รายงานวิชา Computer Security

Assignment II

จัดทำโดย

นายปณิธาน ดวงขวัญ

รหัส 5735512036 Section 02

เสนอ

อาจารย์ฐิตินันท์ เกลี้ยงสุวรรณ

รหัสวิชา 242-312 Computer Security

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

มหาวิทยาลัยสงขลานครินทร์

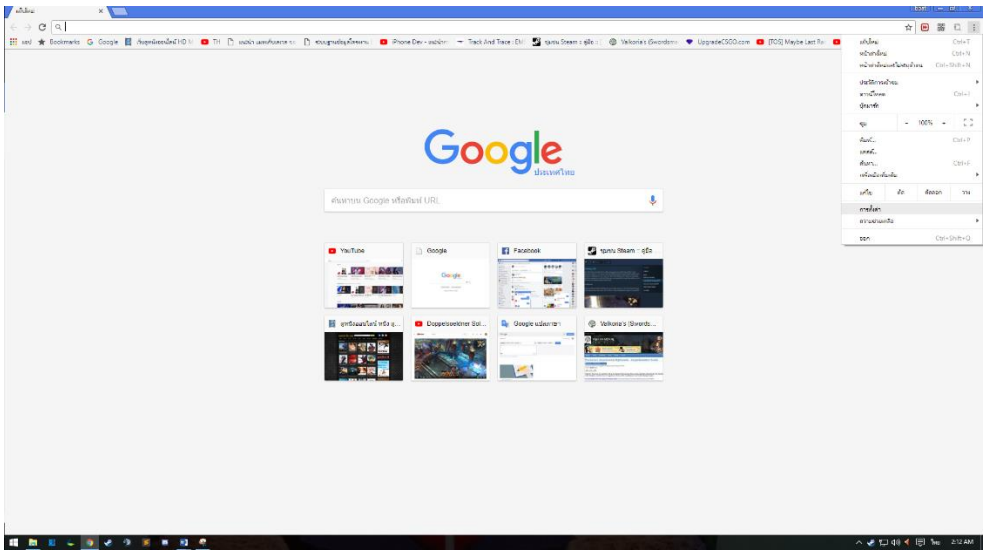
Assignment II

1. Certificate

a. เปิด web browser และให้ค้นหา trusted root certification authority พร้อมทั้งอธิบายถึงวิธีการค้นหาข้อมูลดังกล่าว

