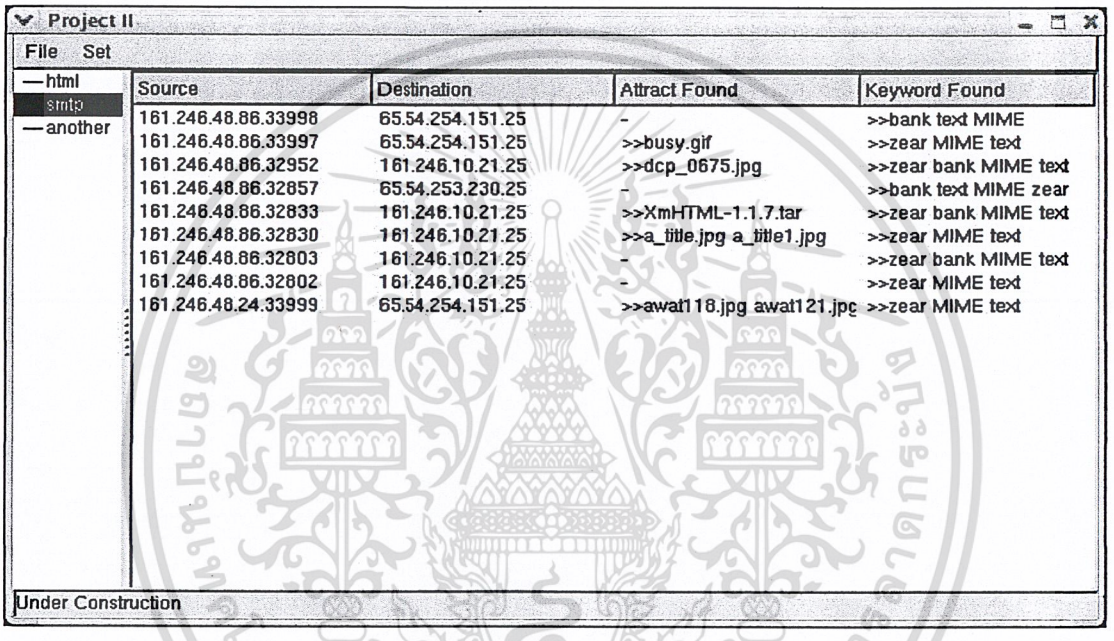
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

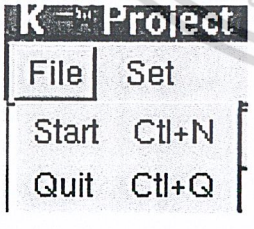
ผลการทดลอง

4.1 เริ่มเปิดโปรแกรม

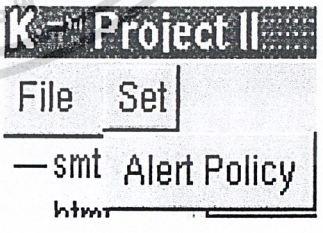
เมื่อเริ่มเปิดโปรแกรมจะแสดงหน้าต่างแรกดังรูป



รูปที่ 4.1 หน้าต่างหลัก



(ก)



(ข)

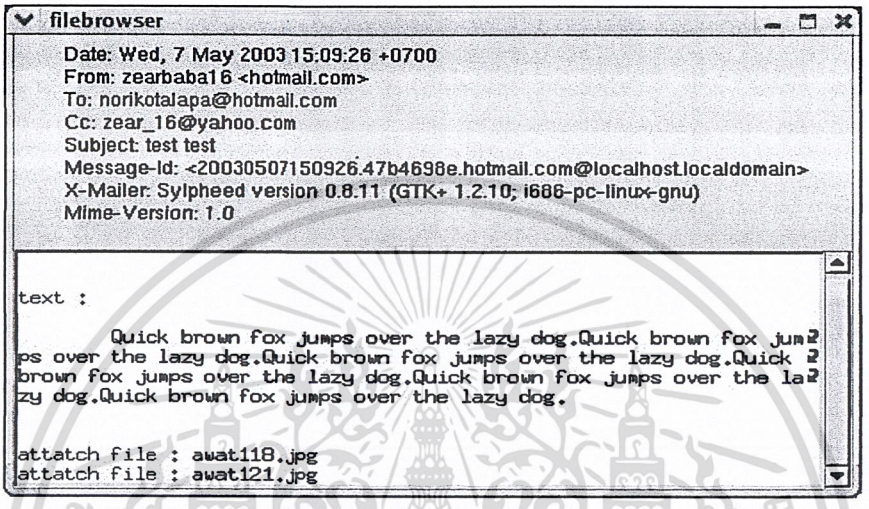
รูปที่ 4.2 (ก) เมนูย่อย ของ เมนูไฟล์

รูปที่ 4.2 (ข)) เมนูย่อย ของ เมนูเซต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

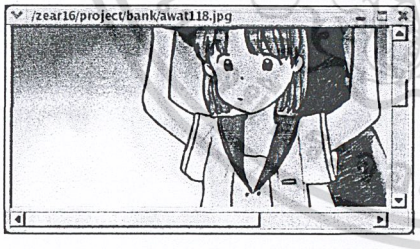
4.2 การแสดงผลของแพ็คเก็ต SMTP

เมื่อเลือกล็อกไฟล์จาก List ขณะที่อยู่ที่ไดเรคเทอร์รี่ SMTP ทำให้โปรแกรมสร้างหน้าต่างที่ใช้แสดงผลขึ้นมาใหม่ดังภาพ

