

การป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์

โดยใช้แฟลชไดรฟ์

SOFTWARE COPYRIGHT PROTECTION

BY USING FLASH DRIVE

นายจักรพันธ์	เอี่ยมเจริญจิตต์	รหัส	49360211
นายนพปฎล	คำแสง	รหัส	49360846
นายนิพนธ์	กุสุโมทย์	รหัส	49360976

ภาควิชาวิศวกรรมศาสตร์ วันที่รับ..... ๑๑ มี.ค. ๒๕๕๕ เลขทะเบียน..... 15729506 เลขเรียกหนังสือ..... น/ร. มหาวิทยาลัยนครสวรรค์ 922511
---

2552

ปริญญาบัตรนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครสวรรค์

ปีการศึกษา 2552

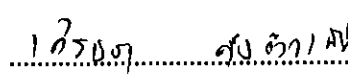



## ใบรับรองโครงการนิสิตกรรม

หัวข้อโครงการ	การป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์โดยใช้เฟลชไดรฟ์		
ผู้ดำเนินโครงการ	นายจักรพันธ์	เอี่ยมเจริญจิตต์	รหัส 49360211
	นายนพภูต	คำแสง	รหัส 49360846
	นายนิพนธ์	กุสุโมทย์	รหัส 49360976
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์	สอนคม	
สาขาวิชา	วิศวกรรมคอมพิวเตอร์		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2552		

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธนบุรี อนุมัติให้โครงการฉบับนี้เป็นส่วนหนึ่งของ  
การศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์  
คณะกรรมการสอบโครงการนิสิตกรรม

  
.....ประธานกรรมการ  
(อาจารย์ภาณุพงศ์ สอนคม)

  
.....กรรมการ  
(อาจารย์เศรษฐา ตั้งคำวานิช)

  
.....กรรมการ  
(ดร.สุรเดช จิตประไพกุลศาล)

หัวข้อโครงการ	การป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์โดยใช้แฟลชไดรฟ์		
ผู้ดำเนินโครงการ	นายจักรพันธ์	เอี่ยมเจริญจิตต์	รหัส 49360211
	นายนพปฎล	คำแสง	รหัส 49360846
	นายนิพนธ์	กุสุโมทย์	รหัส 49360976
อาจารย์ที่ปรึกษา	อาจารย์ภาณุพงศ์	สอนคม	
สาขาวิชา	วิศวกรรมคอมพิวเตอร์		
ภาควิชา	วิศวกรรมไฟฟ้าและคอมพิวเตอร์		
ปีการศึกษา	2552		

บทคัดย่อ

โครงการนี้เป็นการพัฒนาต้นแบบการป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์โดยใช้ Flash Drive เป็นการยืนยันว่า โปรแกรมที่ใช้ถูกลิขสิทธิ์หรือไม่ การพัฒนาโปรแกรมนี้สามารถทดสอบบนระบบปฏิบัติการ Microsoft Windows XP, Microsoft Windows Vista และ Microsoft Windows 7

ผลที่ได้จากการทำโครงการนี้ คือ ได้โปรแกรมที่สามารถตรวจสอบลิขสิทธิ์โดยการใช้แฟลชไดรฟ์ตัวที่กำหนด ซึ่งสามารถป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ ไม่ว่าจะเป็นการคัดลอกโปรแกรมไปใช้ หรือการปลอมแปลงโปรแกรมได้

**Project Title** Software Copyright Protection by using Flash Drive

**Name** Mr. Jakkaphan Aiemcharoenjit ID. 49360211  
Mr. Noppapadon Khumsang ID. 49360846  
Mr. Nipon Kusumot ID. 49360976

**Project Advisor** Mr. Panupong Sornkhom

**Major** Computing Engineering

**Department** Electrical and Computing Engineering

**Academic Year** 2009

---

### ABSTRACT

This project is aimed to develop a legitimate program by putting it in the removable Flash Drive. The Flash Drive is required to verify its legitimacy during the installation. The program is fully compatible with Microsoft XP, Microsoft Windows Vista and Microsoft Windows 7 operating systems.

As a consequence of the project, we have successfully created a program that can detect the software copyright by using the provided Flash Drive, which could thwart software piracy, that is to say, the unauthorized copy of software, or the usage of counterfeit license keys.

## กิตติกรรมประกาศ

โครงการวิศวกรรมคอมพิวเตอร์สำเร็จได้ด้วยดีเนื่องด้วยความอนุเคราะห์จากอาจารย์ที่ปรึกษาโครงการ คือ อาจารย์ ภาณุพงศ์ สอนคม ผู้ซึ่งกรุณาให้ความรู้คำแนะนำและเอาใจใส่เป็นอย่างดีระหว่างการดำเนินโครงการ อีกทั้งยังตรวจสอบข้อบกพร่องต่างๆ จนโครงการนี้เสร็จสมบูรณ์ คณะผู้จัดทำจึงขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณ ดร.สุรเดช จิตประไพกุลศาล และ อาจารย์เสรมฐา ตั้งคำวานิช ที่กรุณามารับเป็นกรรมการตรวจสอบโครงการและให้คำแนะนำ ตรวจสอบแก้ไขโครงการให้สมบูรณ์ยิ่งขึ้น

ในโอกาสที่ทางคณะผู้จัดทำโครงการจึงขอขอบคุณทุกๆท่านที่มีส่วนร่วมช่วยให้โครงการนี้ประสบความสำเร็จด้วยดี



คณะผู้จัดทำ  
จักรพันธ์ เอี่ยมเจริญจิตต์  
นพปฎล คำแสง  
นิพนธ์ กุสุโมทย์

# สารบัญ

	หน้า
บทคัดย่อ.....	ก
ABSTRACT.....	ข
กิตติกรรมประกาศ.....	ค
สารบัญ.....	ง
สารบัญตาราง.....	ฉ
สารบัญรูป.....	ช
<b>บทที่ 1 บทนำ</b>	
1.1 ที่มาและความสำคัญของโครงการ.....	1
1.2 วัตถุประสงค์ของโครงการ.....	1
1.3 ขอบข่ายของโครงการ.....	1
1.4 แผนการดำเนินงาน.....	2
1.5 ผลที่คาดว่าจะได้รับ.....	2
1.6 งบประมาณของโครงการ.....	2
<b>บทที่ 2 หลักการและทฤษฎี</b>	
2.1 ลิขสิทธิ์ซอฟต์แวร์.....	3
2.2 Copy protection.....	5
2.3 The SHA-1 Secure Hash Function.....	6
<b>บทที่ 3 ขั้นตอนและวิธีการดำเนินงาน</b>	
3.1 แนวคิดในการออกแบบซอฟต์แวร์ที่ถูกลิขสิทธิ์.....	10
3.2 แนวคิดในการออกแบบซอฟต์แวร์ที่สร้าง Flash Drive ให้ถูกลิขสิทธิ์.....	15

## สารบัญ (ต่อ)

	หน้า
<b>บทที่ 4 ผลการศึกษาและผลการพัฒนา</b>	
4.1 การสร้าง Flash Drive .....	21
4.2 การศึกษาการป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive.....	24
<b>บทที่ 5 สรุปผลและวิเคราะห์ผล</b>	
5.1 ผลการทดลอง.....	31
5.2 สรุปผลการทดลอง .....	32
5.2 ปัญหาและอุปสรรคที่พบ.....	32
5.3 ข้อเสนอแนะและแนวทางในการพัฒนา.....	32
เอกสารอ้างอิง.....	34
ภาคผนวก.....	35
ประวัติผู้เขียนโครงการ .....	40

## สารบัญตาราง

ตารางที่	หน้า
ตารางที่ 4.1 แสดงการสร้าง Flash Drive ในกรณีต่างๆ .....	21
ตารางที่ 4.2 การทดลองซอฟต์แวร์ที่ป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive .....	25





# สารบัญรูป

รูปที่	หน้า
2.1 Message Digest Generation Using SHA-1.....	7
2.2 SHA-1 Processing of a Single 512-bit Block.....	8
2.3 Elementary SHA Operation (single step).....	8
3.1 แสดง System Overview ของ Copyright Software .....	10
3.2 แสดง Use case diagram ของ Copyright Software.....	11
3.3 แสดง Sequence diagram ของ Copyright Software.....	12
3.4 แสดง Component diagram ของ Copyright Software .....	13
3.5 แสดง Class diagram ของ Copyright Software .....	13
3.6 แสดง Activity diagram ของ Copyright Software.....	14
3.7 แสดง Use case diagram ของ โปรแกรมสร้าง Flash Drive .....	16
3.8 แสดง Sequence diagram ของ โปรแกรมสร้าง Flash Drive .....	17
3.9 แสดง Component diagram ของ โปรแกรมสร้าง Flash Drive .....	18
3.10 แสดง Class diagram ของ โปรแกรมสร้าง Flash Drive .....	18
3.11 แสดง Activity diagram ของ โปรแกรมสร้าง Flash Drive .....	19
3.12 แสดงข้อมูลที่ถูกแปลงให้อยู่ในรูปของ SHA-1 ของไฟล์ protect.hex .....	20
4.1 แสดงการเลือก ไดรฟ์ที่ต้องการบรรจุ โปรแกรม.....	22
4.2 แสดงการเลือกที่อยู่ของ โปรแกรมที่จะบรรจุลงใน Flash Drive .....	22
4.3 แสดงข้อความที่โปรแกรมสามารถสร้าง Flash Drive ได้สมบูรณ์.....	23
4.4 แสดงผลลัพธ์เมื่อทำการสร้าง Flash Drive เสร็จเรียบร้อยแล้ว .....	23
4.5 แสดงข้อมูลที่ถูกแปลงให้อยู่ในรูปของ SHA-1 .....	23
4.6 แสดงการเลือก ไดรฟ์ที่ต้องการบรรจุ โปรแกรม.....	24
4.7 แสดงกล่องตอบโต้ข้อความเมื่อไม่สามารถค้นหาโปรแกรมได้ .....	24
4.8 แสดง โปรแกรมที่ถูกลิขสิทธิ์ซึ่งสามารถทำงานได้ตามปกติ.....	25
4.9 แสดงการคัดลอกโปรแกรมไปไว้ที่ ไดรฟ์ C.....	26
4.10 แสดงกล่องตอบโต้ข้อความเมื่อรัน โปรแกรมใน ไดรฟ์อื่น .....	26
4.11 แสดงการคัดลอกโปรแกรมไปไว้ใน Flash Drive ตัวอื่น.....	27
4.12 แสดงกล่องตอบโต้ข้อความที่ฟอร์มเมทของ Flash Drive ไม่ตรงตามที่กำหนด.....	27
4.13 ข้อมูลที่ถูกต้องก่อนทำการแก้ไขข้อมูล.....	28

## สารบัญรูป (ต่อ)

รูปที่	หน้า
4.14 ข้อมูลที่ถูกแก้ไข .....	28
4.15 แสดงกล่องตอบโต้ข้อความเมื่อทำการแก้ไข ไฟล์ protect.hex.....	28
4.16 ทำการแชร์ Flash Drive ในวง LAN .....	29
4.17 แสดงกล่องตอบโต้ข้อความเมื่อเรียกใช้โปรแกรม โดยคอมพิวเตอร์เครื่องที่อยู่ในวง LAN เดียวกัน.....	29
4.18 แสดงกล่องตอบโต้ข้อความเมื่อผู้ใช้ได้กระทำการใดๆ ขณะที่ไม่มี Flash Drive เสียบอยู่.....	30



## บทที่ 1

### บทนำ

#### 1.1 ที่มาและความสำคัญของโครงการ

เนื่องจากในปัจจุบันมีซอฟต์แวร์ ที่ให้ใช้งานอย่างแพร่หลาย จึงทำให้มีการพัฒนาซอฟต์แวร์ ทางด้านต่างๆ มีอย่างมากมาย แต่ยังมีปัญหาที่เกิดขึ้นตามมาอย่างมาก คือ การละเมิดลิขสิทธิ์การใช้งานซอฟต์แวร์ ไม่ว่าจะเป็นแหล่งจำหน่ายที่คนทั่วไปรู้จักกันดีตั้งแต่ระดับแผงลอยถึงศูนย์การค้า การดาวน์โหลดซอฟต์แวร์ผ่านทางอินเทอร์เน็ต หรือการพยายามหาวิธีทางในการถอดรหัสเพื่อนำ CD-KEY ของซอฟต์แวร์ นั้นๆ มาจำหน่าย หรือแจกฟรี ส่งผลให้เกิดความเสียหายต่อเจ้าของซอฟต์แวร์ นั้นๆ

ในปัจจุบันนี้มีการใช้ Flash Drive เป็นที่ขอมรับกันแพร่หลาย เพราะราคาถูก ความจุค่อนข้างสูง ง่ายต่อการพกพา และมีอายุการใช้งานที่นานกว่าอุปกรณ์บันทึกข้อมูลชนิดอื่น ๆ ดังนั้นผู้จัดทำโครงการจึงเล็งเห็นความสำคัญและมีแนวคิดจัดทำโครงการนี้ เพื่อเป็นแนวทางในการผลิต และจำหน่ายซอฟต์แวร์ ที่มีระบบป้องกันการละเมิดลิขสิทธิ์ โดยใช้ Flash Drive แก่ผู้ที่ทำการผลิตซอฟต์แวร์

#### 1.2 วัตถุประสงค์ของโครงการ

1.2.1 เพื่อศึกษาถึงปัญหาและอุปสรรคที่เกิดขึ้นในระบบป้องกันการละเมิดลิขสิทธิ์ทางซอฟต์แวร์ และสามารถนำไปปรับปรุงแก้ไขเพื่อให้ซอฟต์แวร์ สามารถป้องกันการละเมิดลิขสิทธิ์ได้

1.2.3 เพื่อพัฒนาระบบการป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ โดยใช้ Flash Drive ที่กำหนดไว้ เป็นการยืนยันลิขสิทธิ์

#### 1.3 ขอบข่ายของโครงการ

- 1.3.1 ศึกษาวิธีการละเมิดลิขสิทธิ์โดยวิธีการต่างๆ เช่น การ คัดลอก หรือการถอดรหัส
- 1.3.2 ศึกษาขั้นตอน การทำงาน และการดำเนินงานอย่างเป็นระบบ
- 1.3.3 พัฒนาซอฟต์แวร์ ที่ทำงานร่วมกับ Flash Drive เพื่อเป็นการยืนยันว่าซอฟต์แวร์นั้นถูกลิขสิทธิ์
- 1.3.4 หาวิธีป้องกันการคัดลอกโปรแกรมจาก Flash Drive

#### 1.4 แผนการดำเนินงาน

ขั้นตอนการดำเนินงาน	ระยะเวลาในการดำเนินงาน								
	มี.ย. 52	ก.ค. 52	ธ.ค. 52	ก.ย. 52	ต.ค. 52	พ.ย. 52	ธ.ค. 52	ม.ค. 53	ก.พ. 53
1.4.1 วางแผนการดำเนินงาน	←→								
1.4.2 ศึกษาหาข้อมูล		←→							
1.4.3 เก็บรวบรวมข้อมูล			←→						
1.4.4 ดำเนินการทดลอง				←→					
1.4.5 สรุปผลการทดลอง							←→		
1.4.6 จัดทำรูปเล่มรายงาน								←→	