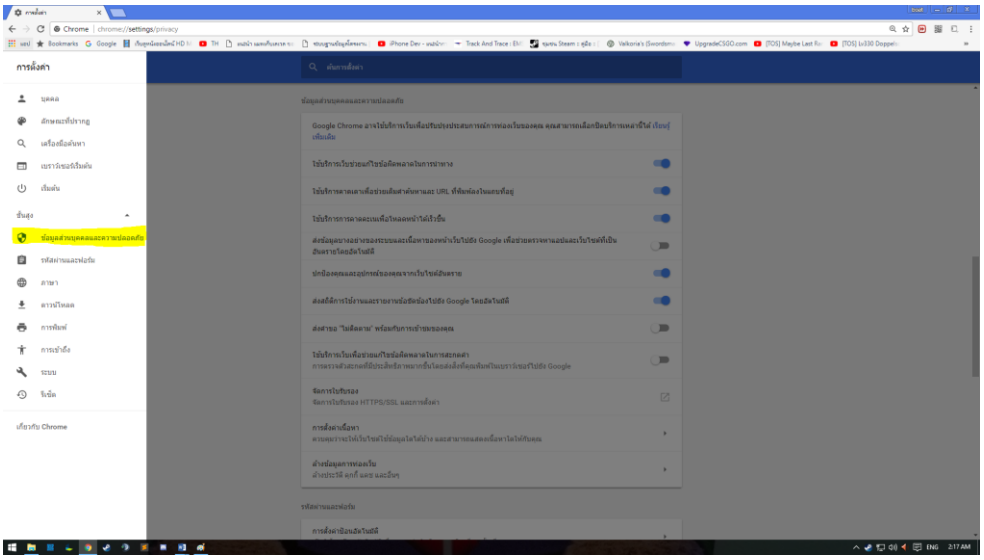
i. เปิด Web Browser

ii. เข้าการตั้งค่า

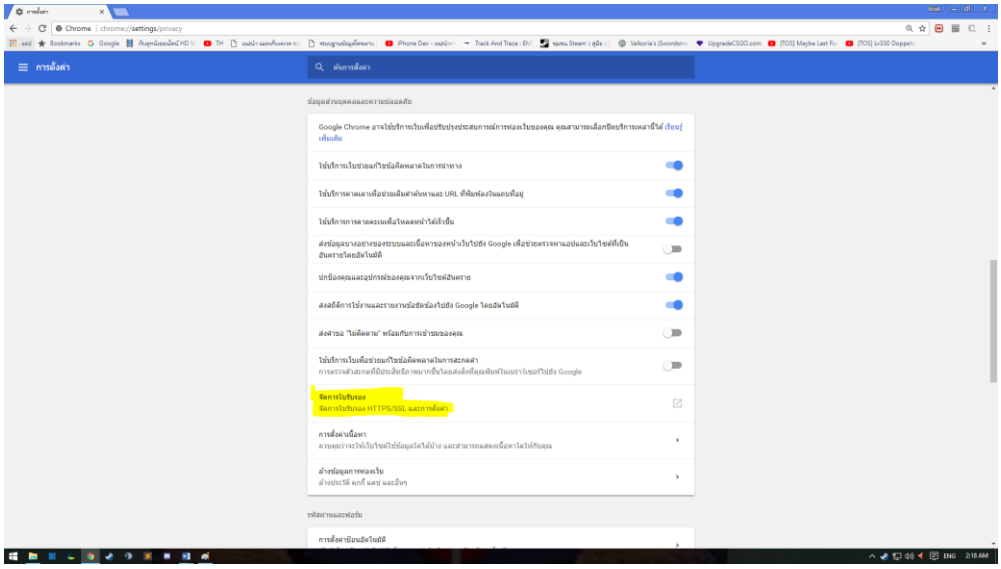


iii. คลิกแถบการตั้งค่าทางด้านซ้ายของ Web Browser

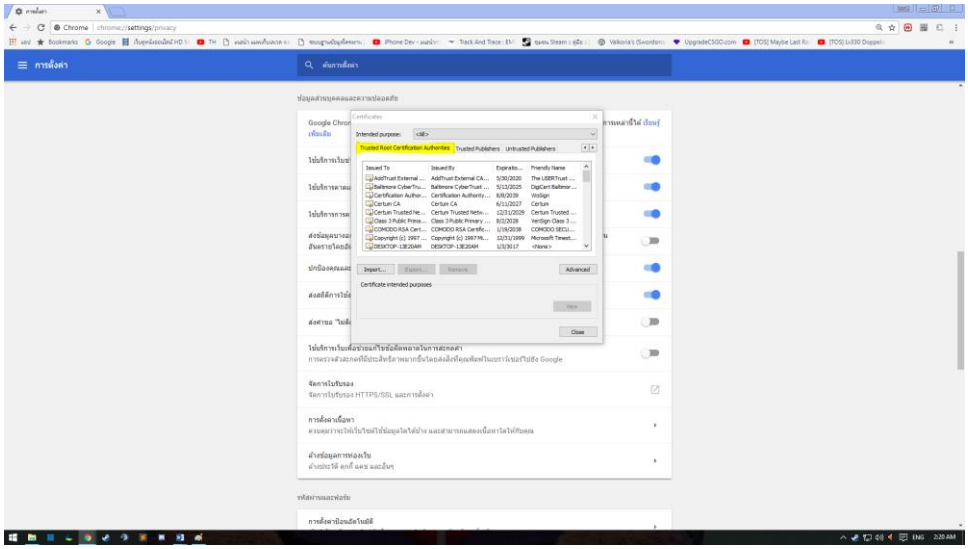
iv. คลิกการตั้งค่า > ข้อมูลส่วนบุคคลและความปลอดภัย