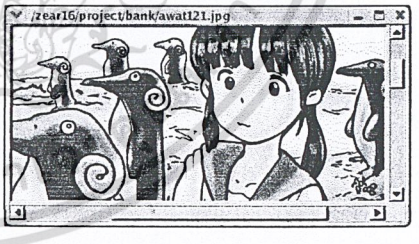


รูปที่ 4.3 หน้าต่างแสดงรายละเอียดของแพ็คเก็ต SMTP

และหากมีไฟล์รูปภาพแนบมาด้วยโปรแกรมจะทำการแสดงนั้นขึ้นมาทั้งหมด



(ก)



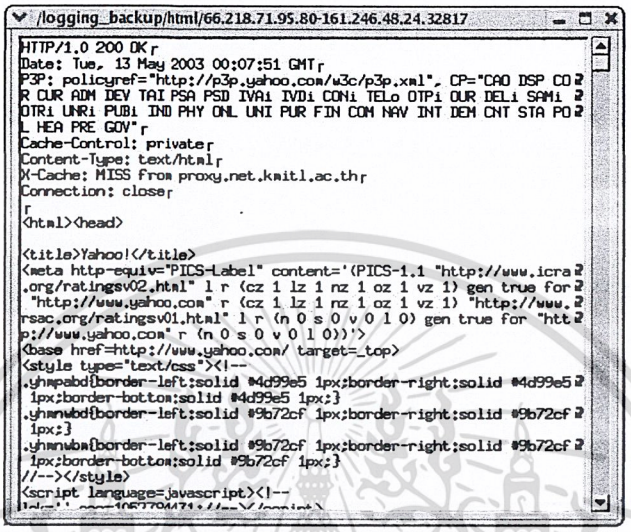
(ข)

รูปที่ 4.4(ก) แสดงรูปภาพที่แนบมากับเอกสาร SMTPรูปที่ 1
รูปที่ 4.4(ข) แสดงรูปภาพที่แนบมากับเอกสาร SMTPรูปที่ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

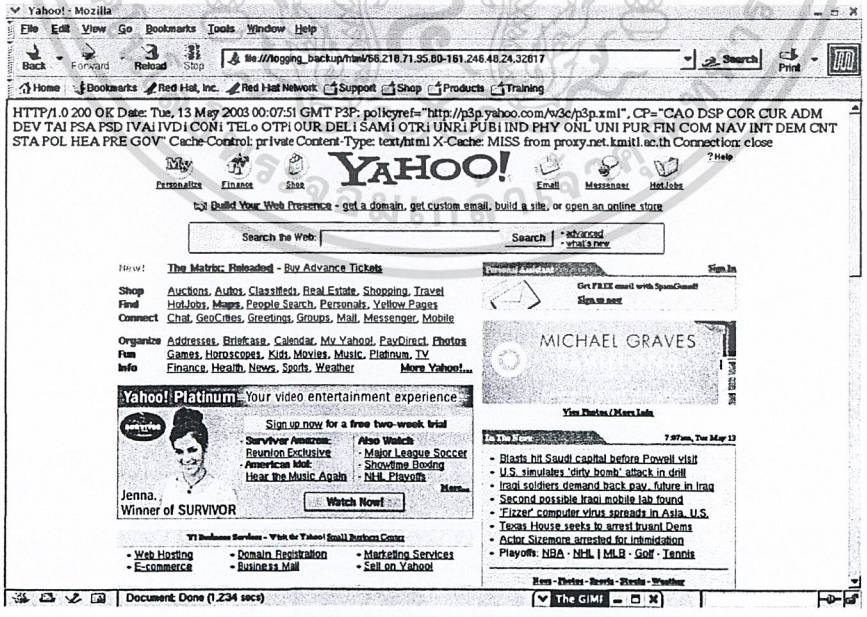
4.3 การแสดงผลของแพ็คเก็ต SMTP

เมื่อเลือกล็อกไฟล์จาก List ขณะที่อยู่ที่ไดเรคเทอร์รี่ HTML ทำให้โปรแกรมสร้างหน้าต่างที่ใช้แสดงผลขึ้นมาใหม่ดังภาพ