ตารางที่ 1.1 แผนการดำเนินงาน

#### 1.5 ผลที่คาดว่าจะได้รับ

1.5.1 สามารถสร้างระบบที่ช่วยป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ โดยการใช้ Flash Drive

1.5.2 ทำให้ทราบถึงการพัฒนาและการจัดกระบวนการต่างๆ ของลิขสิทธิ์ซอฟต์แวร์ ให้มีคุณภาพ และเป็นที่ยอมรับ

1.5.3 ทำให้มีประสบการณ์ในระบบกระบวนการทำงาน และวิธีปฏิบัติงานให้มีประสิทธิภาพ

#### 1.6 งบประมาณของโครงการ

1.6.1 ค่าซื้อ Flash Drive	800	บาท
1.6.2 ค่าถ่ายเอกสารและเข้าเล่มวิทยานิพนธ์	1000	บาท
1.6.3 อื่นๆ	<u>1200</u>	บาท
รวมทั้งสิ้น	<u>3000</u>	บาท (สามพันบาทถ้วน)

หมายเหตุ ถัวเฉลี่ยทุกรายการ

## บทที่ 2

### หลักการและทฤษฎี

#### 2.1 ลิขสิทธิ์ซอฟต์แวร์

ลิขสิทธิ์ซอฟต์แวร์ คือ “สิทธิในการใช้งานซอฟต์แวร์อย่างถูกต้องตามกฎหมาย ที่เจ้าของลิขสิทธิ์ยินยอมให้ผู้ใช้อย่างใดอย่างหนึ่งไปใช้ซอฟต์แวร์นั้นๆ ตามรายละเอียดและเงื่อนไขที่ระบุไว้ในใบอนุญาตใช้งานสำหรับผู้ใช้อย่างใดอย่างหนึ่ง (End User License Agreement หรือ EULA)” ขณะที่แหล่งจำหน่ายซอฟต์แวร์ละเมิดลิขสิทธิ์ที่คนไทยทั่วไปรู้จักกันดีมีอยู่หลายแห่ง โดยแบ่งเป็นตั้งแต่ระดับแผงลอยถึงศูนย์การค้า จากรัฐบาลร่วมมือกับเอกชนในการปราบปรามทำให้ปี 2547 ประเทศไทยมีอัตราการละเมิดลิขสิทธิ์ซอฟต์แวร์ลดลง 1% จากปี 2546 มาอยู่ที่ 79% แต่อัตราการละเมิดลิขสิทธิ์ซอฟต์แวร์ทั่วโลกยังอยู่ที่ 35% ไม่เปลี่ยนแปลง

##### 2.1.1 ประเภทของการละเมิดลิขสิทธิ์ (Types of Software Piracy)

###### 2.1.1.1 การทำสำเนาโดยผู้ใช้งาน (End user Copy)

การละเมิดลิขสิทธิ์ซอฟต์แวร์ที่เกิดขึ้นบ่อยที่สุดในกลุ่มผู้ใช้งาน ได้แก่การติดตั้งซอฟต์แวร์ลงในคอมพิวเตอร์โดยไม่มีลิขสิทธิ์ หรือติดตั้งเกินจำนวนลิขสิทธิ์ รวมทั้งการทำสำเนาแจกจ่ายระหว่างผู้ใช้งานแม้ว่าจะเป็นการทำสำเนาจากซอฟต์แวร์ต้นฉบับของแท้ ก็จัดว่าเป็นการละเมิดประเภทหนึ่ง เนื่องจากการติดตั้งซอฟต์แวร์ หรือการใช้งานซอฟต์แวร์มากกว่าจำนวนที่ได้รับสิทธิการกระทำเช่นนี้มีเพียงแต่เสี่ยงต่อการถูกดำเนินคดีตามกฎหมายเท่านั้น หากแต่ยังเสี่ยงต่อการแพร่ระบาดของไวรัส และความเสียหายของข้อมูล ฯลฯ

โดยปกติผู้ค้าคอมพิวเตอร์จะขายเครื่องที่มีการติดตั้งซอฟต์แวร์ไว้แล้ว โดยเฉพาะอย่างยิ่งระบบปฏิบัติการ เช่น Windows Vista แต่ผู้ค้าคอมพิวเตอร์บางรายกลับติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ลงในเครื่องที่จำหน่ายให้กับลูกค้าเพื่อเป็นการลดต้นทุน ในกรณีนี้ผู้ซื้อมักไม่ได้รับ CD และคู่มือการใช้งาน รวมทั้งใบรับรองสินค้าของแท้ หรือ COA (Certificate of Authenticity) พบว่าผู้จำหน่ายมีเทคนิคและวิธีการละเมิดที่แตกต่างกัน เช่น ทำหน้าที่เป็นผู้ติดตั้งซอฟต์แวร์ให้ โดยแนะนำให้ลูกค้าซื้อซอฟต์แวร์ละเมิดลิขสิทธิ์ โดยตนเอง จะให้บริการติดตั้งเท่านั้น หรือ แนะนำให้ลูกค้ารับเครื่องเปล่าไปก่อน และส่งเจ้าหน้าที่ไปติดตั้งที่บ้านหรือที่ทำงานของลูกค้าภายหลัง

###### 2.1.1.2 การปลอมแปลงสินค้าเพื่อจำหน่าย (Counterfeiting)

ผู้จำหน่ายซอฟต์แวร์บางรายผลิต CD และคู่มือปลอมจำหน่าย โดยจัดทำบรรจุภัณฑ์เหมือน กับสินค้าจริงทุกประการ เพื่อเป็นการหลอกลวงให้ผู้ซื้อเข้าใจว่าได้สินค้าของแท้ การผลิต CD-ROM ที่รวบรวมโปรแกรมคอมพิวเตอร์หลายประเภทไว้ในแผ่นเดียว

ในบางกรณีผู้ค้าซอฟต์แวร์จำหน่ายซอฟต์แวร์ผิดประเภทให้กับลูกค้า ทำให้ผู้ซื้อตกอยู่ในความเสี่ยงทางกฎหมายโดยรู้เท่าไม่ถึงการณ์ ดังต่อไปนี้

- สินค้า Academic Edition (AE) ซึ่งเป็นสินค้าที่ออกแบบมาเพื่อองค์กรการศึกษาและนักศึกษาด้วยราคาต่ำเป็นพิเศษ โดยจะมี ฉลาก "Academic Product" แสดงไว้ แต่มีการนำมาจำหน่ายให้กับองค์กรทั่วไป
- สินค้า NFR (Not for Resale) ซึ่งเป็นสินค้าที่มักนำมาแจกจ่ายในกรณีที่เป็นการส่งเสริมการขาย หรือตัวอย่าง มิได้มีไว้เพื่อจำหน่าย และ EULA ของสินค้าเหล่านี้จะระบุว่า "Not for Resale" ไว้ด้วย
- สินค้า OEM ซึ่งเป็นสินค้าที่ผู้ค้าคอมพิวเตอร์รวบรวมให้กับผู้ซื้อคอมพิวเตอร์ แต่กลับนำมาแจกจำหน่ายต่างหาก สังเกตได้ จากบรรจุภัณฑ์จะระบุว่า "For Distribution only With New PC Hardware"
- สินค้า Fulfillment ซึ่งเป็นสินค้าที่จำหน่ายให้กับลูกค้าที่ซื้อลิขสิทธิ์จำนวนมาก เช่น Select, Open, Enterprise Agreement เพื่อเป็นการประหยัดค่าใช้จ่ายของผู้ซื้อลิขสิทธิ์บรรจุภัณฑ์จะระบุว่า "Microsoft Easy Fulfillment" หรือ "Microsoft Worldwide Fulfillment" สินค้าเหล่านี้ไม่มีลิขสิทธิ์มาด้วยเนื่องจากมีวัตถุประสงค์เพื่อใช้ในการติดตั้งสำหรับผู้ที่มีลิขสิทธิ์ซอฟต์แวร์ถูกต้องแล้ว

#### 2.1.1.3 การละเมิดลิขสิทธิ์แบบ Online (Internet Piracy)

ลักษณะที่เกิดขึ้นมากในปัจจุบันคือการ ความไม่โหลดซอฟต์แวร์ผ่านอินเทอร์เน็ต โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ ซอฟต์แวร์เหล่านี้ไม่ใช่ Shareware ซึ่งเจ้าของลิขสิทธิ์มักเป็นผู้เสนอให้ใช้ฟรี หรือมีค่าใช้จ่ายเพียงเล็กน้อยและมักไม่มีข้อจำกัดในการใช้งาน

ส่วนสาเหตุของการละเมิดลิขสิทธิ์ซอฟต์แวร์บนอินเทอร์เน็ต นายครูเกอร์ แสดงความคิดเห็นว่า มาจาก 3 ปัจจัย คือ

- ประชาชนใช้อินเทอร์เน็ตเพิ่มมากขึ้น โดยปี 2547 มีใช้อินเทอร์เน็ตในประเทศแถบเอเชีย-แปซิฟิก เพิ่มขึ้นถึง 44 ล้านคน
- การขยายตัวของอินเทอร์เน็ตความเร็วสูง หรือบรอดแบนด์ ทำให้ผู้ใช้สามารถดาวน์โหลดไฟล์ขนาดใหญ่ภายในเวลารวดเร็ว
- ความยากในการปราบปราม เพราะทำบนอินเทอร์เน็ต ทำให้ขาดหลักฐาน

## 2.1.2 ความเสี่ยงของการละเมิดลิขสิทธิ์ซอฟต์แวร์

### 2.1.2.1 เสี่ยงต่อการจ่ายต้นทุนระบบคอมพิวเตอร์สูงกว่าที่ควร

ต้นทุนของระบบคอมพิวเตอร์ มีทั้งจากฮาร์ดแวร์ และซอฟต์แวร์ การสนับสนุนทางด้านเทคนิค การให้คำปรึกษาทางด้านการจัดการ และบริการอื่นๆ การติดตั้ง และการบริหารระบบที่มีมาตรฐานเดียวกันทั้งองค์กร จะทำให้ต้นทุนการจัดการระบบลดลงอย่างเห็นได้ชัด ในขณะที่ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์มักอยู่บนอกกฎหมายเหล่านี้ ทำให้ต้นทุนรวมของการบริหารระบบราคาแพงกว่าที่ควรในระยะยาว

### 2.1.2.2 เสี่ยงต่อปัญหาไวรัสซอฟต์แวร์ที่เป็นของปลอม หรือไม่มีลิขสิทธิ์

อาจเป็นสาเหตุของการแพร่ระบาดของไวรัส ซึ่งในกรณีรุนแรงอาจทำให้ข้อมูลทั้งฮาร์ดดิสก์ สูญหายหมด ซื่อซอฟต์แวร์จากตัวแทนจำหน่ายที่เชื่อถือได้เพื่อป้องกันปัญหาไวรัส

### 2.1.2.3 เสี่ยงต่อการละเมิดกฎหมายลิขสิทธิ์

กฎหมายลิขสิทธิ์มีบทลงโทษที่รุนแรงทั้งทางแพ่งและทางอาญา นอกจากบทลงโทษทางดำเนินกฎหมาย ด้วยการปรับ และการจำคุกแล้ว ผลที่ติดตามมา คือ ความเสียหายต่อชื่อเสียงขององค์กร ความยอมรับของลูกค้าและสาธารณชน รวมทั้งชื่อเสียง ในด้านลบของผู้บริหารอีกด้วย การใช้ซอฟต์แวร์ผิดกฎหมาย จึงถือว่าเป็นความเสี่ยงที่ไม่คุ้มค่า

## 2.2 Copy protection

Copy protection คือ วิธีการป้องกันการคัดลอก ทำสำเนา หรือที่เรียกกันว่าการคัดลอก ที่ผู้ผลิตหรือเจ้าของลิขสิทธิ์ซอฟต์แวร์ ซึ่งต้องการป้องกันไม่ให้เกิดการคัดลอกข้อมูลนั้น จะประกอบไปด้วยปัจจัยของ 3 ส่วนนี้ โดยที่จะขาดสิ่งใดสิ่งหนึ่งไม่ได้คือ

### 2.2.1 Dependency on External Action

ตัวโปรแกรมต้นฉบับจะยอมทำงานก็ต่อเมื่อมีการกระทำร่วมกันหรือสั่งงานมาจาก ตัวป้องกัน (Guard module) ด้วย วิธีการที่ใช้ในที่นี่ คือ การเข้ารหัส (Encryption) โปรแกรมจะยอมทำงานก็ต่อเมื่อมันมีตัวถอดรหัส (Decryption) มาด้วย

### 2.2.2 The Guard Module

จะเป็นตัวที่อนุญาตให้โปรแกรมทำงานได้ ด้วยการเช็คค่าเริ่มต้น หรือ key ที่ได้กำหนดแล้วว่าเป็นค่าของตัวต้นฉบับจริง (Authentic key) การทำงานของตัว Guard Module นั้น จะต้องมีการทำงานที่ซับซ้อนมาก เพื่อไม่ให้ผู้อื่นสามารถรู้ถึงกรรมวิธีการทำงาน หรือ ลอกเลียนแบบการทำงานได้ หรือ ไปหลอกให้มันทำงานได้ ถ้าปราศจากค่าเริ่มต้น หรือตัว Authentic Key นี้ แต่ถ้าตัว guard

module มีการ protect ที่ไม่แข็งแรงพอก็สามารถทำการคัดลอกข้อมูลได้ ส่วนหน้าที่ของ Module Guard คือ

- Key Detection ตรวจจับหา Authentic Key
- Initialization
- Code Security
- Debug Trapping

### 2.2.3 The Physical Key

คนที่ซื้อซอฟต์แวร์จะได้รับอุปกรณ์เหล่านี้ เพื่อแสดงถึงความเป็นเจ้าของ และมีสิทธิ์ในการใช้ซอฟต์แวร์ลิขสิทธิ์นั้น ซึ่งอาจเป็นอุปกรณ์ในหลาย ๆ รูปแบบ เช่น

- original CD
- key diskette
- A dongle or a "smart card" หรือ Key lock ที่เอาไว้เสียบที่ com port หรือ printer port หรือ USB port
- Hard Disk
- Plug-in board
- Personal Characteristics (finger prints, voice prints or retinal images) คุณลักษณะส่วนตัวของเจ้าของ โปรแกรม เช่น ลายนิ้วมือ เสียง รูปแบบของเลนส์ดวงตา หรือ Retinal image