v. เลือกจัดการใบรับรอง



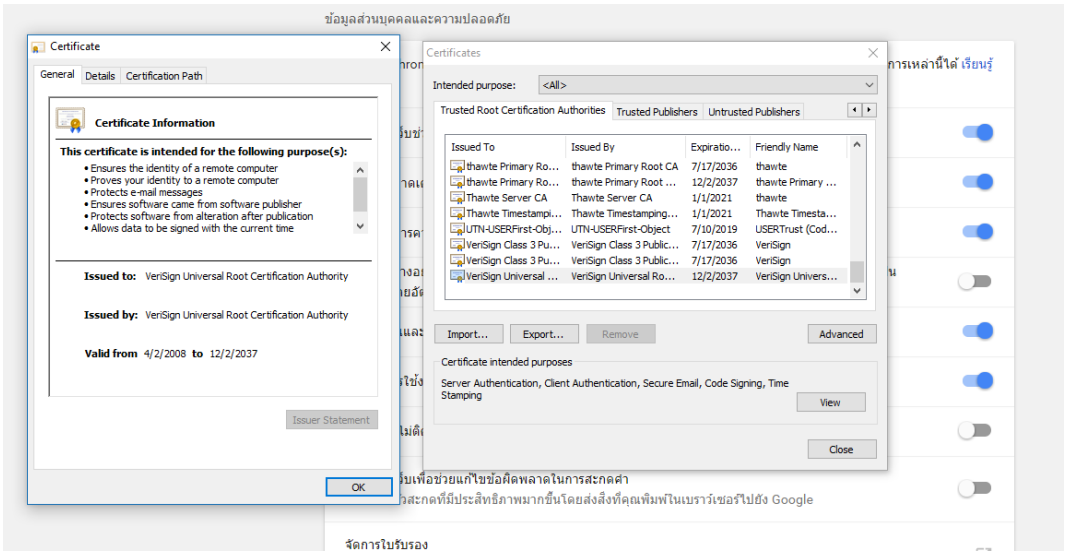
vi. จะได้หน้าต่างดังรูป



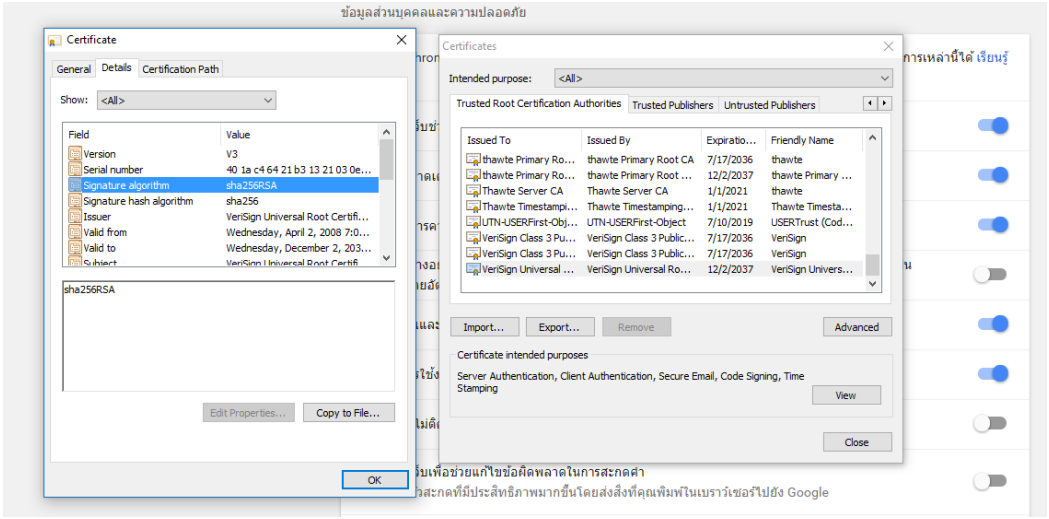
b. **ค้นหา 2 certificate ที่ออกโดย VeriSign Inc. และ Entrust.net เปรียบเทียบข้อมูลต่างๆ ดังนี้ theintension of the certificate(จุดประสงค์), signature algorithms, public-key algorithm (จำนวนบิต) เป็นต้น (อธิบายความแตกต่างของทั้ง 2 certificate)**

i. เลือก VeriSign Inc. จะได้หน้าต่างของ certificate

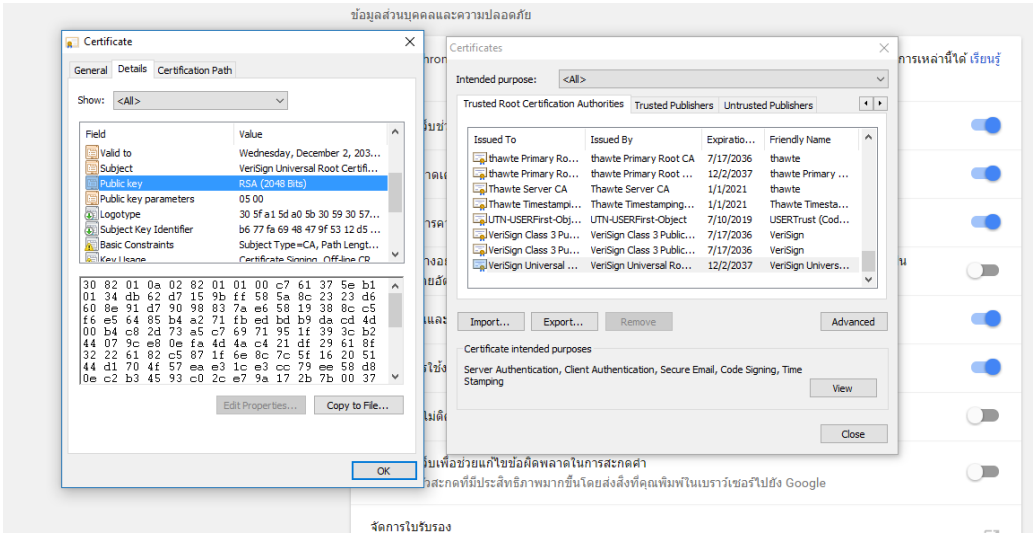
1. ตรวจสอบให้แน่ใจว่าเป็นข้อมูลประจำตัวของคอมพิวเตอร์ระยะไกล
2. พิสูจน์ข้อมูลประจำตัวของคุณกับคอมพิวเตอร์ระยะไกล
3. ป้องกันข้อความอีเมล์
4. ตรวจสอบให้แน่ใจว่าซอฟต์แวร์มาจากผู้เผยแพร่ซอฟต์แวร์
5. ป้องกันซอฟต์แวร์จากการเปลี่ยนแปลงหลังจากออกจำหน่าย
6. อนุญาตให้รับรองข้อมูลในเวลาปัจจุบันได้
7. นโยบายทั้งหมดเกี่ยวกับการอนุมัติ