รูปที่ 4.5 หน้าต่างแสดงรายละเอียดของแพ็คเก็ต HTTP

และแสดงไฟล์นั้นในแบบเวปเพจด้วย Mozilla ดังรูป

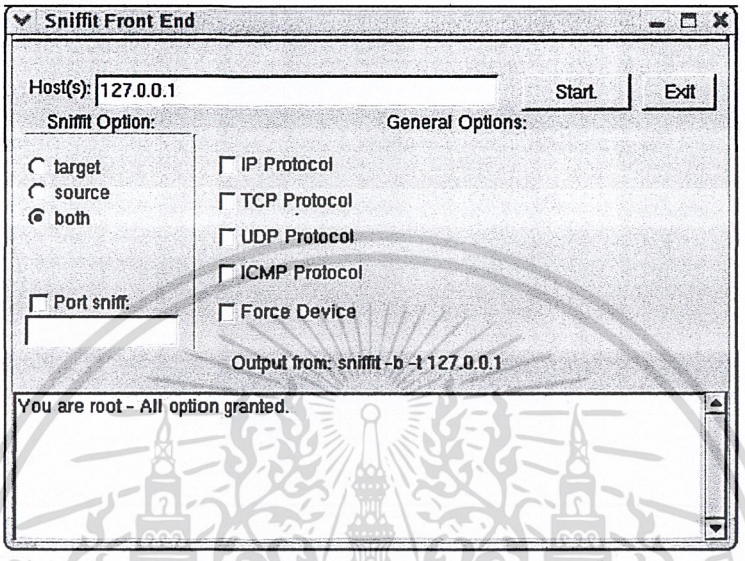


รูปที่ 4.6 แสดงไฟล์ HTTP ด้วย Mozilla

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

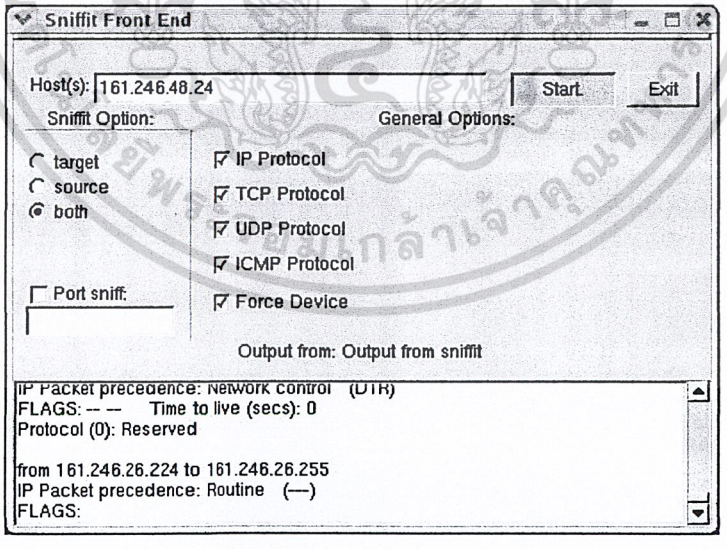
4.4 เลือกเมนู File/Start

จะทำการเรียกหน้าต่าง Sniffit Font End ขึ้นมาดังรูป



รูปที่ 4.7 หน้าต่างSniffit Front End

เมื่อเลือก option เสร็จแล้ว ทำการกดปุ่ม Start โปรแกรมจะเริ่มทำการจับแพ็คเก็ตดังรูป



รูปที่ 4.8 หน้าต่างSniffit Front End ขณะทำงาน

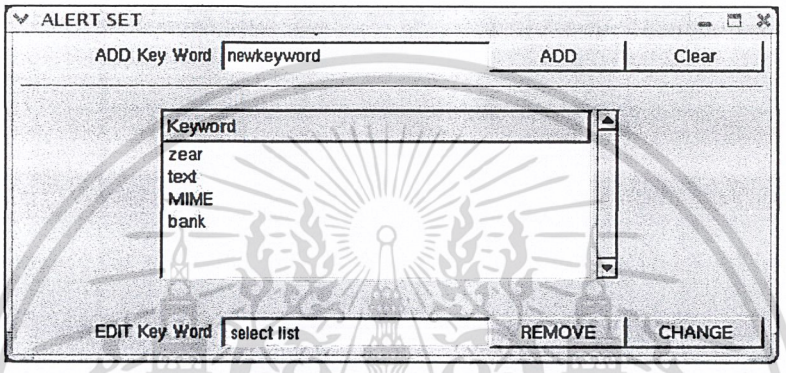
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.5 เลือกเมนู File/Quit