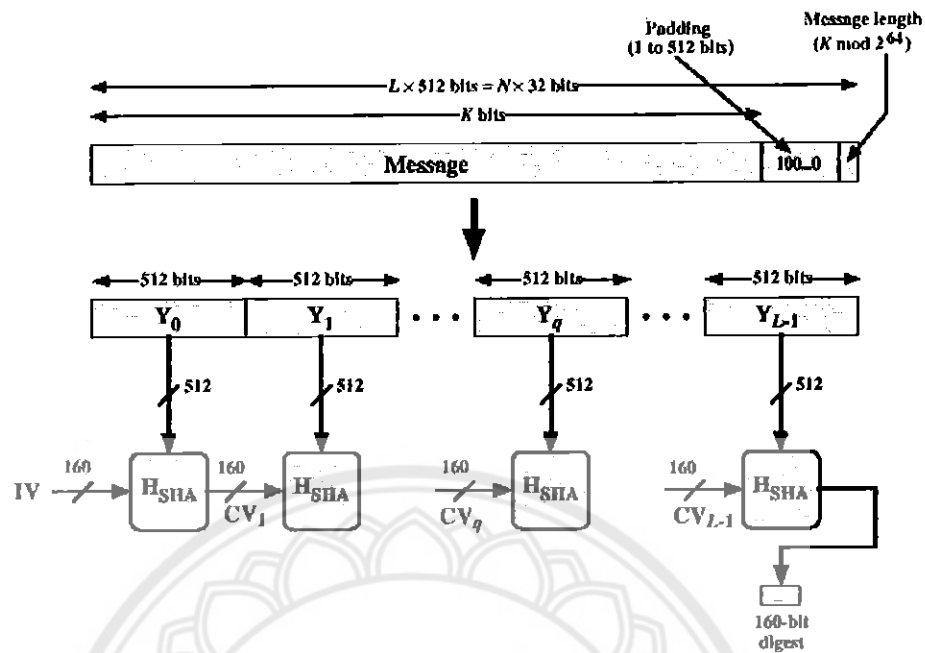
### 2.3 The SHA-1 Secure Hash Function

SHA-1 เป็นอัลกอริทึม Hash ที่ใช้ในการเข้ารหัสเพื่อความปลอดภัย SHA ย่อมาจาก Secure Hash Algorithm ออกแบบโดย NSA (National Security Agency) หรือสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา

ในบรรดาฟังก์ชัน Hash ทั้งหมด ฟังก์ชัน SHA-1 จัดว่าเป็นฟังก์ชันหนึ่งที่เป็นมาตรฐาน และมีการใช้งานกันอย่างกว้างขวาง โดย SHA ได้รับการพัฒนาโดย NIST โดยได้รับการประกาศเป็นมาตรฐานที่ FIPS PUB 180 ในปี 1993 โดยหลังจากนั้นมีการปรับปรุงเป็น SHA-1 ในปี 1995 โดยประกาศเป็นมาตรฐานที่ FIPS PUB 180-1

ฟังก์ชัน SHA-1 จะใช้บล็อกข้อมูลขนาด 512 บิต โดยสร้างผลลัพธ์ MD ความยาว 160 บิตคงที่ โดยการทำงานของฟังก์ชันนี้แสดงในรูปที่ 3.5





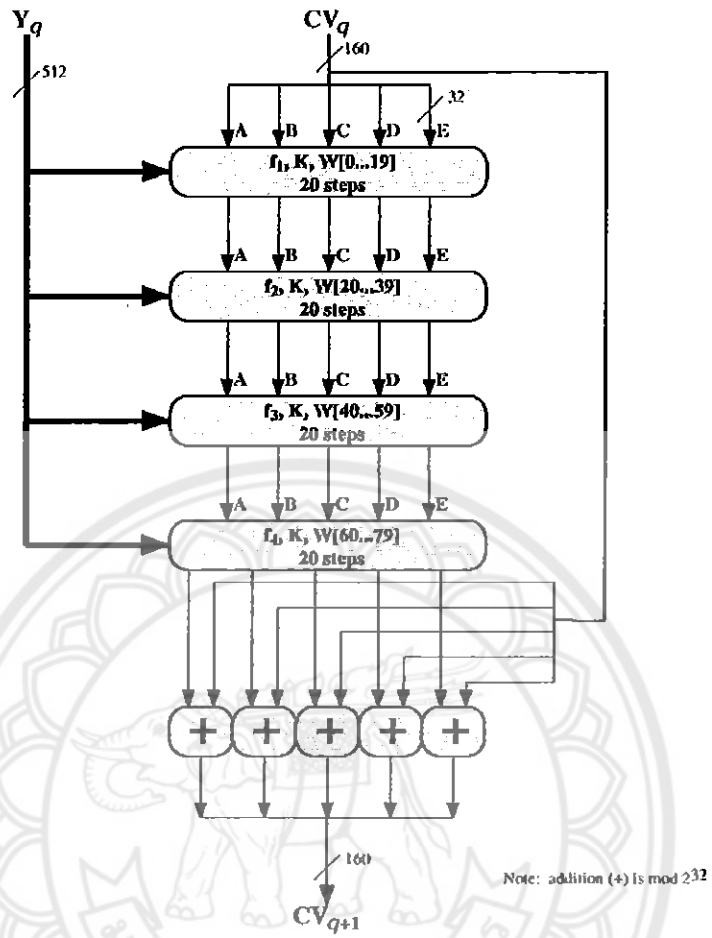
รูปที่ 2.1 Message Digest Generation Using SHA-1

ในขั้นตอนที่ 1 เติมบิต (padding) โดยจะมีการเติมบิตข้อมูลเพิ่มเติม โดยจะเพิ่มเป็นจำนวนเท่ากับ 512-เศษที่ได้จากการหาร 512 แล้วลบออก 64 บิต เนื่องจากจะมีการเพิ่มความยาวอีก 64 บิต ในขั้นตอนที่ 2 ดังนั้นแม้ว่าบล็อกข้อมูลที่หารด้วย 512 ลงตัว ก็จะต้องมีการเติมบิตด้วยเช่นกัน

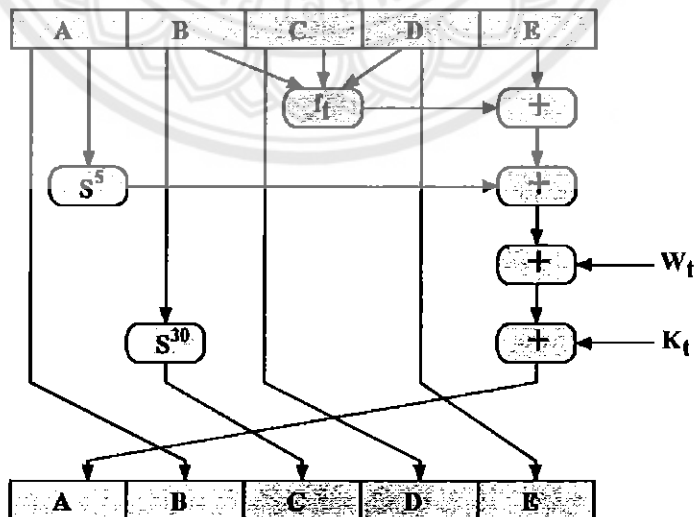
ในขั้นตอนที่ 2 จะมีการเพิ่มข้อมูลความยาว 64 บิต โดยจะเป็นข้อมูลที่ระบุความยาวของข้อมูลก่อนที่จะมีการเติมบิตเข้าไป โดยการเพิ่มข้อมูลความยาวบิตเท่ากับ 64 บิตนี้ จะทำให้ความยาวของข้อมูลที่รวมกับการเติมบิตและเพิ่มอีก 64 บิต จะมีความยาวที่หารด้วย 512 ลงตัวพอดี ซึ่งหมายความว่าแบ่งเป็นบล็อกละ 512 บิตได้อย่างลงตัว

ในขั้นตอนที่ 3 จะมีการกำหนดค่าเริ่มต้นของ MD Buffer โดยมีความยาวเท่ากับ 160 บิต โดยบัพเฟอร์นี้จะเก็บค่าเริ่มต้นของ MD จะแทนด้วยรีจิสเตอร์จำนวน 5 ตัว ตัวละ 32 บิต โดยมีชื่อเป็น A, B, C, D และ E โดยมีค่าเริ่มต้นคงที่ดังนี้ A=67452301, B=EFCDAB89, C=98BADCFE, D=10325476, E=C3D2E1F0

ในขั้นตอนที่ 4 ซึ่งถือเป็นหัวใจของการทำงานทั้งหมด โดยจะมีการประมวลผลข้อมูลเป็นบล็อก ครั้งละ 512 บิต โดยกระทำเป็นรอบ ๆ จนกว่าข้อมูลจะหมด จะมีการทำงานทั้งหมด 4 รอบ โดยในแต่ละรอบจะประกอบด้วย 20 ขั้นตอนย่อย จากนั้นเมื่อผลลัพธ์ของทั้ง 4 รอบออกมา ก็จะมีการนำไปบวกเข้ากับข้อมูล CV ที่เข้ามาอีกที ก็จะได้เป็น Message Digest ของบล็อกนั้น จากนั้น MD ก็จะใช้ในการประมวลผลข้อมูลในบล็อกถัดไปจนหมด ก็จะได้ MD สุดท้ายที่มีความยาว 160 บิตออกมา



รูปที่ 2.2 SHA-1 Processing of a Single 512-bit Block



รูปที่ 2.3 Elementary SHA Operation (single step)

สำหรับการทำงานในแต่ละรอบจะมีรายละเอียดของการทำงานตามรูปข้างต้น โดยเครื่องหมาย S จะหมายถึงการ Shift ตามจำนวนบิตที่กำกับไว้ สำหรับ K คือ ค่าที่นำมาบวก โดยค่าที่กำหนดไว้สำหรับบวกแต่ละรอบ คือ 5A827999, 6ED9EBA1, 8F1BBCDC และ CA62C1D6 สำหรับค่า W เป็นข้อมูล 32 บิตที่ดึงมาจากส่วนของ 512 บิตจาก Input Block โดยคำนวณจากสูตร  $W_t = S_1(W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3})$  โดย W ได้มาจาก Word ในแต่ละรอบของ t ซึ่งจะมีทั้งหมด 16 Word สำหรับ Ft นั้น เป็นฟังก์ชันที่จะใช้ในแต่ละรอบของการทำงาน

จากอัลกอริทึมจะเห็นว่าผลลัพธ์ที่ได้ในแต่ละบิต จะเกิดจากอินพุตในแต่ละบิต โดยในแต่ละรอบการทำงาน มีการทำงานที่ซับซ้อน ซึ่งจะต่างกับการใช้ฟังก์ชันง่าย ๆ อย่าง XOR โดย SHA-1 จะมีความเป็นไปได้ที่ข้อความ 2 ข้อความที่มี MD เดียวกัน เท่ากับ 2 ยกกำลัง 80 และมีความยากในการหาข้อความที่มี MD ที่ได้เท่ากับ 2 ยกกำลัง 160 ซึ่งถือว่ามีความปลอดภัยในการใช้งานมากเพียงพอ

- ข้อดีของ SHA-1 คือเป็นประโยชน์ในการจัดเตรียมคุณลักษณะเฉพาะหรือค่าเฉพาะของข้อความที่มีการ Hash โดยที่ไม่จำเป็นต้องใช้ในการเข้ารหัสเป็นเวลานาน
- ข้อเสียของ SHA-1 คือ ปี 2004 เริ่มพบจุดอ่อนของ SHA-1 ทำให้สหรัฐมีแผนที่จะยกเลิกการใช้งานภายในปี 2010

### บทที่ 3

## ขั้นตอนและวิธีการดำเนินงาน

ขั้นตอนและการดำเนินงานการออกแบบระบบ ที่ใช้ในการป้องกันการ ละเมิดลิขสิทธิ์ทางซอฟต์แวร์โดยใช้ Flash Drive ประกอบด้วยแนวคิดในการออกแบบซอฟต์แวร์ที่รันบน Flash Drive และ โปรแกรมการสร้าง Flash Drive ที่ถูกลิขสิทธิ์ ซึ่งอธิบายการป้องกัน การละเมิดลิขสิทธิ์ การออกแบบซอฟต์แวร์ควบคุมทั้ง 4 มุมมอง ดังรูปที่ 3.1

	Dynamic	Static
External	- Use case diagram - Sequence diagram	Component diagrams
Internal		- Activity diagrams - Class diagrams

รูปที่ 3.1 แสดง System Overview ของ Copyright Software

แต่ละมุมมองมีความหมายดังต่อไปนี้

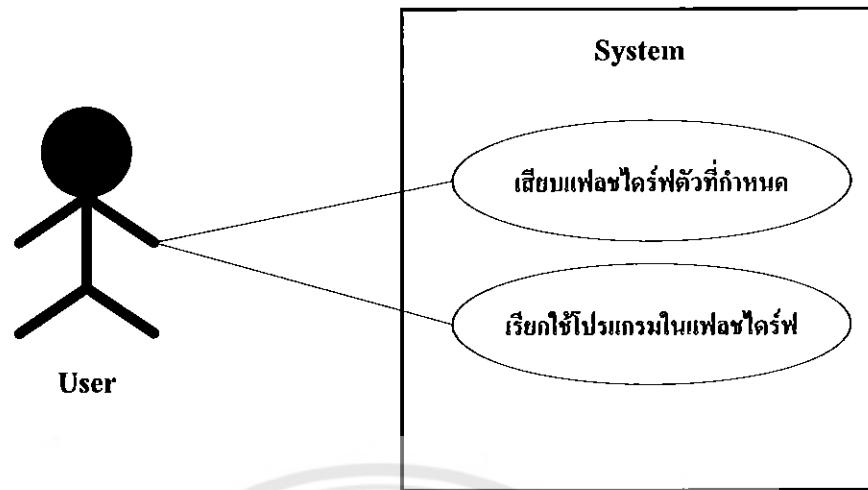
- External-Dynamic แสดงการติดต่อภายนอกที่สามารถมองเห็นได้
- External-Static แสดงโครงสร้างและส่วนประกอบต่างๆ ของระบบที่ติดต่อภายนอก
- Internal-Dynamic แสดงพฤติกรรมและสถานะต่างๆ ของระบบ
- Internal-Static แสดงโครงสร้างและส่วนประกอบต่างๆ ภายในระบบ