ii. หน้าต่างของ signature algorithms

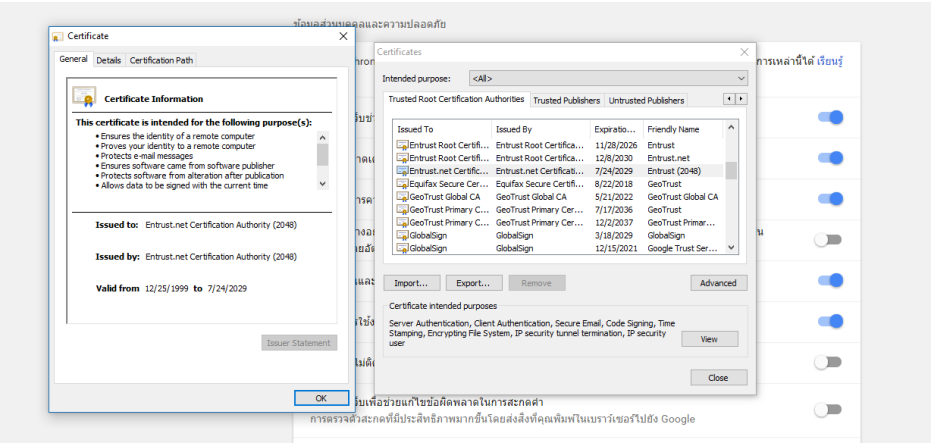


iii. public-key จำนวน 2048 bit

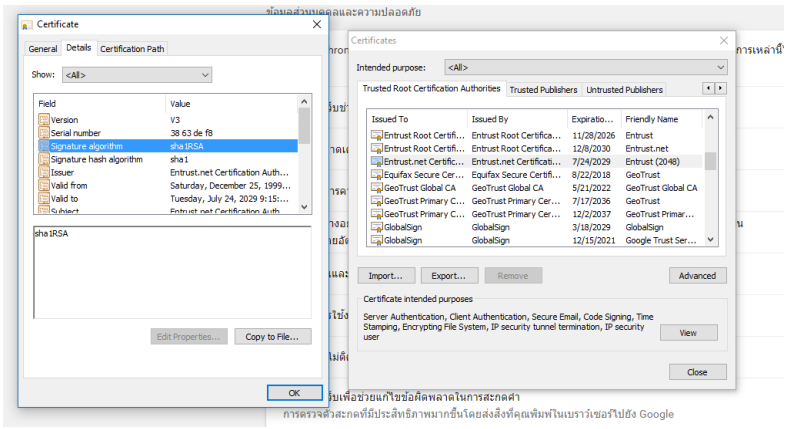


iv. เลือก Entrust.net จะได้หน้าต่างของ certificate

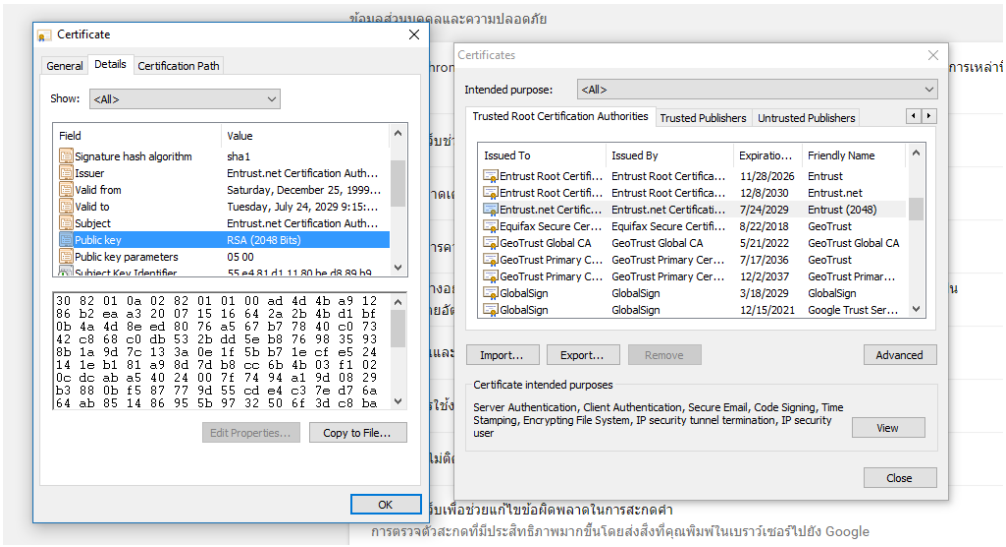
1. ตรวจสอบให้แน่ใจว่าเป็นข้อมูลประจำตัวของคอมพิวเตอร์ระยะไกล
2. พิสูจน์ข้อมูลประจำตัวของคุณกับคอมพิวเตอร์ระยะไกล
3. ป้องกันข้อความอีเมล์
4. ตรวจสอบให้แน่ใจว่าซอฟต์แวร์มาจากผู้เผยแพร่ซอฟต์แวร์
5. ป้องกันซอฟต์แวร์จากการเปลี่ยนแปลงหลังจากออกจำหน่าย
6. อนุญาตให้รับรองข้อมูลในเวลาปัจจุบันได้
7. อนุญาตให้เข้ารหัสลับข้อมูลบนดิสก์
8. อนุญาตการสื่อสารแบบปลอดภัยบนอินเทอร์เน็ต
9. นโยบายทั้งหมดเกี่ยวกับการอนุมัติ