จะทำการปิดโปรแกรม

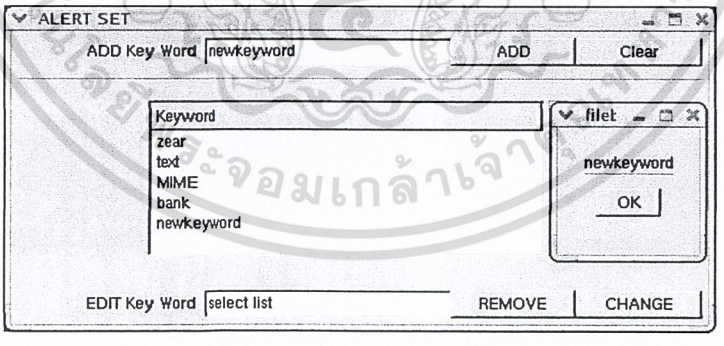
4.6 เลือกเมนู Set/Alert

จะทำการสร้างหน้าต่าง Alert Set



รูปที่ 4.9 หน้าต่าง Alert Set

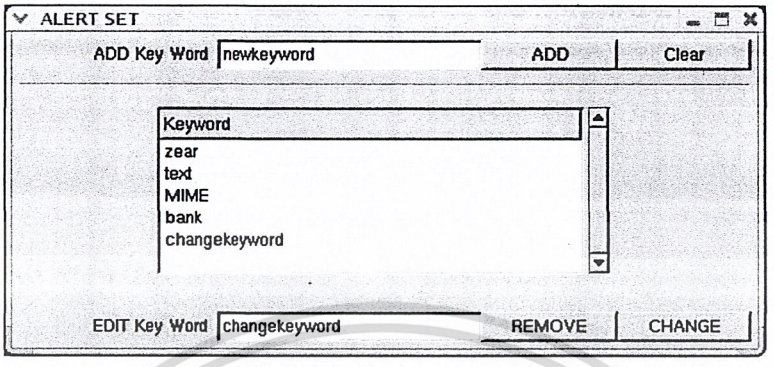
การเพิ่มคีย์เวิร์ด



รูปที่ 4.10 การเพิ่มคีย์เวิร์ด

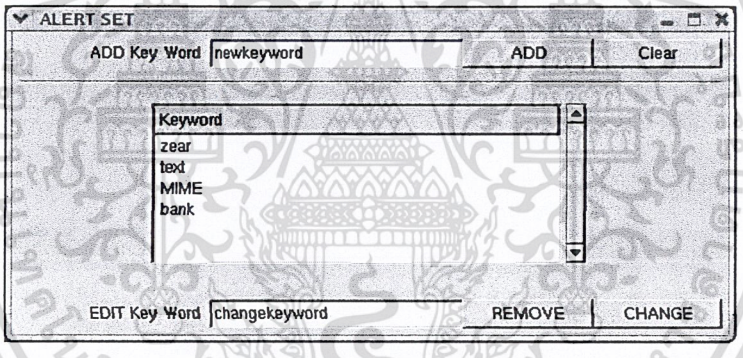
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การแก้ไขคีย์เวิร์ด