### 3.1 แนวคิดในการออกแบบซอฟต์แวร์ที่ถูกลิขสิทธิ์

#### 3.1.1 Use case diagram

การออกแบบโปรแกรมติดต่อกับผู้ใช้งานต่อไปนี้

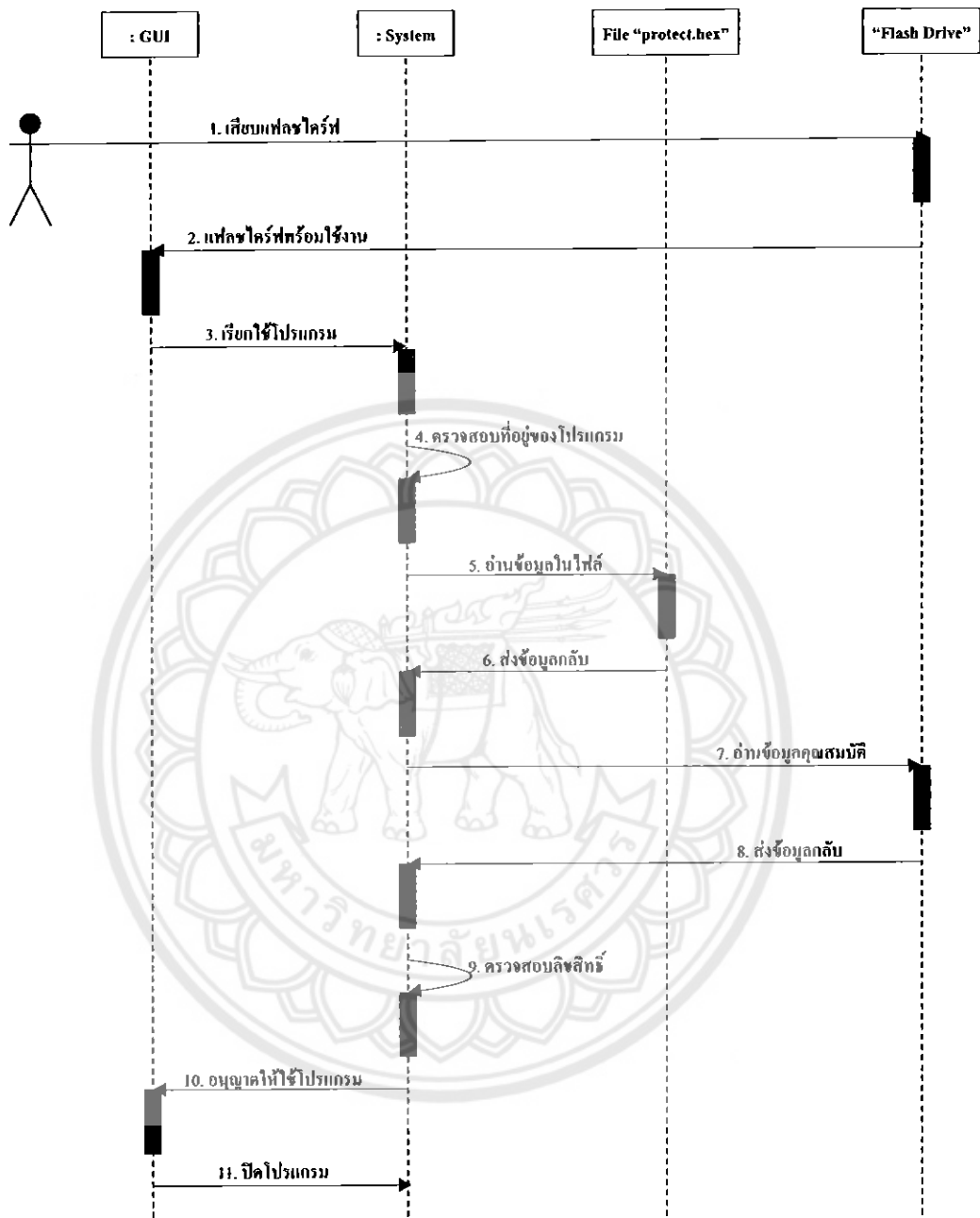
1. ผู้ใช้ทำการเสียบ Flash Drive ตัวที่กำหนด
2. ผู้ใช้ทำการเรียกใช้โปรแกรมใน Flash Drive ตัวที่กำหนด



รูปที่ 3.2 แสดง Use case diagram ของ Copyright Software

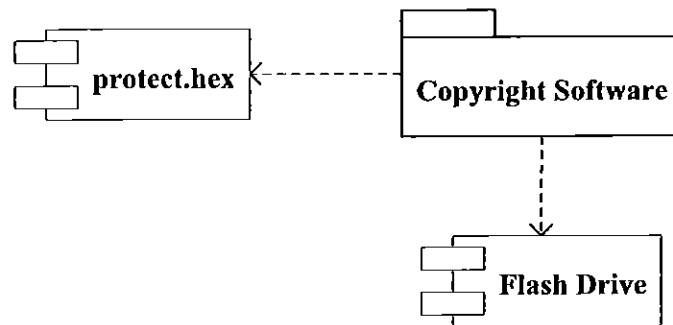
### 3.1.2 Sequence Diagram

สำหรับ Sequence Diagram บ่งบอกลำดับการทำงานของโปรแกรม โดยขั้นแรกผู้ใช้งานจะต้องเสียบ Flash Drive ถูกลิขสิทธิ์ตามที่กำหนด เมื่อผู้ใช้ทำการเรียกใช้โปรแกรม โปรแกรมจะทำการค้นหาที่อยู่ของโปรแกรม อ่านข้อมูลจากไฟล์ protect.hex อ่านคุณสมบัติของ Flash Drive และทำการตรวจสอบลิขสิทธิ์ ถ้าการตรวจสอบผ่าน โปรแกรมจะสามารถทำงานได้เป็นปกติ ดังรูปที่ 3.3



รูปที่ 3.3 แสดง Sequence diagram ของ Copyright Software

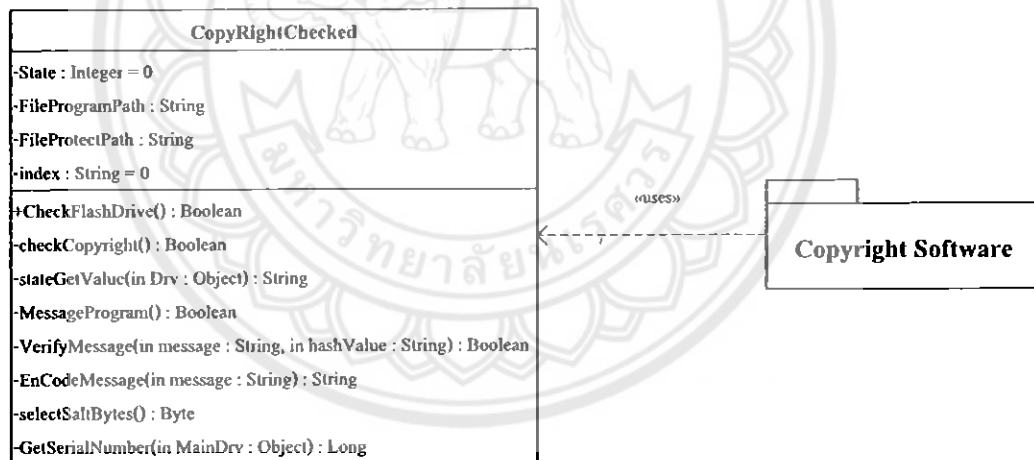
### 3.1.3 Component Diagram



รูปที่ 3.4 แสดง Component diagram ของ Copyright Software

โปรแกรมต้องติดต่อกับ Flash Drive และไฟล์ protect.hex เพื่อให้โปรแกรมนั้นถูกลิขสิทธิ์ และสามารถทำงานได้ตามปกติ

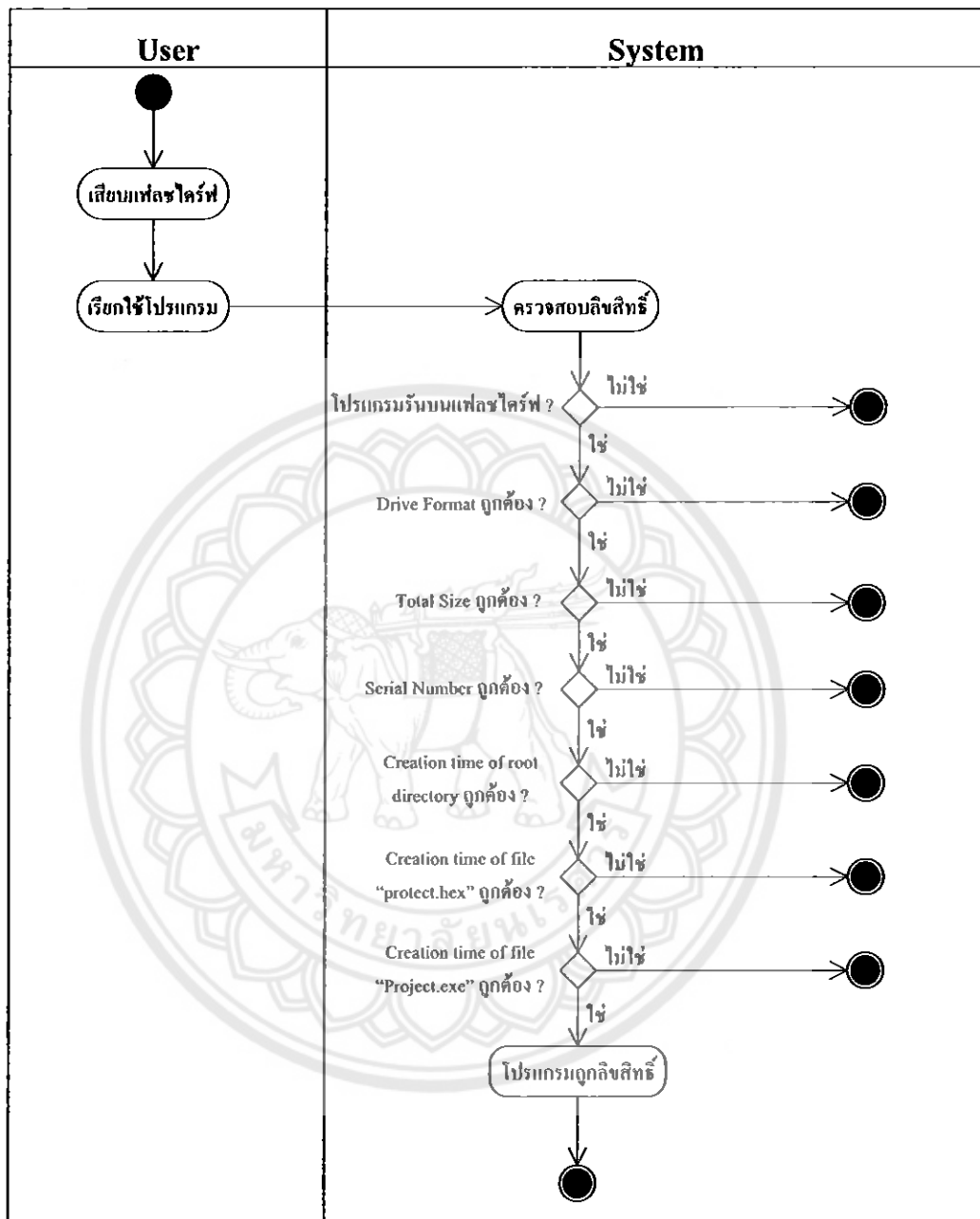
### 3.1.4 Class Diagram



รูปที่ 3.5 แสดง Class diagram ของ Copyright Software

ซอฟต์แวร์ที่ต้องการตรวจสอบลิขสิทธิ์ต้องมี Class ของ CopyRightChecked ในการตรวจสอบลิขสิทธิ์ของซอฟต์แวร์ เพื่อให้ซอฟต์แวร์นั้นสามารถทำงานได้อย่างถูกต้อง

## 3.1.5 Activity Diagram



รูปที่ 3.6 แสดง Activity diagram ของ Copyright Software

จากรูปกระบวนการทำงานของโปรแกรมตรวจสอบลิขสิทธิ์ซอฟต์แวร์ สามารถอธิบายได้ดังนี้

1. ผู้ใช้ทำการเสียบ Flash Drive ถูกลิขสิทธิ์ตัวที่กำหนด



2. ผู้ใช้ทำการเรียกใช้โปรแกรม โปรแกรมจะทำการค้นหาที่อยู่ของโปรแกรมว่าอยู่ใน Flash Drive หรือไม่
3. เมื่อโปรแกรมไม่ได้รับอยู่บน Flash Drive โปรแกรมจะจบการทำงานทันที แต่ถ้าโปรแกรมรับอยู่บน Flash Drive โปรแกรมจะทำการเช็คไฟล์ protect.hex ร่วมกับคุณสมบัติของ Flash Drive ในส่วนของ Drive Format, Total Size, Serial Number, Creation time of root directory ของ Flash Drive , Creation time ของไฟล์ protect.hex และ Creation time ของไฟล์ Project.exe ว่าตรงตามที่กำหนดหรือไม่
4. ถ้าข้อมูลที่ตรวจสอบถูกต้องตามที่กำหนด โปรแกรมก็สามารถทำงานได้ตามปกติ แต่ถ้าข้อมูลที่ตรวจสอบไม่ถูกต้อง โปรแกรมก็ไม่สามารถทำงานได้

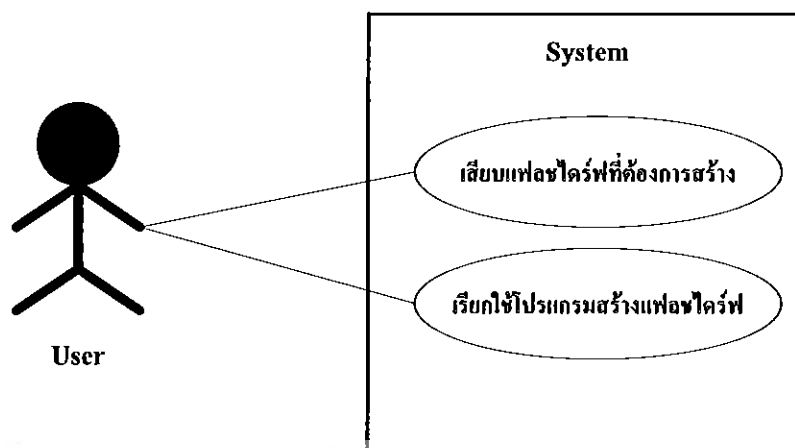
### 3.2 แนวคิดในการออกแบบซอฟต์แวร์ที่สร้าง Flash Drive ให้ถูกลิขสิทธิ์

เมื่อทำการสร้างซอฟต์แวร์ให้สามารถตรวจสอบลิขสิทธิ์โดยใช้ Flash Drive ตามแนวคิดการออกแบบแล้วนั้น สิ่งที่จะต้องอย่างหนึ่งคือ โปรแกรมที่สร้าง Flash Drive ให้ถูกลิขสิทธิ์ แนวคิดในการออกแบบจะคล้ายคลึงกับการสร้างซอฟต์แวร์ที่สามารถตรวจสอบลิขสิทธิ์โดยใช้แฟลชไดรฟ์ โดยโปรแกรมจะทำการสร้างไฟล์ protect.hex และคัดลอกโปรแกรมที่สามารถตรวจสอบลิขสิทธิ์ได้ลงใน Flash Drive โปรแกรมนี้เป็น Window Application พัฒนาโดยภาษา Visual Basic กระบวนการสร้างเป็นดังรูป