v. หน้าต่างของ signature algorithms

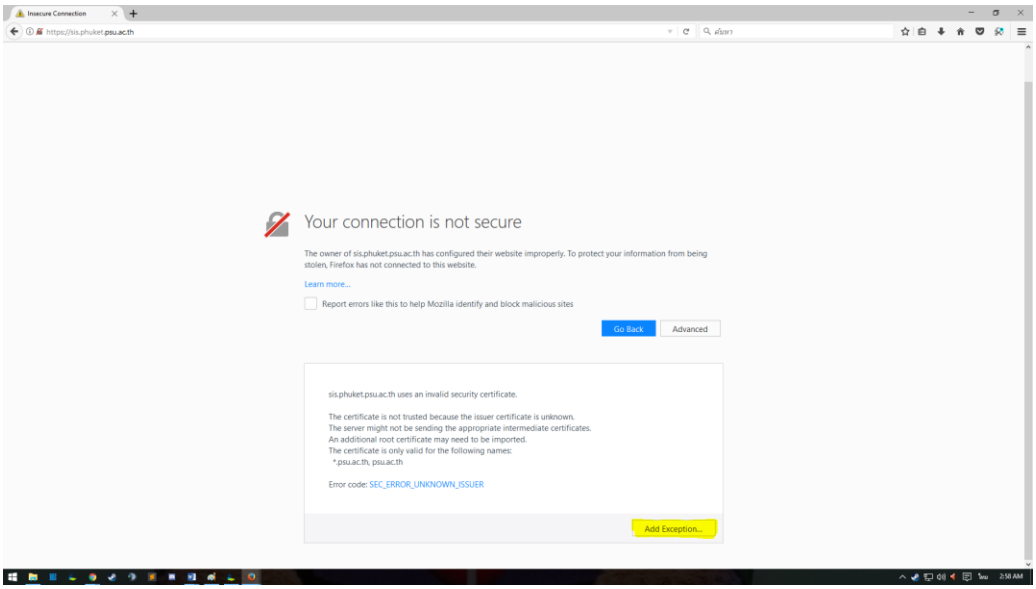


vi. public-key จำนวน 2048 bit



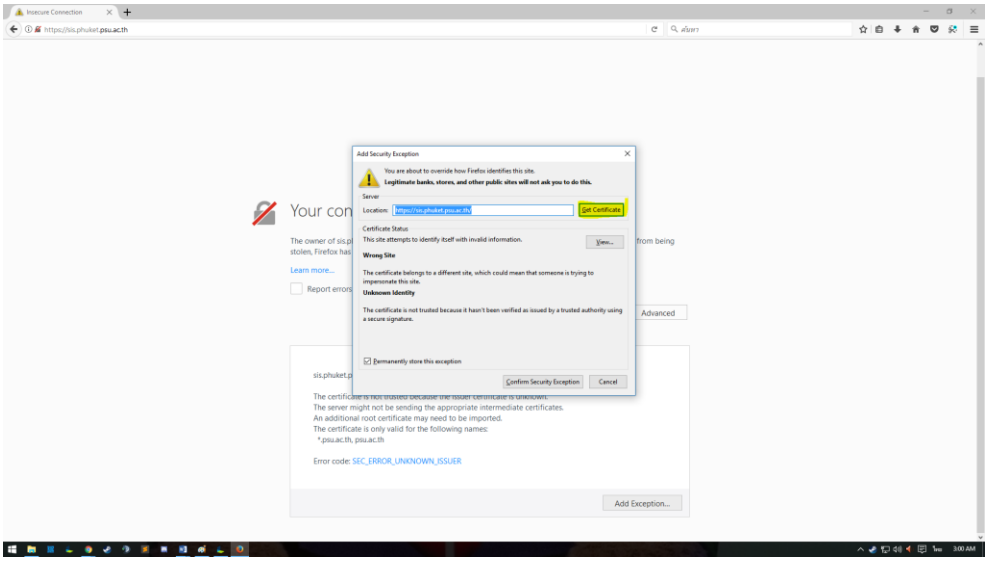
c. ไปที่ http://lms.phuket.psu.ac.th หากขึ้น certificate error ให้แก้ปัญหาดังกล่าว และ save certificate ออกมา หากไม่ขึ้นหน้า certificate error ให้ร้องขอ certificate และsave certificate นั้น พร้อมอธิบายขั้นตอนต่างๆ (ส่งไฟล์ certificate พร้อมกับรายงาน)

i. เข้า http://lms.phuket.psu.ac.th จะเกิด certificate error ให้กดที่ Advanced



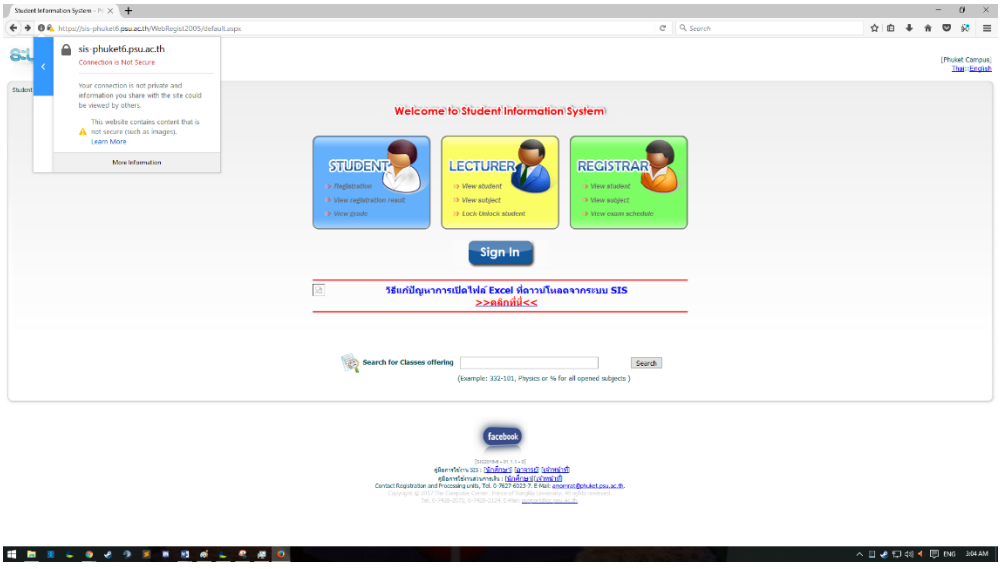
ii. เลือก Add Exception... จะแสดงหน้าต่างดังรูป