รูปที่ 4.11 การแก้ไขคีย์เวิร์ด

การลบคีย์เวิร์ด

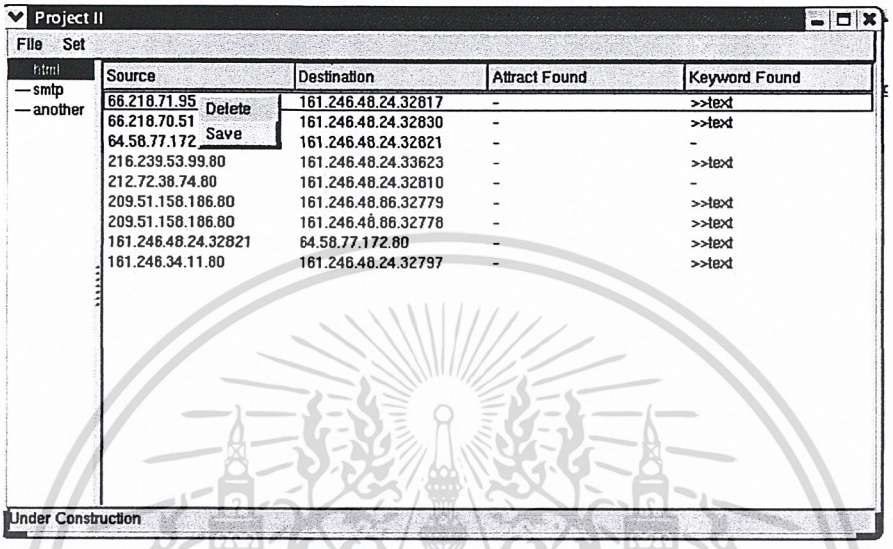


รูปที่ 4.12 การลบคีย์เวิร์ด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

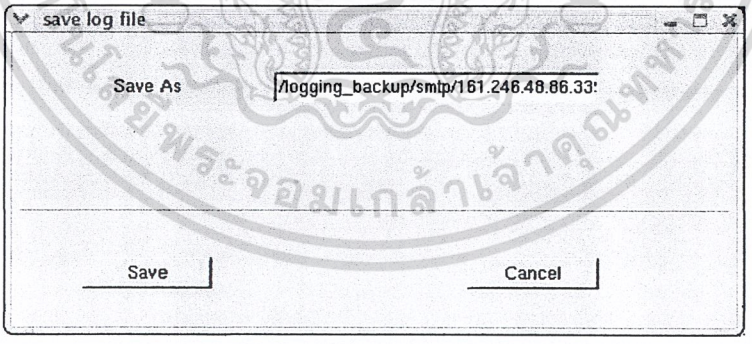
4.7 การลบและบันทึกล็อกไฟล์

เมื่อคลิกขวาที่ล็อกไฟล์จะมีเมนูขึ้นมาดังภาพ



รูปที่ 4.13 เมนูการลบหรือบันทึกล็อกไฟล์

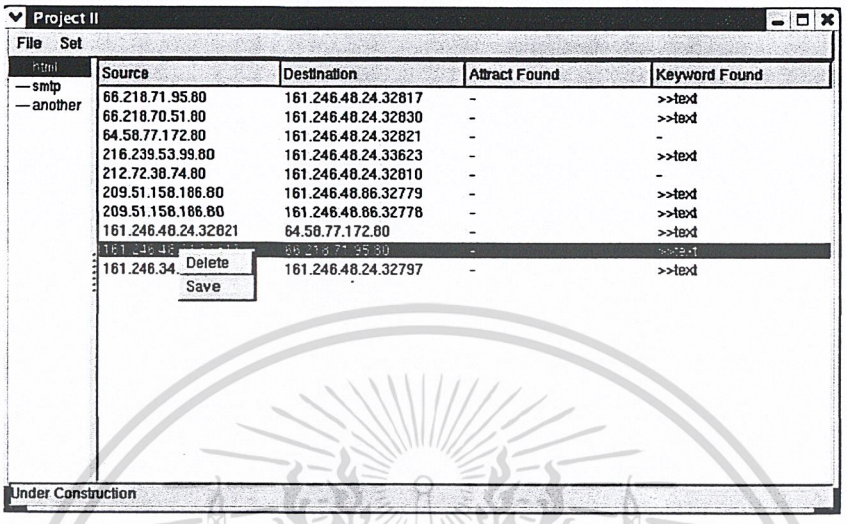
เมื่อเลือกเมนู Save จะมีหน้าต่างขึ้นมาให้ทำการใส่ชื่อที่ต้องการเซฟดังรูป



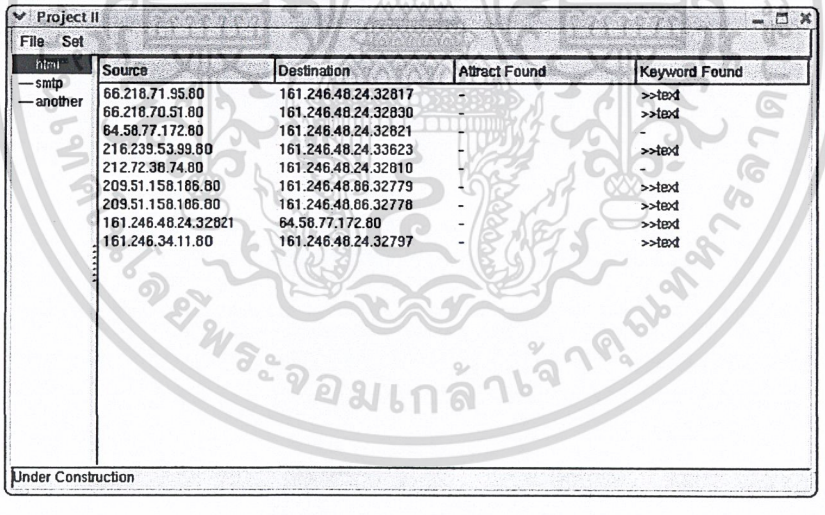
รูปที่ 4.14 หน้าต่างการบันทึกล็อกไฟล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การลบล็อกไฟล์เมื่อเลือกเมนู Delete โปรแกรมจะทำการลบไฟล์โดยทันที



รูปที่ 4.15 เลือกเมนู Delete



รูปที่ 4.16 ลบล็อกไฟล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุป

5.1 สรุปการพัฒนาโครงงาน

จากการศึกษาและพัฒนาโครงงานชิ้นนี้ สรุปว่าสามารถทำได้ใกล้เคียงกับจุดมุ่งหมายที่วางไว้ มีบางส่วนที่ยังไม่สามารถทำตามที่ออกแบบไว้ได้ในขณะนี้ และ ยังมีข้อผิดพลาดอยู่บ้างที่ยังไม่ได้รับการแก้ไข สำหรับสิ่งที่ได้รับจากโครงงานนี้คือประสบการณ์ในการพัฒนาโปรแกรมด้วยภาษา ซี การใช้งานระบบปฏิบัติการลินุกส์และยูนิกส์ และความรู้เกี่ยวกับการใช้งานโพรโตคอลเอสเอ็มทีพี

5.2 ปัญหาที่เกิดขึ้นระหว่างการพัฒนาโครงงาน

ปัญหาที่พบจากการพัฒนาโครงการส่วนใหญ่จะเกี่ยวข้องกับการใช้เครื่องมือ จีทีเคพลัส ที่ต้องทำการศึกษาหาความรู้จากเวปไซต์ต่างๆ ซึ่งส่วนใหญ่เป็นภาษาอังกฤษ ทำให้เรียนรู้และเข้าใจได้ค่อนข้างช้า ต้องมีการทดลองเขียน ลองผิดลองถูก ทำให้ค่อนข้างเสียเวลา ปัญหาที่พบอีกอย่างคือปัญหาเกี่ยวกับเครื่องคอมพิวเตอร์ ที่เสียบ่อย และปัญหาการใช้งานระบบปฏิบัติการลินุกส์

5.3 แนวทางในการพัฒนาโครงงานต่อ

สำหรับแนวทางในการพัฒนาต่อจะเป็นการเพิ่มเติมในส่วนที่ยังไม่สมบูรณ์ การแสดงรายละเอียดของแต่ละแพ็คเก็ตที่มากกว่านี้ เพิ่มตัวถอดรหัสให้สามารถถอดรหัสข้อมูลให้ได้หลายชนิดกว่านี้ และอาจจะทำให้โปรแกรมแสดงผลเป็นแบบเรียลไทม์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