#### 3.2.1 Use case diagram

การออกแบบโปรแกรมติดต่อกับผู้สร้างดังต่อไปนี้

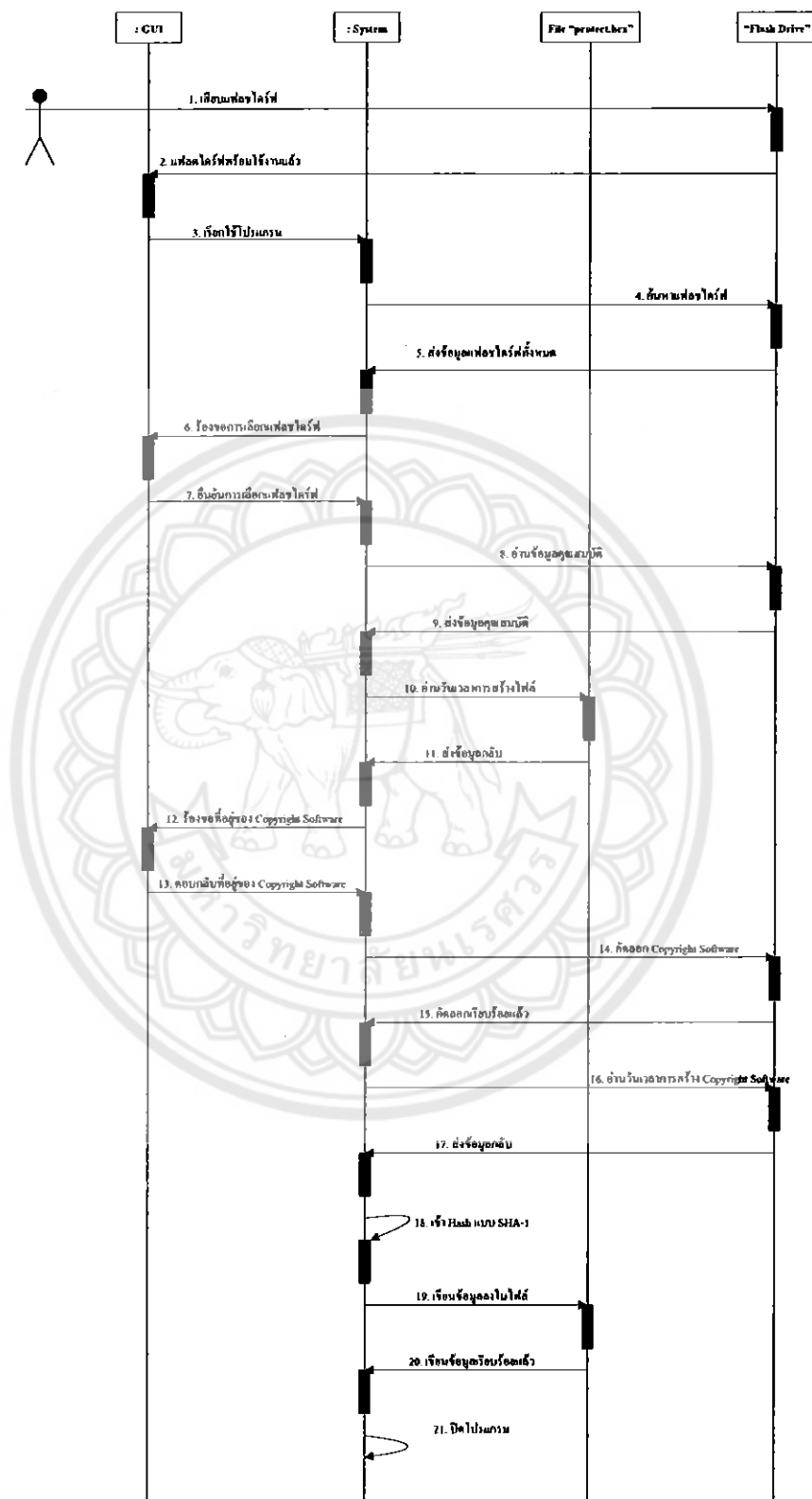
1. ผู้สร้างทำการเสียบ Flash Drive ตัวที่กำหนด
2. ผู้สร้างทำการเรียกใช้โปรแกรมใน Flash Drive ตัวที่กำหนด



รูปที่ 3.7 แสดง Use case diagram ของ โปรแกรมสร้าง Flash Drive

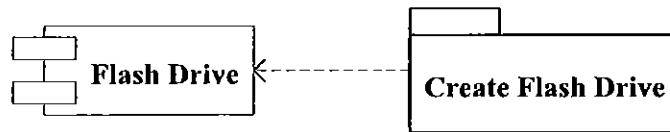
### 3.2.2 Sequence Diagram

สำหรับ Sequence Diagram บ่งบอกลำดับการทำงานของโปรแกรมสร้าง Flash Drive โดยขั้นแรกผู้ใช้จะต้องเสียบ Flash Drive ที่ต้องการสร้าง เมื่อผู้ใช้ทำการเรียกใช้โปรแกรม โปรแกรมจะทำการสร้างไฟล์ protect.hex เพื่อทำการเก็บข้อมูลคุณสมบัติของ Flash Drive เวลาในการสร้างไฟล์ protect.hex และไฟล์ของโปรแกรม ซึ่งข้อมูลเหล่านี้จะถูกเข้ารหัสด้วย Hash แบบ SHA-1 ก่อนแล้วจึงเขียนข้อมูลลงในไฟล์ protect.hex โดยการทำงานจะเป็นตาม Sequence Diagram ดังรูปที่ 3.8



รูปที่ 3.8 แสดง Sequence diagram ของโปรแกรมสร้าง Flash Drive

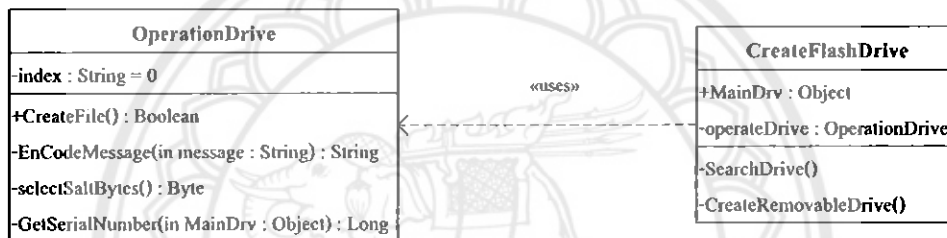
### 3.2.3 Component Diagram



รูปที่ 3.9 แสดง Component diagram ของโปรแกรมสร้าง Flash Drive

โปรแกรมการสร้าง Flash Drive ให้ถูกลิขสิทธิ์จำเป็นต้องติดต่อกับ Flash Drive เพื่อให้โปรแกรมสามารถสร้างไฟล์ protect.hex ได้

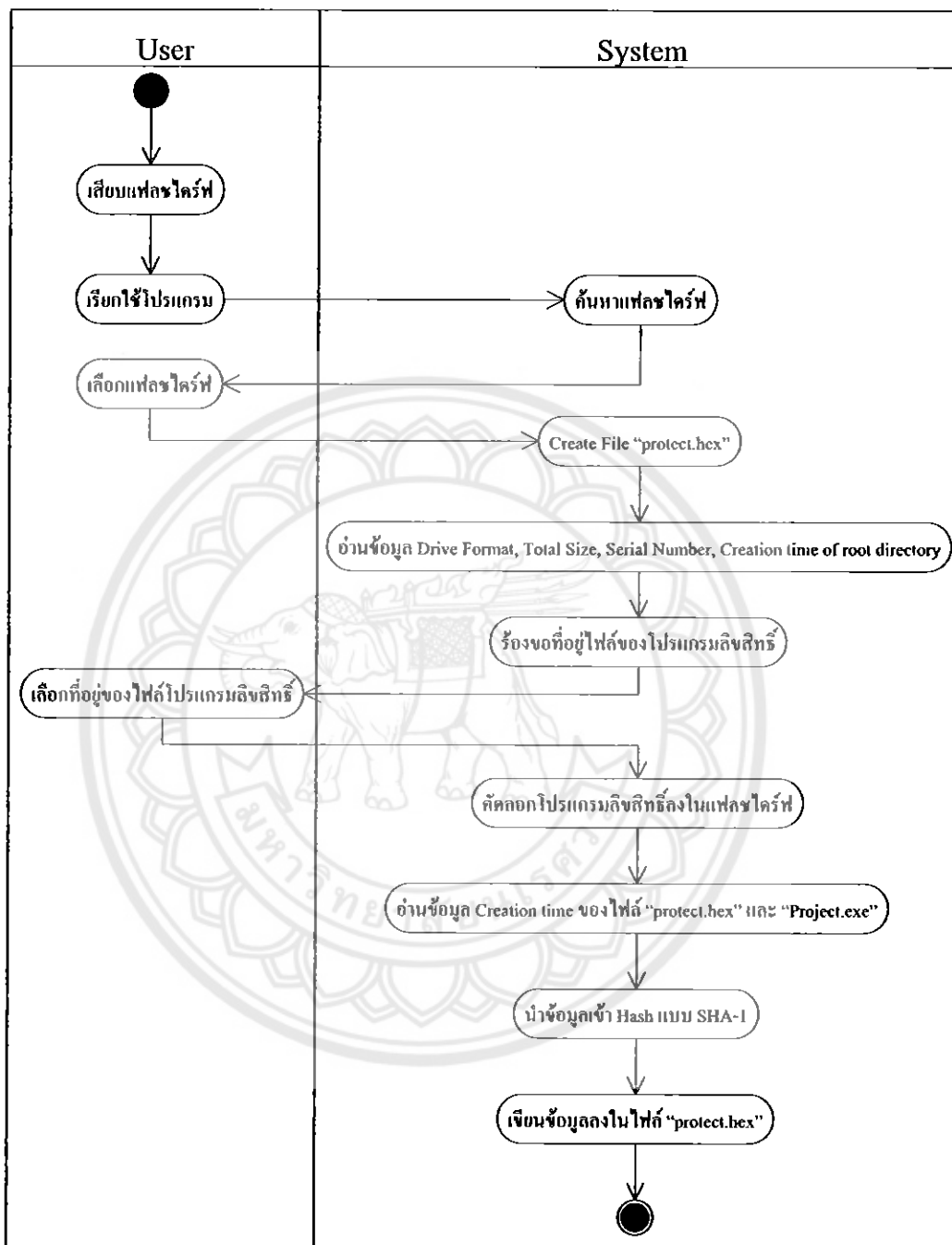
### 3.2.4 Class Diagram



รูปที่ 3.10 แสดง Class diagram ของโปรแกรมสร้าง Flash Drive

การสร้าง Flash Drive จำเป็นต้องมี Class OperationDrive ในการสร้างไฟล์ protect.hex และการทำ Hash แบบ SHA-1 เพื่อเขียนข้อมูลลงในไฟล์ protect.hex

3.2.5 Activity Diagram



รูปที่ 3.11 แสดง Activity diagram ของ โปรแกรมสร้าง Flash Drive

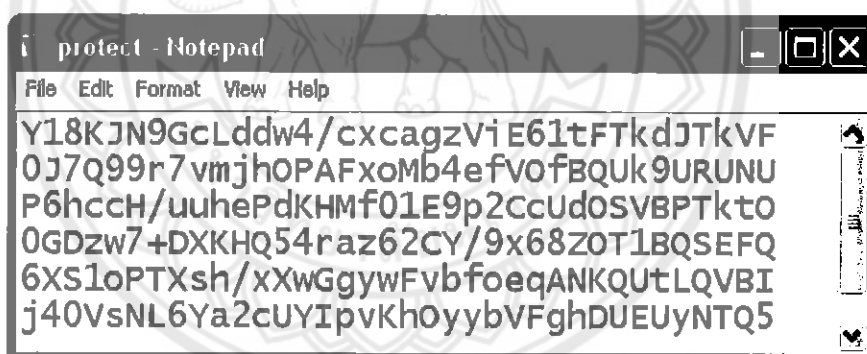
จากรูปกระบวนการทำงานของ โปรแกรมสร้าง Flash Drive ให้ถูกลิขสิทธิ์ สามารถอธิบายได้ดังนี้

1. ผู้สร้างทำการเลือก Flash Drive ตัวที่ต้องการสร้าง

2. ผู้สร้างทำการเรียกใช้โปรแกรม โปรแกรมจะทำการค้นหาไดรฟ์ที่เป็น Removable Drive ทั้งหมด เพื่อให้ผู้สร้างยืนยันว่าจะสร้าง Flash Drive ตัวใด
3. ต่อมาโปรแกรมจะทำการสร้างไฟล์ protect.hex เพื่อเก็บข้อมูลกับคุณสมบัติของ Flash Drive ในส่วนของ Drive Format, Total Size, Serial Number, Creation time of root directory ของ Flash Drive , Creation time ของไฟล์ protect.hex และ Creation time ของไฟล์ Project.exe ซึ่งเป็นไฟล์ของโปรแกรมลิขสิทธิ์ พร้อมคัดลอกโปรแกรมลิขสิทธิ์ดังกล่าวลงใน Flash Drive
4. โปรแกรมจะนำข้อมูลทั้งหมดมาทำการเข้ารหัสแบบ SHA-1 เพื่อไม่ให้ผู้อื่นสามารถอ่านข้อมูลเข้าใจได้ และเขียนข้อมูลที่ได้ทั้งหมดลงในไฟล์ protect.hex เป็นอันเสร็จสิ้น

ดังนั้นข้อมูลในไฟล์ protect.hex ซึ่งเป็นการเข้ารหัสแบบ SHA-1 แล้ว จะได้ผลลัพธ์ตาม รูปที่

3.12



รูปที่ 3.12 แสดงข้อมูลที่ถูกรหัสแบบ SHA-1 ของไฟล์ protect.hex

- บรรทัดที่ 1 เป็นข้อมูลของ Drive Format ของ Flash Drive
- บรรทัดที่ 2 เป็นข้อมูลของ Total Size ของ Flash Drive
- บรรทัดที่ 3 เป็นข้อมูลของ Serial Number ของ Flash Drive
- บรรทัดที่ 4 เป็นข้อมูลของ Creation time of root directory ของ Flash Drive
- บรรทัดที่ 5 เป็นข้อมูล Binary of Creation time ของไฟล์ protect.hex
- บรรทัดที่ 6 เป็นข้อมูล Binary of Creation time ของโปรแกรมลิขสิทธิ์ (Project.exe)

## บทที่ 4

### ผลการศึกษาและผลการพัฒนา

หลังจากทำการที่ ได้ทำการศึกษา กระบวนการทำงานของ โปรแกรมการป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์โดยใช้ Flash Drive ในส่วนของบทที่ 3 และทำการออกแบบโปรแกรมแสดงรูปแบบการทำงาน ซึ่งในบทนี้จะกล่าวถึงการนำโปรแกรมที่ได้ทำการศึกษา มาทดสอบการทำงานของโปรแกรมว่าโปรแกรมที่จัดทำขึ้นดังกล่าวนั้นสามารถทำงานได้อย่างถูกต้องแม่นยำตามกรณีทดสอบที่จัดเตรียมขึ้นหรือไม่ ซึ่งขั้นตอนการดำเนินงานที่กล่าวมาข้างต้นทางผู้จัดทำได้นำเสนอในส่วนของบทที่ 4 ดังนี้

#### 4.1 การสร้าง Flash Drive

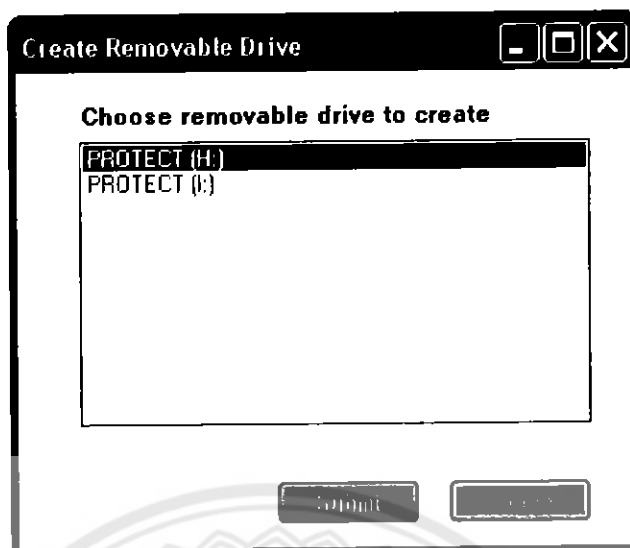
หลังจากผู้จัดทำได้ทำการพัฒนาค้นแบบการป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์โดยใช้ Flash Drive จึงได้ทำการทดลองสร้าง Flash Drive ในกรณีต่างๆ ดังตารางที่ 4.1