iii. กดปุ่ม Get Certificate เพื่อดาวน์โหลดใบรับรอง

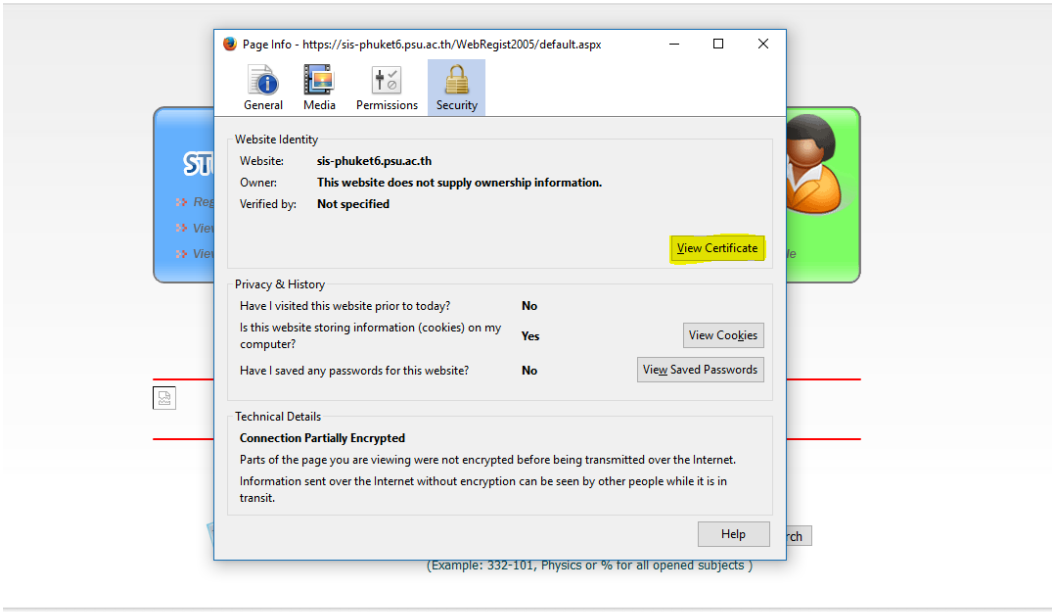


d. ไปที่ https://sis.phuket.psu.ac.th เปรียบเทียบผลลัพธ์กับข้อ 1.3 และอธิบายความแตกต่างรวมถึงข้อมูล certificate(Issued to, Issued by เป็นต้น) และ certification path

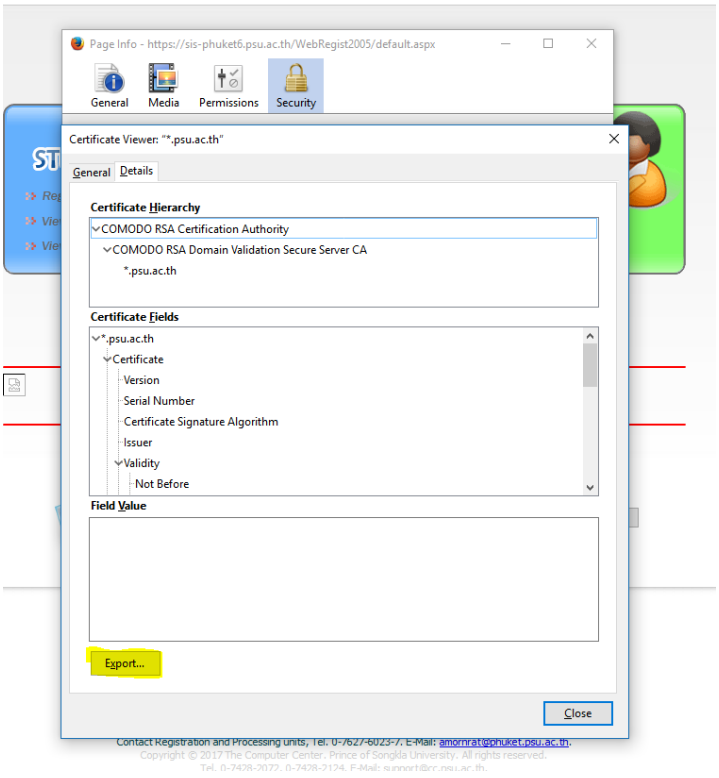
i. เข้า https://sis.phuket.psu.ac.th คลิกข้อมูลเพิ่มเติมทางด้านซ้ายมือ