[1] Jonathan B. Postel: "SIMPLE MAIL TRANSFER PROTOCOL" ,RFC 821 SIMPLE MAIL TRANSFER PROTOCOL

[2] N. Freed, N. Borenstein : "MIME Part One:Format of Internet Message Bodies", **RFC 2045 :** MIME Part One: Format of Internet Message Bodies

[3] Supachai Budsaratij : "How to X-programming with GTK, Part I", http://www.thailinux.com/x-prog/gtk/gtk-01.html

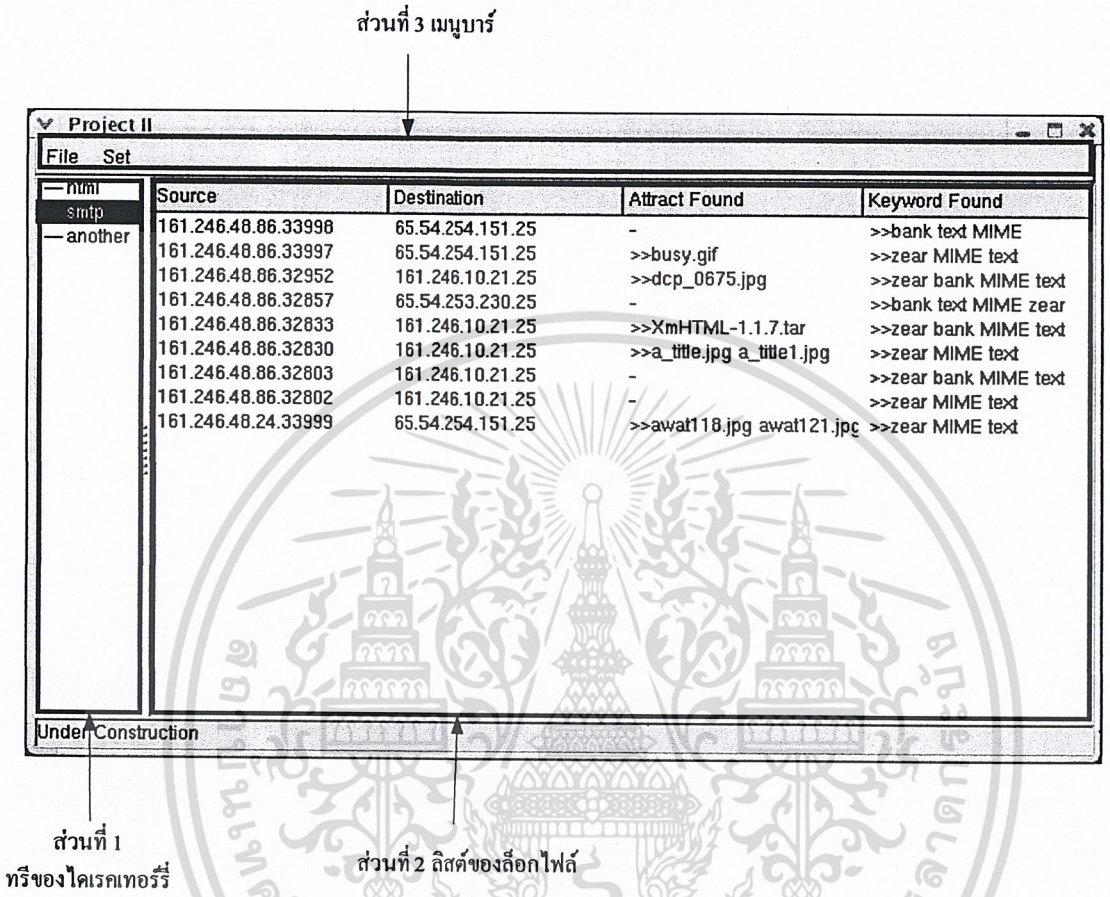
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คู่มือการใช้งานโปรแกรม

1.หน้าต่างหลัก



ส่วนที่ 1 ทรีของไดเรคเทอร์รี่ ใช้ในการเลือกไดเรคเทอร์รี่ของล็อกไฟล์ที่ต้องการให้แสดงผล แบ่งเป็น

- HTML
- SMTP
- Another

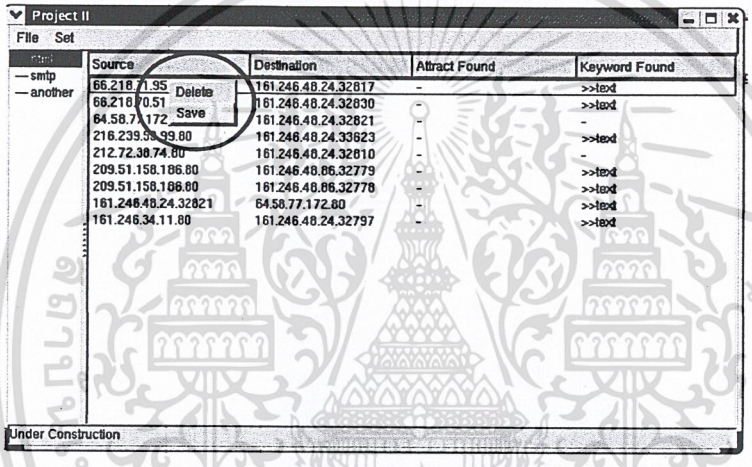
โดยค่าเริ่มต้นอยู่ที่ ไดเรคเทอร์รี่ HTML