ตารางที่ 4.1 แสดงการสร้าง Flash Drive ในกรณีต่างๆ

วิธีการทดลอง	ผลการทดลอง
1. ทำการสร้าง Flash Drive ตามขั้นตอนที่กำหนด	สามารถสร้าง Flash Drive ที่ถูกลิขสิทธิ์ได้
2. ทำการสร้าง Flash Drive ขณะที่ไม่มี Flash Drive ต่ออยู่กับเครื่องคอมพิวเตอร์	ไม่สามารถสร้าง Flash Drive ที่ถูกลิขสิทธิ์ได้
3. ทำการสร้าง Flash Drive โดยการระบุ path การติดตั้งที่ไม่ตรงตามกำหนด	ไม่สามารถสร้าง Flash Drive ที่ถูกลิขสิทธิ์ได้

##### 4.1.1 การสร้าง Flash Drive ตามขั้นตอนที่กำหนด

เมื่อทำการสร้าง Flash Drive โปรแกรมจะแสดง Removable Drive ทั้งหมดที่มีการติดต่อกับคอมพิวเตอร์ เพื่อให้สามารถทำการเลือก Removable Drive ที่จะบรรจุ โปรแกรมดังรูปที่ 4.1



รูปที่ 4.1 แสดงการเลือกไดรฟ์ที่ต้องการบรรจุโปรแกรม

เมื่อทำการเลือก Removable Drive แล้วขั้นต่อไปจะให้ผู้สร้างทำการหาที่อยู่ของโปรแกรมที่ต้องการบรรจุลงใน Flash Drive ดังรูปที่ 4.2



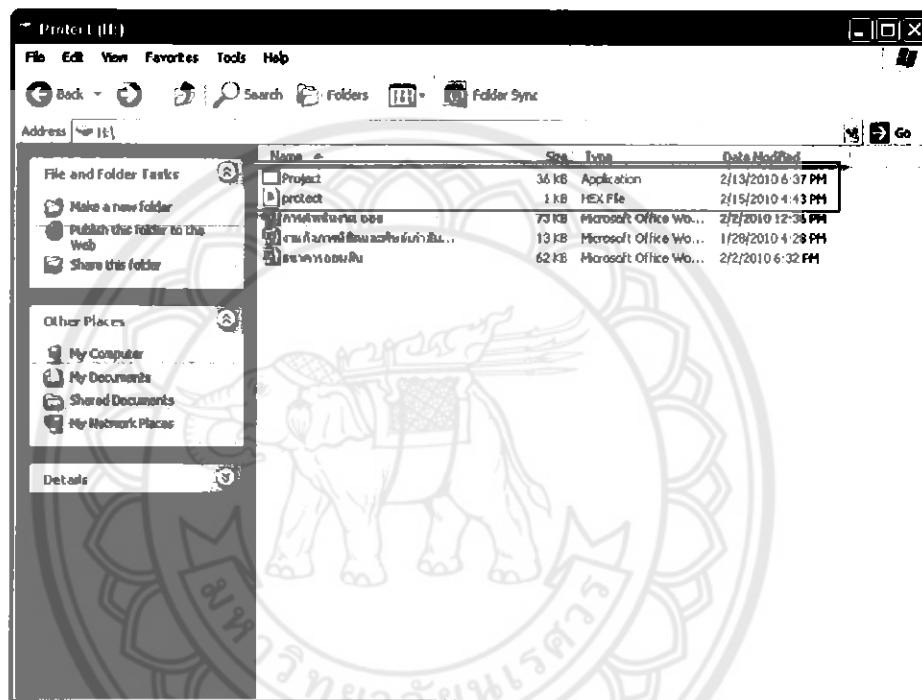
รูปที่ 4.2 แสดงการเลือกที่อยู่ของโปรแกรมที่จะบรรจุลงใน Flash Drive

เมื่อทำการเลือกที่อยู่ของโปรแกรมแล้ว โปรแกรมจะถูกคัดลอกลงใน Flash Drive และสร้างไฟล์ protect.hex เป็นอันเสร็จสิ้นดังรูปที่ 4.3 และ 4.4



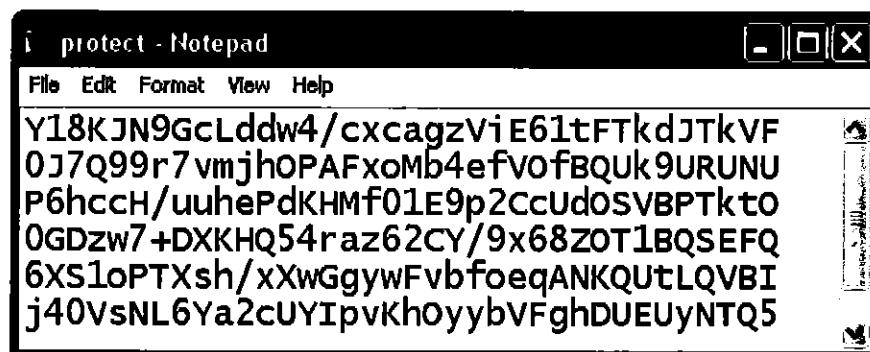


รูปที่ 4.3 แสดงข้อความที่โปรแกรมสามารถสร้าง Flash Drive ได้สมบูรณ์



รูปที่ 4.4 แสดงผลลัพธ์เมื่อทำการสร้าง Flash Drive เสร็จเรียบร้อยแล้ว

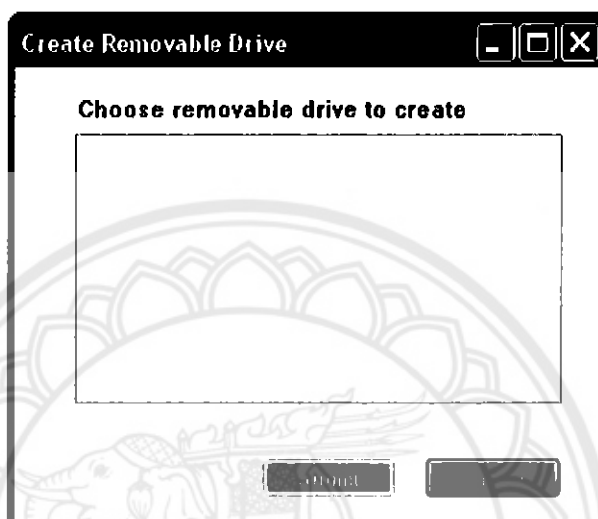
ซึ่ง protect.hex จะบรรจุข้อมูลที่ถูกละเมิดข้อมูลให้อยู่ในรูปของ SHA-1 ดังรูปที่ 4.5



รูปที่ 4.5 แสดงข้อมูลที่ถูกละเมิดให้อยู่ในรูปของ SHA-1

#### 4.1.2 การสร้าง Flash Drive ขณะที่ไม่มี Flash Drive ต่ออยู่กับเครื่องคอมพิวเตอร์

ในกรณีที่ผู้สร้างไม่ได้ทำการเสียบ Flash Drive กับเครื่องคอมพิวเตอร์ แล้วทำการสร้าง Flash Drive จะเห็นได้ว่าไม่มี removable drive ปรากฏให้ผู้สร้างเลือก จึงไม่สามารถสร้าง Flash Drive ที่ถูกลิขสิทธิ์ได้ และจะไม่สามารถสร้างอะไรใดๆ ต่อไปได้ดังรูปที่ 4.6



รูปที่ 4.6 แสดงการเลือกไดรฟ์ที่ต้องการบรรจุโปรแกรม

#### 4.1.3 การสร้าง Flash Drive โดยการระบุ path การติดตั้งที่ไม่ตรงตามกำหนด

ในกรณีที่ผู้สร้างเลือกที่อยู่ของโปรแกรมผิดจะแสดงกล่องตอบโต้ข้อความดังรูปที่ 4.7



รูปที่ 4.7 แสดงกล่องตอบโต้ข้อความเมื่อไม่สามารถค้นหาโปรแกรมได้

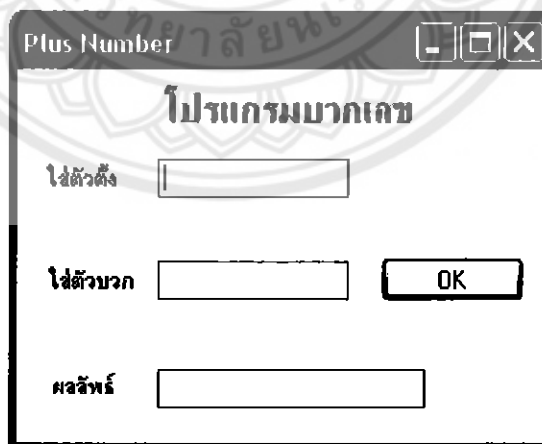
### 4.2 การศึกษาการป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive

หลังจากที่ทำการสร้างซอฟต์แวร์ที่ป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive แล้ว ผู้จัดทำ จะทำการทดลองให้เห็นถึงประสิทธิภาพต่างๆ ของการป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive โดยจะทำการทดลองดังตารางที่ 4.2

ตารางที่ 4.2 การทดลองซอฟต์แวร์ที่ป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive

วิธีการทดลอง	การทำงานของโปรแกรม
1. ทดลองโดยการเรียกใช้ Project.exe ที่บรรจุอยู่ใน Flash Drive ตัวที่กำหนด	โปรแกรมสามารถทำงานได้
2. การทดลองเรียกใช้ Project.exe โดยการคัดลอก Project.exe และ protect.hex ไปใช้งานที่อื่น	โปรแกรมไม่สามารถทำงานได้
3. การทดลองเรียกใช้ Project.exe โดยมีการแก้ไขข้อมูลในไฟล์ protect.hex	โปรแกรมไม่สามารถทำงานได้
4. การทดลองเรียกใช้ Project.exe ผ่านวง LAN โดยเสียบ Flash Drive ที่ถูกลิขสิทธิ์ไว้แล้วทำการแชร์ Flash Drive นั้น	โปรแกรมไม่สามารถทำงานได้
5. ทำการถอด Flash Drive ขณะที่ Project.exe ทำงานอยู่	โปรแกรมไม่สามารถทำงานได้

4.2.1 ทดลองโดยการเรียกใช้ Project.exe ที่บรรจุอยู่ใน Flash Drive ตัวที่กำหนด  
เมื่อทำการเรียกใช้โปรแกรม (Project.exe) และได้เรียกใช้ใน Flash Drive ตัวที่กำหนด  
โปรแกรมนั้นถูกลิขสิทธิ์จึงสามารถใช้งานโปรแกรมได้ตามปกติดังรูปที่ 4.8



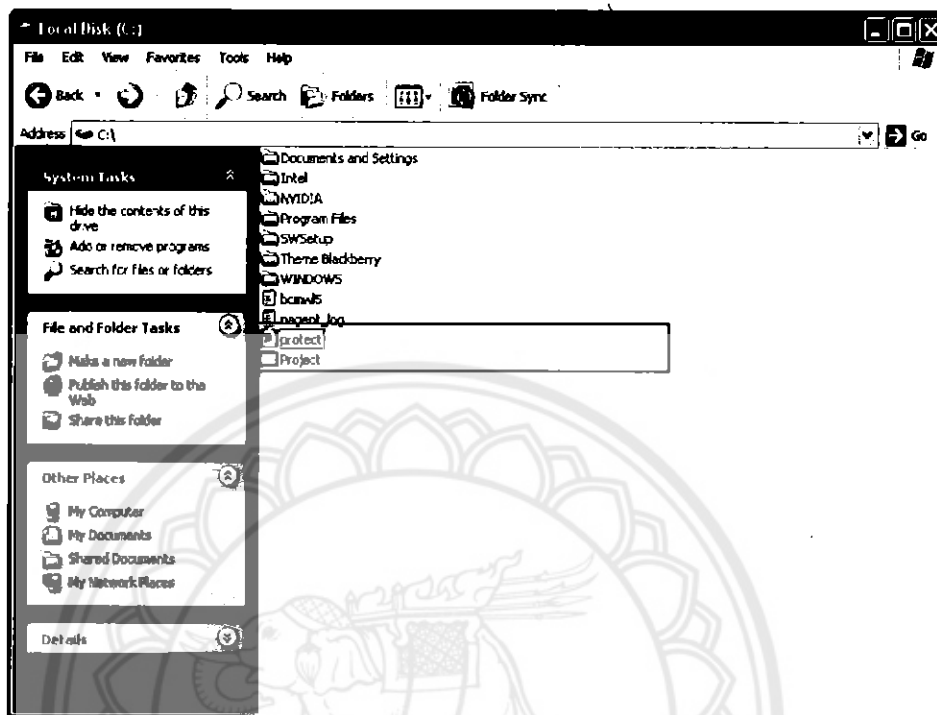
รูปที่ 4.8 แสดงโปรแกรมที่ถูกลิขสิทธิ์ซึ่งสามารถทำงานได้ตามปกติ

4.2.2 การทดลองเรียกใช้ Project.exe โดยการคัดลอก Project.exe และ protect.hex ไปใช้งานที่อื่น  
ในการทดลองนี้เราได้แบ่งการทดลองออกเป็น 2 กรณีคือ