ii. เลือก Security > View Certificate

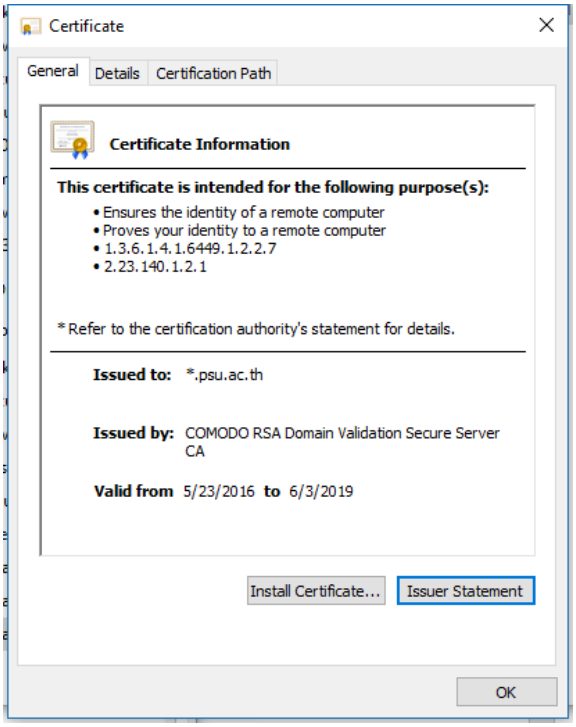


iii. กดปุ่ม Export... เพื่อดาวน์โหลดใบรับรอง

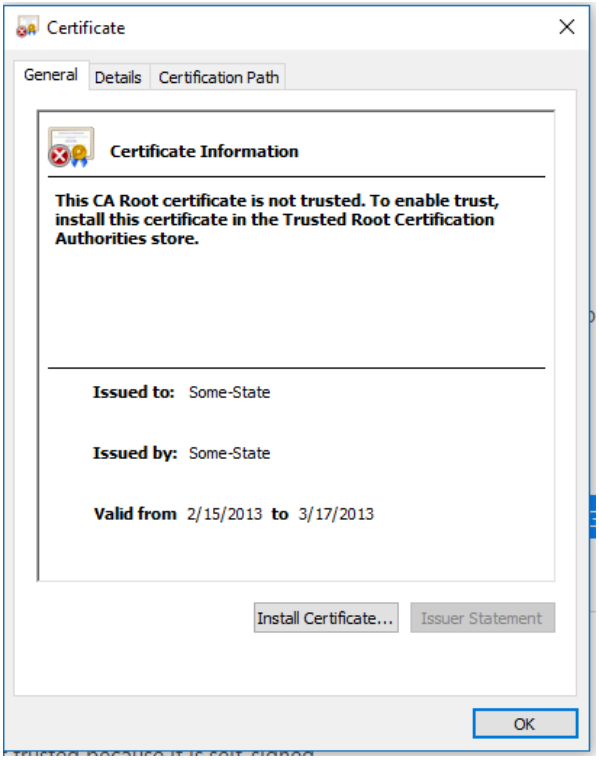


iv. รูป Certificate ทั้ง 2 Website

https://sis.phuket.psu.ac.th



http://lms.phuket.psu.ac.th



v. อธิบายความแตกต่างของทั้งสอง Certificate

ในใบ certificate ของ lms นั้นจะไม่มีความปลอดภัย เพราะ มันจะไม่มี Certificate Path นอกจากนั้นยังไม่มี Issued to, Issued by ส่วนในใบ Certificate ของ sis นั้นมีความปลอดภัย เพราะใช้ https และมี Certificate Path และมี Issued to, Issued by

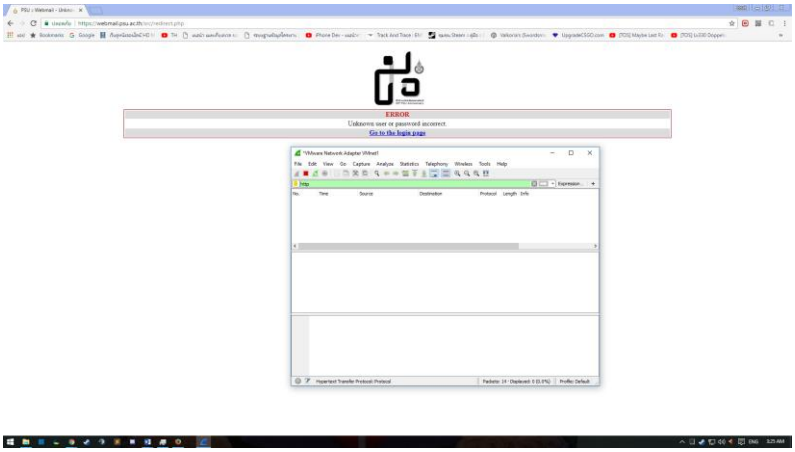
2. Wireshark

a. **ไปที่ https://www.wireshark.org ศึกษาวิธีการใช้งาน**

b. **ดักจับข้อมูล package จาก http://webmail.psu.ac.th และค้นหาข้อมูลที่เป็น username และ password(capture รูปผลลัพธ์และอธิบาย)**