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

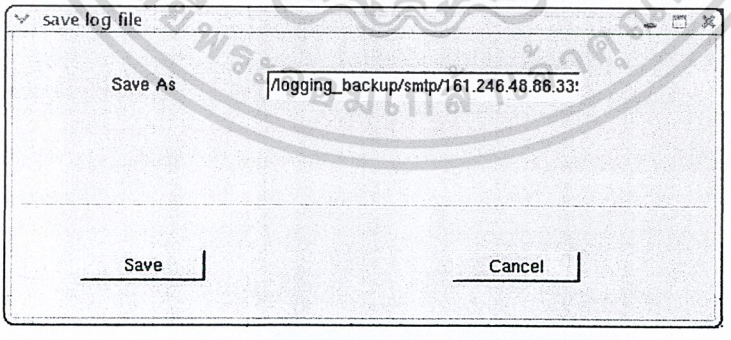
ส่วนที่ 2 ลิสต์ของล็อกไฟล์ ใช้แสดงรายการของล็อกไฟล์จากไดเรคเทอร์รี่ที่เลือก โดยมีหัวข้อดังนี้

- Source แสดงหมายเลขไอพีของต้นทางของแพ็คเก็ต
- Destination แสดงหมายเลขไอพีของปลายทางของแพ็คเก็ต
- Attract Found แสดงว่าแพ็กเก็ตนี้มีเอกสารแนบหรือ หากมี มีชื่อว่าอะไรบ้าง ซึ่งจะแสดงเอกสารแนบทั้งหมดที่มี และถ้าไม่พบเอกสารแนบจะแสดงเป็น " - "
- Keyword Found แสดงคีย์เวิร์ดที่พบในเอกสารนี้ทั้งหมด หากไม่พบจะเป็น " - "

นอกจากนี้ ในส่วนที่2 ยังใช้ในการแสดงผลของแพ็คเก็ต โดยการกดคลิกซ้ายที่ลิสต์ของล็อกไฟล์นั้น และหากต้องการลบหรือบันทึกให้คลิกขวาจะมีเมนูขึ้นมาให้เลือกดังรูป



เมื่อเลือก Save จะมีหน้าต่างขึ้นมาให้ทำการบันทึกชื่อไฟล์ ดังรูป



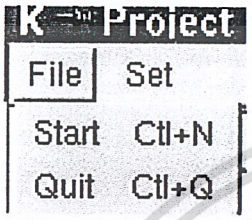
เมื่อพิมพ์ชื่อไฟล์ลงไปแล้วให้กดปุ่ม Save โปรแกรมจะทำการเซฟล็อกไฟล์นั้นไว้ด้วยชื่อที่ป้อนลงไป

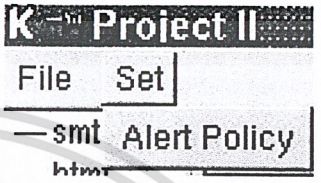
เมื่อ เลือก Delete โปรแกรมจะทำการลบไฟล์นั้นโดยทันที

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนที่ 3 เมนูบาร์ ประกอบด้วย

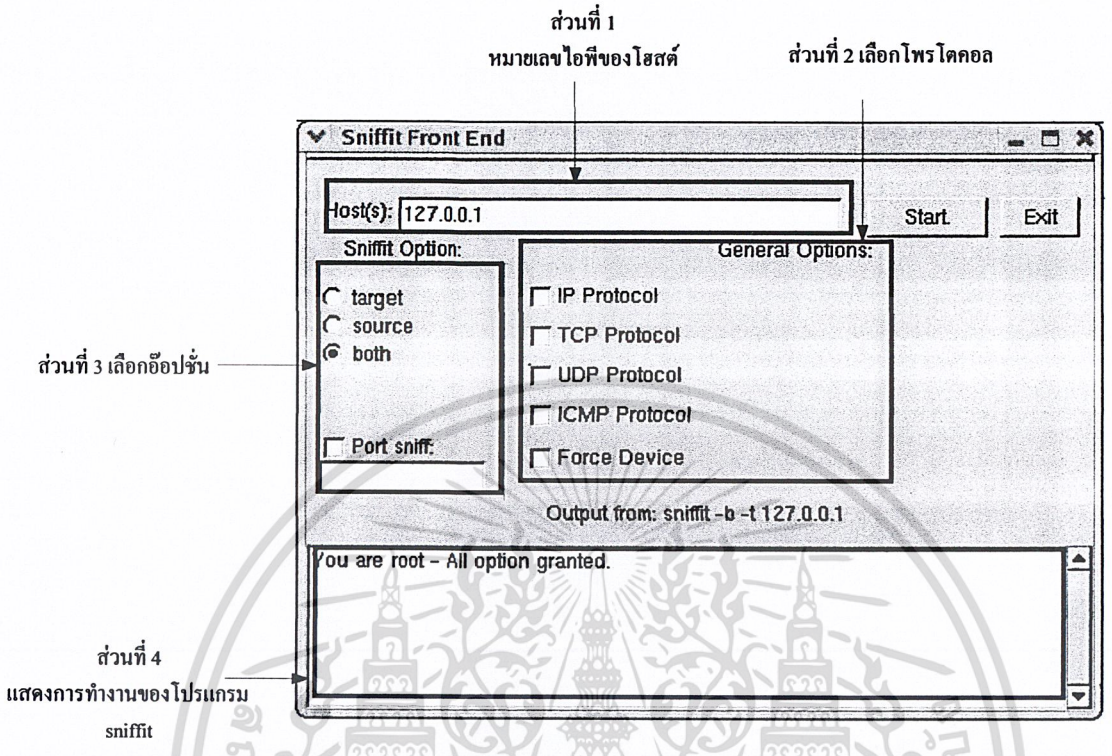
- เมนู File แบ่งเป็น
    - Start ใช้แสดงหน้าต่าง Sniffit Front End
    - Quit ออกจากโปรแกรม
- เมนู Set แบ่งเป็น
    - Alert Policy ใช้แสดงหน้าต่าง Alert Keyword





เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. หน้าต่าง Sniffit Front End



ส่วนที่ 1 หมายเลขไอพีของโฮสต์

ส่วนที่ 2 เลือกโพรโตคอล ของแพ็คเก็จที่ต้องการดักจับ โดยปกติจะเป็นการดักจบทุกโพรโตคอล และส่วน Force Device เป็นการบังคับใช้เน็ตเวิร์กอินเตอร์เฟสที่ต้องการใช้ในการดักจับข้อมูล แทนเน็ตเวิร์คอินเตอร์เฟสปัจจุบัน

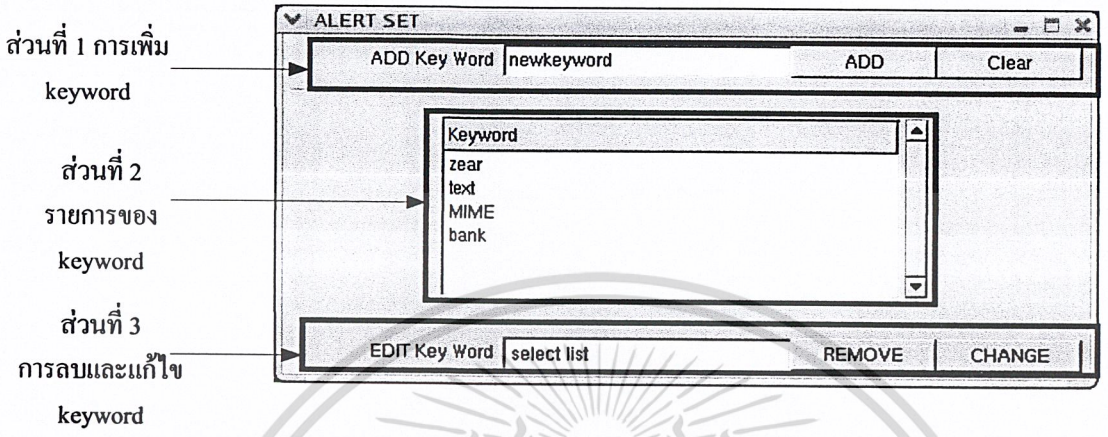
ส่วนที่ 3 เลือกอ๊อปชั่น แบ่งเป็น

- Target คือให้ไอพีของโฮสต์เป็นหมายเลขไอพีปลายทางที่ต้องการจับ
- Source คือให้ไอพีของโฮสต์เป็นหมายเลขไอพีต้นทางที่ต้องการจับ
- Both คือให้ไอพีของโฮสต์เป็นทั้ง ต้นทาง หรือ ปลายทางก็ได้
- เลือกพอร์ตที่ต้องการจับ

ส่วนที่ 4 แสดงการทำงานของโปรแกรม Sniffit

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.หน้าต่าง Alert Keyword



ส่วนที่ 1 การเพิ่มคีย์เวิร์ดเมื่อต้องการเพิ่มคีย์เวิร์ดให้พิมพ์คำที่ต้องการลงใน textbox แล้วกดปุ่ม Add

ส่วนที่ 2 รายการของคีย์เวิร์ด แสดงรายการของคีย์เวิร์ดที่มีอยู่

ส่วนที่ 3 การลบและการแก้ไขคีย์เวิร์ด

เมื่อต้องการลบคีย์เวิร์ด ให้เลือกคีย์เวิร์ดนั้นจากลิสต์ จากนั้น กดปุ่ม Remove

เมื่อต้องการแก้ไขคีย์เวิร์ด ให้เลือกคีย์เวิร์ดนั้นจากลิสต์ คีย์เวิร์ดนั้นจะไปแสดงที่ Textbox ข้างล่าง ซึ่งเดิมไม่สามารถแก้ไขได้ เมื่อมีการเลือกคีย์เวิร์ดจากลิสต์จะทำให้ Textbox นี้สามารถแก้ไขได้ จากนั้นให้แก้ไขเป็นคำที่ต้องการ แล้วจึงกดปุ่ม Change

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้