15729506

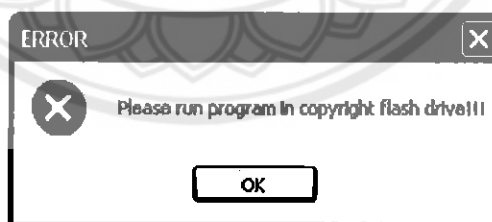
นร.  
92261  
2552

- กรณีที่ 1 การคัดลอกโปรแกรมไปใช้งานที่อื่น ที่ไม่ใช่ Flash Drive คัดที่กำหนด



รูปที่ 4.9 แสดงการคัดลอกโปรแกรมไปไว้ที่ไดร์ฟ C

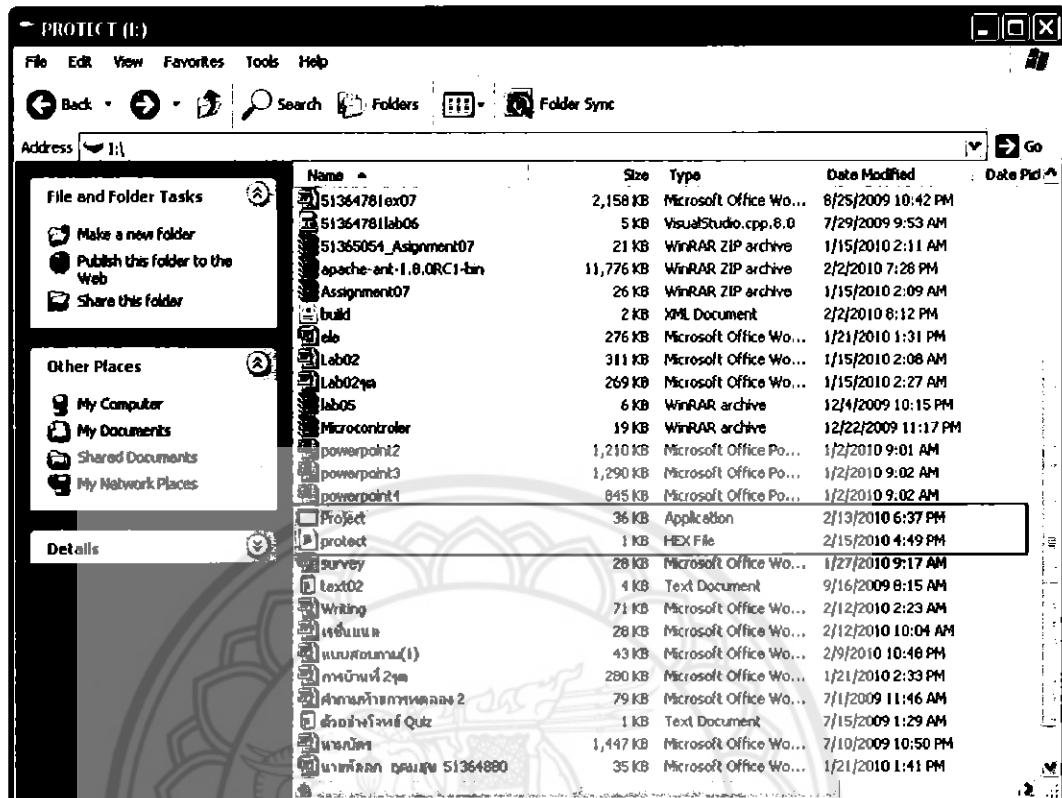
เมื่อทำการคัดลอกโปรแกรมไว้ที่ไดร์ฟ C แล้วทำการรันโปรแกรมจะปรากฏกล่องข้อความ ดังรูปที่ 4.10



รูปที่ 4.10 แสดงกล่องข้อความเมื่อรันโปรแกรมในไดร์ฟอื่น

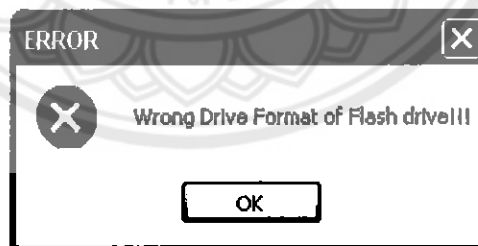
จะเห็นว่าโปรแกรมจะไม่ถูกลิขสิทธิ์ และไม่สามารถใช้งานโปรแกรมนั้นได้ เพราะโปรแกรมที่กำลังรันอยู่นั้น ไม่ได้อยู่ใน Flash Drive คัดที่กำหนด

- กรณีที่ 2 การคัดลอกโปรแกรมไปยัง Flash Drive คัดอื่น



รูปที่ 4.11 แสดงการคัดลอก โปรแกรมไปไว้ใน Flash Drive ตัวอื่น

เมื่อทำการคัดลอก โปรแกรมไปยัง Flash Drive ตัวอื่น แล้วทำการรัน โปรแกรมนั้นจะ ได้ปรากฏ  
กล่องข้อความซึ่งเป็นที่หลายสาเหตุ เช่นดังรูปที่ 4.12

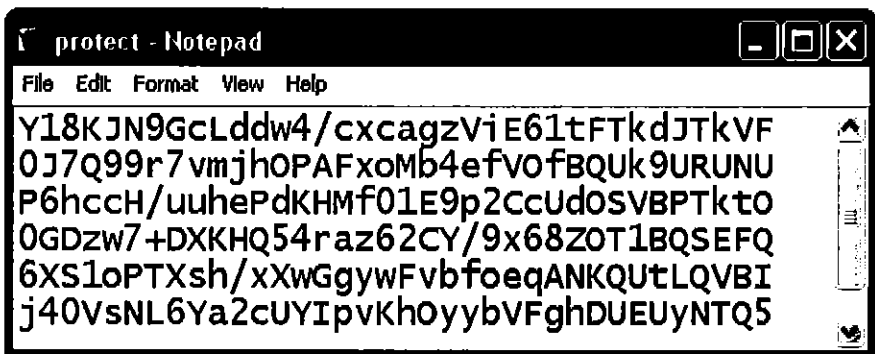


รูปที่ 4.12 แสดงกล่องตอบ ได้ข้อความที่ฟอร์แมตของ Flash Drive ไม่ตรงตามที่กำหนด

จะเห็นว่าโปรแกรมจะไม่ถูกลิขสิทธิ์ และไม่สามารถใช้งาน โปรแกรมนั้น ได้ เพราะไม่รัน โปรแกรม  
บน Flash Drive ตัวที่กำหนด

#### 4.2.3 การทดลองเรียกใช้ Project.exe โดยมีการแก้ไขข้อมูลในไฟล์protect.hex

ในการทดลองนี้ protect.hex ในรูปที่ 4.13 เป็นส่วนที่ถูกต้อง เราได้ทำการแก้ไขข้อมูล  
protect.hex ในรูปที่ 4.14

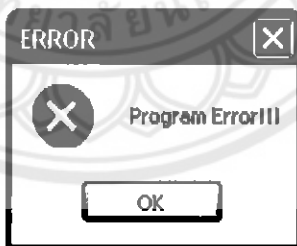


รูปที่ 4.13 ข้อมูลที่ต้องก่อนทำการแก้ไขข้อมูล



รูปที่ 4.14 ข้อมูลที่ถูกแก้ไข

เมื่อทำการรัน โปรแกรมแล้ว จะเกิดกล่องตอบโต้ข้อความดังรูปที่ 4.15

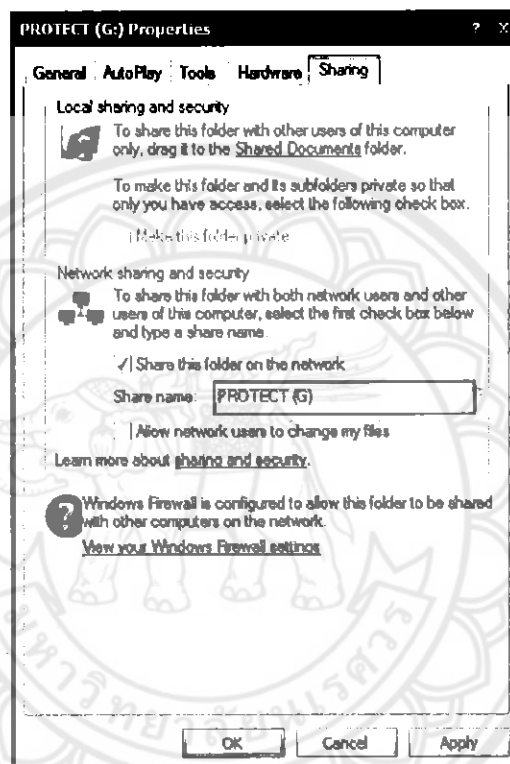


รูปที่ 4.15 แสดงกล่องตอบโต้ข้อความเมื่อทำการแก้ไขไฟล์ protect.hex

จะเห็นว่าโปรแกรมจะไม่ถูกลิขสิทธิ์ และไม่สามารถใช้งาน โปรแกรมนั้นได้ เพราะไฟล์ได้ถูกแก้ไขให้แตกต่างไปจากเดิม

#### 4.2.4 ทดลองเรียกใช้ Project.exe ผ่านวง LAN โดยเสียบ Flash Drive ที่ถูกลิขสิทธิ์ไว้แล้วทำการแชร์ Flash Drive นั้น

เริ่มแรกเราได้ทำการเสียบ Flash Drive ไว้แล้วทำการแชร์ Flash Drive นั้นเพื่อให้คอมพิวเตอร์เครื่องอื่นๆ ที่อยู่ภายในวง LAN เดียวกับคอมพิวเตอร์ที่มี Flash Drive เสียบอยู่เรียกใช้โปรแกรมผ่านวง LAN ดังรูปที่ 4.16



รูปที่ 4.16 ทำการแชร์ Flash Drive ในวง LAN

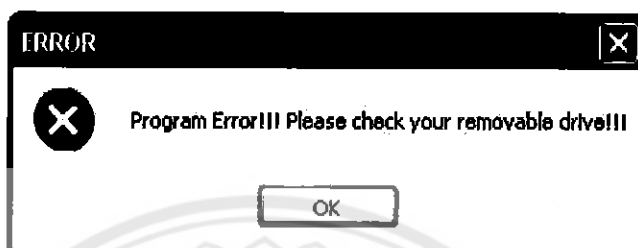
เมื่อทำการแชร์ Flash Drive เรียบร้อยแล้ว จึงเรียกใช้โปรแกรมโดยใช้คอมพิวเตอร์เครื่องอื่นที่อยู่ในวง LAN เดียวกัน โปรแกรมไม่สามารถทำงานได้ และจะปรากฏกล่องข้อความดังรูปที่ 4.17



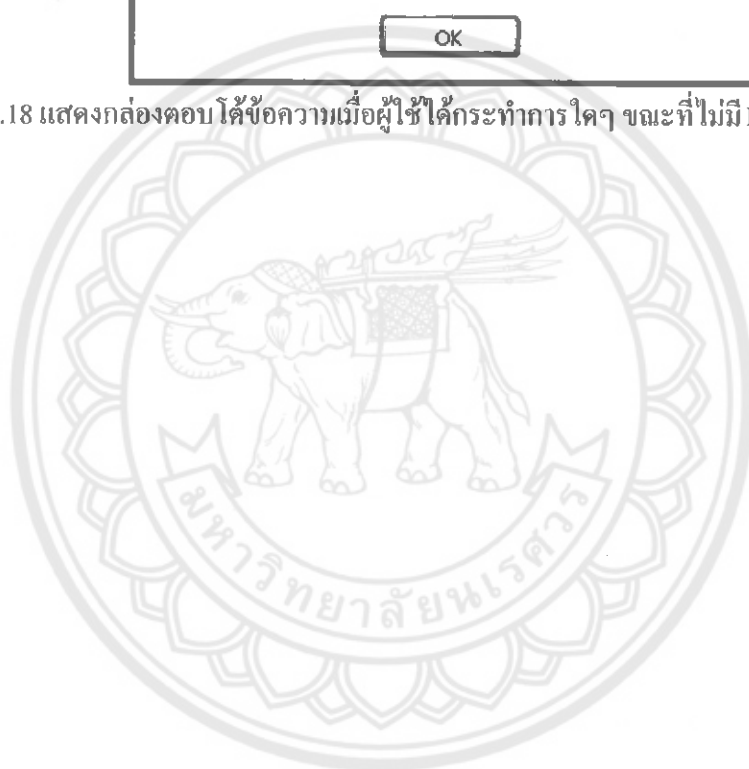
รูปที่ 4.17 แสดงกล่องข้อความเมื่อเรียกใช้โปรแกรมโดยคอมพิวเตอร์เครื่องที่อยู่ในวง LAN เดียวกัน

#### 4.2.5 ทดลองทำการถอด Flash Drive ขณะที่ Project.exe ทำงานอยู่

เราได้ทำการทดลอง โดยถอด Flash Drive ขณะที่โปรแกรมทำงานอยู่โปรแกรม จะไม่สามารถทำงานได้ เมื่อผู้ใช้ได้กระทำการใดๆ กับโปรแกรมนั้นในขณะที่ไม่มี Flash Drive เสียบอยู่กับเครื่องคอมพิวเตอร์ จะแสดงกล่องข้อความดังรูปที่ 4.18



รูปที่ 4.18 แสดงกล่องตอบโต้ข้อความเมื่อผู้ใช้ได้กระทำการใดๆ ขณะที่ไม่มี Flash Drive เสียบอยู่





## บทที่ 5

### สรุปผลและวิเคราะห์ผล

โครงการนี้พัฒนาเพื่อผู้ใช้งานซอฟต์แวร์ในการจำกัดสิทธิ์การใช้งานซอฟต์แวร์ที่ไม่ถูกลิขสิทธิ์และเพื่อเพิ่มความปลอดภัยให้กับซอฟต์แวร์ที่ถูกลิขสิทธิ์ โดยต้องมี Flash Drive ตัวที่กำหนด ในบทนี้ เป็นการสรุปผลการดำเนินงานโครงการ ปัญหาและอุปสรรค และข้อเสนอแนะ เพื่อเป็นแนวทางในการพัฒนาของผู้ที่สนใจต่อไป โครงการถูกพัฒนาด้วยโปรแกรม Microsoft Visual Studio 2005

#### 5.1 ผลการทดลอง

การทดลองได้เริ่มจากการทดลองสร้างโปรแกรมที่มีการป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ โดยใช้ Flash Drive โปรแกรมนี้มีฟังก์ชันที่ใช้ในการตรวจสอบคุณสมบัติของ Flash Drive , Creation time ของโปรแกรม (Project.exe) และ Creation time ของไฟล์ที่เก็บข้อมูลคุณสมบัติของ Flash Drive (protect.hex) ซึ่งนำมาใช้ในการอ้างอิงเพื่อตรวจสอบลิขสิทธิ์ซอฟต์แวร์ ได้ตามที่ต้องการ

การทดลองโดยการเรียกใช้ Project.exe ที่บรรจุอยู่ใน Flash Drive ตัวที่กำหนด โปรแกรมจะสามารถทำงานได้ตามปกติ

การทดลองเรียกใช้ Project.exe โดยการคัดลอก Project.exe และ protect.hex ไปใช้งานที่อื่น โดยจะแบ่งออกเป็น 2 กรณีคือ

- กรณีที่ 1 ทำการคัดลอก Project.exe และ protect.hex ไปไว้ในเครื่องคอมพิวเตอร์จากนั้นก็ทำการเรียกใช้ Project.exe ผลปรากฏว่าโปรแกรมไม่สามารถทำงานเนื่องจากไม่ได้เรียกใช้โปรแกรมใน Flash Drive
- กรณีที่ 2 ทำการคัดลอก Project.exe และ protect.hex ไปไว้ใน Flash Drive ตัวอื่นจากนั้นก็ทำการเรียกใช้ Project.exe ผลปรากฏว่าโปรแกรมไม่สามารถทำงานได้เนื่องจากคุณสมบัติต่างๆ ไม่ตรงตาม Flash Drive ตัวที่กำหนด

การทดลองเรียกใช้ Project.exe โดยมีการแก้ไขข้อมูลในไฟล์ protect.hex ผลปรากฏว่าโปรแกรมไม่สามารถทำงานได้เนื่องจากข้อมูลภายในไฟล์ protect.hex ไม่ตรงตามที่กำหนด

การทดลองเรียกใช้ Project.exe ผ่านวง LAN โดยเสียบ Flash Drive ที่ถูกลิขสิทธิ์ไว้แล้วทำการแชร์ Flash Drive นั้น ให้เครื่องคอมพิวเตอร์อื่นๆ ในวง LAN เดียวกัน แล้วทำการเรียกใช้ Project.exe ผลปรากฏว่าโปรแกรมไม่สามารถทำงานได้เนื่องจาก path ไม่ตรงตามที่กำหนดไว้