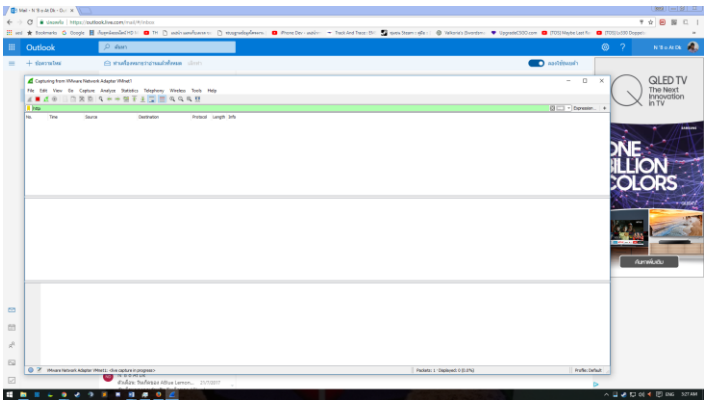
ข้อแนะนำ: ทดลองใส่ username และ password ตอนดักจับข้อมูล

i. จากรูปเมื่อใส่รหัส จะไม่สามารถดักจับข้อมูลได้เนื่องจาก web เป็นแบบ https



c. **ดักจับ package จาก e-mail account ของตนเอง เช่น gmail, hotmail หรือ yahooค้นหาข้อมูลที่เป็น username และ password(capture รูปผลลัพธ์และอธิบาย)**

i. จากรูปเมื่อใส่รหัส จะไม่สามารถดักจับข้อมูลได้เนื่องจาก web เป็นแบบ https

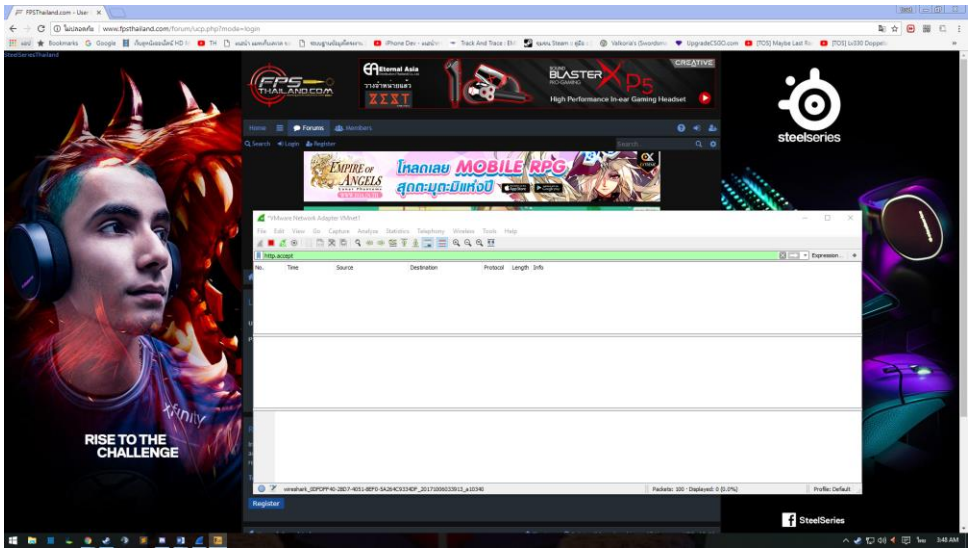


d. อธิบายความแตกต่างของผลลัพธ์ทั้งสอง Website

   i. มีรูปแบบที่เหมือนกันและไม่สามารถดักจับข้อมูลได้เพราะเนื่องจากเว็บไซต์ทั้งสองเว็บไซต์ใช้ Protocol ประเภท https เหมือนกัน

e. ดักจับ package และหาข้อมูล username และpassword จากเว็บไซต์ที่เข้าใช้งานบ่อยๆ (capture รูปผลลัพธ์และอธิบาย)

   i. เปิด website ของ fpsthailand แต่ไม่สามารถดักจับข้อมูลได้ได้



3. Password finding tool: ดาวน์โหลดโปรแกรม password-finder จากลิงค์ด้านล่าง ศึกษาวิธีการใช้งาน ติดตั้งโปรแกรมและใช้โปรแกรมดังกล่าวค้นหาข้อมูล password บนเครื่องคอมพิวเตอร์ของตัวเอง (อธิบายวิธีการค้นหาข้อมูล)

a. เนื่องจาก ลิงค์ดาวโหลดในเว็บไซต์ที่อาจารย์ให้มามันเสีย และไม่สามารถโหลดได้จึงทำการโหลดโปรแกรมที่มีลักษณะคล้ายกันกับตัวโปรแกรมที่อาจารย์ต้องการ หลังจากเปิดใช้โปรแกรมแล้ว โปรแกรมจะให้เราเลือกว่าเราต้องการค้นหา Password ของอะไรบ้างในโปรแกรมจะประกอบด้วยส่วนของ Web Browser และ Key ซึ่งมีให้เลือกทั้งสองแบบนั่นเอง