และการทดลองสุดท้ายของผู้พัฒนาได้ทำการถอด Flash Drive ขณะที่ Project.exe ทำงานอยู่ ผลปรากฏว่าโปรแกรมจะไม่สามารถทำงานต่อไปได้ เนื่องจากไม่มีการเสียบ Flash Drive ตัวที่กำหนดไว้แล้ว

กล่าวโดยสรุป การพัฒนาต้นแบบการป้องกันการละเมิดลิขสิทธิ์โดยใช้ Flash Drive นี้ สามารถป้องกันการละเมิดลิขสิทธิ์ซอฟต์แวร์ได้อย่างมีประสิทธิภาพ มีความปลอดภัย และสามารถใช้งานได้ง่าย

## 5.2 สรุปผลการทดลอง

1. เมื่อทำการเรียกโปรแกรม Create Flash Drive เพื่อทำการสร้างไฟล์และบรรจุโปรแกรมปกติ ที่มีฟังก์ชันการตรวจสอบลิขสิทธิ์ลงใน Flash Drive ตัวที่กำหนด สามารถทำได้อย่างรวดเร็ว และถูกต้องตามที่กำหนดเอาไว้
2. จากการทดลองตรวจสอบ Flash Drive ตัวที่กำหนด โดยการเรียกใช้ฟังก์ชันตรวจสอบแฟลชไดรฟ์ในโปรแกรมปกติ สามารถตรวจสอบลิขสิทธิ์ได้อย่างถูกต้อง และใช้งานได้อย่างปกติ
3. จากการทดลองโดยการพยายามที่จะละเมิดลิขสิทธิ์ในรูปแบบต่างๆ โปรแกรมจะไม่ถูกลิขสิทธิ์ และไม่สามารถทำงานได้
4. จากการทดสอบโปรแกรมแล้วนั้น โปรแกรมที่ถูกลิขสิทธิ์และสามารถทำได้ตามปกติ จะต้องประกอบไปด้วย ตัวโปรแกรมปกติ (Project.exe) ไฟล์ที่บรรจุข้อมูลคุณสมบัติต่างๆ ของ Flash Drive (protect.hex) โดยที่ไม่มีการแก้ไขข้อมูลใดๆ และ Flash Drive ตัวที่กำหนด

## 5.3 ปัญหาและอุปสรรคที่พบ

1. รูปแบบเวลาและวันที่ ของคอมพิวเตอร์ แต่ละเครื่องไม่ตรงกัน จึงส่งผลทำให้ การอ่าน Creation Time ของ Flash Drive ไม่ตรงกัน แก้ไขปัญหาโดยการแปลงวันและเวลาที่ได้อาศัยอยู่ในรูปแบบของ Binary ก่อน
2. เนื่องจาก SHA-1 ถูกถอดรหัสได้แล้ว แก้ไขปัญหาโดยการ เพิ่มตัวอักษรในข้อความที่ต้องการเข้า SHA-1 เพื่อเพิ่มความซับซ้อนให้กับข้อความอีกระดับ

## 5.4 ข้อเสนอแนะและแนวทางในการพัฒนา

1. อาจพัฒนาโดยการสร้าง DLL (Dynamic Link Library) โดยสร้างความปลอดภัยให้กับโปรแกรม เพื่อไม่ให้ระบบปฏิบัติการ WINDOWS สามารถเลี่ยงการใช้ DLL ได้
2. อาจพัฒนาโดยการเพิ่มการใช้รหัสเพื่อยืนยันลิขสิทธิ์เพื่อเพิ่มความปลอดภัยให้มากยิ่งขึ้น

3. อาจพัฒนาโดยการสร้าง Option ให้สามารถทำการติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์ได้
4. อาจพัฒนาโดยทำให้สามารถสร้างเป็นผลิตภัณฑ์ สำหรับจัดจำหน่ายให้ผู้ใช้อื่นๆ



## เอกสารอ้างอิง

- [1] ไมโครซอฟท์ประเทศไทย. “การละเมิดลิขสิทธิ์ซอฟต์แวร์” [Online] Available :  
<http://www.microsoft.com/thailand/Piracy>.
- [2] NetMaNia. “เรื่องของ CD Copy Protection” [Online] Available :  
<http://www.nutthnet.com/forum/topic.php?id=173>.
- [3] ธนา หงษ์สุวรรณ. “Message Authentication and Digital Signaure” [Online] Available :  
[http://www.msit.mut.ac.th/member/filemanager/share\\_file/bon/security/Digital%20Signature.doc](http://www.msit.mut.ac.th/member/filemanager/share_file/bon/security/Digital%20Signature.doc).
- [4] กิตติพงษ์ กลมกล่อม. “การวิเคราะห์และออกแบบระบบเชิงวัตถุด้วย UML”. พิมพ์ครั้งที่ 1.  
กรุงเทพมหานคร : สำนักพิมพ์ เคทีพี. 2552.





## นิยามคำศัพท์

**Flash Drive (หรือ Handy Drive, Thumb Drive, USB Drive)** หมายถึง อุปกรณ์ที่ใช้ในการเก็บข้อมูลหรือไฟล์จากคอมพิวเตอร์

**Software (ซอฟต์แวร์)** หมายถึง ชุดคำสั่งหรือ โปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงาน

**Copyright Protection** หมายถึง วิธีการป้องกันไม่ให้ผู้ใดสามารถคัดลอกได้ ผู้เขียนโปรแกรมมักพยายามทำทุกวิถีทางที่จะกันไม่ให้ผู้หนึ่งผู้ใดมาคัดลอกโปรแกรม หรือเพิ่มข้อมูลที่เขาสร้างขึ้นไว้

**End User License Agreement (หรือ EULA)** หมายถึง ข้อตกลงในการใช้โปรแกรม

**Types of Software Piracy** หมายถึง ประเภทของการละเมิดลิขสิทธิ์

**Certificate of Authenticity (หรือ COA)** หมายถึง ฉลากที่ใช้ระบุซอฟต์แวร์ของแท้ของ Microsoft ซึ่งประกอบด้วยคุณสมบัติในการป้องกันของเทียม เพื่อให้คุณสามารถตรวจสอบความถูกต้องของซอฟต์แวร์ที่ได้รับ

**Academic Edition (หรือ AE)** หมายถึง สินค้าที่ออกแบบมาเพื่อองค์กรการศึกษา และนักศึกษาด้วยราคาต่ำเป็นพิเศษ

**Not for Resale (หรือ NFR)** หมายถึง ห้ามนำไปขายต่อ เช่น สินค้าที่นำมาแจกจ่ายในกรณีที่เป็นการส่งเสริมการขาย หรือตัวอย่าง มิได้มีไว้เพื่อจำหน่าย

**Original Equipment Manufacturer (หรือ OEM)** หมายถึง ลิขสิทธิ์ผลิตภัณฑ์ไมโครซอฟท์ ซึ่งจำหน่ายให้กับผู้ผลิต และผู้ประกอบคอมพิวเตอร์ สำหรับการติดตั้งไปพร้อมกับการจำหน่ายคอมพิวเตอร์

**Fulfillment** หมายถึง การทำให้บรรลุผล

**Open License** หมายถึง โปรแกรมการจัดซื้อลิขสิทธิ์ซอฟต์แวร์สำหรับองค์กรธุรกิจขนาดเล็กและขนาดกลางที่ต้องการใช้ลิขสิทธิ์ไมโครซอฟท์ตั้งแต่ 5 ชุดขึ้นไป

**Select License** หมายถึง โปรแกรมการจัดซื้อลิขสิทธิ์ซอฟต์แวร์สำหรับองค์กรขนาดกลางถึงขนาดใหญ่ที่มีเครื่องคอมพิวเตอร์ตั้งแต่ 200 เครื่องขึ้นไปสามารถจัดซื้อผลิตภัณฑ์ไมโครซอฟท์ที่ต้องการใช้ในราคาที่คุ้มค่าและรูปแบบการซื้อที่ยืดหยุ่น และสะดวก

**Enterprise Agreement (หรือ EA)** หมายถึง การปรับเปลี่ยนเทคโนโลยีในองค์กรเป็นเรื่องที่ยากสำหรับผู้บริหาร โดยเฉพาะอย่างยิ่งองค์กรที่มีการใช้เทคโนโลยีหลากหลาย เหมาะสำหรับองค์กรที่มีการบริหารจัดการจากศูนย์กลาง

**Internet Piracy** หมายถึง การใช้อินเทอร์เน็ตเป็นสื่อในการทำสำเนาอย่างผิดกฎหมาย หรือใช้จำหน่ายซอฟต์แวร์ที่ไม่ถูกต้อง

**Shareware** หมายถึง ซอฟต์แวร์ที่สามารถใช้งานได้ฟรีภายใต้เงื่อนไขต่าง ๆ คือให้ทดลองใช้ก่อน ถ้าผู้ใช้งานถูกใจก็ค่อยจ่ายเงินแล้วก็จะได้ใช้งานได้เต็มประสิทธิภาพ

**Dependency on External Action** หมายถึง การขึ้นอยู่กับการกระทำจากภายนอกเช่นตัวโปรแกรมต้นฉบับจะยอมทำงานก็ต่อเมื่อมีการกระทำร่วมกันหรือส่งงานมาจาก guard module (ตัวป้องกัน) ด้วย วิธีการที่ใช้ในที่นี้ คือ การเข้ารหัส หรือ Encryption ครับ โปรแกรมจะยอมทำงานก็ต่อเมื่อมันมีตัวถอดรหัสมาด้วย

**Encryption (การเข้ารหัส)** หมายถึง การเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต

**Decryption (การถอดรหัส)** หมายถึง การทำให้ผู้มีสิทธิเท่านั้นที่จะทำการอ่านข้อมูลนั้นได้

**The Guard Module** หมายถึง ตัวป้องกันแบบจับต้องสัมผัสไม่ได้ จะเป็นตัวที่อนุญาตให้โปรแกรมทำงานได้ ด้วยการเช็คค่าเริ่มต้น หรือ key ที่ได้กำหนดแล้วว่าเป็นค่าของตัวต้นฉบับจริง (Authentic key) การทำงานของตัว Guard Module นั้น จะต้องมีการทำงานที่ซับซ้อนมาก เพื่อไม่ให้เราสามารถ

รู้ถึงกรรมวิธีการทำงาน หรือ ลอกเลียนแบบการทำงานได้ หรือ ไปหลอกให้มันทำงานได้ ถ้าปราศจากค่าเริ่มต้น หรือคีย์ Authentic Key นี้

**Authentic key** หมายถึง ค่าเริ่มต้น หรือ key ที่ได้กำหนดแล้วว่าเป็นค่าของตัวต้นฉบับจริง

**Key Detection** หมายถึง ตัวตรวจจับหา Authentic Key

**Initialization** หมายถึง กระบวนการของการตั้งและใช้กำหนดค่าสำหรับข้อมูลตัวแปรที่ได้รับการใช้ โดยโปรแกรมคอมพิวเตอร์ ตัวอย่าง ระบบปฏิบัติการหรือโปรแกรมประยุกต์ที่ได้รับการติดตั้งด้วยค่าเริ่มต้นหรือ ค่าผู้ใช้เจาะจงที่ค้นหาตามมุมมองแน่นอนของระบบหรือโปรแกรมทำงานอย่างไร ตามปกติ ค่าเหล่านี้ได้รับการเก็บในไฟล์เริ่มต้น (ใน Windows สิ่งเหล่านี้สามารถได้รับการระบุเป็นไฟล์ด้วยนามสกุล INI) เมื่อระบบปฏิบัติการหรือโปรแกรมประยุกต์ได้รับการโหลดขึ้นเข้าสู่หน่วยความจำครั้งแรก ส่วนของโปรแกรมทำ initialization นั่นคือ การมองหาไฟล์เริ่มต้นค่าค้นหาข้อกำหนดค่าให้แทนที่สำหรับตัวแปร และกระทำตามนั้น ตัวอย่างหน้าจอ desktop และโปรแกรมประยุกต์ที่ได้รับการเริ่มตลอดจนถึงระบบปฏิบัติการได้รับการกำหนดค่า และโหลด

**Code Security** หมายถึง การรักษาความปลอดภัยของ Code

**Debug Trapping** หมายถึง การทำให้เกิด Debug

**The Physical Key** หมายถึง ตัวป้องกันทางกายภาพแบบจับต้องสัมผัสได้ ซึ่งคนที่ซื้อ software จะได้รับอุปกรณ์เหล่านี้ เพื่อแสดงถึงความเป็นเจ้าของ และมีสิทธิ์ในการใช้ software ลิขสิทธิ์นั้น ซึ่งอาจเป็นอุปกรณ์ในหลายๆรูปแบบ

**Original CD** หมายถึง CD ต้นฉบับ

**Key Diskette** หมายถึง ระบบป้องกันการคัดลอกซอฟต์แวร์รูปแบบหนึ่งที่อยู่ในรูปแบบของ diskette

**Hard Disk** หมายถึง อุปกรณ์บรรจุข้อมูลแบบไม่ลบเลือน มีลักษณะเป็นจานโลหะที่เคลือบด้วยสารแม่เหล็กซึ่งหมุนอย่างรวดเร็วเมื่อทำงาน การติดตั้งเข้ากับตัวคอมพิวเตอร์สามารถทำได้ผ่านการต่อ



เข้ากับมาเธอร์บอร์ด (motherboard) ที่มีอินเตอร์เฟซแบบขนาน (PATA) , แบบอนุกรม (SATA) และแบบเล็ก (SCSI)

**Plug-in board** หมายถึง การเชื่อมต่อกับ board

**Personal Characteristics** หมายถึง ลักษณะส่วนบุคคล



## ประวัติผู้เขียนโครงการ



ชื่อ นายจักรพันธ์ เอี่ยมเจริญจิตต์

ภูมิลำเนา 93 ม.11 ต.วัดป่า อ.หล่มสัก จ.เพชรบูรณ์

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจาก โรงเรียนกาญจนาภิเษก วิทยาลัย  
เพชรบูรณ์

- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์  
มหาวิทยาลัยนเรศวร

E-mail : bati\_boy@hotmail.com



ชื่อ นายนพภูล คำแสง

ภูมิลำเนา 12/2 ม.6 ต.ไกรกลาง อ.กงไกรลาศ จ.สุโขทัย

ประวัติการศึกษา

- จบระดับมัธยมศึกษาจาก โรงเรียนสวรรคค่อนันต์วิทยา

- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์  
มหาวิทยาลัยนเรศวร

E-mail : romance\_\_04@hotmail.com

## ประวัติผู้เขียนโครงการ (ต่อ)



ชื่อ นายนิพนธ์ กุสุโมทย์  
ภูมิลำเนา 2/4 ม.1 ต.หนองสรวง อ.หนองฉาง จ.อุทัยธานี  
ประวัติการศึกษา

- จบระดับมัธยมศึกษาจากโรงเรียนหนองฉางวิทยา
- ปัจจุบันกำลังศึกษาในระดับปริญญาตรีชั้นปีที่ 4

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์  
มหาวิทยาลัยนเรศวร

E-mail : nipon\_kn@hotmail.com

